GNSS Vulnerabilities

Common-Sense Solutions

NASPI Work Group Meeting

Charlotte, NC

27 September 2023

Allan Armstrong

Allan.Armstrong@meinberg-usa.com

MEINBERG

The Synchronization Experts.

Agenda

GNSS Vulnerabilities: Jamming & Spoofing
Mitigation Tools

Jamming: Civilian vs. Military Jamming
Strike3 project
Holdover Oscillators
Redundant Receivers & Remote Antennas
Terrestrial Time Transport

Spoofing – How They Do It
Raising the Bar
GNSS Consistency Checks
Trusted Reference Source
Navigation Message Authentication

LAB & Field Testing
Summary & Recommendations

GNSS Vulnerabilities

Jamming

- Quite common problem, easy to solve
- Usually an unintentional “drive-by”
- Military jamming rare

Spoofing

- Rare problem
- Very serious if it happens
- Good mitigation tools available

Mitigation Tools

- Holdover Oscillators
- Redundant Receivers & Remote Antennas
- Terrestrial Time Transport – PTP & DTM
- Multi-Constellation & Multi-Band Receivers
- GNSS Consistency Checks
- Trusted Reference Source
- Navigation Message Authentication

How are these used? What are they used for? What is most effective?

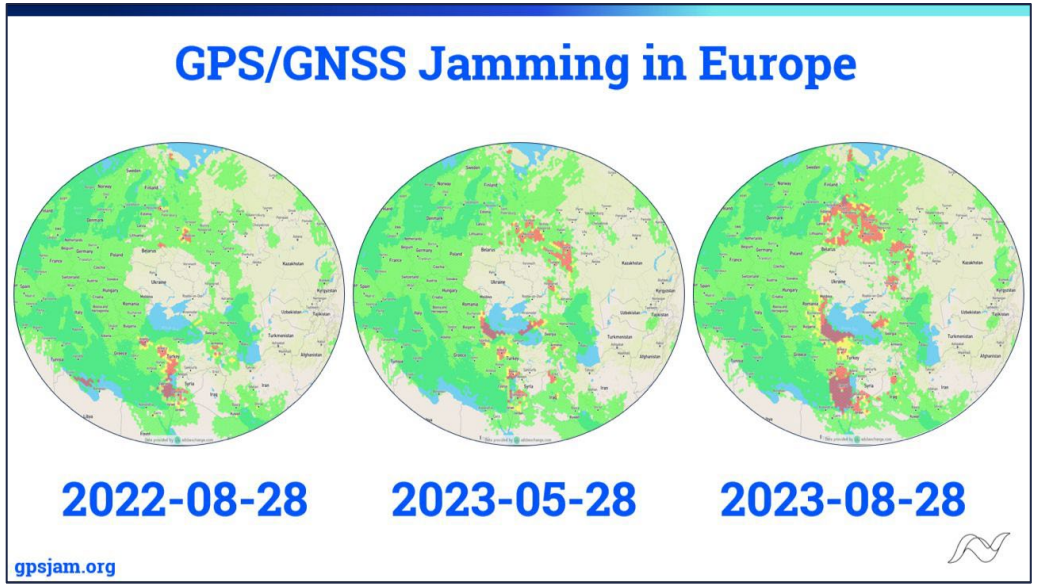
GPS Jamming

Civilian “Accidental” Jamming

- Drivers trying to hide their location
  - From their employer – drivers
  - From authorities – professional car thieves
- Short-term
- Holdover oscillators a good (great) solution

Military Jamming

- Affected areas include Scandinavia, Baltic States, Balkans, Ukraine, Middle-East
- Rapidly increasing to counter drone usage
- Persistent
- Terrestrial time transport generally needed



How Serious is GNSS Jamming?

