

Jammertest - concept, plans and some results

Anders M. Solberg, Norwegian Mapping Authority (NMA).

Credits for content to the Jammertest partners (listed on the last slides).

EuroSDR online workshop "Beyond GNSS: Resilient Positioning and Aerial Mapping",
2 December 2025.



Outline

1. The Jammertest concept – background and philosophy
2. High-level technical information about Jammertest
 - Test areas
 - Attack vectors applied
 - Technical documentation
 - GNSS reference data
 - General findings from previous Jammertest events
3. Spoofing example from Jammertest 2025

Jammertest

«An open GNSS interference test arena to accelerate the development of resilient GNSS applications»



A black banner containing eight logos of partner organizations. From left to right: 1. Statens vegvesen logo with a crown and the text 'Statens vegvesen'. 2. Justervesenet logo with a vertical bar and the text 'Justervesenet'. 3. Norwegian Space Agency logo with a circular icon and the text 'Norwegian Space Agency'. 4. Kartverket logo with a square icon and the text 'Kartverket'. 5. Nasjonal kommunikasjonsmyndighet logo with the letters 'N', 'K', 'O', 'M' and the text 'Nasjonalt kommunikasjonsmyndighet'. 6. FFI Forsvarets forskningsinstitutt logo with the text 'FFI Forsvarets forskningsinstitutt' and 'Norwegian Defence Research Establishment' below it. 7. AVINOR logo with a stylized 'A' and the text 'AVINOR'. 8. TESTNOR logo with a triangle icon and the text 'TESTNOR'.

Background

- GNSS is a fantastic PNT enabler, but its radio signals are weak → Vulnerable to RFI
- PNT information is often an “invisible” resource, used in other systems → a lot of dependencies of GNSS in different sectors
- The needs for testing were expressed in discussions in a forum of Norwegian authorities through the years 2018-2020

→ Pilot test event in 2021



- Promising results and feedback from the pilot test event
→ Jammertest, September 2022: Full week of of operative GNSS interference testing at Andøya (4 organisers)



- Success and growing interest. Jammertest repeated in 2023, 2024 and 2025 with a rapidly growing number of participants, and eventually with some more organising institutions.



The philosophy of Jammertest

Jammertest is founded on the following “key values”:

- Facilitation
 - Offer a location where GNSS RFI signals can be transmitted in orderly forms without large disadvantages for society
- Transparency and openness
- Cooperation
- Resilience building over time
- An alternative to strict regulation



Photo: David Jensen

Facilitation

Regulation and enforcement of signal transmissions in GNSS frequency bands for anything else than space-to-earth radionavigation is (fortunately) extremely strict. In most countries, only very few exceptions are made, and then mainly for military exercises.

→ Lack of testing opportunities

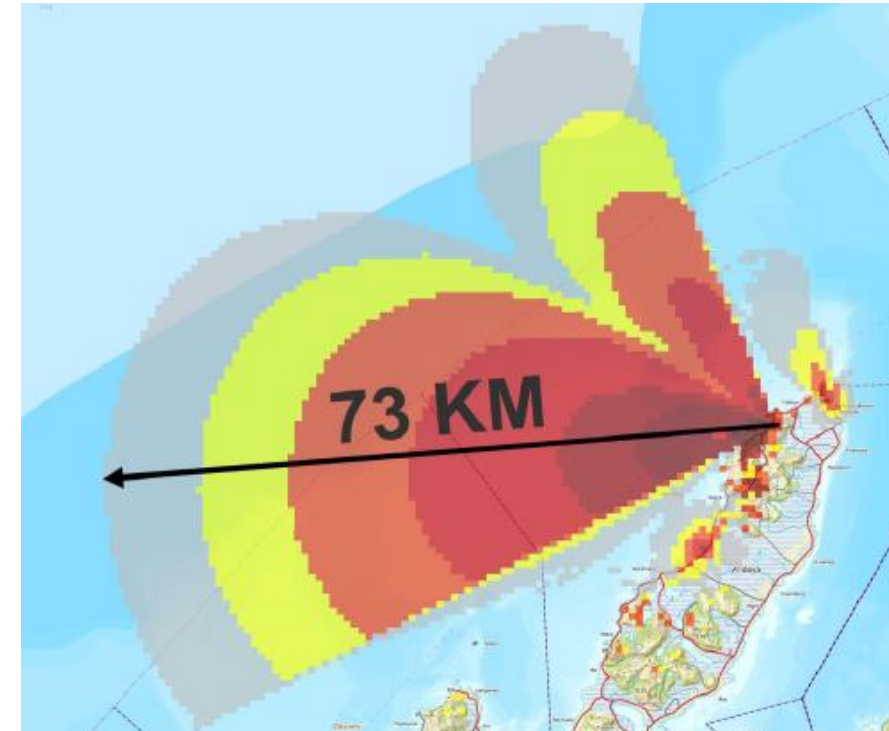
+

Growing need for testing. Lab testing is sometimes too clean/synthetic, and/or too physically restrictive (e.g. driving cars, flying helicopters).

