Norwegian Communications Authority

Testplan for the event “Jammertest 2023”

Technical descriptions for all centrally planned testcases

Norwegian
Communications
Authority

Summary

The Test plan:

This Test plan describes all official, centrally planned test cases relevant for execution at the event "Jammertest 2023".

The intent behind this document is numbering, planned structure and technical details for test cases that are predefined and shared among the attendees prior to the event.

Each test case is described with its (proposed) main objectives, some suggestive information concerning setup and enough information to understand what type of RF environment will be created during that test case. The attendees are free to choose how they would like to test their own equipment in this given RF environment.

Test cases that are not listed here is seen as "private tests". These private tests will not be documented by the event organisers[1]. There is a dedicated location for these types of tests, the official test area number 2 (*Grunnvatn*), that can be booked for private, small-scale testing. The centrally planned test cases will mainly take place in test areas 1 or 3. All three test areas can be used in parallel with each other during the event. See appendix for general documentation of the test area, motorcade route and technical documentation on the RF equipment.

The numbering system in the test plan is unique, and all tests will be given a unique identifier:

1. = Title/name of the test group.
1.1 = Preconditions and setup required prior to testing.
1.1.1 = Test number 1 in test group 1
1.1.2 = Test number 2 in test group 1
1.1.3 = Test number 3 in test group 1
Etc.

If there must be made changes to test 1.1.2, it will be ~~striked out~~ and a new test will be given a new number, e.g., 1.1.4.

If there must be made changes to preconditions and setup a new identifier will be given, e.g., 1.2.

[1] Event organisers: the Norwegian Communications Authority (Nkom), the Norwegian Defense Research Establishment (FFI), the Norwegian Public Roads Administration (NPRA), the Norwegian Metrology Service (JV) and the Norwegian Space Agency (NRS)

The Transmission plan:

The transmission plan contains information related to ***location***, ***time*** and ***duration*** for a given ***session*** with the associated ***test group***. The transmission plan "call out" the numbering system from the test plan.

The transmission plan may be altered during the live event, due to unexpected events like weather conditions, people being delayed, equipment failure, etc. In the event of alterations, there will be a rescheduling of the Transmission plan.

There is a likelihood that not all test cases will be performed during the live event, Jammertest 2023. The *event organizers* will prioritise and set the transmission plan.

The time schedule during the live event will be given in local time, UTC time + 2 (CEST).

Jamming, son. Nothing else in the world works like that.

I love the effect of jamming in the morning.

You know, one time we had a hill jammed, for 12 hours.

When it was all over, I walked up.

We didn't find one of 'em, not one stinkin' receiver with reliable PNT.

Table of Contents

Acronyms & Descriptions

Technical acronyms:

Jamming = Malicious attempt to disrupt the GNSS signal so that reception of GNSS signal is no longer possible.

Spoofing = Malicious attempt to alter GNSS signal or GNSS data, resulting in intended incorrect PNT data.

Meaconing = Retransmission. In this given case retransmission of GNSS signals.

Ephemerides = Clock and orbit (trajectory) parameters for GNSS satellites.

Synthetic ephemerides = clock and orbit parameters that are different from current true/broadcast parameters.

True ephemerides = Current clock and orbit parameters as broadcast by the GNSS satellites themselves.

Coherent spoofing = Transmission of simulated GNSS signals using true/broadcast ephemerides and where signal reception *at a designated target location* is code-phase aligned with live sky signals to better than half the code chip length[2].

Incoherent spoofing = Reception of transmitted simulated GNSS signals that are *not* code-phase aligned with live sky signals[3].

CEST = Central European Summer Time.

OSNMA = Open Service Navigation Message Authentication.

CW = Continuous Wave.

PRN = Pseudo Random Noise.

PNT = Position, Navigation and Timing.

PR ratio = Protection ratio defines a minimum relative power ratio of wanted to unwanted signals in the interfered receiving system.

UTC = Universal Time Coordinated. International reference time scale coordinated by the International Bureau of Weights and Measures (BIPM).

GST = Galileo System Time

GPST = GPS System Time

[2] For L1 C/A code the spoofing signals have to be synchronized to live sky signals within 0.5 microsecond or better. L5/E5 coherent spoofing requires 50 ns sync or better. Even if spoofing signals are well synchronized to live sky signals at a designated target location, spoofing signals received a distance away from the target location will not in general be code-phase aligned. For L1, signals received more than 150 m away from the target location will not be coherent. For L5/E5, the relevant distance is 15 m.

[3] Incoherence i.e. lack of code phase alignment at a particular receiver location may be due to either

- Simulated GNSS signals using synthetic ephemerides. In this case the spoofing signals will in general be different from live sky signals.
- Reception of simulated GNSS 'coherent' spoofing signals a distance away from the designated coherent spoofing target location.
- Reception of simulated GNSS signals using true/broadcast ephemerides that are generated to induce a time step and/or position jump.

J/S = Jammer to GNSS signal ratio.

S/S = Spoofing to GNSS signal ratio.

1 Continuous stationary low power jamming with commercially available jammers

1.1 Preconditions and setup

The main objective is to observe how the J/S signal affect the availability of PNT, and/or how it produces inaccurate PNT data, when the jamming signal (J) is generated by low-power jammers commercially available online. It will also allow participants to create a reference against other, more sophisticated transmission test cases. Additionally, as these types of jammers are the ones one is most likely to meet in the real world, capturing and storing the signals from these jammers for later use in labs could be useful. The use of continuous low power jamming will block out only a certain area. The attendees may therefore test the range of such a low-power jammer. Technical information on jammers can be found as appendix. The jammers used are acquirable from the internet, and each will either be representable for a specific jammer category, or be of special interest for the rest of the test week.

All tests will be performed as follows: The jammer will be activated while placed outside, on top of a stationary vehicle. The jammer will be kept turned on for two (2) minutes, and a two-minute break will be held between each test case. This scenario can be performed and/or repeated at multiple test areas. When activated, all jammers will have all possible GNSS jamming bands activate. If all 28 low effect jammers are tested in sequence, the test will take approximately 2 hours and 2 minutes, which include a 10-minute extra break at the end of the last jammer.

Test Area:	1 (3)
Operational Contact:	Nicolai Gerrard, Nkom (Tomas Levin, NPRA)
Technical Contact:	Nicolai Gerrard, Nkom
Time estimate:	2 hours & 2 minutes

1.1.1 Test: Jammer S1.1

1.1.2 Test: Jammer S1.2

1.1.3 Test: Jammer S1.3

1.1.4 Test: Jammer S2.1

1.1.5 Test: Jammer S2.2

1.1.6 Test: Jammer S2.3

1.1.7 Test: Jammer S2.4

1.1.8 Test: Jammer U1.1

1.1.9 Test: Jammer U1.2

1.1.10 Test: Jammer U1.3

1.1.11 Test: Jammer U1.4

1.1.12 Test: Jammer H1.1 – high power, GPS L1+L2, wideband modulation

Will be activated in high power mode, for GPS L1 and L2 with modulation set for wideband.

1.1.13 Test: Jammer H1.2

1.1.14 Test: Jammer H3.1

1.1.15 Test: Jammer H3.2

1.1.16 Test: Jammer H3.3

1.1.17 Test: Jammer H4.1

1.1.18 Test: Jammer H6.1

1.1.19 Test: Jammer H6.2

1.1.20 Test: Jammer H6.3

1.1.21 Test: Jammer H6.4

1.1.22 Test: Jammer H6.5

1.1.23 Test: Jammer H6.6

1.1.24 Test: Jammer H8.1

1.1.25 Test: Jammer F6.1 – Full power antenna F2 to F6

1.1.26 Test: Jammer H1.3

1.1.27 Test: Jammer H2.1

1.1.28 Test: Jammer H2.2

2 Continuous stationary high-power jamming with CW

2.1 Preconditions and setup

The main objective is to observe how the Jammer signal to GNSS signal (J/S) ratio affect the availability of PNT, and/or how it produces inaccurate PNT data. The use of continuous high-power jamming will block GNSS signals in a large area at the event. The attendees may therefore test their equipment at different ranges to such a high-power jammer. There will be transmitted with a continuous wave (CW) modulation (single frequency component) using Right Hand Circular Polarized (RHCP) antennas. The use of a 20 W jammer will result in among the highest J/S ratios during the event. The attendees can change distance to the transmitter and observe the changes and try to identify the protection ratio for their GNSS receiving system.

Each jamming session will last 10 minutes, with a 10-minute break between each test. The jammer employed will be “Porcus Major”, see appendix 26.9.19.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Anders Rødningsby, FFI
Time estimate:	1 hour & 20 minutes

2.1.1 Test: 20 W CW: L1

2.1.2 Test: 20 W CW: L1, G1

2.1.3 Test: 20 W CW: L1, G1, L2

2.1.4 Test: 20 W CW: L1, G1, L2, L5

3 Continuous stationary high-power jamming with sweep/chirp

3.1 Preconditions and setup

The main objective is to observe how the Jammer signal to GNSS signal (J/S) ratio affect the availability of PNT, and/or how it produces inaccurate PNT data. The use of continuous high-power jamming will block GNSS signals in a large area at the event. The attendees may therefore test their equipment at different ranges to such a high-power jammer. There will be transmitted with a sweep/chirp modulation using Right Hand Circular Polarized (RHCP) antennas. Sweep/chirp modulation means that the frequency component will sweep back and forth inside the specific frequency band with a given sweep rate. The use of a 20 W jammer will result in among the highest J/S ratios during the event. The attendees can change distance to the transmitter and observe the changes and try to identify the protection ratio for your GNSS receiving system.

Each jamming session will last 10 minutes, with a 10-minute break between each test. The jammer employed will be “Porcus Major”, see appendix 26.9.19.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Anders Rødningsby, FFI
Time estimate:	1 hour & 20 minutes

3.1.1 Test: 20 W chirp: L1

3.1.2 Test: 20 W chirp: L1, G1

3.1.3 Test: 20 W chirp: L1, G1, L2

3.1.4 Test: 20 W chirp: L1, G1, L2, L5

4 Continuous stationary high-power jamming with PRN

4.1 Preconditions and setup

The main objective is to observe how the Jammer signal to GNSS signal (J/S) ratio affect the availability of PNT, and/or how it produces inaccurate PNT data. The use of continuous high-power jamming will block out a large area at the event. The attendees may therefore test the range of such a high-power jammer. There will be transmitted with a Pseudo Random Noise (PRN) modulation using Right Hand Circular Polarized (RHCP) antennas. PRN signals have the same spectral form as the true signals sent from the GNSS satellites but with different spreading codes. The spreading codes are Binary Phase Shift Keying (BPSK) modulated onto the centre frequency of the specific GNSS band. The use of a 20 W jammer will result in among the highest J/S ratios during the event. The attendees can change distance to the transmitter and observe the changes and try to identify the protection ratio for your GNSS receiving system.

Each jamming session will last 10 minutes, with a 10-minute break between each test (except for the last test, which will last 30 minutes with a 10-minute break after). The jammer employed will be "Porcus Major", see appendix 26.9.19.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Anders Rødningsby, FFI
Time estimate:	2 hours

4.1.1 Test: 20 W PRN: L1

4.1.2 Test: 20 W PRN: L1, G1

4.1.3 Test: 20 W PRN: L1, G1, L2

4.1.4 Test: 20 W PRN: L1, G1, L2, L5

4.1.5 Test: 20 W PRN: 30-minute jamming of L1, G1, L2, L5

Repeat of test 4.1.4, but with longer duration.

5 Continuous stationary high-power jamming with “real world” PRN

5.1 Preconditions and setup

The type of jamming employed in this test is the same as real world signals observed in Europe, where the jammer parameters were found after demodulating a captured baseband stream.

The tests will be performed with BPSK modulation with a pseudo random symbol rate of 3 Mbaud at GPS L1 and 10.23 Mbaud at Glonass G1. The test cases refer to which centre frequency the signal will be centred at, based on the named GNSS bands.

Each jamming session will last 10 minutes, with a 10-minute break between each test. The jammer employed will be “Porcus Major”, see appendix 26.9.19.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Anders Rødningsby, FFI
Time estimate:	40 minutes

5.1.1 Test: 20 W: L1, PRN (BPSK-modulated with 3 Mbaud symbolrate)

5.1.2 Test: 20 W: G1 (BPSK-modulated with 10 Mbaud symbolrate)

6 Stationary high-power jamming, ramp power with PRN - Cemetery

6.1 Preconditions and setup

The main objective is to observe how the J/S signal affect the loss of PNT, and/or how it produces inaccurate PNT data, and at which power level. This will allow for evaluation of the sensitivity thresholds for various systems. The transmitted power will be ramped up and down from 0.1 µW to 20 W EIRP for each test with 10 seconds hold time for each power level, with ramping steps of 2 dB. The modulation will be PRN.

The attendees should be at a stationary location with a known distance to the jammer, so they can observe how different levels will affect the PNT. Comparing the ramping tests from both Cemetery (6) and Ramnan (7), will give the opportunity to compare signals arriving from different angles and also to see the difference between signals going along earth/ground and coming from above.

The jammer will be placed at the cemetery, north of Bleik. This is point A in 26.2.

Each test will last for 13.67 minutes, with a 15-minute break between each test. The jammer employed will be “Porcus Major”, see appendix26.9.19. The last step, from 42 dBm to 43.0103 dBm (20 W), will be a 1.0103 dB increment, not a 2 dB increment.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Anders Rødningsby, FFI
Time estimate:	2 hours

6.1.1 Test: 0.1 µW to 20 W, 2 dB increments PRN: L1

6.1.2 Test: 0.1 µW to 20 W, 2 dB increments PRN: L1, G1

6.1.3 Test: 0.1 µW to 20 W, 2 dB increments PRN: L1, G1, L2

6.1.4 Test: 0.1 µW to 20 W, 2 dB increments PRN: L1, G1, L2, L5

7 Stationary high-power jamming, ramp power with PRN - Ramnan

7.1 Preconditions and setup

The main objective is to observe how the J/S signal affect the loss of PNT, and/or how it produces inaccurate PNT data, and at which power level. This will allow for evaluation of the sensitivity thresholds for various systems. The transmitted power will be ramped up and down from 0.1 µW to 20 W EIRP for each test with 10 seconds hold time for each power level, with ramping steps of 2 dB. The modulation will be PRN. The attendees should be at a stationary location with a known distance to the jammer, so they can observe how different levels will affect the PNT.

The jammer will be placed at Ramnan, up the mountainside northwest of Bleik. This is point B in 26.2. This will allow for attendees to evaluate the difference between signals arriving from in the horizontal plane (as is the case with the cemetery placement (6)) and signals arriving with some elevation above the horizontal (this testcase).

Each test will last for 13.67 minutes, with a 15-minute break between each test. The jammer employed will be “Porcus Major”, see appendix26.9.19. The last step, from 42 dBm to 43.0103 dBm (20 W), will be a 1.0103 dB increment, not a 2 dB increment.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Anders Rødningsby, FFI
Time estimate:	2 hours

7.1.1 Test: 0.1 µW to 20 W, 2 dB increments PRN: L1

7.1.2 Test: 0.1 µW to 20 W, 2 dB increments PRN: L1, G1

7.1.3 Test: 0.1 µW to 20 W, 2 dB increments PRN: L1, G1, L2

7.1.4 Test: 0.1 µW to 20 W, 2 dB increments PRN: L1, G1, L2, L5

8 Stationary high-power jamming, ramp power with CW

8.1 Preconditions and setup

The main objective is to observe how the J/S signal affect the loss of PNT, and/or how it produces inaccurate PNT data, and at which power level. This will allow for evaluation of the sensitivity thresholds of various systems. The transmitted power will be ramped up and down from 0.1 µW to 20 W EIRP for each test with 10 seconds hold time for each power level, with ramping steps of 2 dB. The modulation will be CW. The attendees should be at a stationary location with a known distance to the jammer, so they can observe how different levels will affect the PNT.

Each test will last for 13.67 minutes, with a 15-minute break between each test. The jammer employed will be “Porcus Major”, see appendix26.9.19. The last step, from 42 dBm to 43.0103 dBm (20 W), will be a 1.0103 dB increment, not a 2 dB increment.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Anders Rødningsby, FFI
Time estimate:	2 hours

8.1.1 Test: 0.1 µW to 20 W, 2 dB increments CW: L1

8.1.2 Test: 0.1 µW to 20 W, 2 dB increments CW: L1, G1

8.1.3 Test: 0.1 µW to 20 W, 2 dB increments CW: L1, G1, L2

8.1.4 Test: 0.1 µW to 20 W, 2 dB increments CW: L1, G1, L2, L5

9 Stationary pyramid jamming with PRN for all GNSS bands sequentially

9.1 Preconditions and setup

The jamming is performed with PRN modulation. The transmission time is 3 minutes for each test. There are planned 2-minute breaks between tests. The tests will jam most GNSS bands, incrementally adding bands to the list of jammed signals, then removing them in the reverse order. After the last test, 15 minutes will be added as a last break, to allow receivers to default back to normal. This 'pyramid' is intended to test the potential fallback behaviour of modern multi-constellation multi-frequency receivers. The jammer employed will be "Porcus Major", see appendix 26.9.19.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Anders Rødningsby, FFI
Time estimate:	1 hour & 30 minutes

9.1.1 Test: 20 W PRN: E6

9.1.2 Test: 20 W PRN: E6, E5b

9.1.3 Test: 20 W PRN: E6, E5b, L5

9.1.4 Test: 20 W PRN: E6, E5b, L5, G2

9.1.5 Test: 20 W PRN: E6, E5b, L5, G2, L2

9.1.6 Test: 20 W PRN: E6, E5b, L5, G2, L2, B1I

9.1.7 Test: 20 W PRN: E6, E5b, L5, G2, L2, B1I, G1

9.1.8 Test: 20 W PRN: E6, E5b, L5, G2, L2, B1I, G1, L1

9.1.9 Test: 20 W PRN: E6, E5b, L5, G2, L2, B1I, G1

9.1.10 Test: 20 W PRN: E6, E5b, L5, G2, L2, B1I

9.1.11 Test: 20 W PRN: E6, E5b, L5, G2, L2

9.1.12 Test: 20 W PRN: E6, E5b, L5, G2

9.1.13 Test: 20 W PRN: E6, E5b, L5

9.1.14 Test: 20 W PRN: E6, E5b

9.1.15 Test: 20 W PRN: E6

10 Stationary inverted pyramid jamming with PRN for all GNSS bands sequentially

10.1 Preconditions and setup

The jamming is performed with PRN modulation. The transmission time is 3 minutes for each test. There are planned 2-minute breaks between tests. The tests will jam most GNSS bands, incrementally removing bands to the list of jammed signals, then adding them in the reverse order. After the last test, 15 minutes will be added as a last break, to allow receivers to default back to normal. This 'inverted pyramid' is intended to test the potential fallback behaviour of modern multi-constellation multi-frequency receivers. The jammer employed will be "Porcus Major", see appendix 26.9.19.

Test Area: 1
Operational Contact: Nicolai Gerrard, Nkom
Technical Contact: Anders Rødningsby, FFI
Time estimate: 1 hour & 30 minutes

10.1.1 Test: 20 W PRN: E5b, L5, E6, G2, L2, B1l, G1, L1

10.1.2 Test: 20 W PRN: E5b, L5, E6, G2, L2, B1l, G1

10.1.3 Test: 20 W PRN: E5b, L5, E6, G2, L2, B1l

10.1.4 Test: 20 W PRN: E5b, L5, E6, G2, L2

10.1.5 Test: 20 W PRN: E5b, L5, E6, G2

10.1.6 Test: 20 W PRN: E5b, L5, E6

10.1.7 Test: 20 W PRN: E5b, L5

10.1.8 Test: 20 W PRN: E5b

10.1.9 Test: 20 W PRN: E5b, L5

10.1.10 Test: 20 W PRN: E5b, L5, E6

10.1.11 Test: 20 W PRN: E5b, L5, E6, G2

10.1.12 Test: 20 W PRN: E5b, L5, E6, G2, L2

10.1.13 Test: 20 W PRN: E5b, L5, E6, G2, L2, B1l

10.1.14 Test: 20 W PRN: E5b, L5, E6, G2, L2, B1l, G1

10.1.15 Test: 20 W PRN: E5b, L5, E6, G2, L2, B1l, G1, L1

11 Stationary meaconing with varying power and time exposure

11.1 Preconditions and setup

The objective is to observe how equipment and systems behave under meaconing.