STRIKE3 Project

- 3-year EU-H2020 project co-funded by European GNSS Agency (GSA)
- Monitoring stations in 23 countries around the globe
- > 450,000 interference events
  - 73,000 major impact on GNSS
  - 59,000 from jamming devices
- Extensive reports available here: https://aric-aachen.de/strike3/S3-work/

Duration of Jamming Events

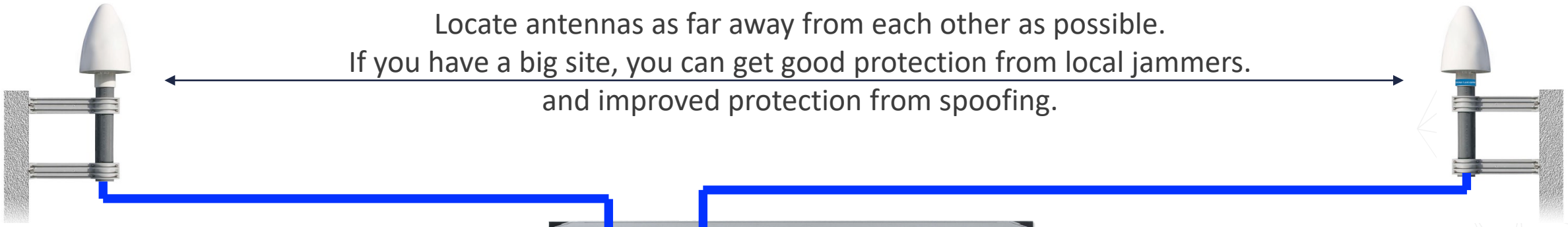
- Vast majority short duration

Fraction of events	Duration
0.015	> 5 minutes
0.0022	> 30 minutes
0.0012	> 60 minutes
$1.0x10^{-5}$	> 1 day

Holdover Oscillator Performance

Holdover Accuracy		OCXO SQ	OCXO MQ	OCXO HQ	OCXO DHQ	Rubidium
Frequency	1 day	$5x10^{-9}$	$1.5x10^{-9}$	$5x10^{-10}$	$1x10^{-10}$	$2x10^{-11}$
	1 year	$2x10^{-7}$	$1x10^{-7}$	$5x10^{-8}$	$1x10^{-8}$	$5x10^{-10}$
Time	1 day	± 220 µs	± 65 µs	± 22 µs	± 4.5 µs	± 0.8 µs
	1 week	± 9.2 ms	± 2.9 ms	± 1.0 ms	± 204 µs	± 34 µs
	1 month	± 120 ms	± 44 ms	± 16 ms	± 3.3 ms	± 370 µs
	1 year	± 4.7 s	± 1.6 s	± 788 ms	± 158 ms	± 8 ms

Redundant Receivers & Remote Antennas



Locate antennas as far away from each other as possible.
If you have a big site, you can get good protection from local jammers.
and improved protection from spoofing.

Down-converted (35.4 MHz IF) Receiver

- 300 m RG-58
- 700 m RG-213
- 2 km MMF
- 20 km SMF

Standard L1 (1.5 GHz) Receiver

- 70 m H155
- 150 m H2010
- 50 km SMF

Does the jammer know the location of both antennas?
Can a spoofer hit the “power window” of both antennas?

Terrestrial Time Transport

External time sources

- NIST, National Labs, Stock Exchanges (NYSE), TaaS providers (Equinix, Hoptroff, …)

G.8275.1 ±1.5 µs

- Requires Full Timing Support,
  all switches in path must be PTP-aware (BC or TC),
  unlikely in existing networks

G.8275.2 ±1.5 µs

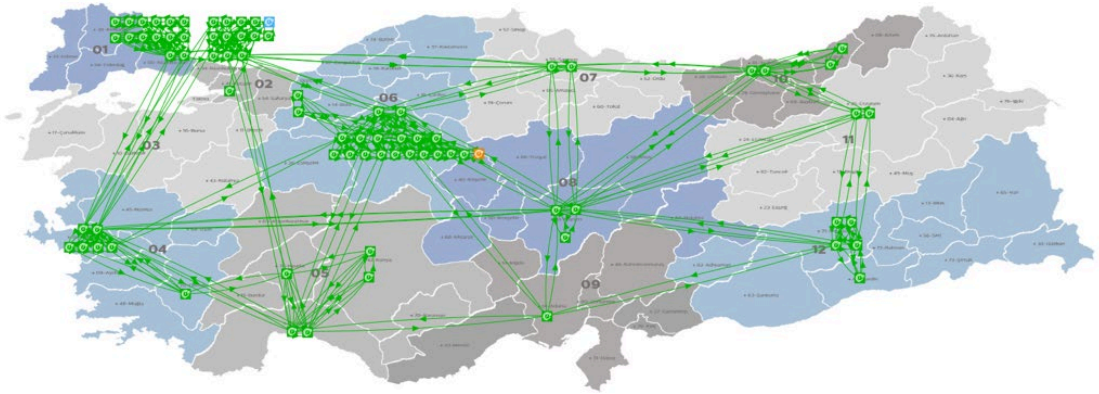
- Requires Partial Timing Support,
  performance depends topology & traffic conditions,
  dependent on GNSS so not a backup for jamming