=

Motivation for a test event.

Need for a location where GNSS RFI transmissions can be done with minimal disadvantages for society, while the location is still fairly accessible (travel, accommodation, HQ building, electrical power, internet, mobile phone coverage).



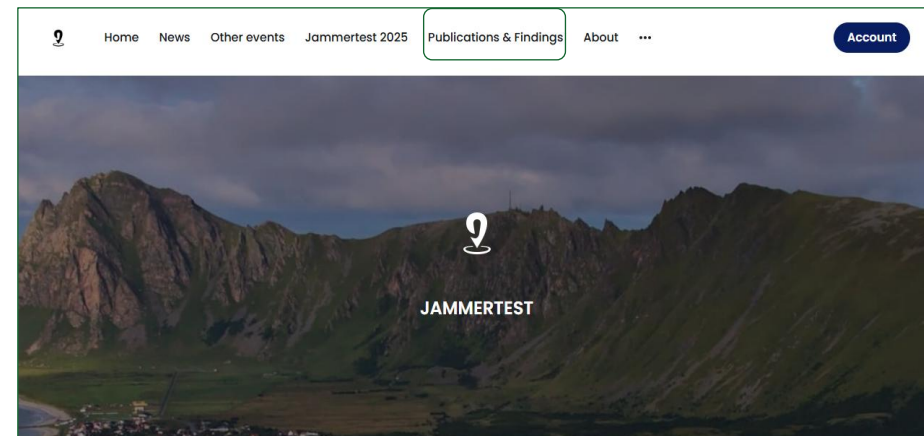
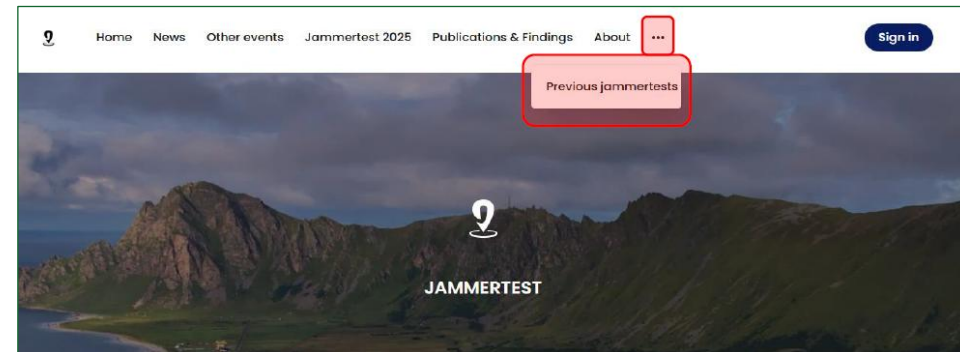
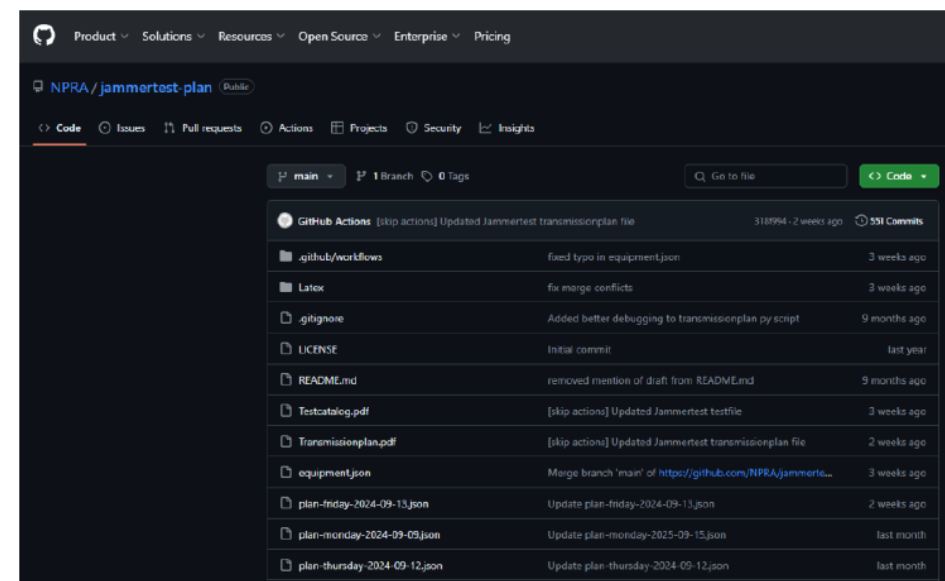
Why Andøya?