GNSS re-transmission of real live sky signals, where the GNSS environment will have wrong position with real satellite data, only slightly time delayed.

The test will re-transmitt only* the GPS L1 and L2 bands. The re-transmitted signals needs a lot of amplification, with the added risk of amplifying background noise. Therefore, it is hard to give precise estimates of effective power levels and range. Attendees should try to observe PNT changes and/or loss of PNT, and monitor the changes when their equipment and systems are exposed to two different power levels and varying degrees of time exposure to the meaconed signal. Maybe especially interesting is to see if the effects of movement and speed, coupled with other sensor data, will result on the total output. The tests are performed with constant power outputs (0.1 W or 1 W), and with varying lengths of transmission times [see above for power levels]. There are planned a 15-minute break between each test. Many tests will be performed twice, so that it is possible to try to detect differences between stationary and mobile test objects.

The meaconed position is 69.2803484 N, 16.0074695 E.

The jammer employed will be “Porcus Major”, see appendix 26.9.19. Power levels denoted in the specific tests below are indications and will only be known during setup the days before Jammertest. Information will be provided during daily pre-test morning briefings.

* To re-transmitt on other GNSS bands requires an extensive filterbank to exclude all signals outside GNSS frequencies.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Anders Rødningsby, FFI
Time estimate:	3 hours & 49 minutes

11.1.1 Test: 0.1 W meaconing: 3 minutes

11.1.2 Test: 0.1 W meaconing: 3 minutes (repeat 11.1.1)

11.1.3 Test: 0.1 W meaconing: 3 minutes preceded by 5 min jamming (20 W PRN L1 , L2, L5 and G1)

11.1.4 Test: 10 W meaconing: 30 seconds

11.1.5 Test: 10 W meaconing: 3 minutes

11.1.6 Test: 10 W meaconing: 3 minutes (repeat 11.1.5)

11.1.7 Test: 10 W meaconing: 3 minutes preceded by 5 min jamming (PRN L1 , L2, L5 and G1)

11.1.8 Test: 10 W meaconing: 15 minutes

11.1.9 Test: 10 W meaconing: 15 minutes (repeat 11.1.8)

11.1.10 Test: 10 W meaconing: 15 minutes preceded by 5 min jamming (PRN L1 , L2, L5 and G1)

12 Motorcade with low-power commercially available jammers (placed on stationary vehicle)

12.1 Preconditions and setup

Tests in this setup will explore the impact on other cars caused by a jammer placed in a parked car. Jammers used in this test are commercially available jammers. The jammers are to be placed on the roof of a vehicle (in clear plastic box in case of adverse weather.

For each test, the jammer will be active for 5 minutes. A 5 minute break between each test will be held. Additionally, as these tests will include a lot of vehicles, tests will probably be repeated and some extra time will have to be added, to allow for the practical side of coordination.

Test area:	3
Operational Contact:	NPRA
Technical Contact:	Tomas Levin, NPRA
Time estimate:	1,5 hours

12.1.1 Test: Driving while passing a parked car with GPS (L1 & L2) jammer – jammer S2.1

12.1.2 Test: Driving while passing a parked car with multi-band jammer – jammer H6.4

12.1.3 Test: Vehicle starting in GPS (L1 & L2) denied environment – jammer S2.1

12.1.4 Test: Vehicle starting in multi-band denied environment – jammer H6.4

13 Motorcade with low-power commercially available jammers (mobile placement in cars)

13.1 Preconditions and setup

This setup is to simulate meeting a vehicle with a jammer inside of it.

For each test, the jammer will be active for 10 minutes. A 5-minute break between each test will be held. Additionally, as these tests will include a lot of vehicles, tests will probably be repeated and some extra time will have to be added, to allow for the practical side of coordination.

Test area:	3
Operational Contact:	NPRA
Technical Contact:	Tomas Levin, NPRA
Time estimate:	3 hours

13.1.1 Test: Driving with GPS (L1 & L2) jammer in test vehicle – jammer S2.1

13.1.2 Test: Driving with GPS (L1 & L2) jammer in vehicle in front of the test vehicle – jammer S2.1

13.1.3 Test: Driving with GPS (L1 & L2) jammer in vehicle behind the test vehicle – jammer S2.1

13.1.4 Test: Driving with GPS (L1 & L2) jammer in vehicle overtaking the test vehicle – jammer S2.1

13.1.5 Test: Driving with GPS (L1 & L2) jammer in vehicle being overtaken by the test vehicle – jammer S2.1

13.1.6 Test: Driving with multi-band jammer in test vehicle – jammer H6.4

13.1.7 Test: Driving with multi-band jammer in vehicle in front of the test vehicle – jammer H6.4

13.1.8 Test: Driving with multi-band jammer in vehicle behind the test vehicle – jammer H6.4

13.1.9 Test: Driving with multi-band jammer in vehicle overtaking the test vehicle – jammer H6.4

13.1.10 Test: Driving with multi-band jammer in vehicle being overtaken by the test vehicle –jammer H6.4

14 Low power jamming with commercially available multi-band jammers in different placements in the terrain

14.1 Preconditions and setup

The main objective is to simulate meeting several “more dangerous” jammers, multi-band jammers. The test will use three multiband jammers, spaced out in the terrain in different places. Attendees can move around or station themselves so that they can experience the different constellation and observe how their equipment and systems behave in a complicated GNSS RFI environment.

When the jammers are activated sequentially, they will be activated with one minute between them and be kept active for five minutes after the last is activated. When all jammers are activated at the same time, they will be kept active for 5 minutes. If all jammers are activated simultaneously, they will be kept active for 7 minutes. A 10-minute break will be held between each test.

The precise positions for each jammer will have to be decided in field, to best accommodate participants wishes and practical concerns (like terrain). The coordinates for each position, X, Y and Z, will have to be written down in field to help later analysis of the test results.

Test Area:	1 (3)
Operational Contact:	Nicolai Gerrard, Nkom (Tomas Levin, NPRA)
Technical Contact:	Nicolai Gerrard, Nkom
Time estimate:	1 hour & 42 minutes

14.1.1 Test: All jammers stationary; activate Jammer F6.1, H6.5 and H3.3 sequentially

14.1.2 Test: All jammers stationary; activate Jammer F6.1, H6.5 and H3.3 sequentially (repeat 14.1.1)

14.1.3 Test: All jammers stationary in new placements; activate Jammer F6.1, H6.5 and H3.3 sequentially

14.1.4 Test: All jammers stationary in new placements; activate Jammer F6.1, H6.5 and H3.3 sequentially (repeat 14.1.3)

14.1.5 Test: Jammers F6.1 and H6.5 stationary, Jammer H3.3 mobile; all jammers activated simultaneously

14.1.6 Test: Jammers F6.1 and H6.5 stationary, Jammer H3.3 mobile; all jammers activated simultaneously (repeat 14.1.5)

15 Incoherent spoofing from stationary spoofer using synthetic ephemerides

15.1 Preconditions and setup

Simulated signals will be transmitted from a stationary antenna near Bleik community house. Generated spoofing scenarios will use satellite ephemerides *different* from live sky satellites. Simulated signals may use one or more constellations and one or more signal bands.

Initial positions are either *False* (e.g. 70 N, 10 E) or *True* (target location at Bleik community house). Initial time is either *False* (e.g. a jump in time) or *True* (< 100 ns timing error for a receiver at target location). Some test scenarios may be started with jamming (lasting for 5 min, one or several signal bands, before the spoofing transmission is activated). Some spoofing scenarios may be accompanied by continuous jamming (one or several signal bands).

Static scenarios are a fixed position, while motion scenarios are a drive around Andøya. Each test runs for between 10 and 20 minutes with 5 –10 minutes break between each test. For each dynamic test, the motion is first spoofed to a fixed start position (see 26.8) for 5 minutes before the dynamic motion starts.

Expected range/power of spoofing signals: A radius of approximately 1.5 kilometre from the community house, depending on terrain and building signal shielding.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Harald Hauglin, Justervesenet, (Anders Rødningsby, FFI)
Time estimate:	1 hour 50 minutes

15.1.1 Test: Large position and time jump, gradually increasing signal strength

Signals: GPS L1 C/A, L2C, L5
Galileo E1, E5
No jamming
Simulated position: 70 N, 10 E
Simulated start time: 01.10.2023 12:00

15.1.2 Test: Large position and time jump

Signals: GPS L1 C/A

Galileo E1

No jamming

Position: 70 N, 10 E

Simulated start time: 01.10.2023 12:00

15.1.3 Test: Large position and time jump, with jamming

Signals: GPS L1 C/A

Galileo E1

5 minutes of initial jamming (L1, G1, B1I, E6, L2, E5b, L5 with 2 W) prior to spoofing transmission, then continuous on other bands than the ones spoofed.

Simulated position: 70 N, 10 E

Simulated start time: 01.10.2023 12:00

15.1.4 Test: Simulated driving (route 1)

Signals: GPS L1 C/A, L2C, L5

Galileo E1, E5

5 minutes of initial jamming (L1, G1, B1I, E6, L2, E5b, L5 with 2 W) prior to spoofing transmission.

Simulated start position: Bleik community house

Simulated start time: 01.10.2023 12:00

15.1.5 Test: Simulated driving, true reference time (route 1)

Signals: GPS L1 C/A, L2C, L5

Galileo E1, E5

5 minutes of initial jamming (L1, G1, B1I, E6, L2, E5b, L5 with 2 W) prior to spoofing transmission.

Simulated start position: Bleik community house

Simulated start time: Referenced to live GPS-signals

15.2 Rationale

These are very basic attacks that can be performed with easily available software and hardware. These attacks can give an indication to the receivers' resiliency to spoofing attacks. Most receivers will probably see these attacks as noise initially, effectively working as a jamming signal.

16 Incoherent spoofing from stationary spoofer using broadcast(true) ephemerides

16.1 Preconditions and setup

Simulated signals will be transmitted from a stationary antenna near Bleik community house. Generated spoofing scenarios will use broadcast satellite ephemeris data. Simulated signals may use one or more constellations and one or more signal bands.

Initial positions are either *False* (e.g. 70 N, 10 E) or *True* (target location at Bleik community house). Initial time is either *False* (e.g. a jump in time/date) or *True* (< 100 ns timing error for a receiver at target location). Some test scenarios may be started with jamming ((lasting for 5 min, one or several signal bands, before the spoofing transmission is activated). Some spoofing scenarios may be accompanied by continuous jamming (one or several signal bands).

Static scenarios are a fixed position, while motion scenarios are a simulated drive around Andøya. Each test runs for between 10 and 20 minutes with 5 –10 minutes break between each test to allow receivers to reacquire fix onto real satellite signals. For each dynamic test, the motion is first spoofed to a fixed start position (see 26.8) for 5 minutes before the dynamic motion starts.

Expected range/power of spoofing signals: A radius of approximately 1.5 kilometre from the community house, depending on terrain and building signal shielding.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Harald Hauglin, Justervesenet, (Anders Rødningsby, FFI)
Time estimate:	1 hour 45 minutes

16.1.1 Test: Large position jump

Signals: GPS L1 C/A, L2C, L5

Galileo E1, E5

No jamming

Simulated position: 70 N, 10 E

Simulated start time: Referenced to live GPS-signals

16.1.2 Test: Small position jump, large time jump

Signals: GPS L1 C/A, L2C, L5

Galileo E1, E5

5 minutes of initial jamming (L1, G1, B1I, E6, L2, E5b, L5 with 2 W) prior to spoofing transmission, then continuous on other bands than the ones spoofed.

Simulated position: North end of the football field – 69.27701401, 15.96932835[4], 45 m hae. (Height Above Ellipsoid)

Simulated start time: 01.10.2023 12:00

16.1.3 Test: Small position jump

Signals: GPS L1 C/A, L2C, L5

Galileo E1, E5

No jamming

Simulated position: North end of the football field – 69.27701401, 15.96932835, 45 m hae. (Height Above Ellipsoid)

Simulated start time: Referenced to live GPS-signals

16.1.4 Test: Flying (route 2) – "helicopter scenario"

Signals: GPS L1 C/A, L2C, L5

Galileo E1, E5

No jamming

Simulated start position: Over the sea 1 km N (Midnattskjæran) at 200 m height

Simulated start time: Referenced to live GPS-signals

Spoofing transmission will be corrected for signal delay to simulated start position. Helicopter at start position should see coherent signals.

[4] Decimal Degrees

16.1.5 Test: Fixed position

Signals: GPS L1 C/A, L2C, L5
Galileo E1, E5

No jamming

Simulated position: Cemetery – 69.2824699, 15.9906568, 48 m hae. (Height Above Ellipsoid)

Simulated start time: Referenced to live GPS-signals

16.1.6 Test: Large position jump #2

Signals: GPS L1 C/A, L2C, L5
Galileo E1, E5

No jamming

Simulated position: 69.25 N, 14,9 E

Simulated start time: Referenced to live GPS-signals

16.2 Rationale

These spoofing tests use ephemerides (navigation data) identical to those broadcasted by the actual satellites, but the transmitted spoofing signals do not align with those received from actual satellites. Receivers using the spoofed signals will generate jumps in the navigation solution, either in position, timing and/or velocity.

17 Coherent spoofing from stationary spoofer using broadcast(true) ephemerides

17.1 Preconditions and setup

Simulated signals will be transmitted from a stationary antenna near Bleik community house. Generated spoofing scenarios will use broadcast satellite ephemeris data. Simulated signals may use one or more constellations and one or more signal bands.

Initial positions are *True* (target location at Bleik community house). Initial time is *True* (< 100 ns timing error for a receiver at target location). Some test scenarios may be started with jamming (lasting for 5 min, one or several signal bands, before the spoofing transmission is activated). Some spoofing scenarios may be accompanied by continuous jamming (one or several signal bands).

For all of test group 17, spoofing transmission will be corrected for signal delay to simulated start position.

Static scenarios are a fixed position, while motion scenarios are a drive around Andøya. Each test runs for between 10 and 20 minutes with 5 –10 minutes break between each test to allow receivers to reacquire fix onto real satellite signals. For each dynamic test, the motion is first spoofed to a fixed start position (see 26.8) for 5 minutes before the dynamic motion starts.

Expected range/power of spoofing signals: A radius of approximately 1.5 kilometre from the community house, depending on terrain and building signal shielding.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Harald Hauglin, Justervesenet, (Anders Rødningsby, FFI)
Time estimate:	4 hours

17.1.1 Test: Simulated driving (route 1). GPS only with initial jamming.

Signals: GPS L1 C/A, L2C, L5
5 minutes of initial jamming (L1, G1, B1I, E6, L2, E5b, L5 with 2 W) prior to spoofing transmission.
Simulated start position: Bleik community house parking lot
Simulated start time: Referenced to live GPS-signals

17.1.2 Test: Simulated driving (route 1). Galileo only with initial jamming.

Signals: Galileo E1, E5

5 minutes of initial jamming (L1, G1, B1I, E6, L2, E5b, L5 with 2 W) prior to spoofing transmission.

Simulated start position: Bleik community house parking lot

Simulated start time: Referenced to live GPS-signals

17.1.3 Test: Simulated driving (route 1) with initial jamming.

Signals: GPS L1 C/A, L2C, L5

Galileo E1, E5

5 minutes of initial jamming (L1, G1, B1I, E6, L2, E5b, L5 with 2 W) prior to spoofing transmission.

Simulated start position: Bleik community house parking lot

Simulated start time: Referenced to live GPS-signals

17.1.4 Test: Simulated driving (route 1). GPS only.

Signals: GPS L1 C/A, L2C, L5

No jamming

Simulated start position: Bleik community house parking lot

Simulated start time: Referenced to live GPS-signals

17.1.5 Test: Simulated driving (route 1). GPS L1 and Galileo E1.

Signals: GPS L1 C/A

Galileo E1

No jamming

Simulated start position: Bleik community house parking lot

Simulated start time: Referenced to live GPS-signals

17.1.6 Test: Simulated driving (route 1).

Signals: GPS L1 C/A, L2C, L5

Galileo E1, E5

No jamming

Simulated start position: Bleik community house parking lot

Simulated start time: Referenced to live GPS-signals

17.1.7 Test: Flying (route 4) – "drone scenario"

Signals: GPS L1 C/A, L2C, L5
Galileo E1, E5
No jamming
Simulated start position: 69.277014014, 15.969328354, 40 mhae.
Simulated start time: Referenced to live GPS-signals

17.1.8 Test: Sailing (route 5) – "ship scenario"

Signals: GPS L1 C/A, L2C, L5
Galileo E1, E5
No jamming
Simulated start position: Bleik harbour
Simulated start time: Referenced to live GPS-signals

17.2 Rationale

These spoofing tests use ephemerides (navigation data) identical to those broadcasted by the actual satellites. The transmitted spoofing signals are intended to align (to within a few 100 ns) with those received from actual satellites at the target location. Receivers using the spoofed signals at rest at the target location will initially generate no major changes in the navigation solution, either in position, timing and/or velocity, compared to the solution estimated from actual satellite signals.

18 Incoherent time spoofing from stationary spoofer using synthetic ephemerides

18.1 Preconditions and setup

Simulated signals will be transmitted from a stationary antenna near Bleik community house. Generated spoofing scenarios will use satellite ephemerides different from live sky satellites. Simulated signals may use one or more constellations and one or more signal bands.

Initial positions are *True* (target location at Bleik community house). Some test scenarios may be started with jamming (5 min, one or several signal bands). Some spoofing scenarios may be accompanied by continuous jamming (one or several signal bands).

The tests are organised so that similar tests are grouped (18.1.1 - 18.1.3, 18.1.4 - 18.1.5) with a 10 minute break between each test and then a 30 minute break between groups to allow receivers to reacquire fix onto real satellite signals.

Expected range/power of spoofing signals: A radius of approximately a few hundred metres from the community house, depending on terrain and building signal shielding.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Harald Hauglin, Justervesenet, (Anders Rødningsby, FFI)
Time estimate:	2 hours & 30 minutes

18.1.1 Test: Time offset 15 minutes from real time.

Signals: GPS L1 C/A and Galileo E1 only.

18.1.2 Test: Time offset 15 minutes from real time.

Signals: GPS L1 C/A, L2C, L5
Galileo E1, E5
No jamming.
Fixed spoofed position: 69.27547832, 15.96832496, 35 m hae.
Time offset is + 15 minutes (900 seconds), so “into the future”.
Spoofing power ramp –35 dBm to +15 dBm in steps of 5 dB every two minutes.

18.1.3 Test: Time offset -3 minutes from real time.

Signals: GPS L1 C/A, L2C, L5

Galileo E1, E5

No jamming.

Fixed spoofed position: 69.27547832, 15.96832496, 35 m hae.

Time offset is - 3 minutes (180 seconds), so “back into the past”.

Spoofing power will start at -20 dBm and be stepped up to 15 dBm in one step.

18.1.4 Test: Static + Frequency step (spoofing signal transmission rate change). GPS L1 C/A only

18.1.5 Test: Static + Frequency step (spoofing signal transmission rate change).

Signals: GPS L1 C/A

Galileo E1

5 minutes of initial jamming (L1, G1, B1I, L2, E5b, L5 with 2 W) prior to spoofing transmission.

Fixed spoofed position: 69.27547832, 15.96832496, 35 m hae.