Dark fiber, dedicated λ

- Expensive, latency is a function of λ

PTN

- PTN = Precision Time Network
  first implemented by NetInsight Nimbra
  ITU-T SG15.Q13 contrib WD13-15
- Turk Telekom has achieved ≤ 138 ns MTIE over an existing MPLS PTN from Adana-Istanbul ~1200 km with no on-path timing support



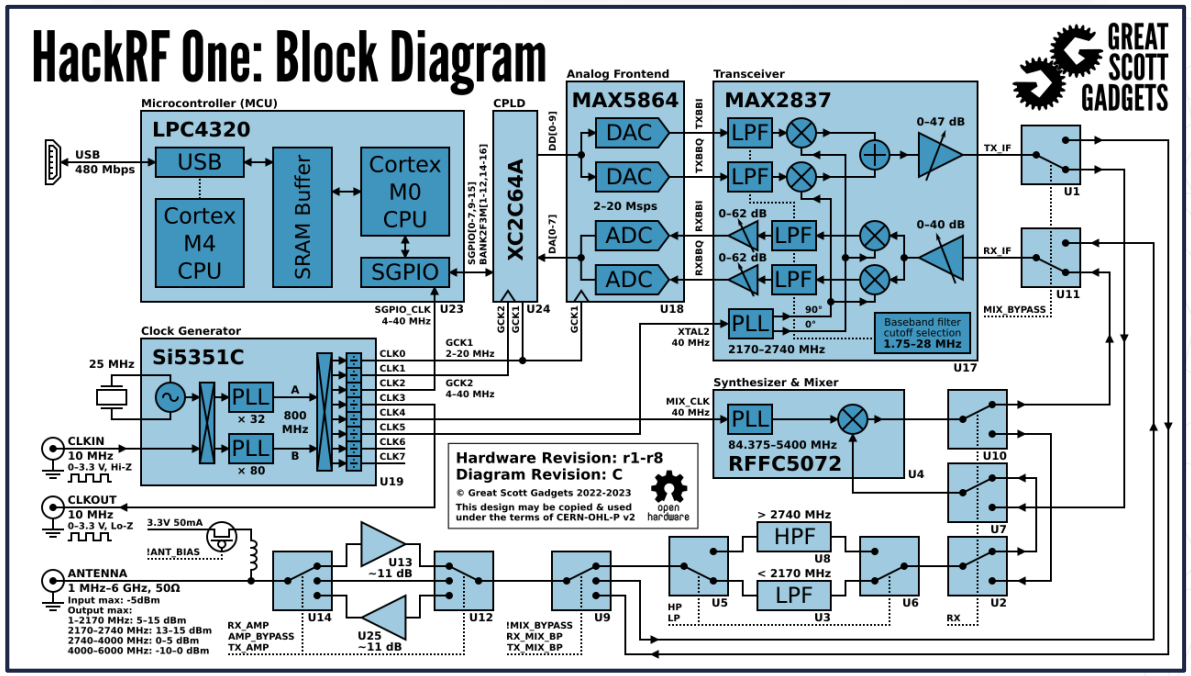
Spoofing – How They Do It

STEP 1 – build the hardware

- Sophisticated software defined radios (SDR) available on-line for affordable prices -- $320 for this example
- Capable hardware
  - 256 & 1024 QAM
  - Covers GNSS frequency ranges
- Free open-source GPS-spoofing software available on github

STEP 2 – target your infrastructure

- Find out where your antennas are
- Get close to you to avoid general detection



Raising the Bar on Spoofers

TABLE STAKES

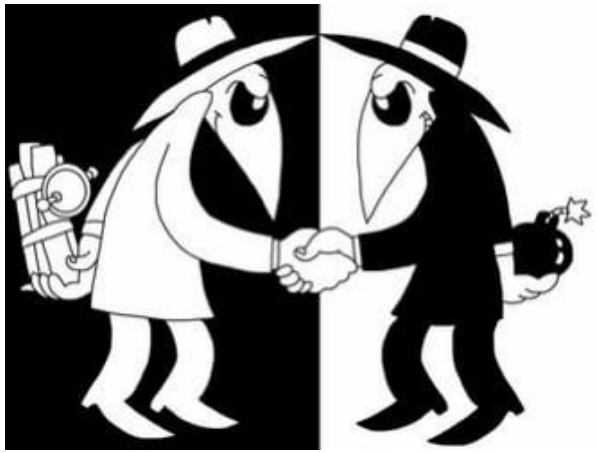
- They must build one spoofing transmitter for each satellite you are tracking
- How many are you tracking? How do they know? Typically ~8 satellites in view
- So, they need 8-10 SDRs