- Mountains to the east of the village of Bleik → mainland Norway shielded
- > 900 km to nearest neighbour to the west across the ocean (Jan Mayen)
- Tourist destination in summertime (accommodation available in September)
- Airport available
- Local inhabitants are used to military and restrictive activities (e.g. rocket launches)



Transparency and openness

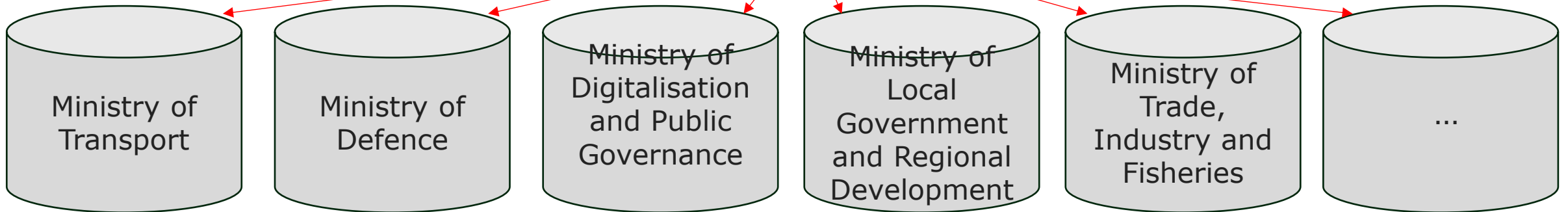
- All test-related information (technical and practical) is first shared with participants, then archived on the official website <https://jammertest.no>
- The development of the Test Catalogue (TC) and Transmission Plan (TP) is public, with documents available in both JSON and PDF formats on the Jammertest GitHub.
- The planning process is open to contributions, and after each Jammertest, technical details like the TP, TC, and logs are published.
- Participants are free to use their own recorded data without restrictions. While sharing is encouraged to support the broader community, only acknowledgements in publications are requested.
- A library of public results is also maintained on the official website.



Cooperation

Governance of many countries is sector based.

Vulnerabilities of PNT systems can affect several sectors, but who should take action to mitigate the risks?



- Jammertest raises cross-sectorial awareness of RFI threats against PNT systems.
- Organic development of roles and responsibilities, aligned with each organiser's strengths and expertise
- Participants' contributions are also important (requests/ideas for new/modified tests, ...).

Resilience building over time

- Being an annual event where several tests are repeated year after year, Jammertest provides the opportunity to test and validate improvements to equipment, systems and algorithms against the same RFI environment, so that the value of these improvements can be assessed.

An alternative to strict regulation (of receivers)

- Strict regulation of receiver equipment → Difficult for legislation to keep up with the technical innovation speed.
- Some overall goals of Jammertest:
 - There should be no place in the market for devices and services that are not resilient to GNSS RFI.
 - It should be a main selling point that your product has survived Jammertest.

Outline

1. The Jammertest concept – background and philosophy
2. High-level technical information about Jammertest
 - Test areas
 - Attack vectors applied
 - Technical documentation
 - GNSS reference data
 - General findings from previous Jammertest events
3. Spoofing example from Jammertest 2025

Test areas

- Area 1:
 - High power jamming
 - Meaconing
 - Advanced spoofing (stationary transmitter)
- Area 2:
 - Low-power jammer devices
 - Spoofing (stationary transmitter) with circle of jammers
 - Jamming from drone
- Area 3:
 - Motorcade area: Low power jammers, mobile spoofing
- Area 4:
 - Local airport: Tests for airplanes, helicopters, fixed-wing drones that want to fly instrument approach procedures. Only on one of the days.



