NORWEGIAN FORUM FOR OFFSHORE SURVEY AND POSITIONING

GNSS Cyber Security

Risks and Mitigations for GNSS Systems

NOSP Evening Event, Bergen, 16. October 2025 – John Vint (Product Manager Starfix)

GNSS Cyber Security

Terminology

Intrusion

Jamming

Spoofing

GNSS Cyber Security

Security Risks

Intrusion and/or Hacking	Complicated IT Systems – IT Departments look after this.
Unintentional Interference	Any RF source transmitting into the GNSS frequency bands.
Intentional Interference (Jamming)	Disruption of GNSS signals by transmitting strong radio signals in the frequency bands used by GNSS satellites
Spoofing (Tampering)	Transmitting counterfeit GNSS signals to a GNSS receiver causing it to calculate a false position, time or velocity.
Meaconing (Duplication)	Intercepting, amplifying and transmitting a GNSS receiver's signals, creating a false position for other receivers.

Unintentional Interference

Jamming

- Well known issue.
- Often local to vessel or region.
- Most common support case throughout the years.
- At times difficult and time consuming to resolve.
- No “system” to mitigate this.

Intentional Interference

Jamming

- GNSS Signals are weak -130 to -160 dBm at the receiver.
- 1W jammers can affect a few km square area.
- Military jammers can cause interference in a much larger areas.
- Intentional transmission of strong radio signals “noise” in the frequency bands used by GNSS systems.
- The transmitted “noise” disrupts the receiver's reception that blocks the receiver from acquiring and tracking the GNSS satellite signals.

Signal Spoofing

Spoofing

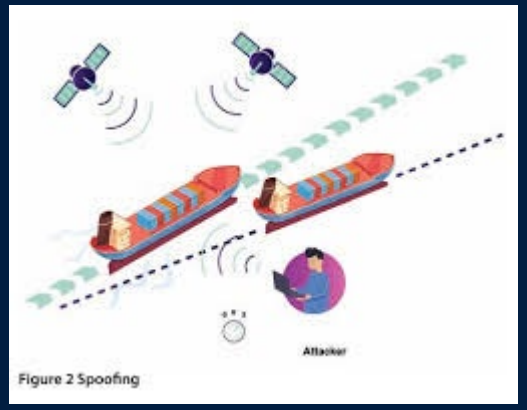
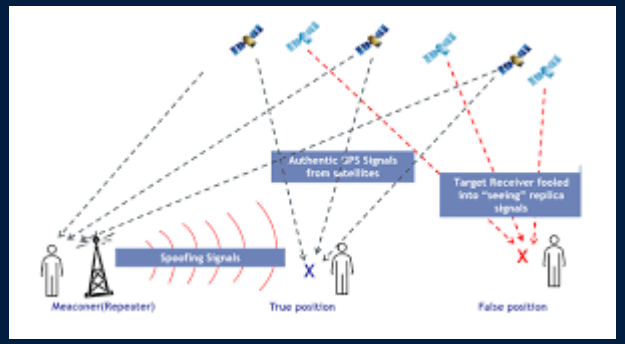


Figure 2 Spoofing

- Transmitting fake signals that mimic legitimate GNSS signals, causing the receiver to misinterpret its position, time or velocity.
- GNSS Satellite Signals, GNSS Navigation Message or GNSS Corrections (e.g. Starfix) can be attacked.
- Unlike jamming which disrupts the signals, spoofing tricks the receiver into using inaccurate data.
- A more subtle and potentially more dangerous attack.
- More difficult to detect than jamming as receiver appears to operate normally.