Spoofing power will be at 0 dBm.

Frequency steps are added (10 ns/s) and starts five minutes after the spoofing starts.

18.2 Rationale:

These are synchronized spoofing scenarios in the sense that the navigation solution (position, velocity and clock bias) should not initially change significantly for a receiver at the target location. The scenarios are incoherent in the sense that spoofing signals are different from those received from the actual satellites.

19 Coherent time spoofing from stationary spoofer using broadcast(true) ephemerides

19.1 Preconditions and setup

Simulated signals will be transmitted from a stationary antenna near Bleik community house. Generated spoofing scenarios will use broadcast satellite ephemeris data. Simulated signals may use one or more constellations and one or more signal bands.

Initial positions are *True* (target location at Bleik community house). Initial time is *True* (< 100 ns timing error for a receiver at target location). Some test scenarios may be started with jamming (5 min, one or several signal bands). Some spoofing scenarios may be accompanied by continuous jamming (one or several signal bands).

The tests are organised so that similar tests are grouped (19.1.1 - 19.1.2, 19.1.3 - 19.1.6, 19.1.7) with a 10 minute break between each test and then a 30 minute break between groups to allow receivers to reacquire fix onto real satellite signals.

Expected range/power of spoofing signals: A radius of approximately few hundred metres from the community house, depending on terrain and building signal shielding.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Harald Hauglin, Justervesenet, Anders Rødningsby, FFI
Time estimate:	3 hours

19.1.1 Test: Static + Frequency step (spoofing signal transmission rate change).

Signals: GPS L1 C/A
Galileo E1
No jamming.
Fixed spoofed position: 69.27547832, 15.96832496, 35 m hae.
Frequency steps are added (10 ns/s), and starts five minutes after the spoofing starts.
Spoofing power will be at -20 dBm.

19.1.2 Test: Static + Frequency step (spoofing signal transmission rate change).

Signals: GPS L1 C/A
Galileo E1

5 minutes of initial jamming (L1, G1, B1l, L2, E5b, L5 with 2 W) prior to spoofing transmission, then continuous on other bands than the ones spoofed.

Fixed spoofed position: 69.27547832, 15.96832496, 35 m hae.

Frequency steps are removed (10 ns/s) and starts five minutes after the spoofing starts.

Spoofing power will be at 0 dBm.

19.1.3 Test: Static + Frequency step (spoofing signal transmission rate change). GPS L1 C/A and Galileo E1 only.

19.1.4 Test: Static + Nav data manipulation (clock/frequency related). L1/E1 only

Signals: GPS L1 C/A
Galileo E1

No jamming.

Fixed spoofed position: 69.27547832, 15.96832496, 35 m hae.

Spoofing power will be at -20 dBm.

19.1.5 Test: Static + Nav data manipulation (clock/frequency related) with jamming.

Signals: GPS L1 C/A, L2C, L5
Galileo E1, E5.

No jamming.

Fixed spoofed position: 69.27547832, 15.96832496, 35 m hae.

Spoofing power ramp –35 dBm to +15 dBm in steps of 5 dB every two minutes.

19.1.6 Test: Static + UTC-parameter navigation data manipulation.

Signals: GPS L1 C/A, L2C, L5
Galileo E1, E5.

5 minutes of initial jamming (L1, G1, B1l, L2, E5b, L5 with 2 W) prior to spoofing transmission.

Fixed spoofed position: 69.27547832, 15.96832496, 35 m hae.

Spoofing power will be at -20 dBm.

Spoofing says that back in 2016, there was 19 leap seconds instead of 18.

19.1.7 Test: Static + UTC-parameter navigation data manipulation.

Signals: GPS L1 C/A, L2C, L5

Galileo E1, E5.

No jamming.

Fixed spoofed position: 69.27547832, 15.96832496, 35 m hae.

Different data manipulation than in 19.1.6.

Spoofing power will be at -20 dBm.

Spoofing says that back in 2016, there was counter-factual extra amount of -127 leap seconds, which in total means that there is removed -145 leap seconds.

19.1.8 Test: Time offset 15 minutes from real time - harbour

Signals: GPS L1 C/A, L2C, L5

Galileo E1, E5

No jamming.

Fixed spoofed position: Bleik harbour

Time offset is + 15 minutes (900 seconds), so “into the future”.

19.2 Rationale:

Scenarios in these tests is intended not to alter the navigation solution at for receivers at the target position for position and velocity estimates. Clock bias estimates should be affected by the frequency step in 19.1.1 - 19.1.3, but not in 19.1.4 - 19.1.7.

20 Incoherent GPS position and time spoofing from mobile spoofer

20.1 Preconditions and setup

The objective is to simulate a vehicle-borne spoofing device “out in the wild”, so that attendees can experience how a mobile spoofing source affects their (stationary or mobile) equipment and systems.

Each transmission will last for 20 minutes with a 30-minute break between each test to allow receivers to reacquire fix onto real satellite signals (total of 50 min for each test). The spoofed signals will be on GPS L1 only. All spoofing tests will be combined with jamming on Glonass G1. Starting position will be approximately 69.194875 N, 15.837719 E in all scenarios.

Test Area:	3
Operational Contact:	Tomas Levin, NPRA
Technical Contact:	Anders Rødningsby, FFI
Time estimate:	3 hours & 20 minutes

20.1.1 Test: Spoofer (in vehicle) stationary with moving spoofed position.

Spoofer (in vehicle) stationary; spoofed position starts static and approximately true. After 10 min spoofed position starts to move south with constant speed (15 m/s) while spoofer is still stationary.

20.1.2 Test: Spoofer (in vehicle) stationary and then moving with fixed spoofed position.

Spoofer (in vehicle) starts stationary for 10 min, and then begins to drive south along Stavedalsveien (FV7702); spoofed position remains fixed and approximately as the true position from start throughout the test.

20.1.3 Test: Spoofer (in vehicle) moving with fixed spoofed position.

Spoofer (in vehicle) moves south along Stavedalsveien (FV7702) from the start while being spoofed to a fixed position at 70 N, 10 E.

20.1.4 Test: Spoofer (in vehicle) stationary and then moving with first fixed and then moving spoofed position.

Spoofer (in vehicle) starts stationary for 10 min, then vehicle begins to drive south along Stavedalsveien (FV7702); spoofed position is approximately true for the first 10 min, then starts to move directly south with constant speed (15 m/s) in a slightly different direction than the vehicle.

21 Executive day – spoofing and jamming for high-level representatives

21.1 Preconditions and setup

The purpose is to expose the participants of the executive day to a set of GNSS attacks, primary targets are the cell phones of the participants. Participants should have installed and app to see which satellites are in use and show their location, for example GPS Test (Android).

Each jamming session will last 3 minutes, with a 5-minute break between. The spoofing sessions will last as long as necessary, but not longer than 40 minutes in total. For each dynamic test, the motion is first spoofed to a fixed start position (see 26.8) for 5 minutes before the dynamic motion starts.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom; Tomas Levin, SVV
Technical Contact:	Harald Hauglin, Justervesenet, (Anders Rødningsby, FFI)
Time estimate:	1 hour

21.1.1 Test: Jamming with small 1 W Jammer H6.6

21.1.2 Test: Jamming with Porcus Major

21.1.3 Test: Stationary coherent spoofing using broadcast(true) ephemerides

Sends participants back in time – a week or so.

21.1.4 Test: Stationary coherent spoofing using broadcast(true) ephemerides (route 3)

Signals: GPS L1 C/A, L2C, L5
Galileo E1, E5
No jamming
Simulated start position: Bleik community house parking lot
Simulated start time: Referenced to live GPS-signals.
Coherent spoofing from stationary spoofer using broadcast(true) ephemerides.

21.1.5 Test: Fixed position Bleiksøya

Signals: GPS L1 C/A, L2C, L5
Galileo E1, E5
No jamming
Simulated position: Bleiksøya –, m hae. (Height Above Ellipsoid)
Simulated start time: Referenced to live GPS-signals.
Coherent spoofing from stationary spoofer using broadcast(true) ephemerides.

22 Stationary incoherent spoofing with extreme timeshifts (+/- 1 to 2 years)

Some equipment will use GNSS to synchronize time and this time and different subsystems can use this time for checking validity of licences etc. Providing a date 2 years back in time or 2 years ahead can cause denial of service for certain services. The effect on subsystems is not known and hence care should be taken to limit the range of the transmission to include only systems that we want to test.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Harald Hauglin, Justervesenet, (Anders Rødningsby, FFI)
Time estimate:	? hours

22.1.1 Test: Pos=True; Time=2 years backwards, Jam_initial=All; Jam_cont=all except L1/E1; Scenario=Static+motion

Test: Pos=True; Time=2 years forward, Jam_initial=All; Jam_cont=all except L1/E1; Scenario=Static+motion

23 Jamming attacks on ships

23.1 Preconditions and setup

The objective is to simulate the conditions of which a jammer can appear on ships like ferries. Exact locations and tests will be chosen on site according to layout of ship and available time schedule.

Each test will last 5 minutes with grace period of 5 minutes. Some minutes are made available to move the jammer around between test 23.1.6, 23.1.7 and 23.1.8.

Test Area:	1 (off the coast)
Operational Contact:	Tomas Levin, SVV
Technical Contact:	Tomas Levin SVV
Time estimate:	1 hour & 30 minutes

23.1.1 Test: Mobile jammer (H8.1) (L1 only) - on the car deck outside car

23.1.2 Test: Mobile jammer (H8.1) (L1 only) - on the car deck outside car

23.1.3 Test: Mobile jammer (H6.6) (L1+L2) - on the car deck outside car

23.1.4 Test: Mobile jammer (H6.6) (L1+L2) - on the car deck outside car

23.1.5 Test: Mobile jammer (H6.6) (multi-band) – on the car deck outside car

23.1.6 Test: Mobile jammer (H6.6) (multi-band) – on the car deck inside car

23.1.7 Test: Mobile jammer (H6.6) (multi-band) – on deck close to the ship's antennas (by the bridge)

23.1.8 Test: Mobile jammer (H6.6) (multi-band) – inside public areas of boat (under the bridge)

24 Stationary high-power jamming, ramp power with PRN - Ramnan (200 W)

24.1 Preconditions and setup

The main objective is to observe how the J/S signal affect the loss of PNT, and/or how it produces inaccurate PNT data, and at which power level. This will allow for evaluation of the sensitivity thresholds for various systems. The transmitted power will be ramped up and down from 0.1 µW to 200 W EIRP for each test with 10 seconds hold time for each power level, with ramping steps of 2 dB. The modulation will be PRN. The attendees should be at a stationary location with a known distance to the jammer, so they can observe how different levels will affect the PNT.

The jammer will be placed at Ramnan, up the mountainside northwest of Bleik. This is point B in 26.2. This will allow for attendees to evaluate the difference between signals arriving from in the horizontal plane (as is the case with the cemetery placement (6)) and signals arriving with some elevation above the horizontal (this testcase).

Each test will last for 15.67 minutes, with a 15-minute break between each test. The jammer employed will be “Porcus Major”, see appendix26.9.19. The last step, from 52 dBm to 53.0103 dBm (200 W), will be a 1.0103 dB increment, not a 2 dB increment.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Anders Rødningsby, FFI
Time estimate:	2 hours

24.1.1 Test: 0.1 µW to 200 W, 2 dB increments PRN: L1

24.1.2 Test: 0.1 µW to 200 W, 2 dB increments PRN: L1, G1

24.1.3 Test: 0.1 µW to 200 W, 2 dB increments PRN: L1, G1, L2

24.1.4 Test: 0.1 µW to 200 W, 2 dB increments PRN: L1, G1, L2, L5

25 Stationary low-power jamming of L1-only and G1-only

25.1 Preconditions and setup

A 20 MHz wideband (WB) white noise signal will be active on either L1 or G1. The idea is to test receivers' ability to change between using GPS and Glonass when one or the other is denied.

Signal power will be ramped up during the first test, and then kept at the achieved maximum power for the reminder of the tests.

Each test will have a short break after it is completed. When L1-only and G1-only is combined in a test, the transmission will change from the first to the second instantly.

Test Area:	1
Operational Contact:	Nicolai Gerrard, Nkom
Technical Contact:	Harald Hauglin, Justervesenet
Time estimate:	40 minutes

25.1.1 Test: WB, L1-only

25.1.2 Test: WB, G1-only

25.1.3 Test: WB, G1-only then L1-only

25.1.4 Test: WB, L1-only then G1-only

26 Appendix list

26.1 Description of test areas at Andøya

RED = Official test area **1**, **Bleik**

Green = Official test area **2**, **Grunnvatn**

Blue = Official test area **3**, **Stave**

26.2 Important locations

Position A: N 69.2826°, Ø 15.9906° (Kirkegård) High power jamming

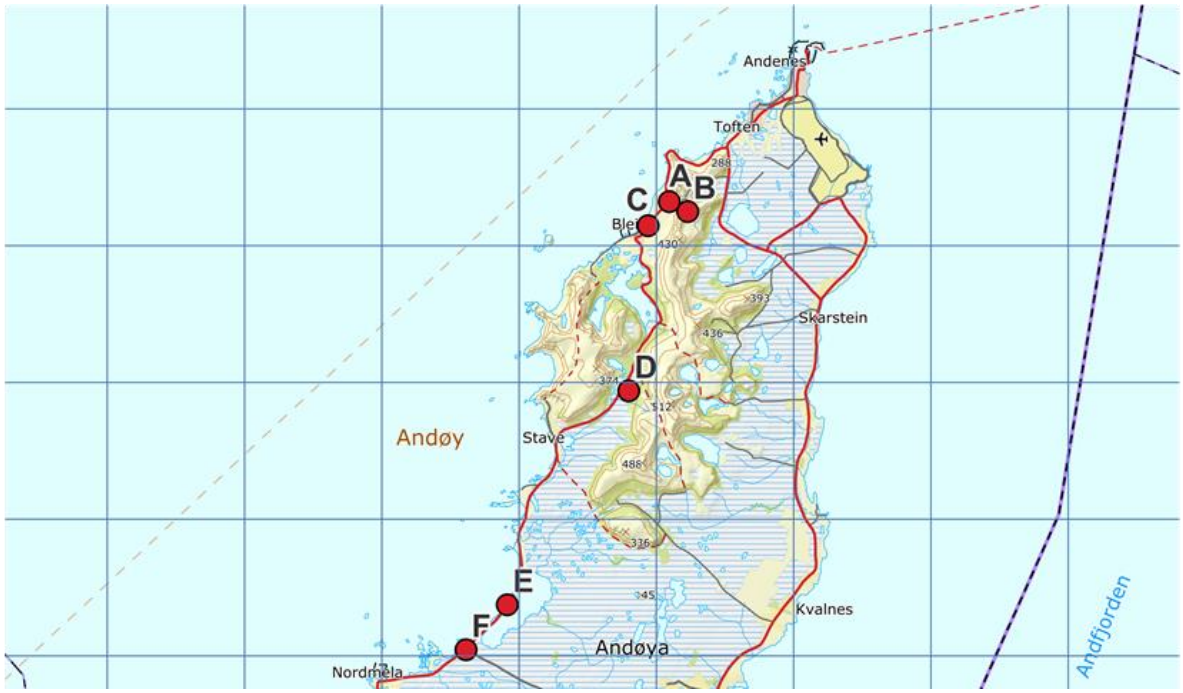
Position B: N 69.2801°, Ø 16.0062° (Laserveien/Ramnan) High power jamming and meaconing

Position C: N 69.2757°, Ø 15.9684° (Samfunnshuset) High power spoofing

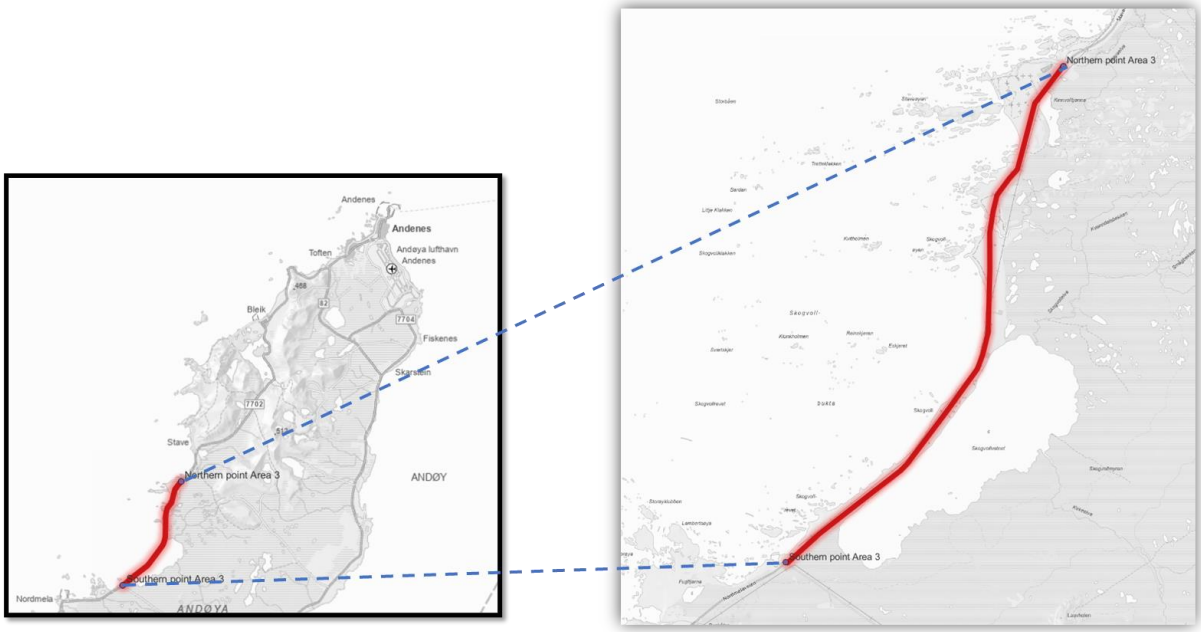
Position D: N 69.2225°, Ø 15.9335° (Grunnvatn) "Sand box", low power jammers

Position E: N 69.1572°, Ø 15.8005° (Skogvollvatnet)

Position F: N 69.1440°, Ø 15.7585° (Nordmela) Southern end-point for mobile low power jammers



26.3 Description of motorcade route(s) on Andøya



Small Jammers can be turned on between these two locations
Northern point: **69.19461** North **15.84028** East
Southern point: **69.14409** North **15.75847** East

Driving tests with small jammers and simple low-power spoofers will be carried out in test area 3. In this area jammers will be operated between two locations. The southern location is at the intersection of county road FV7702 and communal road 71206 (the small road that goes across the island. On the west side of this intersection there is a small grass parking lot that can be used to turn the vehicles around. At the Northern end there is a road taking off to the west, this can also be used to turn vehicles around.

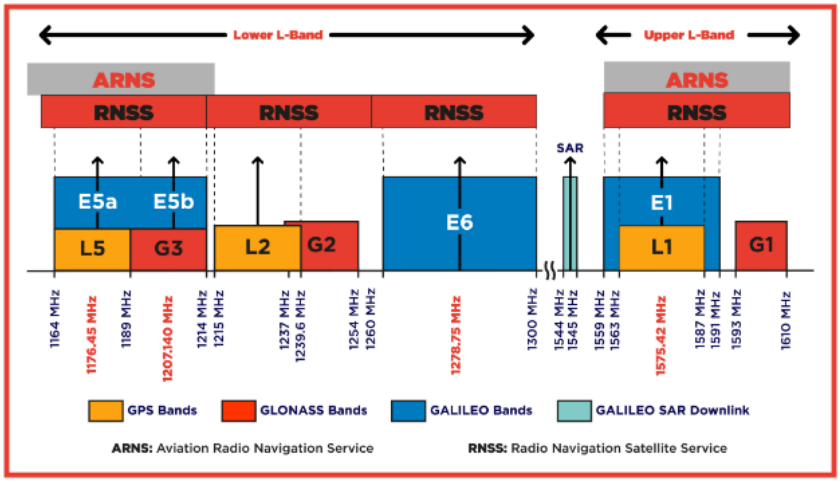
The road width is about 5.1 meters and speed limit is 80 km/h, traffic volume on the road is low around 1000 vehicles per day.