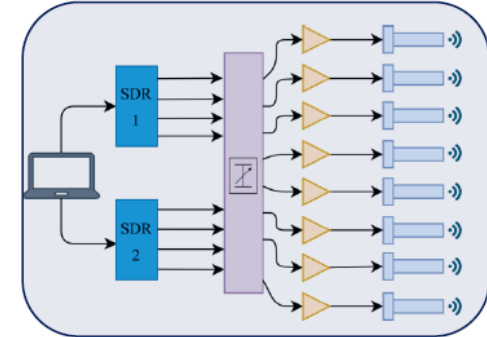
Attack vectors at Jammertest

GNSS RFI transmissions

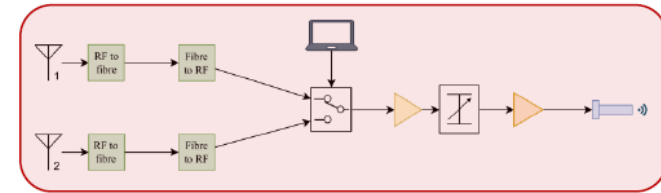
Transmission group
Stationary high-power jamming
Stationary low-power jamming
Mobile low-power jamming
Stationary spoofing
Stationary meaconing
Mobile spoofing

Generated with:

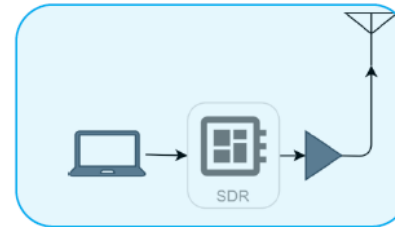
- Porcus Major – The big jammer



- Porcellum – The meaconing system



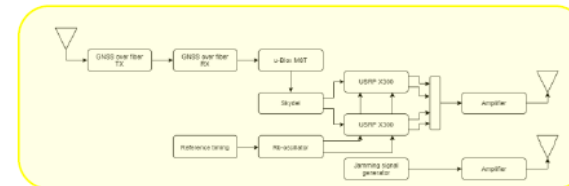
- Mobile SDR Spoofer



- “Low-power” jammers



- Stationary Spoofer



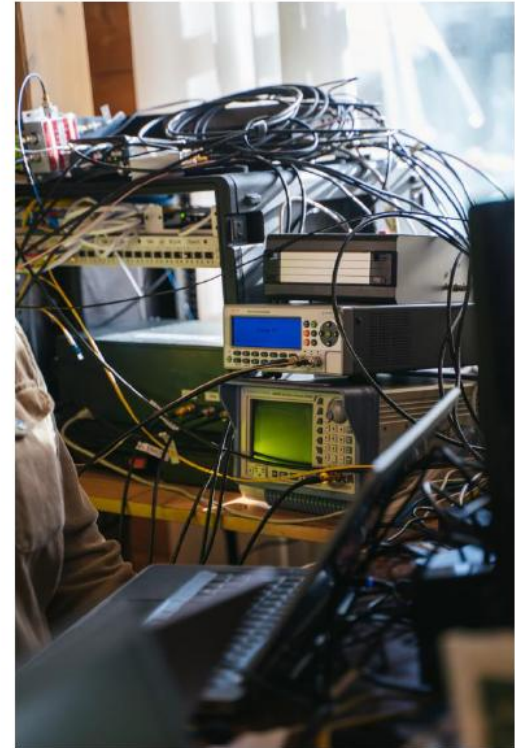
Attack vectors at Jammertest

GNSS RFI transmissions

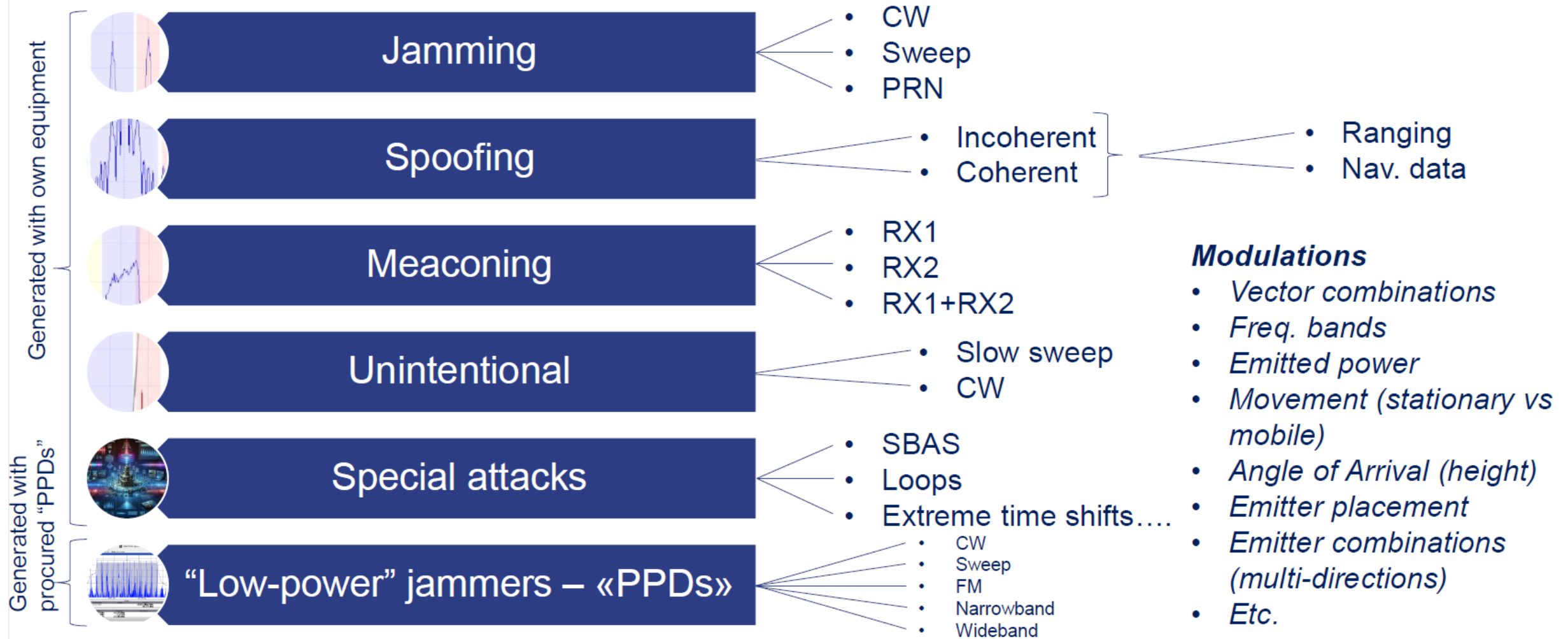
Transmission group
<i>Stationary high-power jamming</i>
<i>Stationary low-power jamming</i>
<i>Mobile low-power jamming</i>
<i>Stationary spoofing</i>
<i>Stationary meaconing</i>
<i>Mobile spoofing</i>



Photo: David Jensen



The Attack Vectors



Jammertest: Test catalogue, transmission plan and test log

Test catalogue of GNSS interference scenarios

2.4: Incoherent time spoofing from stationary spoofer using synthetic ephemerides	92
2.4.1 Time offset 15 minutes from real time. GPS L1 and Galileo E1 only, with power ramp	93
2.4.2 Time offset 15 minutes from real time, with power ramp	93
2.4.3 Time offset -3 minutes from real time, with power jump	94