Meaconing

Spoofing

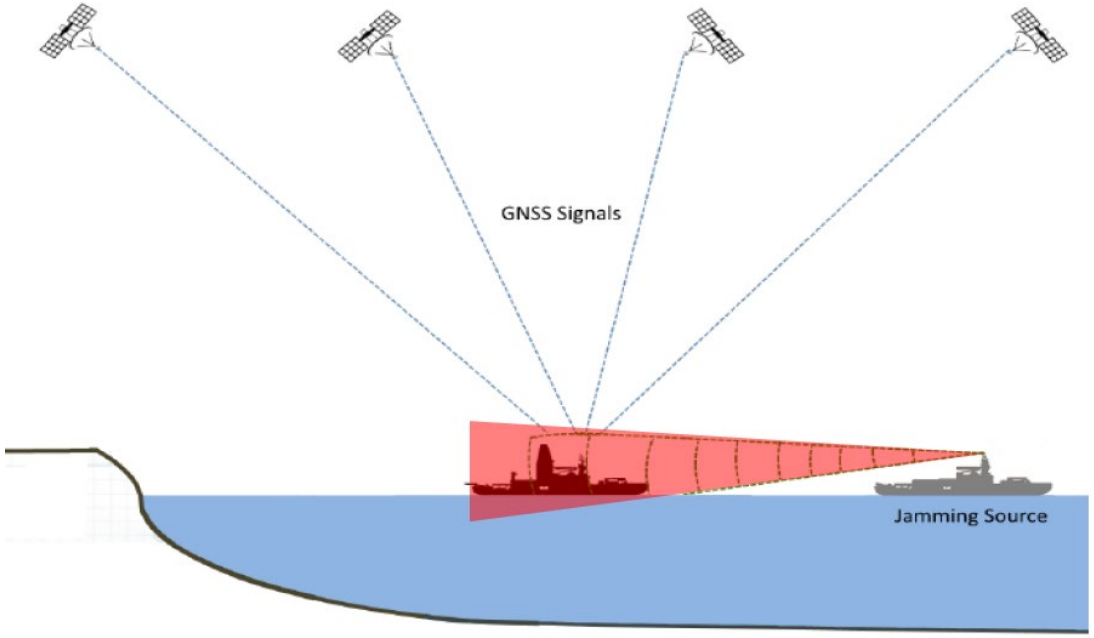


- Intercepting, amplifying and transmitting a GNSS receiver's signals, creating a false position for other receivers.
- All GNSS receivers receiving this signal will "move" to the location being transmitted.
- Uses a re-transmission of legitimate GNSS signals often at a higher power level than the original signal.
- Unlike spoofing attacks, meaconing doesn't require the attacker to generate new signals. A simpler and more accessible method.
- All receivers on a vessel will calculate identical positions.