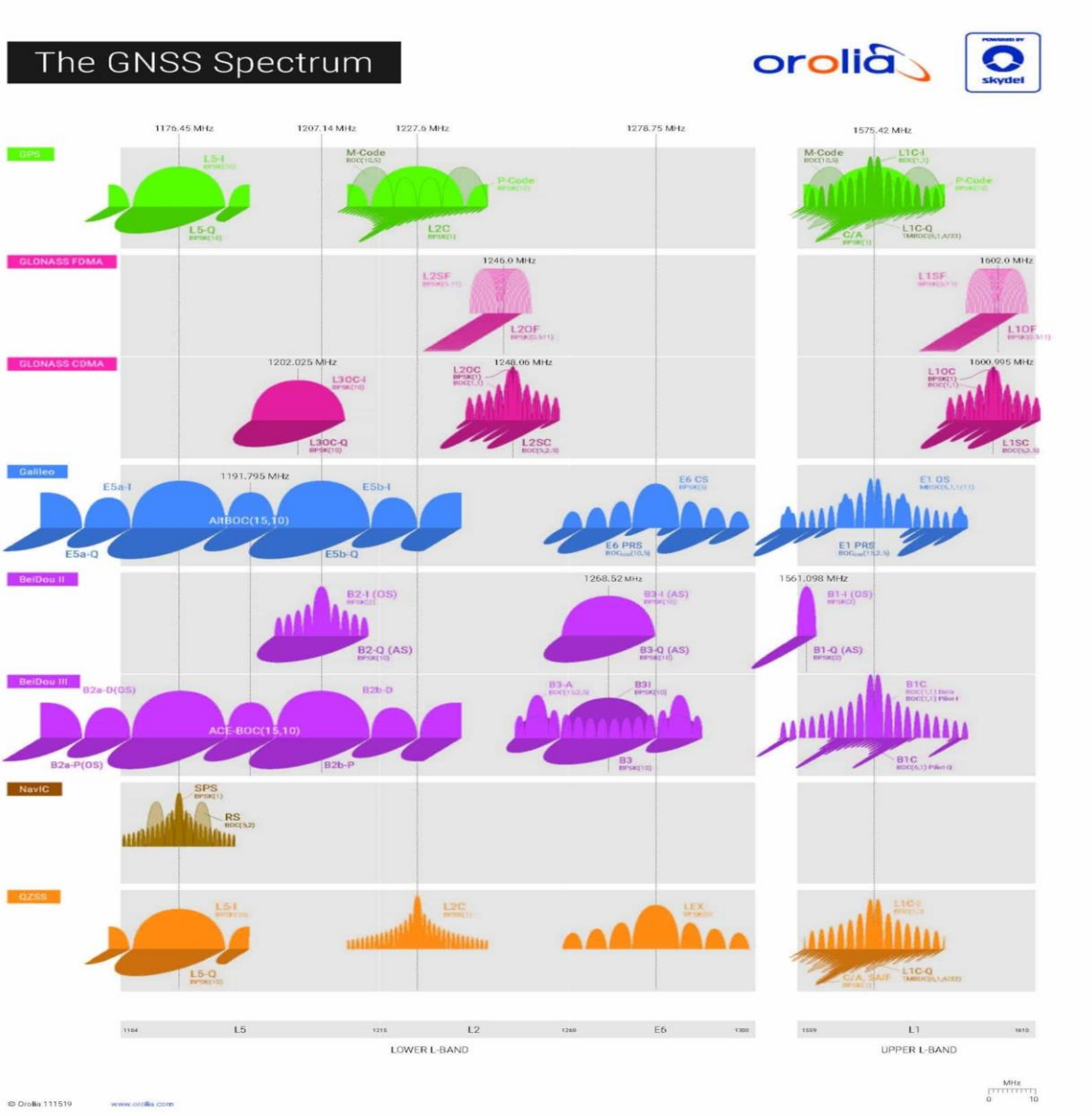
26.4 GNSS systems overview with signal notation and frequency

GNSS band acronym	Frequency band
L1 = GPS band L1,	1563 – 1587 MHz
L2 = GPS band L2,	1215 – 1240 MHz
L5 = GPS band L5,	1164 – 1189 MHz
G1 = Glonass band G1	1593 – 1610 MHz
G2 = Glonass band G2	1237 – 1254 MHz
G3 = Glonass band G3	1189 – 1214 MHz
B1L = Beidou legacy band B1l	1559 – 1563 MHz
B1C = Beidou band B1	1559 – 1592 MHz
B2a = Beidou band B2a	1166 – 1187 MHz
B2b = Beidou band B2b	1197 – 1217 MHz
B3l = Beidou band B3	1258 – 1279 MHz
E5a = Galileo band E5a	1164 – 1189 MHz
E5b = Galileo band E5b	1189 – 1214 MHz
E1 = Galileo band E1	1559 – 1591 MHz
E6 = Galileo band E6	1260 – 1300 MHz

When bands are proclaimed in testcases, the transmissions will be somewhere in the above-mentioned frequency ranges.

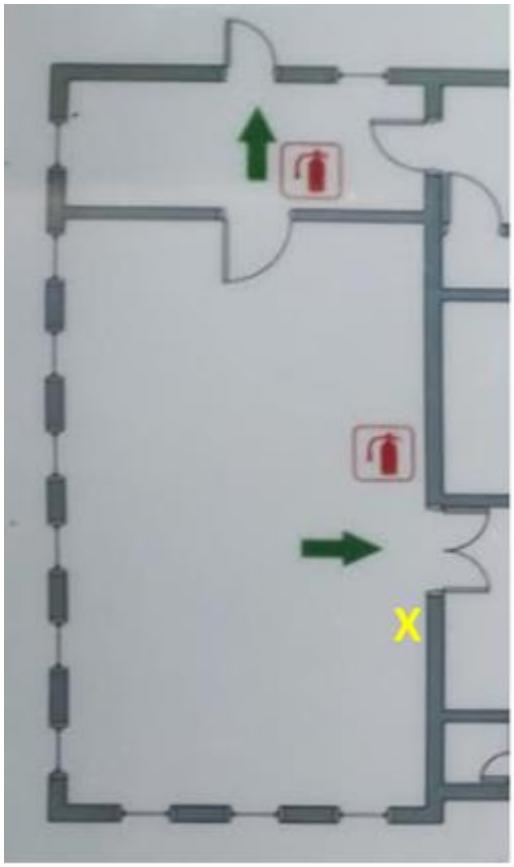
GNSS System	Signal Notation	Signal Frequency (MHz)
GPS	L1 C/A	1575.42
	L1C	1575.42
	L2 C	1227.6
	L2 P	1227.6
	L5	1176.45
GLONASS	L1 C/A	1598.0625-1609.3125
	L2 C	1242.9375-1251.6875
	L2 P	1242.9375-1251.6875
	L3 OC	1202.025
Galileo	E1	1575.42
	E5a	1176.45
	E5b	1207.14
	E5 AltBOC	1191.795
	E6	1278.75
BeiDou	B1I	1561.098
	B2I	1207.14
	B3I	1268.52
	B1C	1575.42
	B2a	1176.45
	B2b	1207.14
NAVIC	L5	1176.45
SBAS	L1	1575.42
	L5	1176.45
QZSS	L1 C/A	1575.42
	L1 C	1575.42
	L1S	1575.42
	L2C	1227.6
	L5	1176.45
	L6	1278.75




The GNSS Spectrum
orolia
skydel
1176.45 MHz
1207.14 MHz
1227.6 MHz
1278.75 MHz
1575.42 MHz
GPS
L5-I
L5-Q
M-Code
L2C
P-Code
M-Code
L1C-I
P-Code
C/A
L1C-Q
GLONASS FDMA
1246.0 MHz
L2SF
L2OF
1602.0 MHz
L1SF
L1OF
GLONASS CDMA
1202.025 MHz
L3OC-I
L3OC-Q
1248.06 MHz
L2OC
L2SC
1600.995 MHz
L1OC
L1SC
Galileo
E5a-I
1191.795 MHz
E5b-I
AltBOC(15,10)
E5a-Q
E5b-Q
E6 CS
E6 PRS
E1 OS
E1 PRS
BeiDou II
B2-I (OS)
B2-Q (AS)
1268.52 MHz
B3-I (AS)
B3-Q (AS)
1561.098 MHz
B1-I (OS)
B1-Q (AS)
BeiDou III
B2a-D(OS)
B2b-D
ACE-BOC(15,10)
B2a-P(OS)
B2b-P
B3-A
B3I
B3
B1C
B1C
NavIC
SPS
RS
QZSS
L5-I
L5-Q
L2C
LEX
L1C-I
C/A, SAIF
L1C-Q
1164
L5
1215
L2
1260
E6
1300
1559
L1
1610
LOWER L-BAND
UPPER L-BAND
MHz
0
10
© Orolia 111519
www.orolia.com

26.5 Technical details on timing references at the Event

Note: Details on reference timing will be updated after setup and calibration during week 37.



Reference timing will be available in the room in the southwest part of Bleik community house. The room is approximately 10 m x 20 m. Timing distribution amplifiers will be located near the yellow 'X' in the sketch above.

We will distribute 1 PPS and 10 MHz derived from a SRS FS725 Rb clock. The SRS FS725 in turn will be phase locked to the 1 PPS output from a White Rabbit Switch (IEEE1588 PTP-HA), ultimately locked to a Cs based ePRTC clock located a few 100 km from Bleik. Given appropriate calibration and network asymmetry compensation the network timing should be accurate to within +- 30 ns from UTC for an ePRTC class clock.

TTL level 1 PPS and 10 MHz timing signals will be distributed to test participants using Meinberg SDUs (https://www.meinbergglobal.com/english/products/sdu.htm):
Connectors: BNC
Signal: Between 0 and 2.7 V into 50 Ohm
The 10 MHz square wave signal will have 50 ns pulse duration.

In total there will 48 timing outputs available in any combination of 1 PPS and 10 MHz in blocks of 12.

We are working on an alternative reference timing which may be even more accurate and stable than the network timing.

26.6 Overview of Bleik community house

Figure 26.1 gives an overview of the layout of Bleik community house.

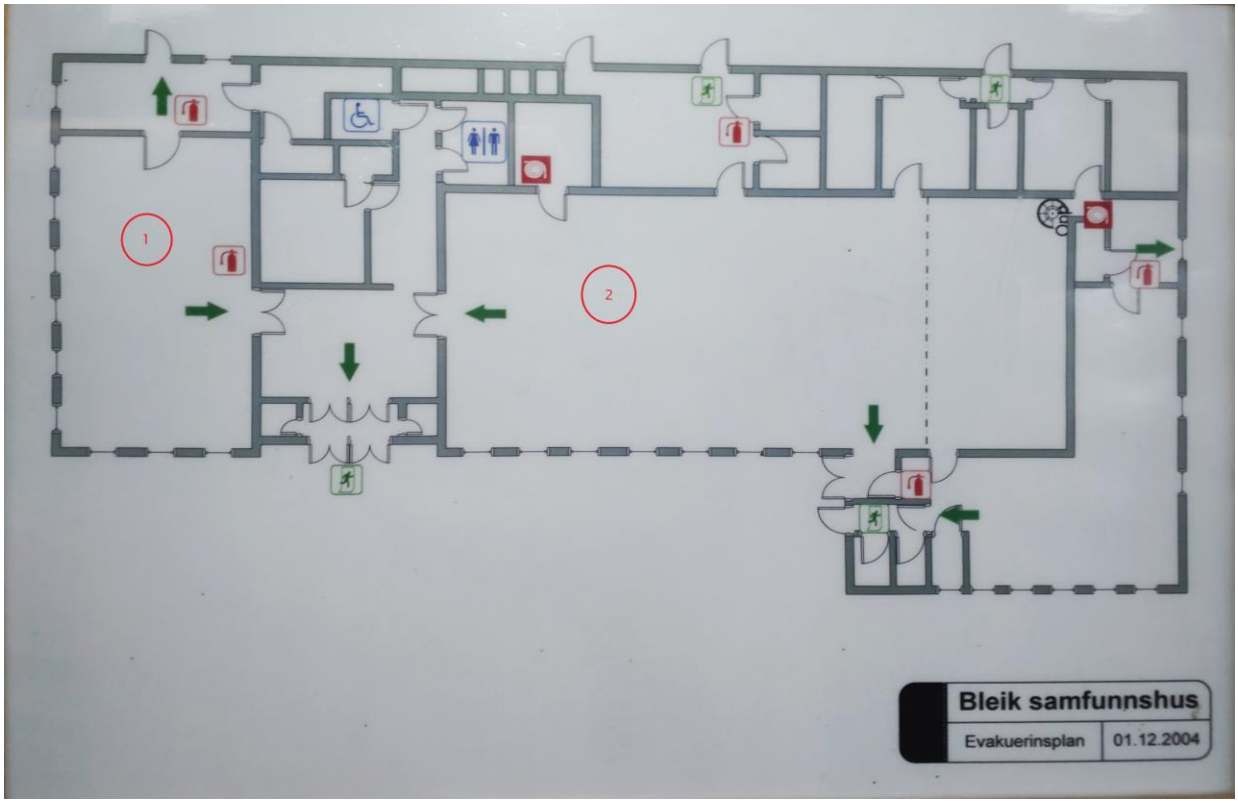


Figure 26.1: Floor plan of Bleik samfunnshus ('Bleik community house').

The community house has installed Wi-Fi, that the participants are free to use.

Room number 1 (indicated with the left red circle in Figure 26.1) is prioritised for participants with timing equipment.

Room number 2 is for briefings, equipment, lunch, and gatherings.

26.7 Overview of OSNMA

Galileo Open Service Navigation Message Authentication (OSNMA) is a free authentication service, available worldwide to allow users to verify whether the navigation message is received from a genuine Galileo satellite. Authentication information is provided through the E1-B component.

Navigation data authenticated by OSNMA are satellite ephemeris and clock data in addition to GST, GPST and UTC timing offset parameters.

data from Word Type 1					data from Word Type 2					data from Word Type 3								data from Word Type 4						data from Word Type 5																				
IOD_{nav}	Ephemeris (1/4)				IOD_{nav}	Ephemeris (2/4)				IOD_{nav}	Ephemeris (3/4)							IOD_{nav}	SVID	Ephemeris (4/4)		Clock Correction			Ionospheric correction					BGD(E1,E5a)	BGD(E1,E5b)	$E5b_{HS}$	$E1B_{HS}$	$E5b_{DVS}$	$E1B_{DVS}$	Total (bits)																		
	t_{0e}	M_0	e	$A^{1/2}$		Ω_0	i_0	ω	$\dot{i}$		$\dot{\Omega}$	Δn	C_{UC}	C_{US}	C_{RC}	C_{RS}	SISA(E1,E5b)			C_{ic}	C_{is}	t_{0c}	a_{f0}	a_{f1}	a_{f2}	a_{i0}	a_{i1}	a_{i2}	Region 1	Region 2	Region 3	Region 4	Region 5																
10	14	32	32	32	10	32	32	32	14	10	24	16	16	16	16	16	8	10	6	16	16	14	31	21	6	11	11	14	1	1	1	1	1	10	10	2	2	1	1	549																		

data from Word Type 6								data from Word Type 10			
GST-UTC conversion parameters								GST-GPS conversion parameters			
A_0	A_1	Δt_{LS}	t_{ot}	WN_{0t}	WN_{LSF}	DN	Δt_{LSF}	A_{0G}	A_{1G}	t_{0G}	WN_{0G}
32	24	8	8	8	8	3	8	16	12	8	6

Further information:

Galileo OSNMA FAQ: https://www.gsc-europa.eu/galileo/faq#OSNMAsection

Galileo OSNMA reference documents: https://www.gsc-europa.eu/electronic-library/programme-reference-documents#OSNMA

26.8 Overview of spoofed routes

26.8.1 Route 1

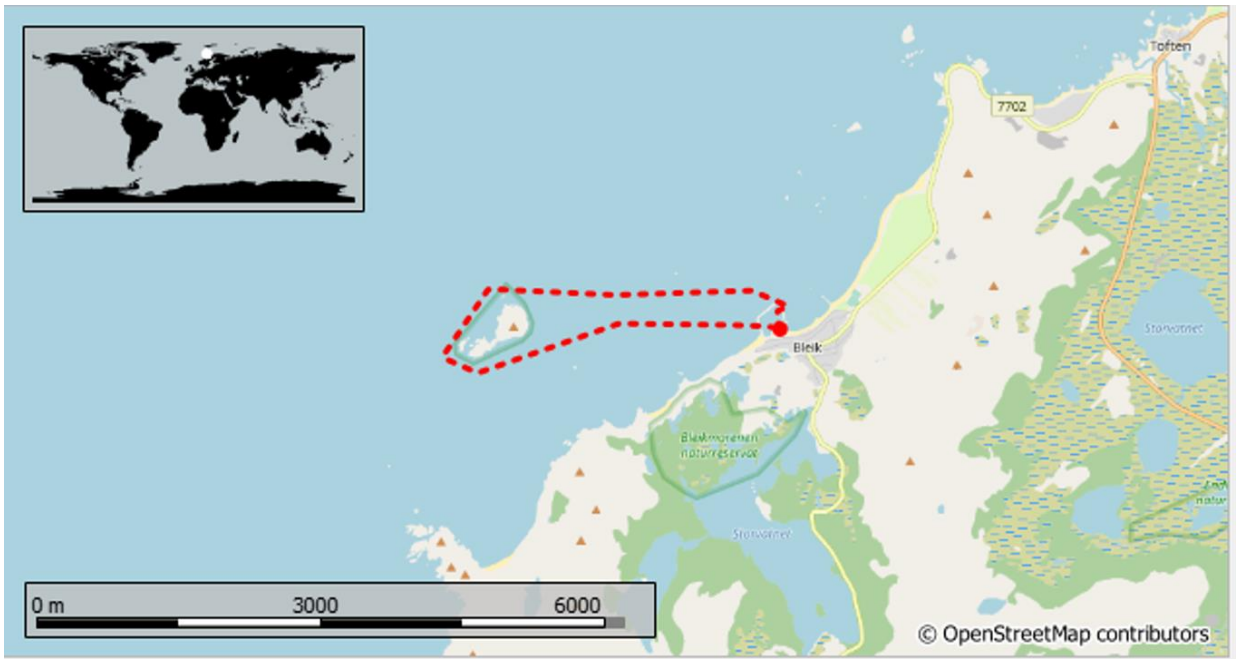
26.8.2 Route 2

Not in use

26.8.3 Route 3

26.8.4 Route 4

26.8.5 Route 5



26.9 Technical details on jammer equipment

The nomenclature for naming of the jammer equipment is as follows:

1st Letter (Norwegian / English)	1St digit	2nd digit
S = Sigarett / Cigarette	**Number of antennas**	**# jammer within same category**
H = Håndholdt / Handheld		
U = USB / USB stick		
F = Fastmontert / Permanently installed (Fixed)		

Exempli gratia:

S1.2, is a cigarette type jammer, that has 1 antenna, and is unit nr.2 in this category.

Technical details on low power jammers given in this appendix are from uncalibrated measurements. They are rough estimates given for both the frequency and time domain. Power levels are not correctly displayed on the chart, because of external attenuators used during measurements with a signal analyser. There may also have been some constraints in the measurement device, causing fast frequency components to not be correctly displayed.

26.9.1 Technical details on low-power jammer “S1.1 to S1.3”

Cigarette jammers is category of jammers that is often installed in the cigarette lighter outlet in cars. They are intended to cover the car, and a given radius around the car.