2.4.4 Static + Frequency step. GPS L1 only	94
2.4.5 Static + Frequency step. GPS L1 and Galileo E1 only	94
2.4.6 Static + Frequency step. GPS L1 and Galileo E1 only, with initial and continuous jamming	95
2.4.7 Static + Frequency step	95
2.4.8 Static + Frequency step, with initial and continous jamming	96
2.4.9 Static + Pseudorange error. GPS L1 only	96
2.4.10 Static + Pseudorange error. GPS L1 and Galileo E1 only	96
2.4.11 Static + Pseudorange error. GPS L1 and Galileo E1 only, with initial and continuous jamming	97
2.4.12 Static + Pseudorange error	97
2.4.13 Static + Pseudorange error, with initial and continous jamming	98

A subset of catalogued tests are actually transmitted



Transmission plan 2024

09:00	<p>09:00-09:25 - 2.4.2 Time offset 15 minutes from real time, with power ramp Power: 0.0316W Contact: Nicolai Gerrard (NKOM)</p> <hr/> <p>09:40-09:55 - 2.4.3 Time offset -3 minutes from real time, with power jump Power: 0.0316W Contact: Nicolai Gerrard (NKOM)</p>
10:00	<p>10:10-10:25 - 2.4.12 Static + Pseudorange error Power: 0.0316W Contact: Nicolai Gerrard (NKOM)</p> <hr/> <p>10:40-10:55 - 2.4.13 Static + Pseudorange error, with initial and continous jamming Power: 0.001W Contact: Nicolai Gerrard (NKOM)</p>

Test documents are machine readable (.json + .xls) to help automated data collection and analysis