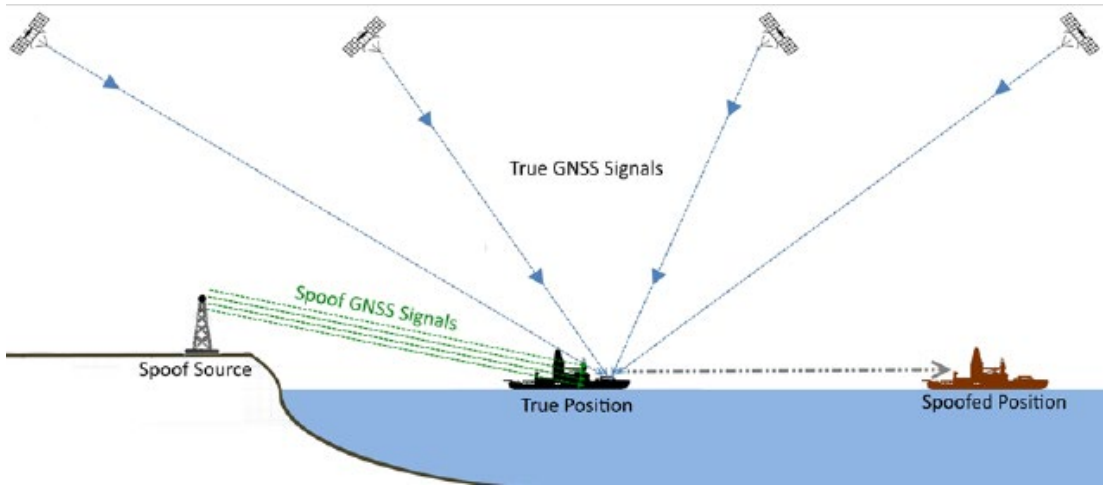
Jamming vs Spoofing

GNSS Cyber Security

Jamming



Spoofing



Signal Spoofing vs Meaconing

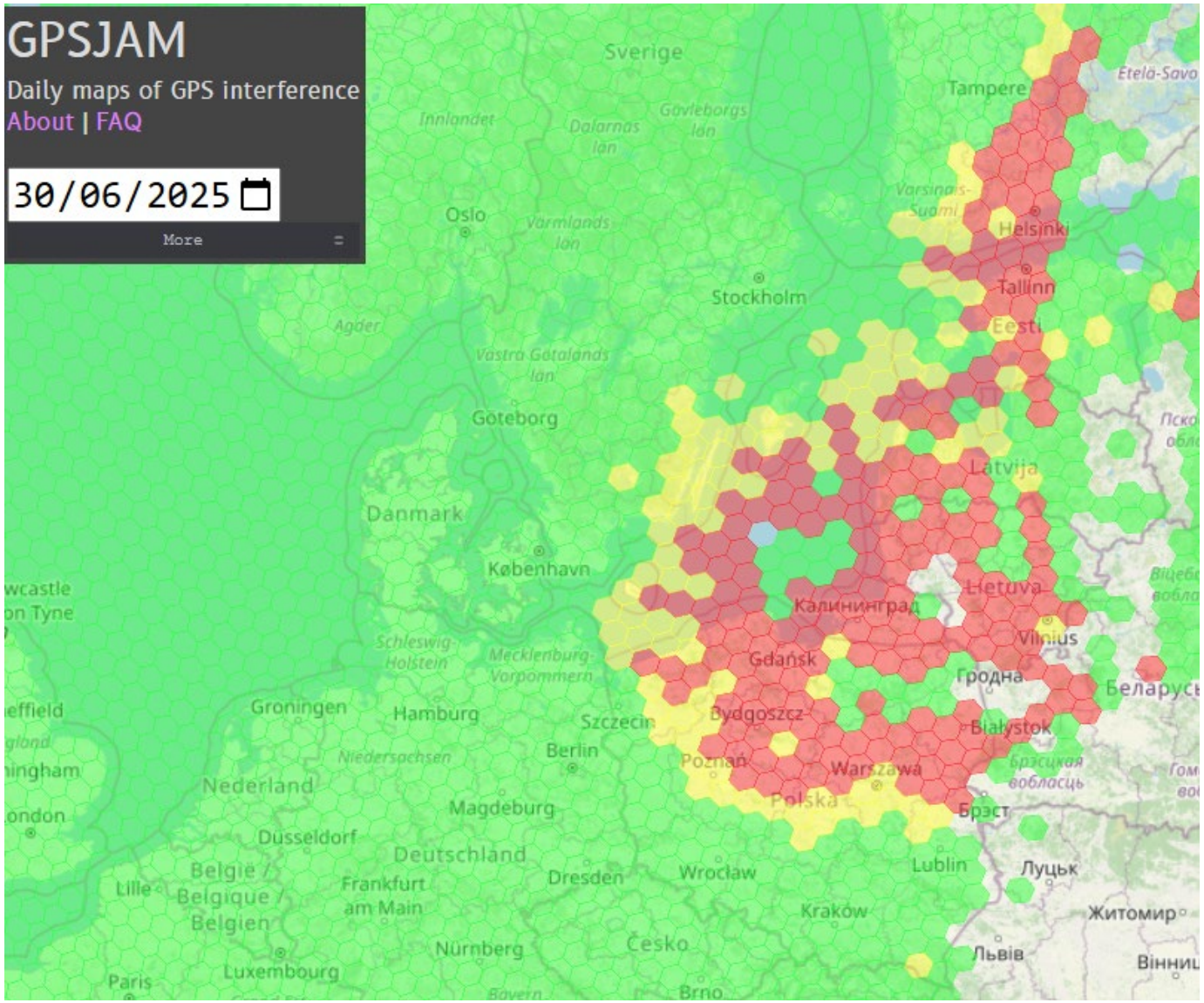
Spoofing

Meaconing involves retransmitting real “captured” GNSS signals.

Spoofing involves generation and transmitting false GNSS signals.