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands
1575	30 - 40	L1, E1, B1I, B1C

- Estimated output power (conducted): 10 - 15 dBm
- Type of modulation: sweep
    - Sweep rate: 22 - 37 µs

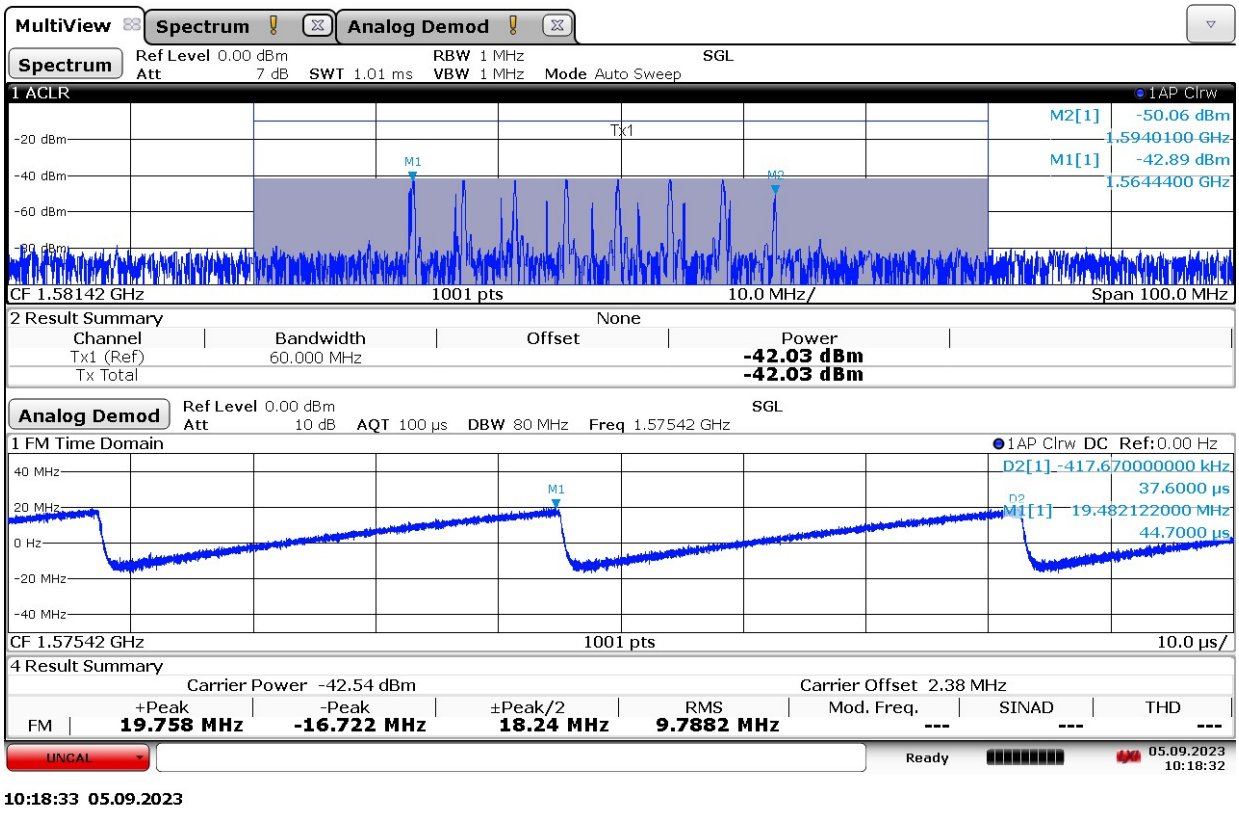


Figure 26.2: Example measurement of a S1.1 - S1.3 jammer.

26.9.2 Technical details on low-power jammer “S2.1 to S2.4”

Cigarette jammers is category of jammers that is often installed in the cigarette lighter outlet in cars. They are intended to cover the car, and a given radius around the car. This type of cigarette jammer has two antennas for jamming two bands simultaneously.

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands
1575	70 - 90	L1, E1, B1I, B1C, G1
1227	70 - 90	L5, E5a/b, B2a/b, G3

- Estimated output power (conducted): 15-20 dBm
- Type of modulation: sweep
    - Sweep rate: 40 - 60 µs

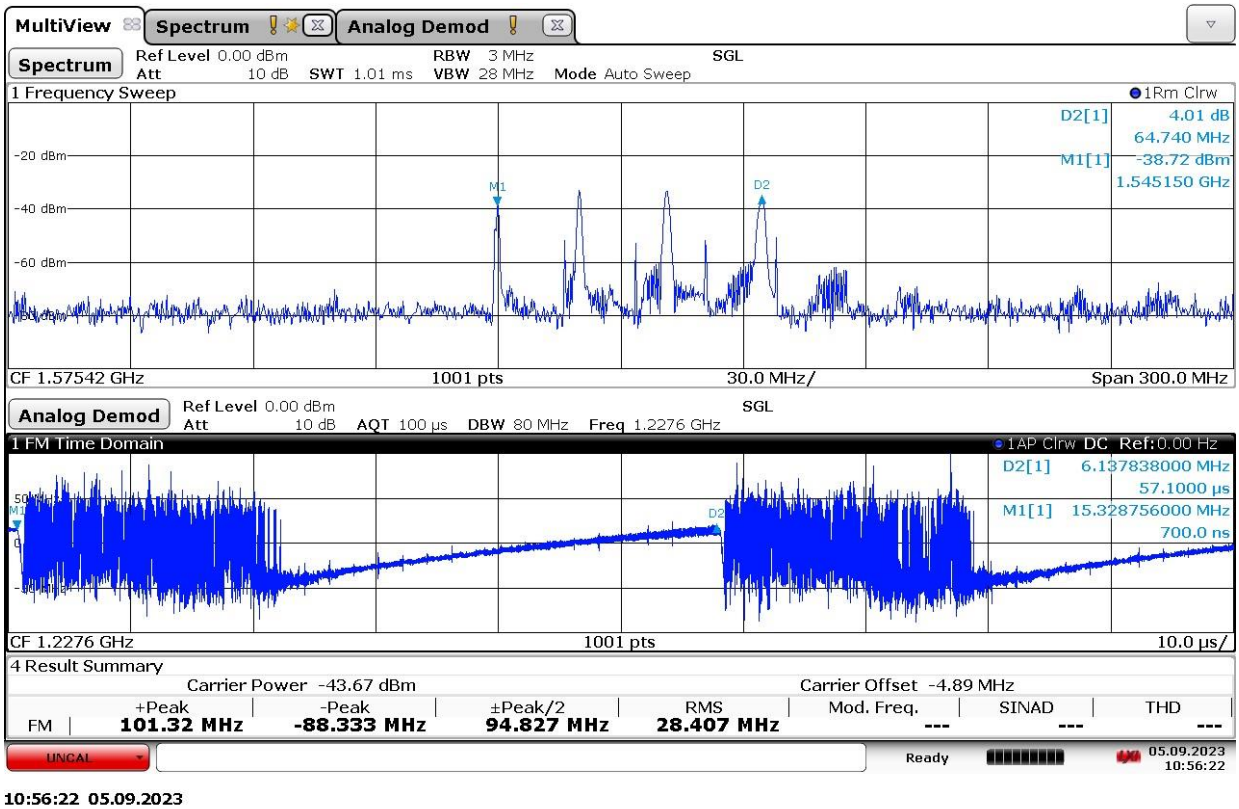


Figure 26.3: Example measurement of a S2.1 – S2.4 jammer on GPS L1 band.

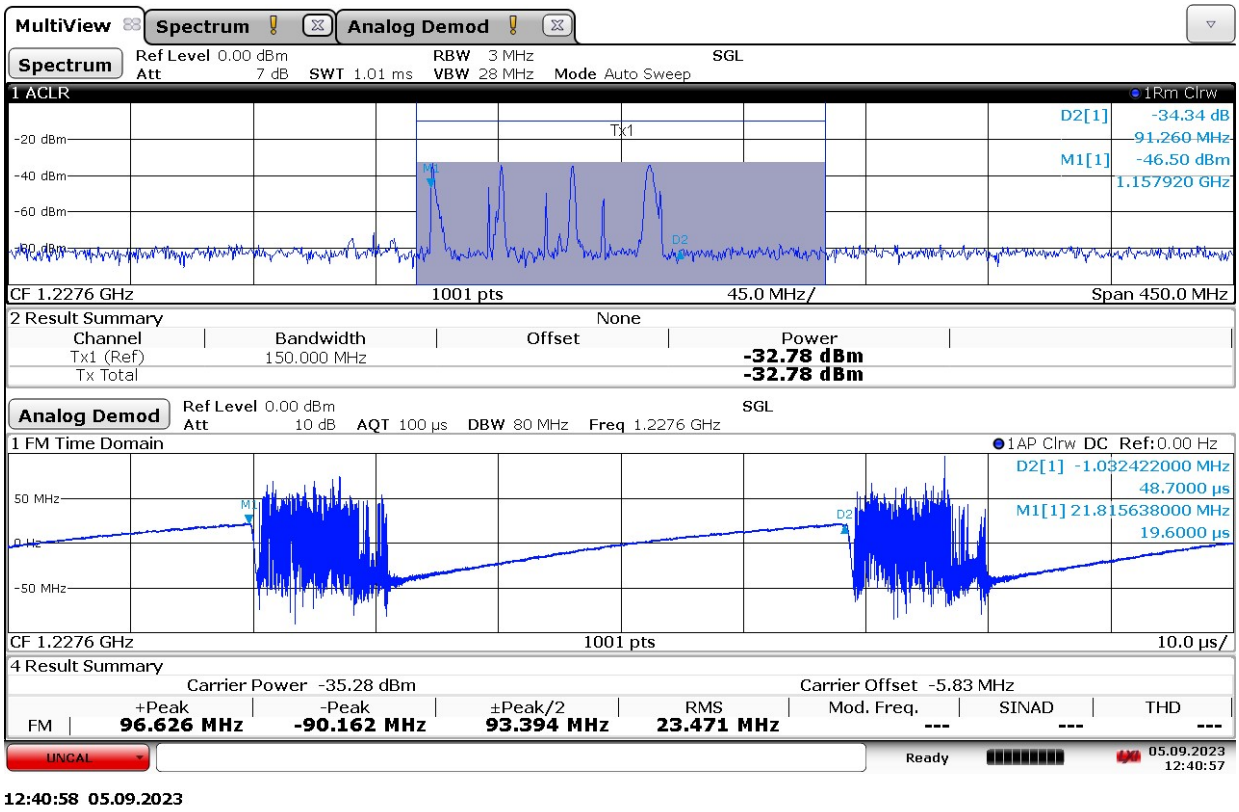


Figure 26.4. Example measurement of a S2.1 - S2.4 jammer on GPS L2 band.

26.9.3 Technical details on low-power jammer “U1.1 to U1.4”

USB jammers is category of jammers that is often installed in the USB outlet. The are intended to cover a small radius. These particular jammers suggest in the LED screen that they jam two bands, although this is not the case (see below).

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands
1590 - 1600	70 - 80	L1, E1, B1I, B1C, G1

- Estimated output power (radiated): N/A
- Type of modulation: sweep
    - Sweep rate: 5 - 8 µs

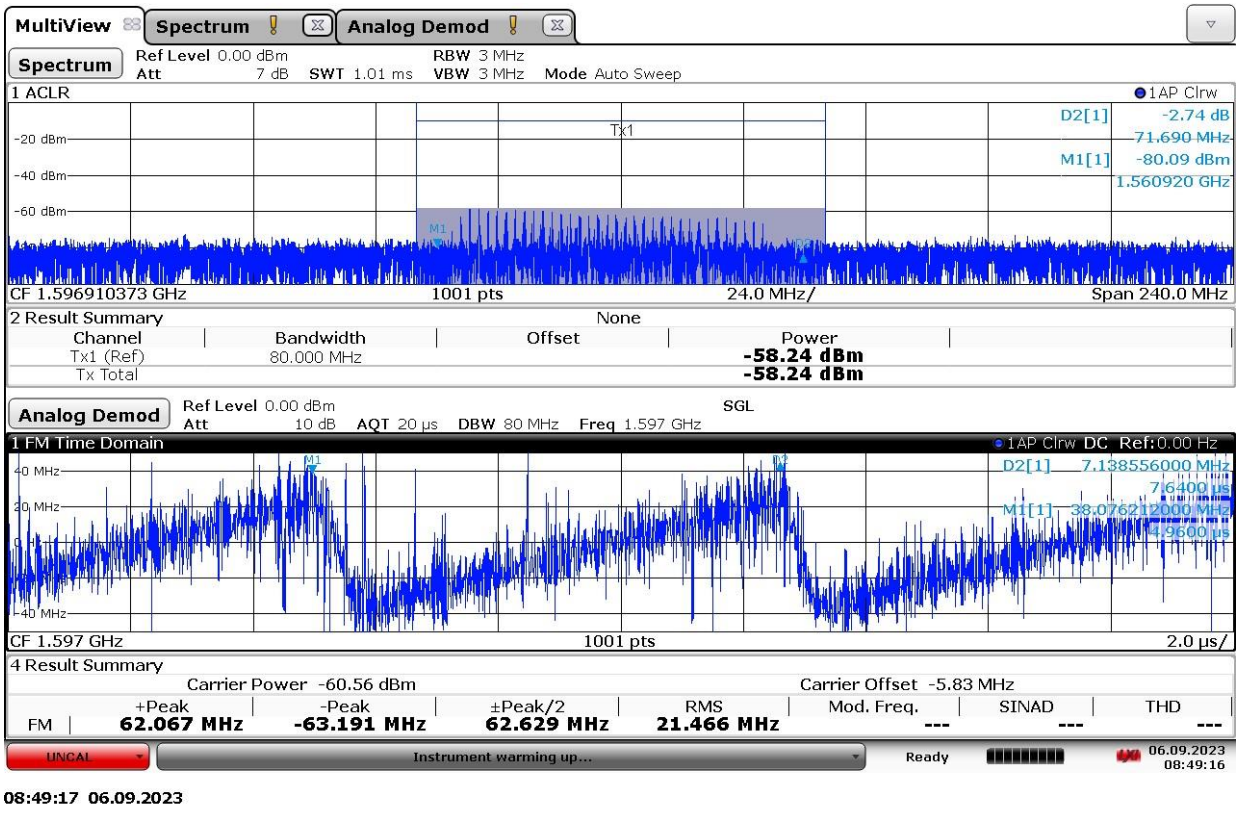


Figure 26.5: Example measurement of a U1.1 – U1.4 jammer.

26.9.4 Technical details on low-power jammer “H1.1”

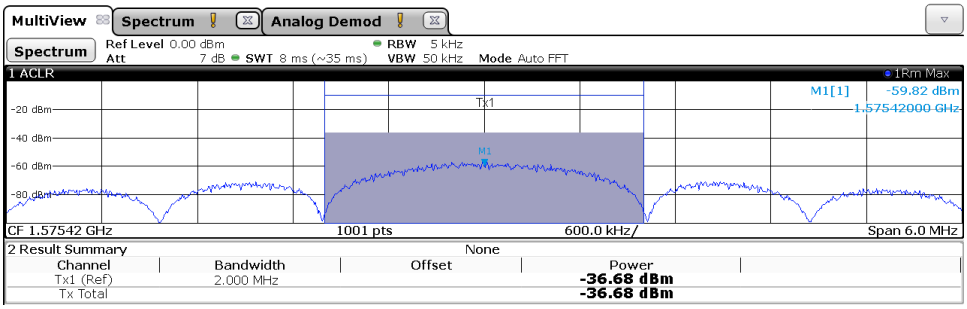
Novatel’s NEAT-jammer is a commercial multi-frequency – multi-modulation type jammer for GPS L1 and L2, with both low and high output power. Antenna has TNC-connector. Signals are turned on and off by different buttons. Potentially afflicted GNSS bands will vary with the chosen modulation and frequency.

Technical characteristics

- Centre frequency: 1575.42 MHz and 1227.6 MHz
- Estimated output power conducted: low power -5 dBm, high power 20 dBm
- Type of modulation: narrow band (NB), wide band (WB), continuous wave (CW), chirp/sweep and other (optional to program)

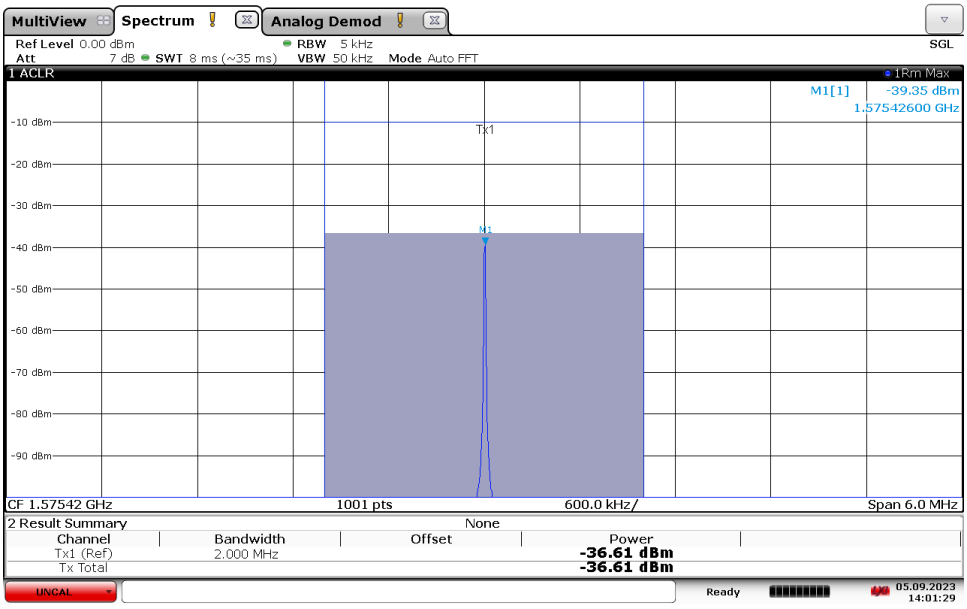
Modulations (signal forms) for L1-signals (assumed similar for L2), centre frequency at 1575.42 MHz:

- NB L1 – Narrowband L1 BPSK-modulated with approximately 1 MHz PRN-code. Bandwidth: 2 MHz



- WB L1 – Wide band L1 BPSK-modulated with approximately 10 MHz PRN-code. Bandwidth: 20 MHz

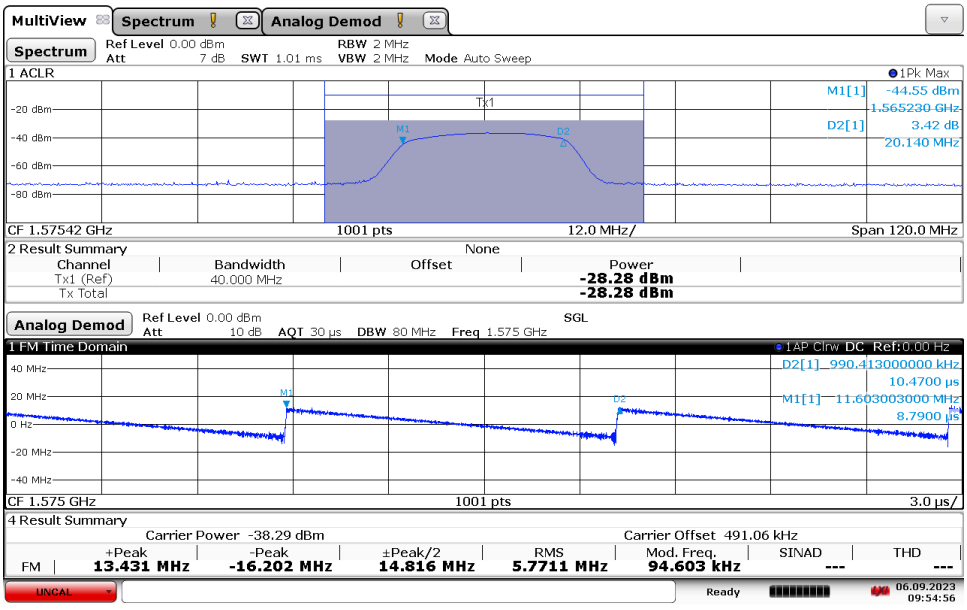
- CW L1 – Continuous wave at 1575.42 MHz



14:01:30 05.09.2023

- Chirp L1 – Sawtooth swept signal, 10 µs sweep rate

  Bandwidth: 21 MHz



09:54:56 06.09.2023

- Other – Optional to program

26.9.5 Technical details on low-power jammer “H1.2”

Small, light and easily operated handheld jammer with one output, intended to cover the main GPS band.