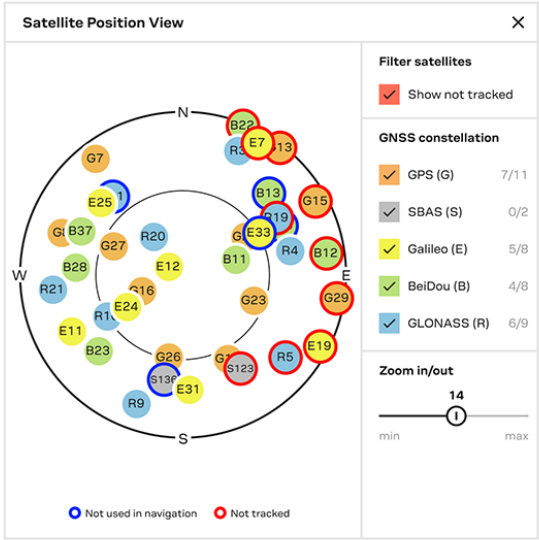
MULTI-CONSTELLATION RECEIVER

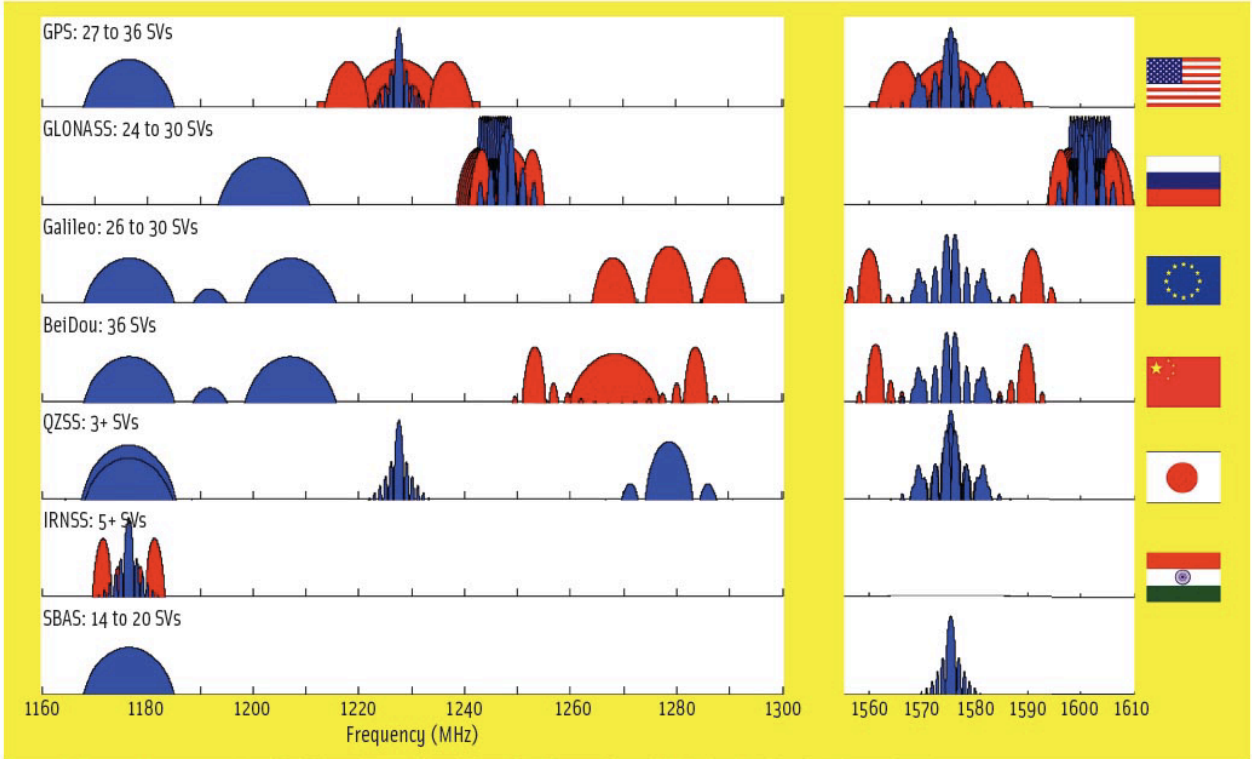
- If you track all four constellations – GPS, Galileo, GLONASS, Beidou – they must simulate 4x more
- Now, they need 32-40 SDRs