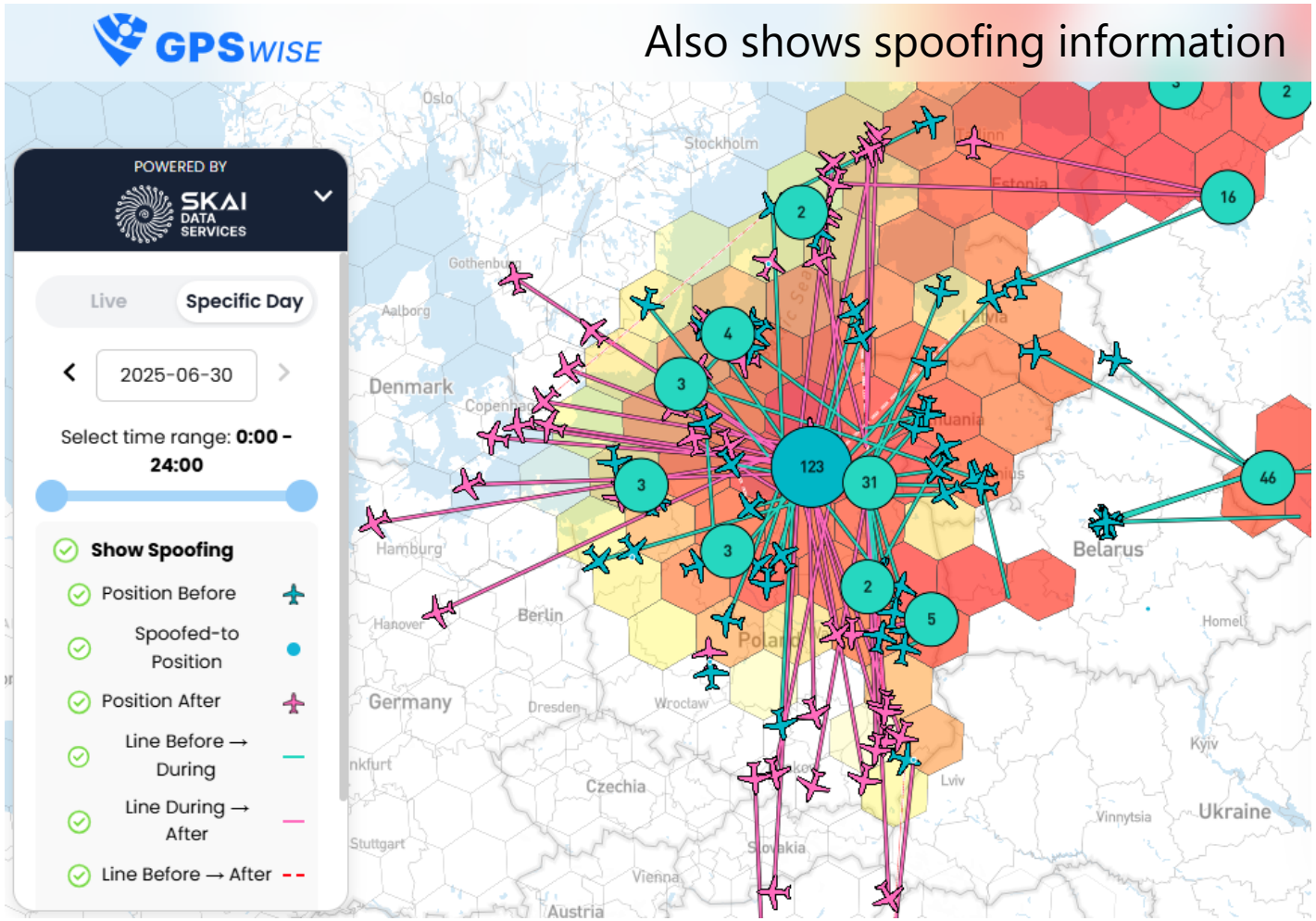
Jamming on GPSJAM

https://gpsjam.org/



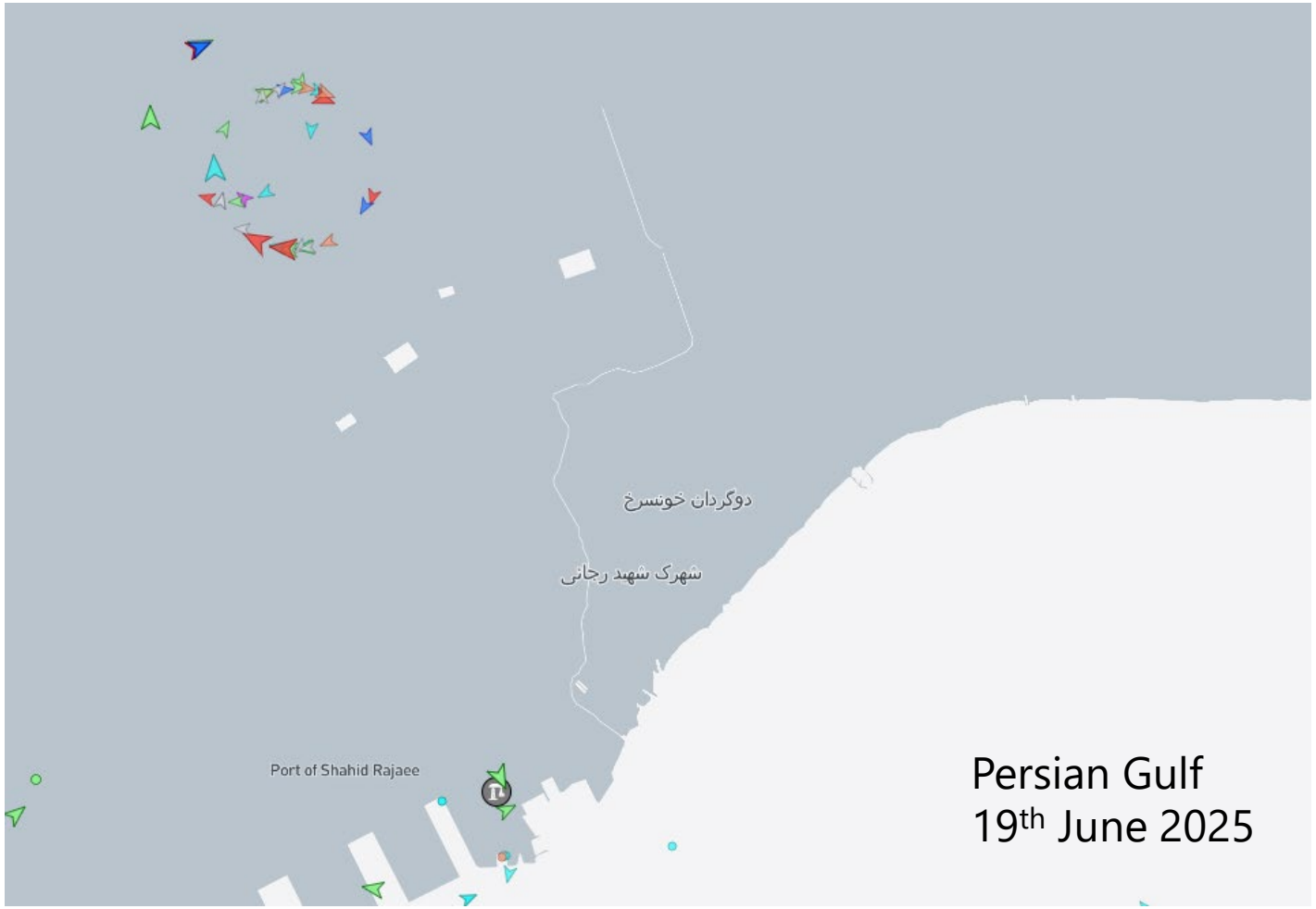
Jamming on GPSwise

https://gpswise.aero/



Jamming on Marine Traffic

https://www.marinetraffic.com/



GNSS Interference Resolution

Fugro Solutions

FUGRO SATGUARD™

AJT – Anti Jamming Technology

NMA – Navigation Message Authentication

SIA – Spatial Integrity Analysis

FUGRO

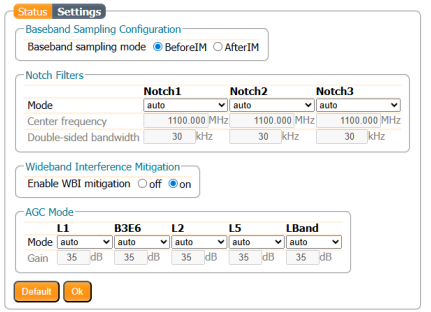
Anti Jamming Technology

Mitigation of Intentional Interference

- Narrow band filter antennas.
- Antennas with low sensitivity to ground signals.
- Receiver Firmware – wide band mitigation, notch filters, automatic gain control.
- Modern GNSS Receivers
- Counter Measures – Anti Jamming Units (AJU).