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands
1575	20	L1, E1, B1C

- Estimated output power (conducted): 18 dBm
- Type of modulation: sweep
    - Sweep rate: 6 µs

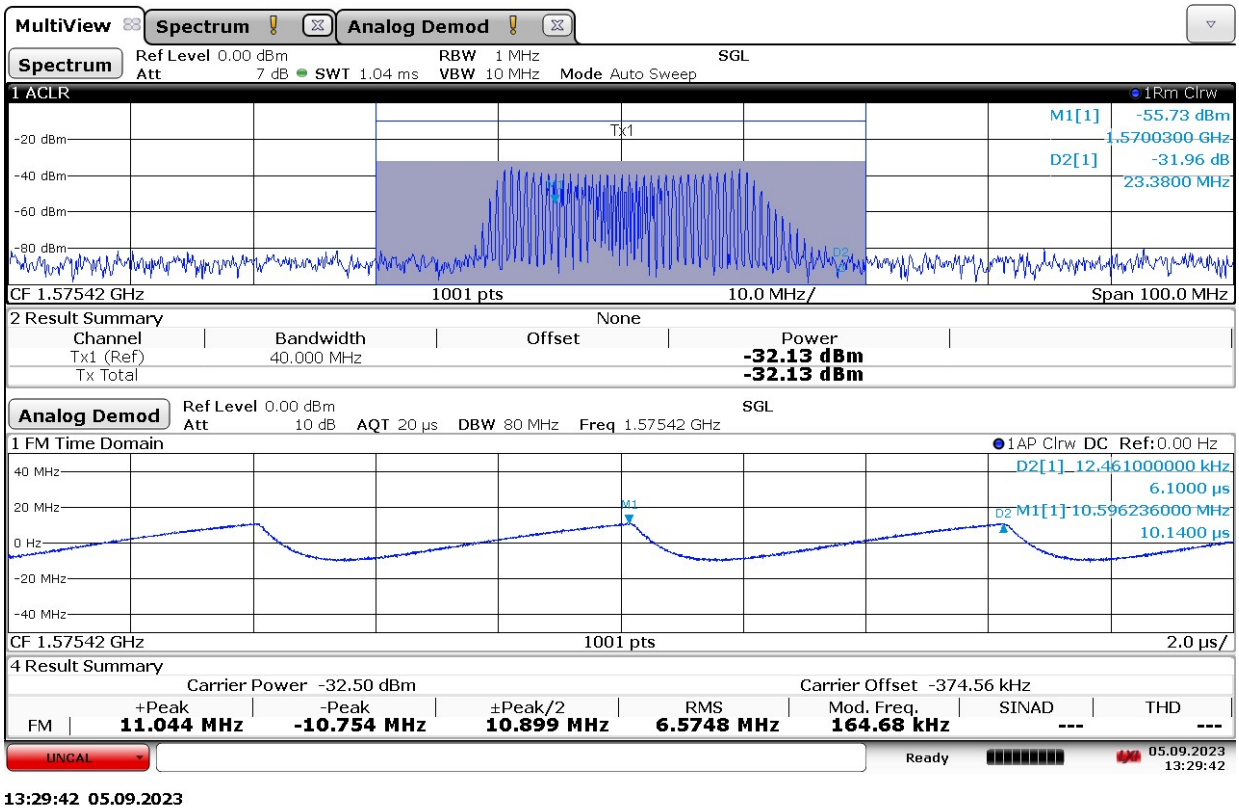


Figure 26.6: Example measurement of a H1.2 jammer.

26.9.6 Technical details on low-power jammer “H1.3”

Small handheld jammer using frequency hopping (normally commercially available jammers employ chirp signals).

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands
1575	1	L1, E1, B1C

- Type of modulation: frequency hopping
  - Jumping between 6 separated frequencies. Every 50 ms the frequency increases 200 kHz, starting with 1574.62 MHz. After approximately 1 MHz the frequency jumps back to the start frequency at 1574.62 MHz.

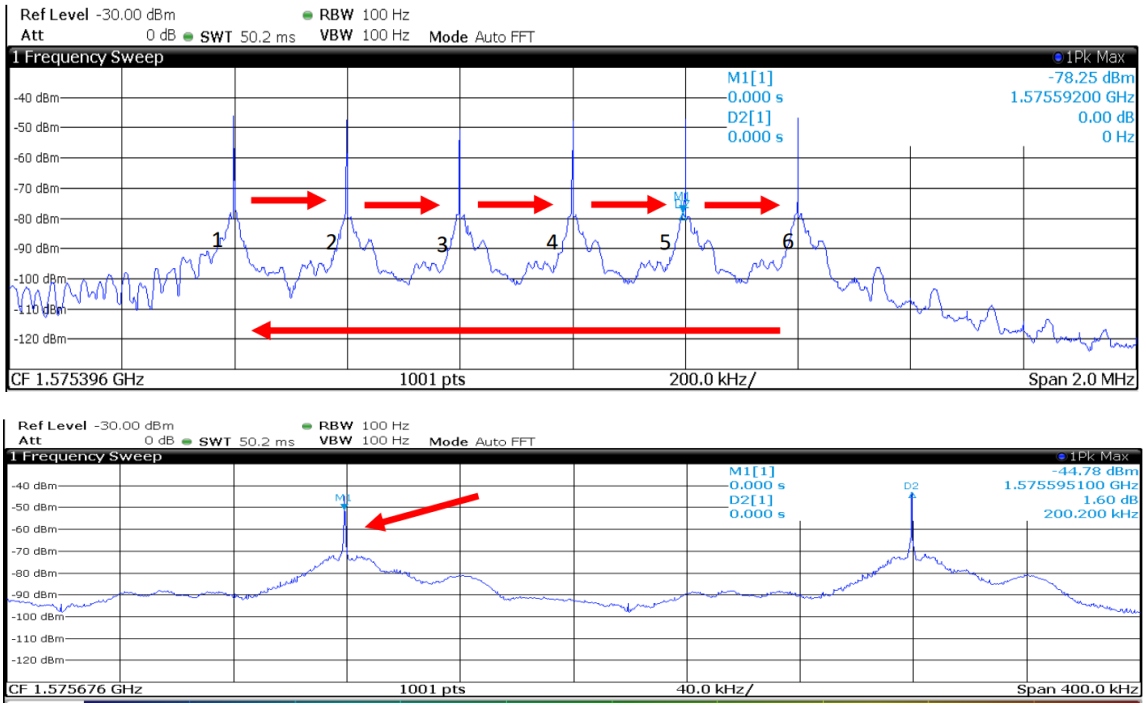


Figure 26.7: Example measurement of H1.3 jammer.

26.9.7 Technical details on low-power jammer “H2.1 to H2.2”

Small handheld jammers with built-in antennas.

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands
1580	20	L1, E1, B1C
1227	20	L2

- Type of modulation: sweep
  - Sweep rate: 9 µs

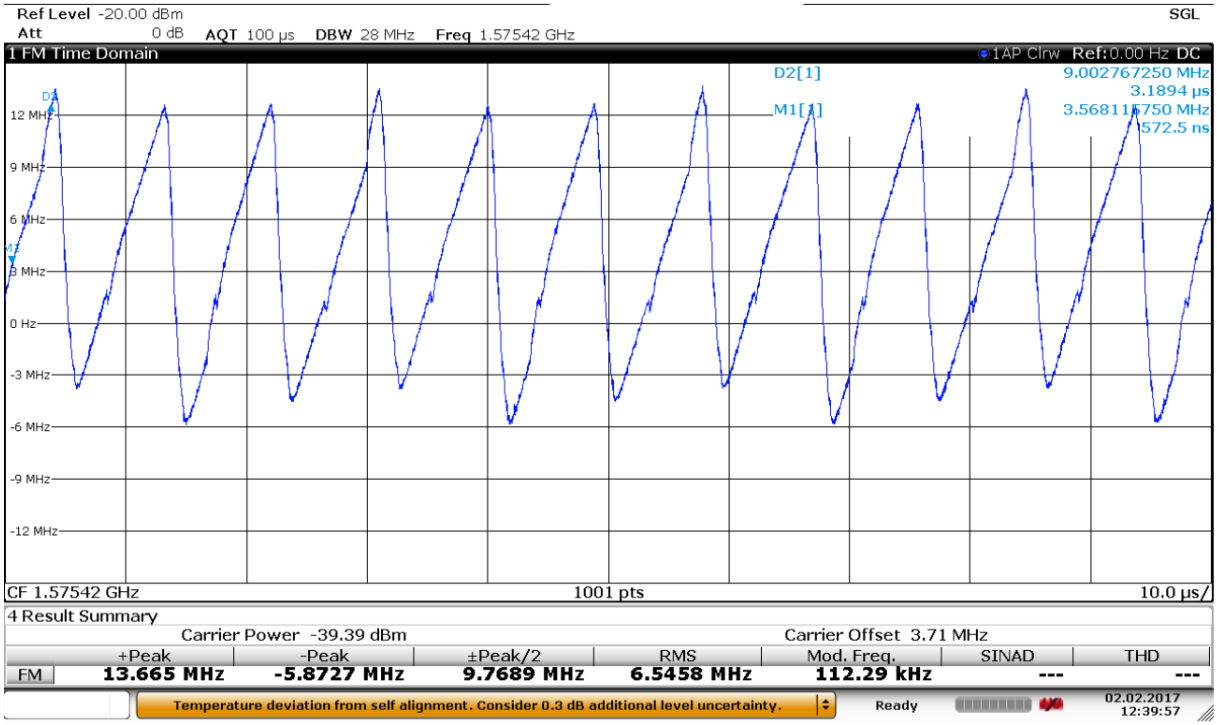


Figure 26.8: Example measurement of H2.1 to H2.2 jammer.

26.9.8 Technical details on low-power jammer “H3.1 to H3.2”

Small handheld jammer intended to cover GPS L1, along with several mobile bands (GSM and DCS).

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands	Relevant GNSS antenna #
1575	23-27	L1, E1, B1C, B1I	2

- Estimated output power (conducted): 20 dBm.
- Type of modulation: sweep
    - Sweep rate: 6 µs

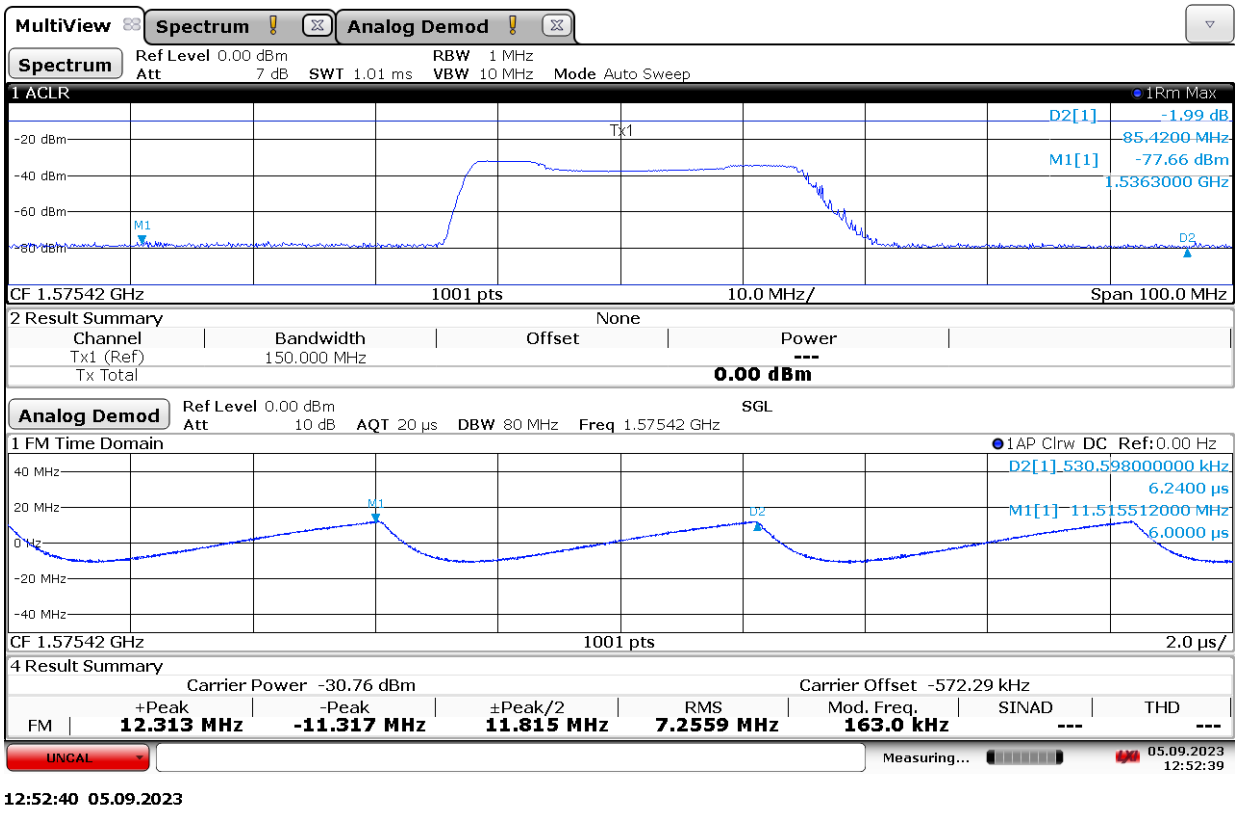


Figure 26.9: Example measurement of H3.1 to H3.2 jammer.

26.9.9 Technical details on low-power jammer “H3.3”

Handheld 3-band GNSS-jammer on L1, L2 and L5. The jammer is precise on centre frequency and has a reasonable bandwidth, working well for GNSS jamming. The individual bands cannot be switched on and off. The three antennas are marked with white lines (short=L1, medium=L2, long=L5).

The jammer has additional noise in several other frequency bands, but with significant lower power.

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands
1575	25	L1, E1, B1C
1227	14	L2
1176	17	L5, E5a, B2a

- Estimated output power (conducted): ca 30 dBm for each band
- Type of modulation: sweep
    - Sweep rate: 1-13 µs

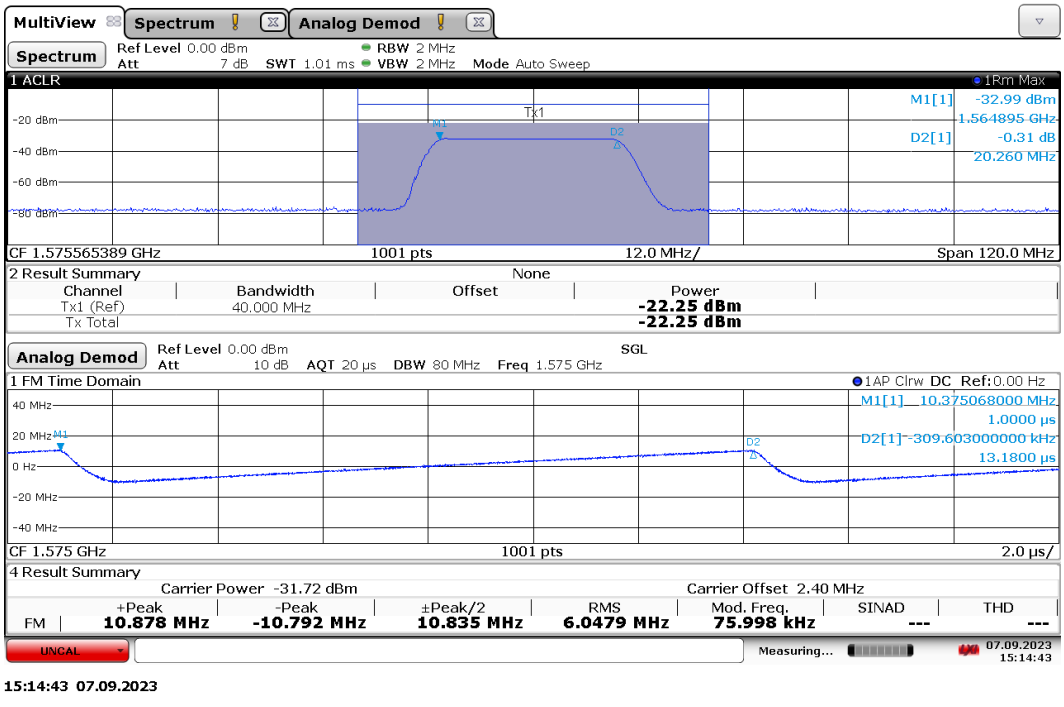


Figure 26.10: Example measurement of H3.3 jammer.

26.9.10 Technical details on low-power jammer H4.1

Handheld 4-band GNSS-jammer. The individual bands can be switched on and off. In addition to the four GNSS-bands this jammer has some harmonics from each main signal.

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands	Relevant GNSS antenna #
1550	100	L1, E1, B1C, B1I	1
1260	45	E6, G2, B3I	2
1220	45	L2, G2, B2b, E5b	3
1182	38	L5, G3, B2a, E5a/b	4

- Estimated output power (conducted): ca 28 dBm on channel/antenna 1, 27 dBm on channel/antenna 2, 26 dBm on channel/antenna 3 and 27 dBm on channel/antenna 4
- Type of modulation: sweep
    - Sweep rate: 9 µs

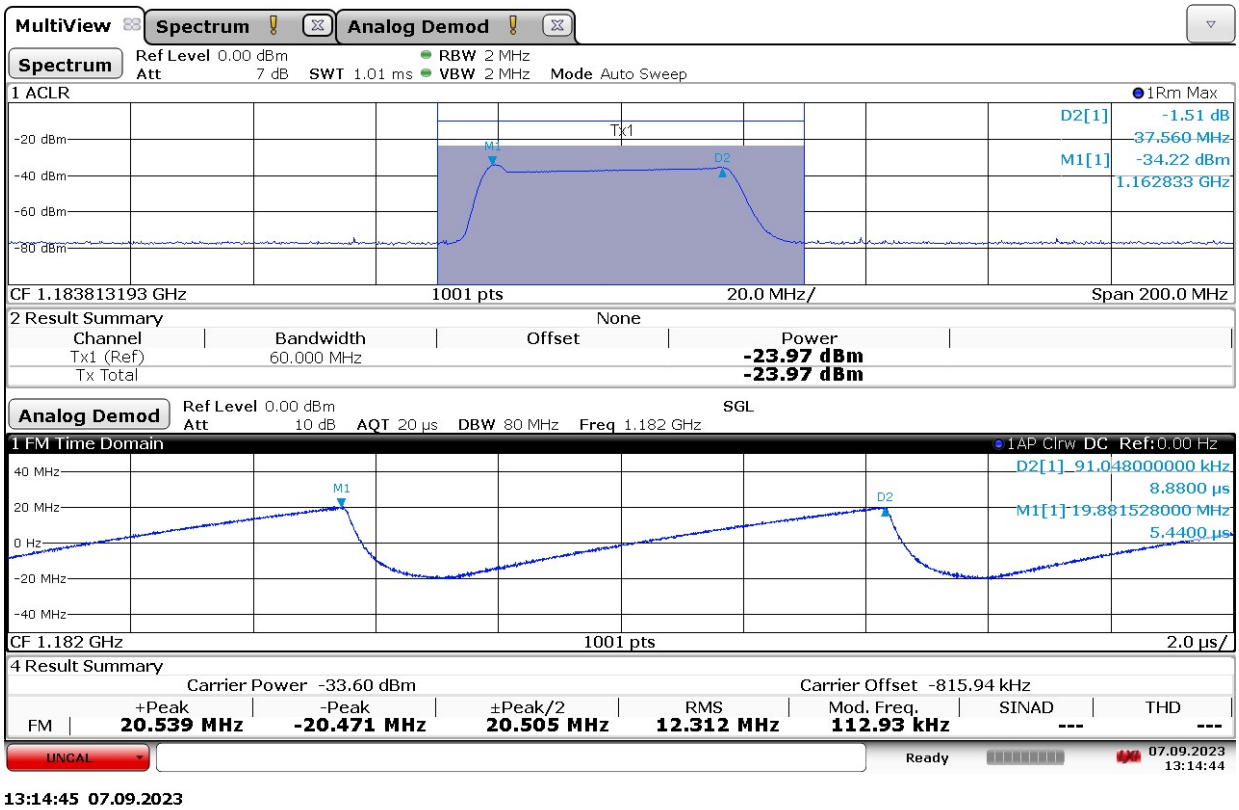


Figure 26.11: Example measurement of H4.1 jammer.