MULTI-BAND RECEIVER

- Each constellation broadcasts in 3 different bands
- If you monitor all 3, and check for consistency, …
- Now, they need 96-120 SDRs







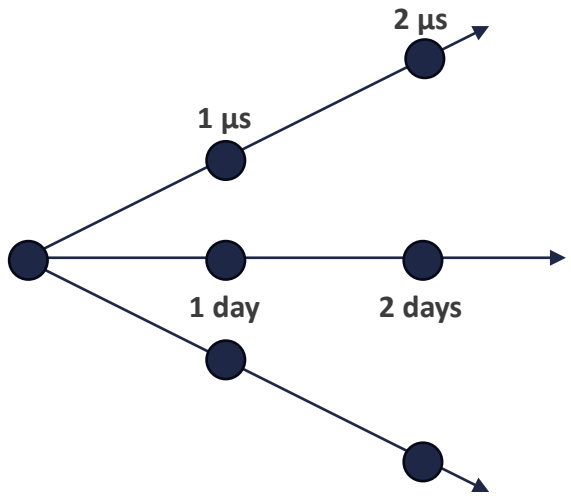
How Do We Ensure GNSS Inputs are Legit?

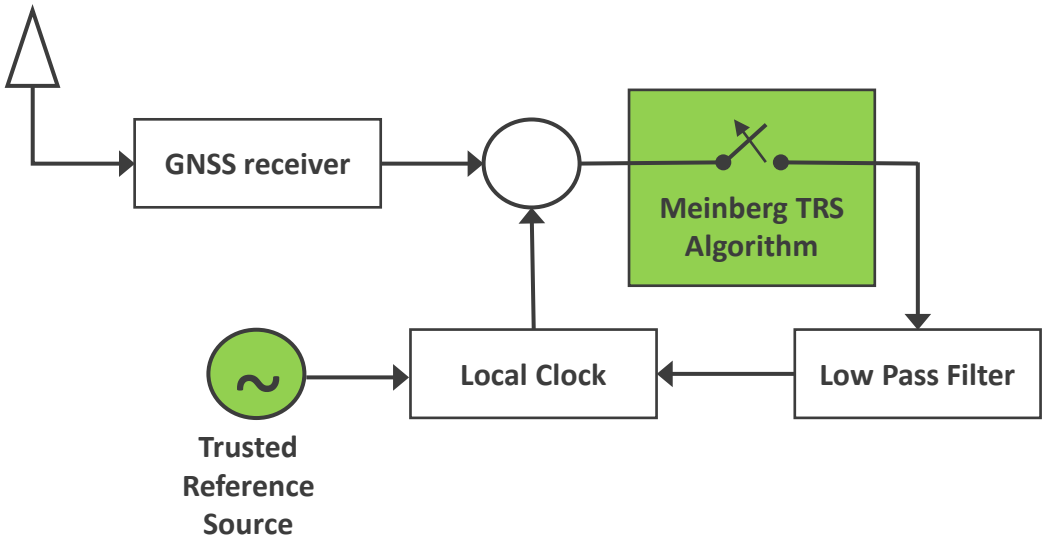
Consistency Checks

1. **Power**
   - Spoofer must overpower existing GNSS signal
   - Set a maximum received power, must be measured after demodulation, not RF front end
   - How does the spoofer know he is using enough power? Can the spoofer observe the receiver?
   - Can work really well as a consistency check
2. **Modulation**
   - Sounds good and sophisticated, but GNSS signals are well documented and SDRs are very capable
3. **# Satellites**
   - Interesting information, worth alarming or notifying of changes
   - Not a direct indication of spoofing
4. **Position**
   - May change as time is hacked, you probably know where your receiver is and it’s probably not moving
   - Well worth it
5. **Time** – a simple and very powerful check