Calian AJ977XF
20db Attenuation below 15° elevation

Septentrio AIM+



StarPack 2 and Starfix X5

Tualcom TUALAJ 8300-D
CRPA / GAJT

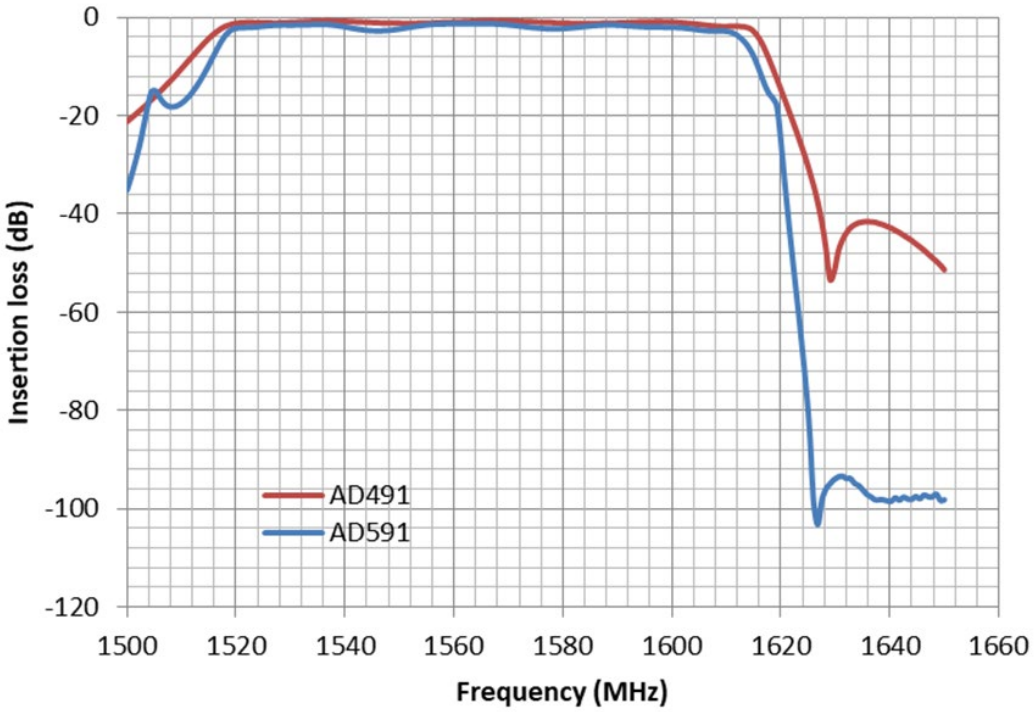
Narrow Band Antenna Filters

Anti Jamming Technology

Allison AD492 – against Inmarsat C

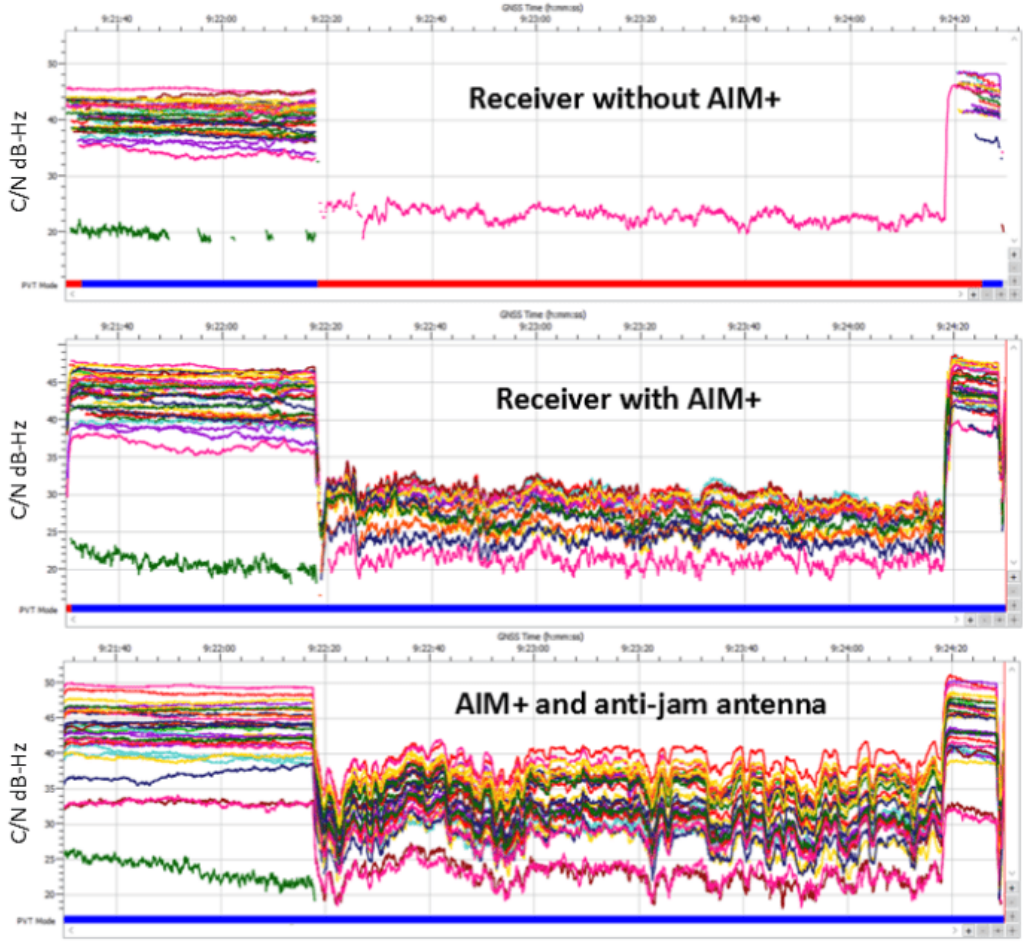
Trimble GA830 – against Iridium

Trimble Zephyr3 - against Iridium and 5G



Receiver Firmware

Anti Jamming Technology



Standard antenna: loss of position without AIM+

Standard antenna: positioning during jamming with AIM+

Anti-jam antenna: positioning with AIM+ and a small improvement in signal quality due to antenna

Septentrio from 2024 Andøya Jammer Test:

WBI and Notch Filters (AIM+) work better than CRPA Antenna

Source: https://www.septentrio.com/en/learn-more/insights/most-resilient-receiver-withstanding-gnss-jamming-and-spoofing?utm_source=substack&utm_medium=email

StarPack 2

Modern GNSS Receiver

- Trimble BD992 GNSS Card.
- Supported GNSS Frequencies:
  - GPS L1C/A, L2E, L2C, L5.
  - GLONASS L1C/A, L2C/A, L3CDMA.
  - Galileo E1, E5A, E5B, E5AltBOC, E6.
  - BeiDou B1, B2, B3.
- Raw data available for replay and analysis.