26.9.11 Technical details on low-power jammer “H6.1 ”

Handheld multi band jammer with 6 channels, where number six has centre frequency around GPS L1. The jammer has dip switches on the side to turn the different channels on and off. During testing, a lot of noise was noticed throughout the spectrum on most channels.

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands	Relevant GNSS antenna #
1580	20	L1, E1, B1C	6

- Estimated output power (conducted): ca 28 dBm
- Type of modulation: sweep
    - Sweep rate: 6 µs

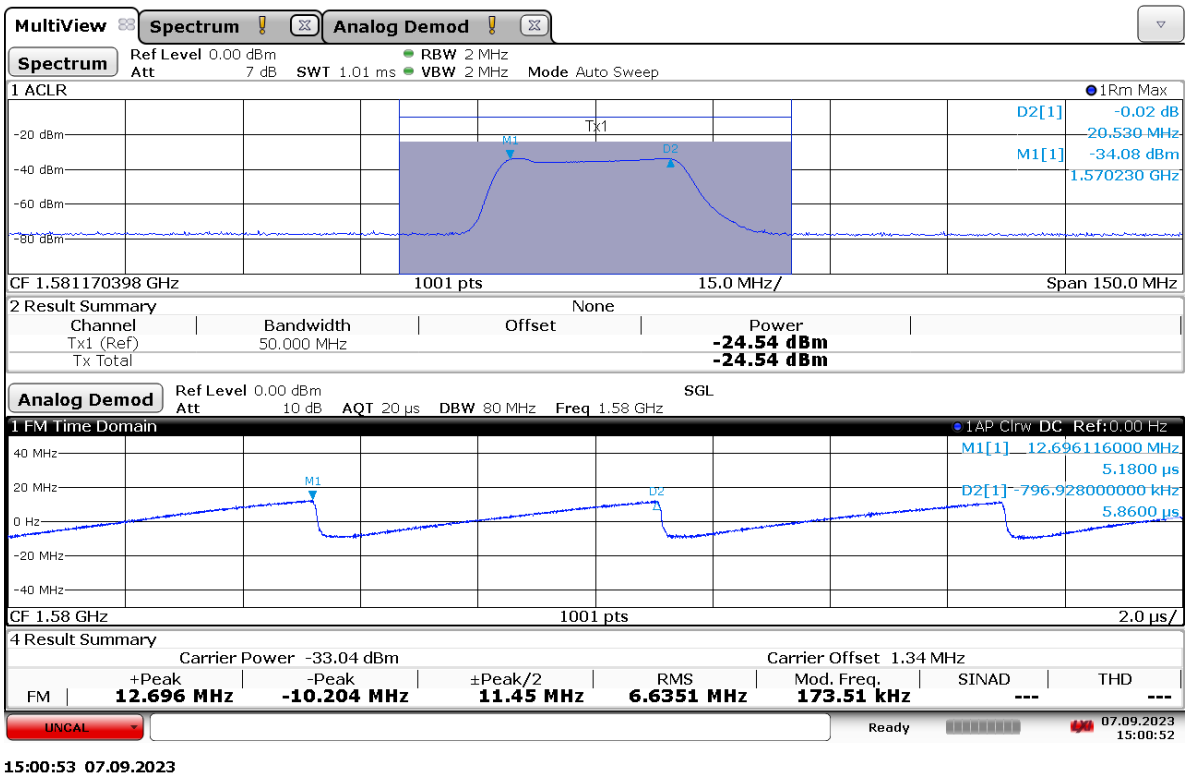


Figure 26.12: Example measurement of H6.1 jammer.

26.9.12 Technical details on low-power jammer “H6.2 ”

Handheld multi band jammer with 6 channels, where number 4 covers GPS L1, number 5 L5, and number 6 L2. The jammer has dip switches on the side to turn the different channels on and off. During testing, a lot of noise was noticed throughout the spectrum on most channels.

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands	Relevant GNSS antenna #
1580	28	L1, E1, B1C	4
1155	105	L5, G3, B2a/b, E5a/b	5
1248	109	L2, G2, G3, B2b, B3I, E5b, E6	6

- Estimated output power (conducted): ca. 30 dBm on channel/antenna 4, 26 dBm on channel/antenna 5, and 28 dBm on channel/antenna 6
- Type of modulation: sweep
    - Sweep rate: 7 µs

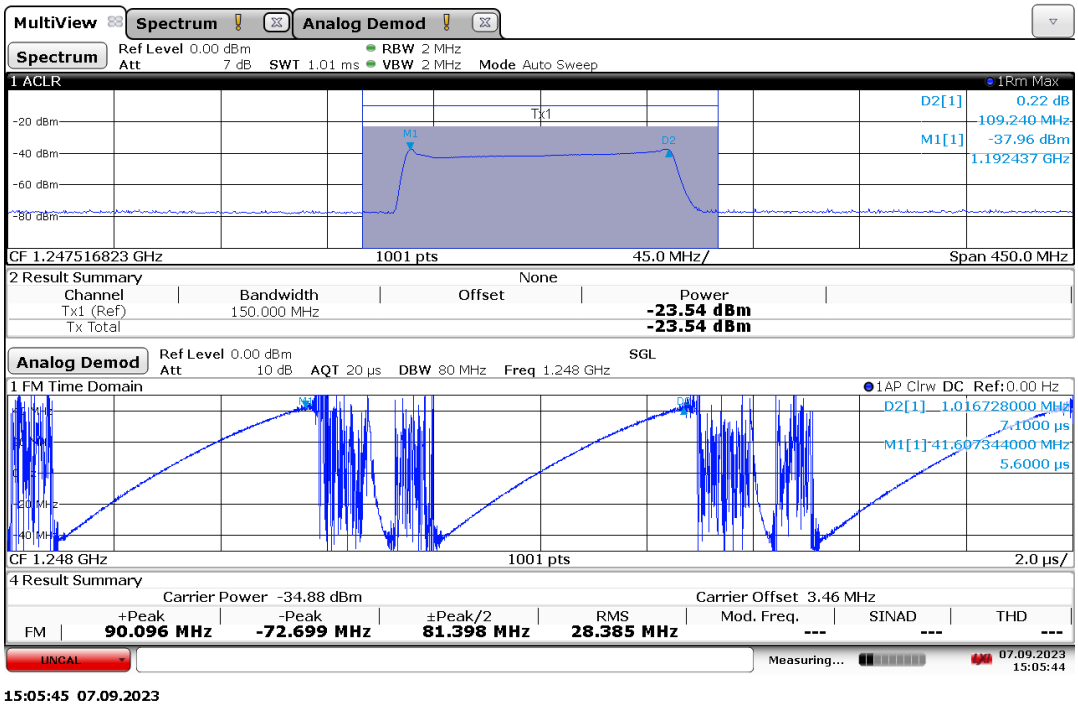


Figure 26.13: Example measurement of H6.2 jammer.

26.9.13 Technical details on low-power jammer “H6.3 ”

Handheld multi band jammer with 6 channels, where number 4 covers GPS L1, number 5 L5, and number 6 L2. The jammer has dip switches on the side to turn the different channels on and off. During testing, a lot of noise was noticed throughout the spectrum on most channels.

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands	Relevant GNSS antenna #
1580	25	L1, E1, B1C	4
1152	108	L5, G3, B2a/b, E5a/b	5
1246	107	L2, G2, G3, B2b, B3I, E5b, E6	6

- Estimated output power (conducted): ca. 30 dBm on channel/antenna 4, 26 dBm on channel/antenna 5, and 28 dBm on channel/antenna 6
- Type of modulation: sweep
    - Sweep rate: 7 µs

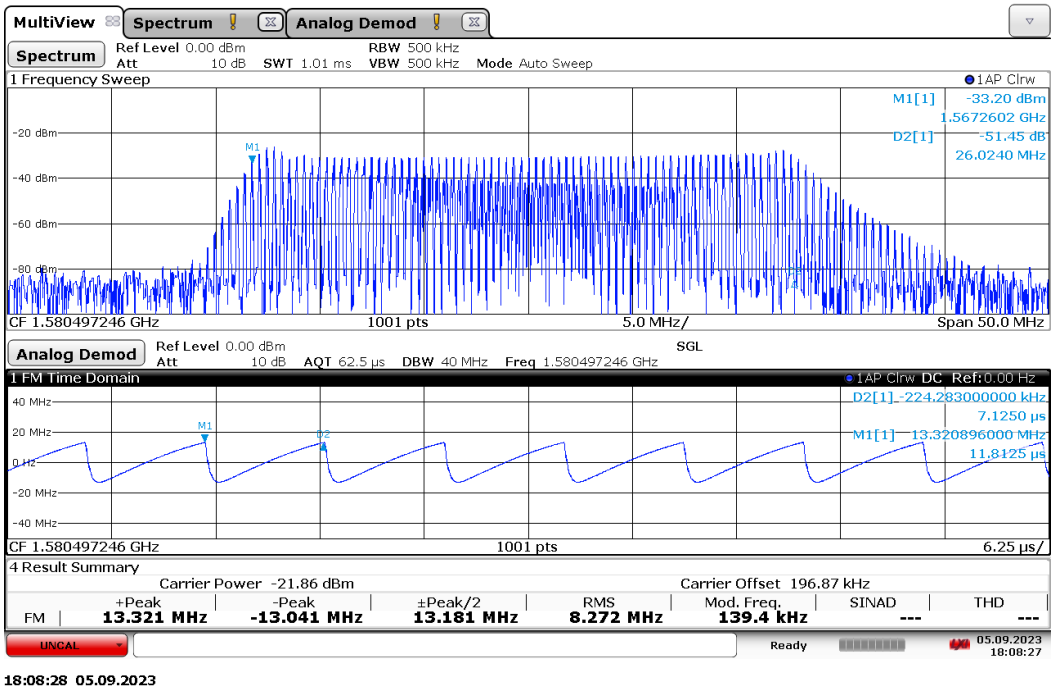


Figure 26.14. Example measurement of H6.3 jammer.

26.9.14 Technical details on low-power jammer “H6.4”

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands	Relevant GNSS antenna #
1176	8.6	L5, B2a, E5a	1
1247	80	L2, G2, B3I, E6	3
1593	80	L1, E1, B1C, B1I, G1	5

- Estimated output power (conducted): ca. 30 dBm on channel/antenna 1, 32 dBm on channel/antenna 3, and 31 dBm on channel/antenna 5
- Type of modulation: sweep
    - Sweep rate: 10 µs

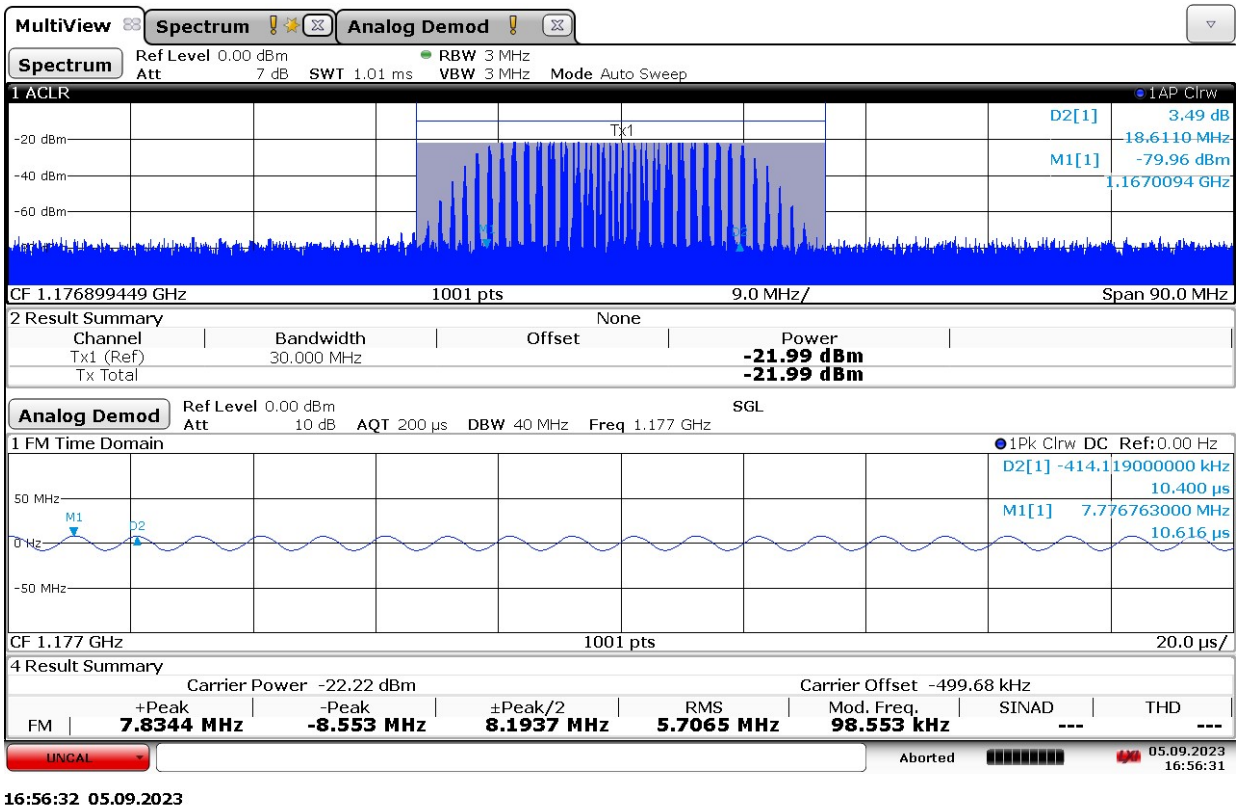
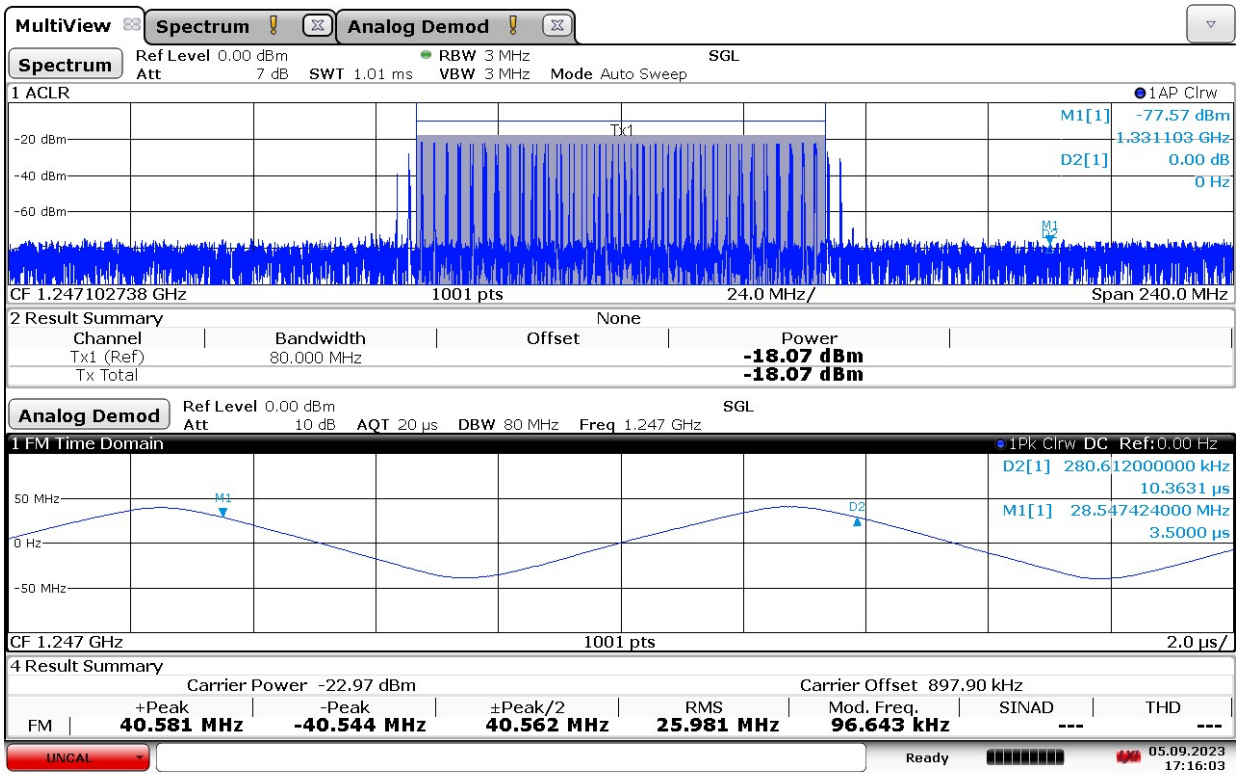
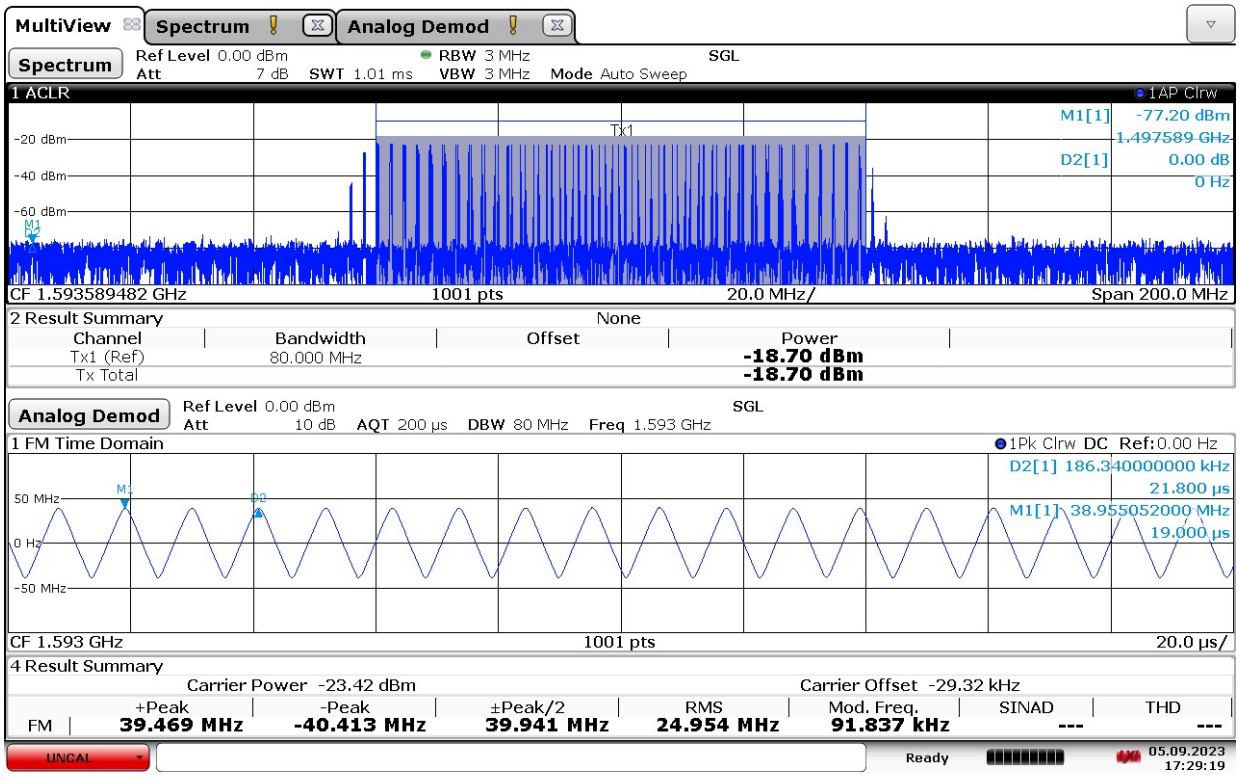


Figure 26.15: Example measurement of a H6.4 jammer (antenna 1).