2.4.13	Static + Pseudorange error, with initial and continous jamming	2024-09-12	10:50:08	10:50:21	Initial jamming (E6, L2, E5b, L5)
2.4.13	Static + Pseudorange error, with initial and continous jamming	2024-09-12	10:50:21	10:55:19	Jamming of L1, G1, B1I activated
2.4.13	Static + Pseudorange error, with initial and continous jamming	2024-09-12	10:55:19	10:55:23	Spoofing activated. Spoofing power different than TP
2.4.13	Static + Pseudorange error, with initial and continous jamming	2024-09-12	10:55:23	10:55:24	Jamming of E5b deactivated
2.4.13	Static + Pseudorange error, with initial and continous jamming	2024-09-12	10:55:24	10:55:25	Jamming of L5 deactivated
2.4.13	Static + Pseudorange error, with initial and continous jamming	2024-09-12	10:55:25	10:55:26	Jamming of L2 deactivated
2.4.13	Static + Pseudorange error, with initial and continous jamming	2024-09-12	10:55:26	11:05:21	Jamming of L1 deactivated. Time error of 9 ns/s. A total accumulated time error of 6 µs



Log of actual transmissions

New features at Jammertest 2025



- More high-power tests that include jamming of the E6 frequency band
- High power jamming from two different locations (and therefore different elevation and azimuth angles) at the same time
- Spoofing tests in Test Area 2
- Jamming tests designed for drones in Test Area 2
- Tests with drone with jammer onboard in Test Area 2 (Technical University of Denmark (DTU) conducted a related special test at Jammertest 2024)

GNSS reference data

NMA (Kartverket) provides GNSS reference data based on geodetic grade receivers (mostly outside the affected areas) free of charge for participants during the Jammertest week.

2 options for RTCM formatted real-time data:

- CPOS (NRTK service). Requires NMEA input from user equipment.
- RTCM data streams from individual GNSS reference stations nearby the test areas (distances \sim 10-60 km)

Stored data for post-processing:

- RINEX (v3.05) files from individual GNSS reference stations nearby the test areas (distances \sim 10-60 km)
 - 1 Hz data rate
 - Choose between 1hour and 24hour files



Important findings from Jammertest 2022-2024

- Many defense mechanisms are based on insufficient assumptions
 - E.g. a too “binary” handling of interference → Transition phases (from undisturbed to disturbed or vice versa) can cause problems
- Source dependencies in sensor fusion (GNSS weighted too heavily) → problems, even though non-GNSS sensors are also used
- Some attack vectors are fairly simple, but have been totally overlooked by industry
- GNSS RFI can have effects looking like cyber attacks (licences can be outdated etc.)
- Lots of learning when problem owners and problem solvers are gathered
- The systems need to be tested! Assumptions and manufacturers’ statements regarding their products can sometimes be defective.

*Text taken from “Trusselens omfang” (eng.: “The extent of the threat”). Nicolai Gerrard, NKOM.
Presented at FFI breakfast meeting, Oslo, 18 March 2025*