Trusted Reference Source

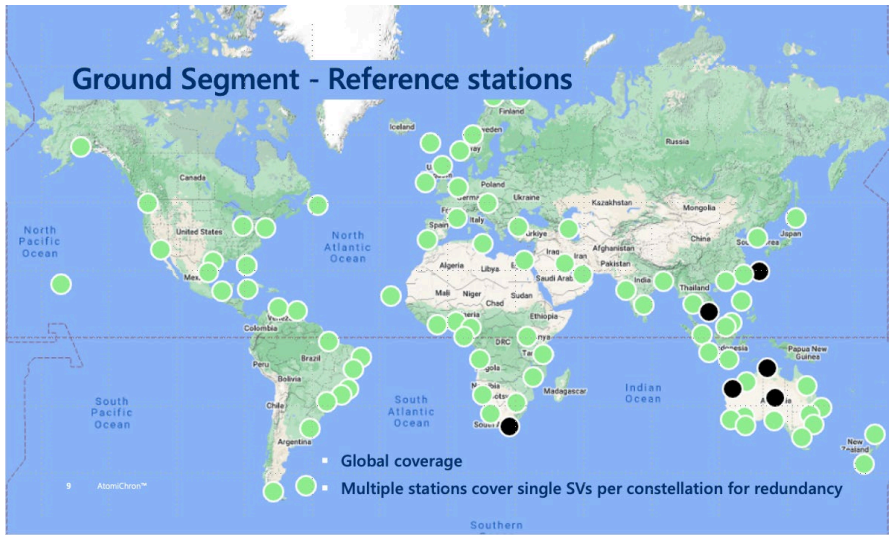
- Time is not supposed to drift
- if you know your reference well,
  you know how much it can drift
- If the signal drifts more than the reference,
  you know you are getting spoofed
- If your reference is good, e.g. quite stable,
  any spoofing that ”fits the envelope” isn’t useful





Navigation Message Authentication

4 GNSS Constellations



Fugro AtomiChron™
90 Ground Reference Stations
orbital and clock corrections
security hash

GNSS NMA Hash
asymmetric cryptography

2 NCCs Network Control Centers

14 Inmarsat Satellites

L-BAND RX

GNSS RX

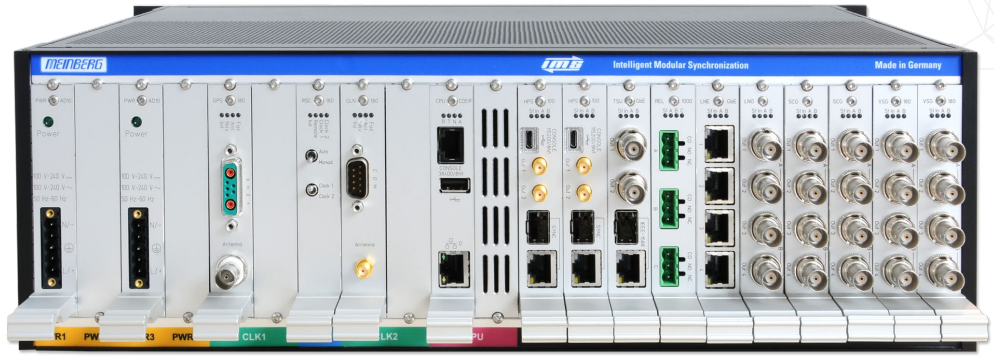
Fugro AtomiChron™ Timescale

Septentrio mosaic-T GNSS RX chipset

Meinberg GXL Receiver

Jamming & Spoofing Testing in the Lab

GNSS Simulator



GNSS Timing Receiver

Jamming & Spoofing in the Field: Norwegian Anti-Jamming Project

Location: Andøya, Norway
(near Andenes)

Dates: 18-22 September 2023

Low population density,
favorable geography (no neighbors)

3 Test Locations

1. Main, high-effect jammer & sophisticated spoofing attacks
2. Small, low-effect jammers, “sand box”
3. Small, low-effect jammers in and on cars

Summary & Recommendations

Problem	Baseline Solution	Enhanced Solution
Jamming	• Holdover Oscillator • Terrestrial Time Transport	• Redundant Receiver & Remote Antenna
Spoofing	• Multi-Constellation & Multi-Band Receiver • Resilient Receiver	• Redundant Receiver & Remote Antenna • Trusted Reference Source • Navigation Message Authentication

Thank You!

MEINBERG

The Synchronization Experts.