17:16:04 05.09.2023

Figure 26.16: Example measurement of a H6.4 jammer (antenna 3).



17:29:20 05.09.2023

Figure 26.17: Example measurement of a H6.4 jammer (antenna 5).

26.9.15 Technical details on low-power jammer “H6.5”

Jammer H6.5 is assumed more or less identical to jammer H6.4 (originating from the same source).

26.9.16 Technical details on low-power jammer “H6.6”

Jammer H6.6 is assumed more or less identical to jammer H6.4 (originating from the same source).

26.9.17 Technical details on low-power jammer “F6.1”

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands	Relevant GNSS antenna #
1591	68	L1, E1, B1C, B1I, G1	2
1589	72	L1, E1, B1C, B1I, G1	3
1242	80	L2, G2, B3I, B2b, E6	4
1176	17	L5, E5a, B2a	6

- Estimated output power (conducted): ca. 35 dBm on channel/antenna 2, 38 dBm on channel/antenna 3, 27 dBm on channel/antenna 4, 30 dBm on channel/antenna 6
- Type of modulation: Sweep
    - Sweep rate: 5 - 7 µs

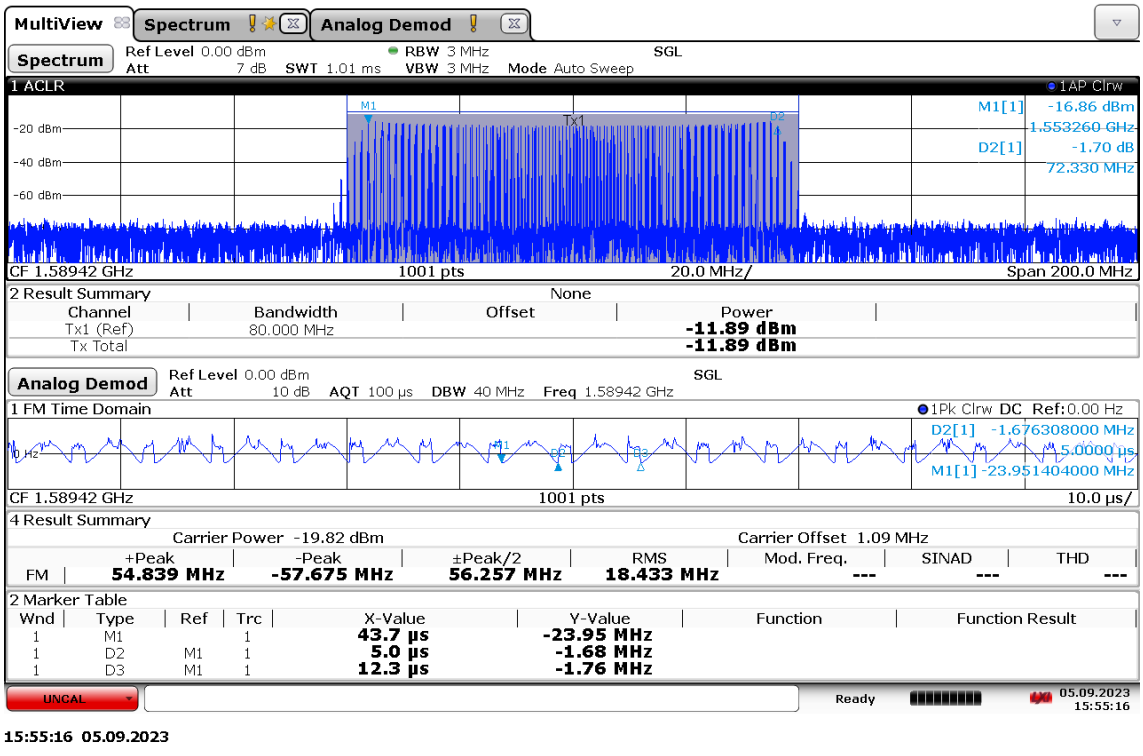
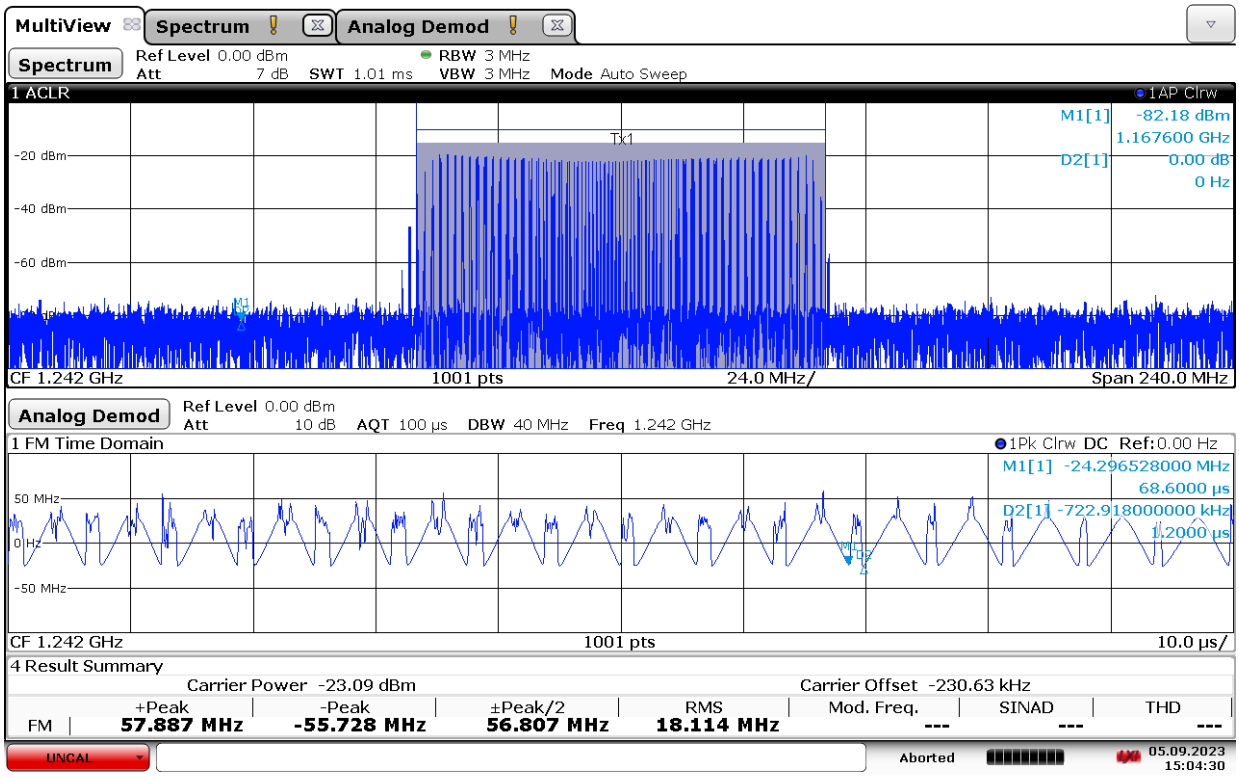
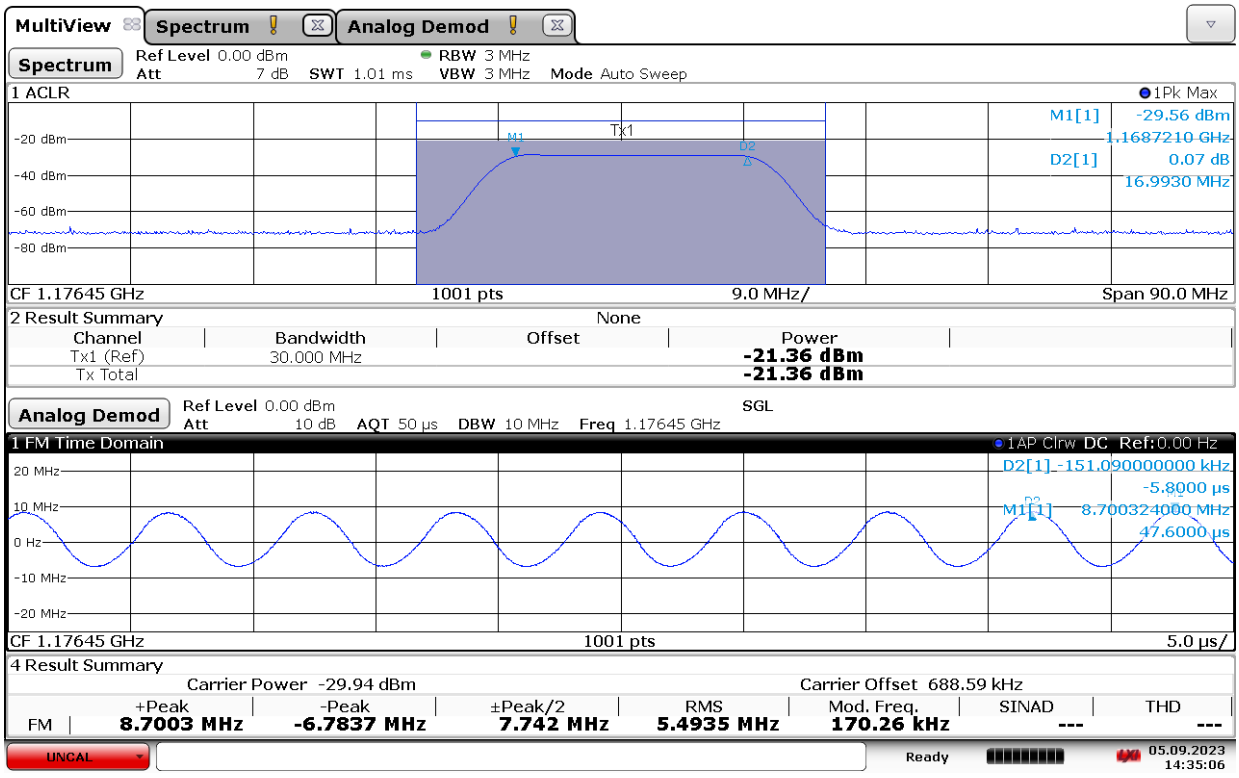


Figure 26.18: Example measurement of jammer F6.1 (antenna 3).



15:04:31 05.09.2023

Figure 26.19: Example measurement of jammer F6.1 (antenna 4).



14:35:06 05.09.2023

Figure 26.20: Example measurement of jammer F6.1 (antenna 6).

26.9.18 Technical details on low-power jammer H8.1

Handheld 8-band jammer where only one band (antenna 6) covers GNSS. The individual bands/antennas can be switched on and off.

Technical characteristics

Centre frequency (MHz)	Bandwidth (MHz)	Potentially afflicted GNSS bands	Relevant GNSS antenna #
1590	75	L1, E1, B1C, B1l, G1	6

- Estimated output power (conducted): 28 dBm
- Type of modulation: sweep (triangle)
    - Sweep rate: 10 µs

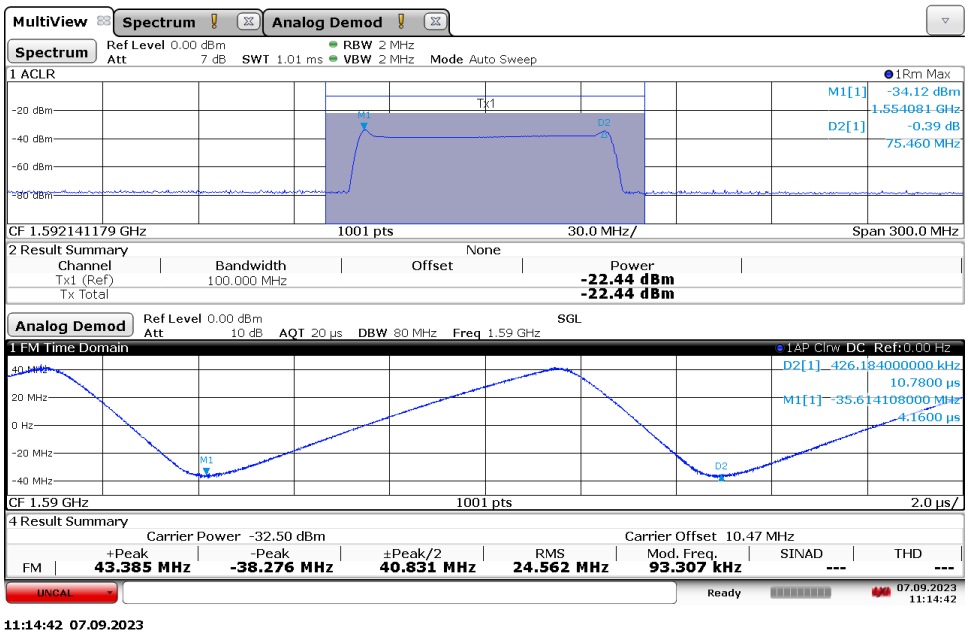


Figure 26.21: Example measurement of a jammer H8.1.

26.9.19 Technical details on the high-power jammer “Porcus Major” F8.1

The high-power jammer can provide jamming signals with up to 20 W EIRP simultaneously on eight GNSS bands. Figure 24.1 shows the block diagram of the high-power jammer. The jammer uses two USRP X410 SDR from Ettus Research as exciters. Each SDR have four output channels covering the frequency range of 1 MHz to 7.2 GHz, with maximum 400 MHz instantaneous bandwidth. The SDRs have an internal gain range of 60 dB in 1 dB steps. Each of the exciter output signals are fed to the corresponding channel of the programmable step-attenuator. The attenuator has an attenuation range of 95 dB in 0.25 dB steps. The output signal from the attenuators is then fed to the power amplifiers. The amplifiers connect to eight individual antennas via a 10 m coax. The antennas are directional helical antennas with right hand circular polarization (RHCP) and 10 dB gain.

An overview of the jammer signal modulations is given in Table 25.1.

Frequency band name	CW	PRN		Sweep/chirp		
	Frequency (MHz)	Center freq (MHz)	BPSK modulated chip rate (MHz)	Center freq (MHz)	Sweep rate (kHz)	Frequency band (MHz)
L1	1575.42	1575.42	10	1575.42	100	± 3
L2	1227.6	1227.6	10	1227.6	100	± 3
L5	1176.45	1176.45	10	1176.45	100	± 3
G1	1602	1602	5*	1602	100	± 3
G2	1246	1246	3	1246	100	± 3
E5b	1207.14	1207.14	10	1207.14	100	± 3
E6	1278.75	1278.75	10	1278.75	100	± 3
B1I	1561.098	1561.098	3	1561.098	100	± 3

*3MHz may be used in the pyramid jamming (test groups 9 and 10).

Table 25.1: Overview of the signal modulations employed by ‘Porcus Major’.

A PC running Linux controls the high-power jammer. It controls both exciters and the step-attenuators. The software on the PC allows the jammer to automatically execute the individual tests described for the high-power jammer and supports all jamming signals described therein.

The high-power jammer is connected to Internet and time synchronized using Network Time Protocol (NTP). After a jamming activity, it can upload the activity log to the central server.

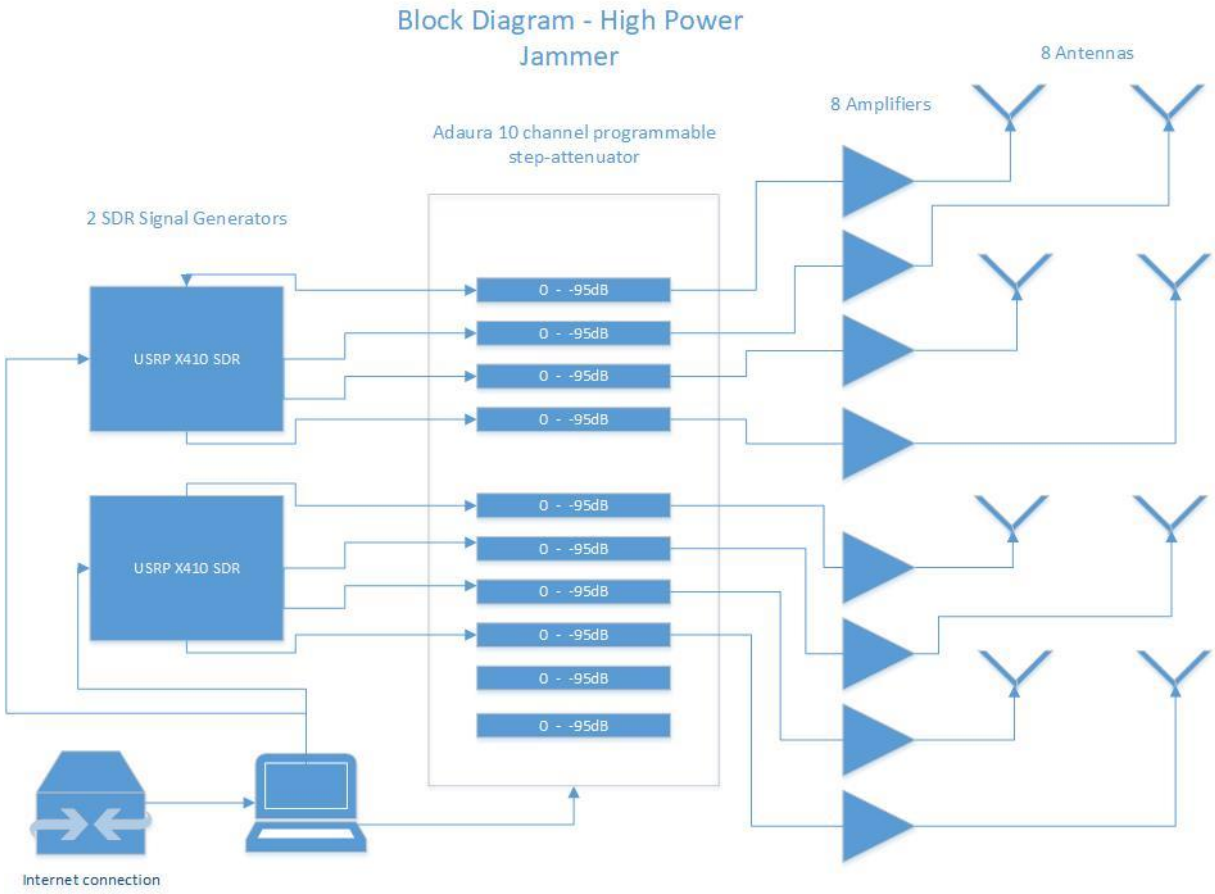


Figure 26.22: Diagram of the high power jammer.