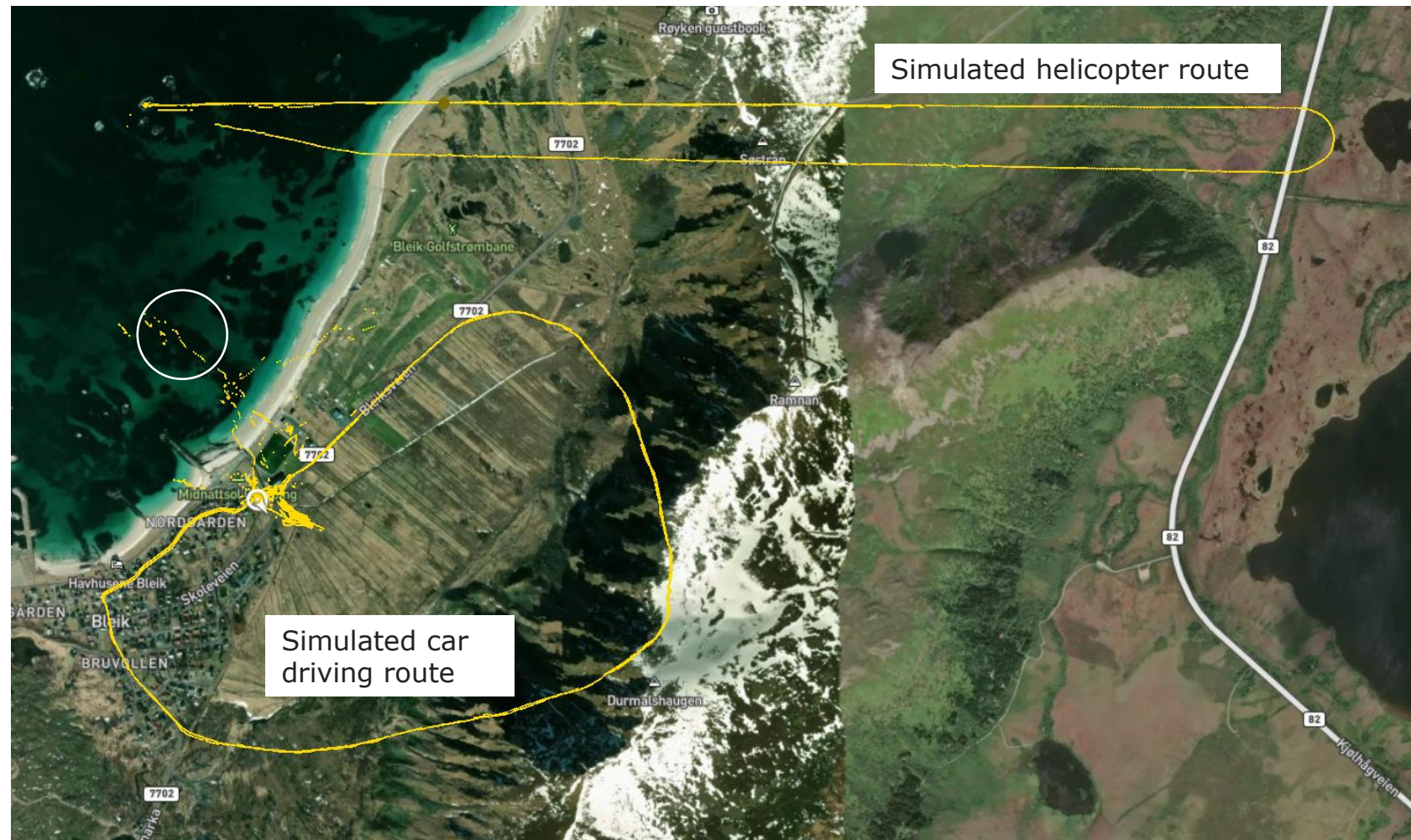
Outline

1. The Jammertest concept – background and philosophy
2. High-level technical information about Jammertest
 - Test areas
 - Attack vectors applied
 - Technical documentation
 - GNSS reference data
 - General findings from previous Jammertest events
3. Spoofing example from Jammertest 2025

Spoofing example (page 1/3)

High-end (but a bit outdated) GNSS receiver at rest at ground spoofed → producing positions in simulated routes.

Very large position errors also caused by jamming (ref. white circle).



Spoofing example (page 2/3)

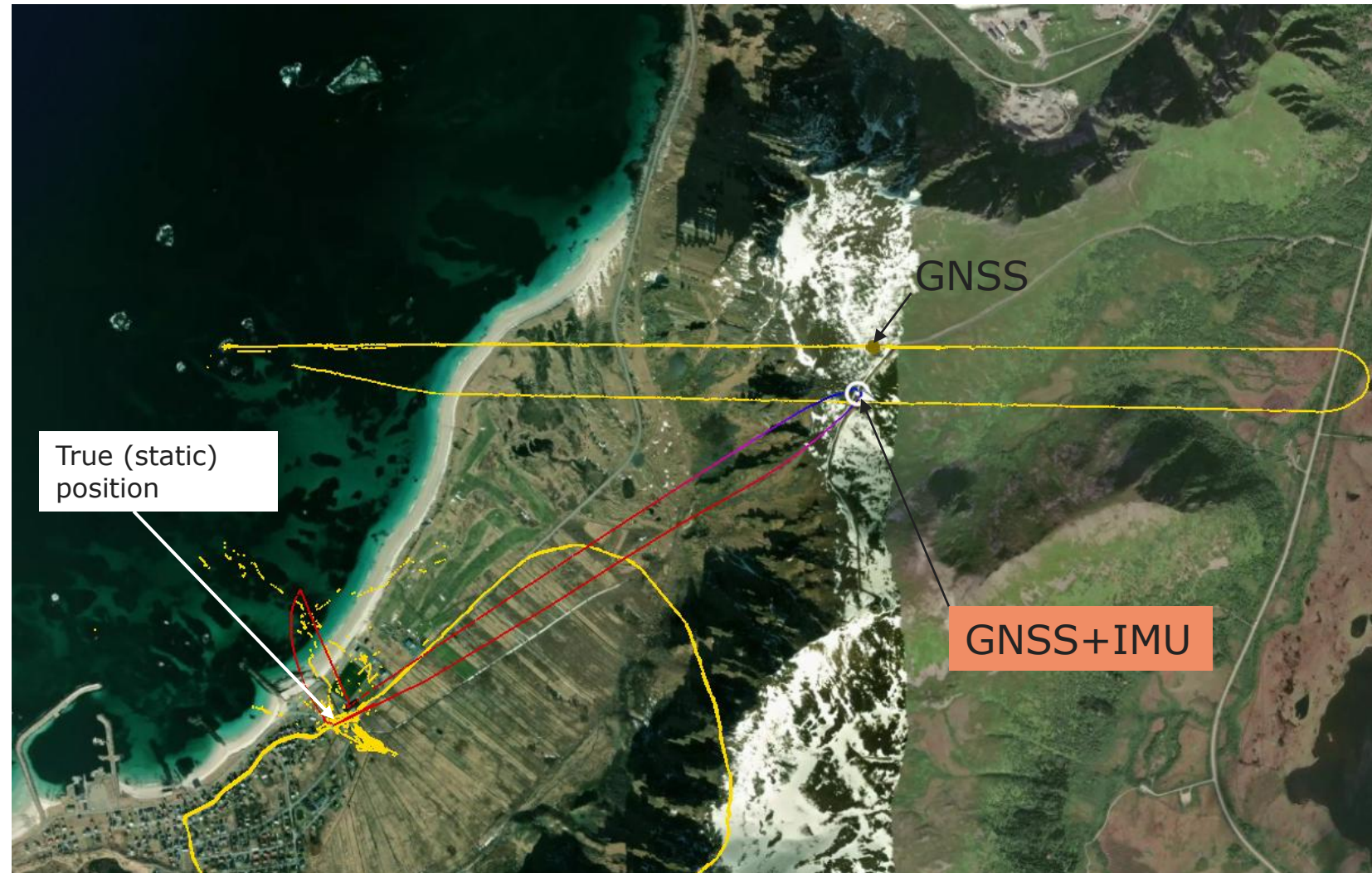
Real-time GNSS+IMU solution (solid curve in figure) keeps position within a few meters of true position



Spoofing example (page 3/3) (unrealistic processing choice)

High-end GNSS receiver at rest at ground spoofed → producing positions in a simulated helicopter route.

GNSS+IMU simple post-processed solution (loosely coupled forward/backward solution with automotive profile) produces a very strange trajectory. It starts close to the true position, but seems influenced by the GNSS simulated helicopter trajectory. Quality is marked as bad, though (blue/red colour (good quality is marked with green colour)). Obviously not a good processing option for an IMU at rest, but the result is a bit interesting.



Credits (1)

A large part of this presentation is extracted from the article

“Jammertest: An open GNSS interference test arena to accelerate the development of resilient GNSS applications”. Nicolai Gerrard¹, Tor Atle Solend², Anders Rødningsby², Øystein Karlsen¹, Tomas Levin³, Harald Hauglin⁴, Kristian Svartveit⁵, Christian Berg Skjetne³, Anders Martin Solberg⁶, Thomas Rødningen⁴ and Øystein Borlaug². Proceeding paper from ENC 2025, Wroclaw, Poland.

1. Norwegian Communications Authority (NKOM – Nasjonal kommunikasjonsmyndighet)
2. Norwegian Defence Research Establishment (FFI – Forsvarets forskningsinstitutt)
3. Norwegian Public Roads Administration (Statens vegvesen)
4. Norwegian Metrology Service (Justervesenet)
5. Norwegian Space Agency (Norsk Romsenter)
6. Norwegian Mapping Authority (Kartverket)

Credits (2)

PowerPoint presentation "Jammertest".

Presented by Nicolai Gerrard (NKOM) at ENC 2025, Wroclaw, Poland, May 2025.

Credits (3)

Trusselens omfang (eng.: "The extent of the threat").

Nicolai Gerrard, NKOM.

Presented at FFI breakfast meeting, Oslo, Norway, 18 March 2025

Credits (4)

General credits:

Norwegian Public Roads Administration (Statens vegvesen)

Norwegian Communications Authority (NKOM - Nasjonal kommunikasjonsmyndighet)

Norwegian Defence Research Establishment (FFI – Forsvarets forskningsinstitutt)

Norwegian Metrology Service (Justervesenet)

Norwegian Space Agency (Norsk Romsenter)

Avinor AS

Testnor AS



Questions?

Contact information

→ Anders M. Solberg

→ anders.martin.solberg@kartverket.no

<https://jammertest.no>



Kartverket