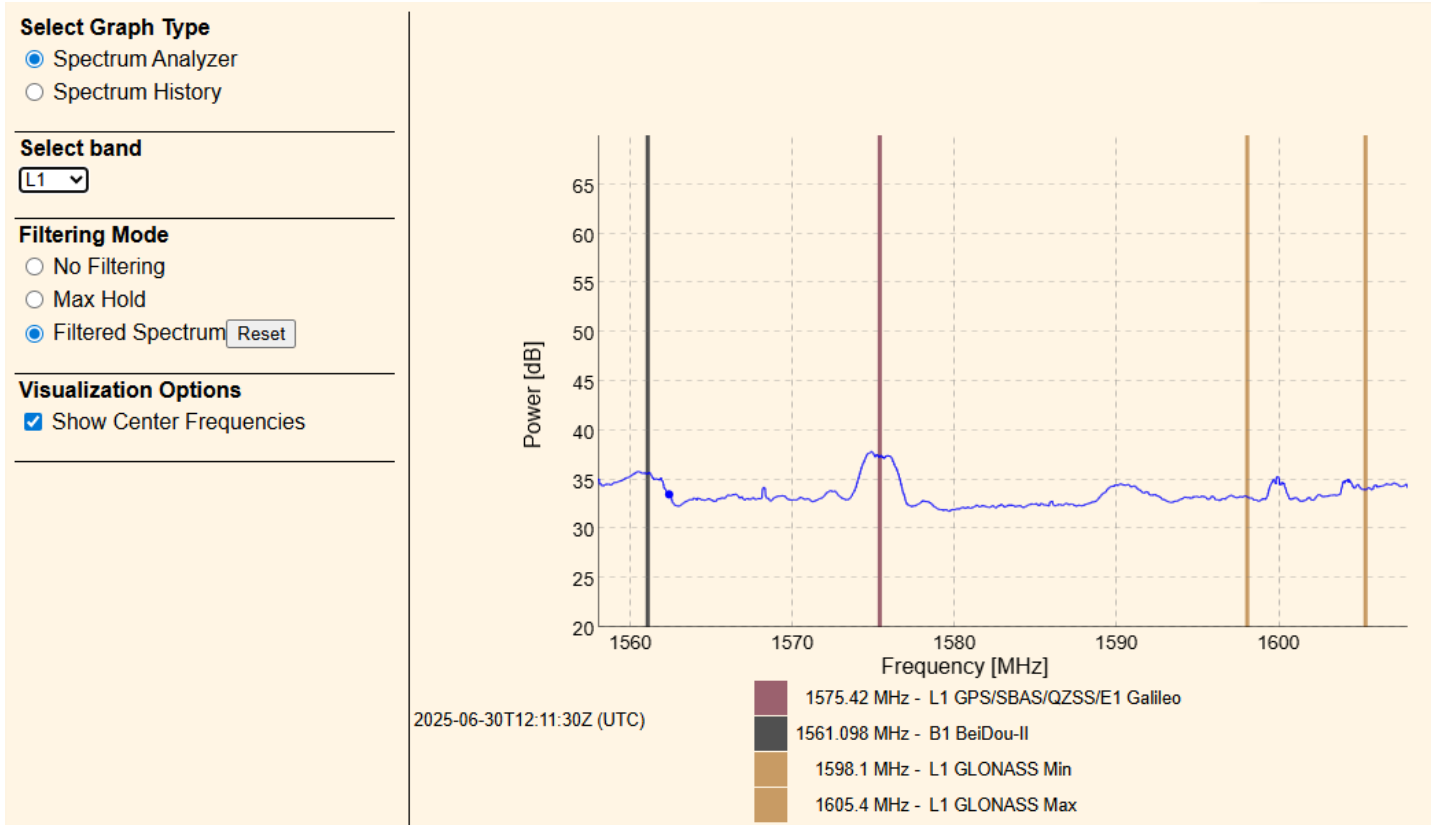
StarPack 2

Modern GNSS Receiver

Signal Tracking

Type	Signal	Enable	Options
GPS	L1 - C/A	☑	
GPS	L2E	☑	L2C and L2E
GPS	L2C	☑	CM + CL
GPS	L5	☑	I + Q
SBAS	L1 - C/A	☐	
SBAS	L5	☐	
GLONASS	L1 - C/A	☑	
GLONASS	L1P	☐	
GLONASS	L2P	☑	L2 - C/A(M) and P
GLONASS	L2 - C/A	☑	
GLONASS	L3	☐	
Galileo	E1	☑	
Galileo	E5 - A	☑	
Galileo	E5 - B	☑	
Galileo	E5 - AltBOC	☑	
Galileo	E6	☑	
BeiDou	B1	☑	
BeiDou	B1C	☐	
BeiDou	B2	☐	
BeiDou	B2A	☑	
BeiDou	B3	☑	

Spectrum Analyser



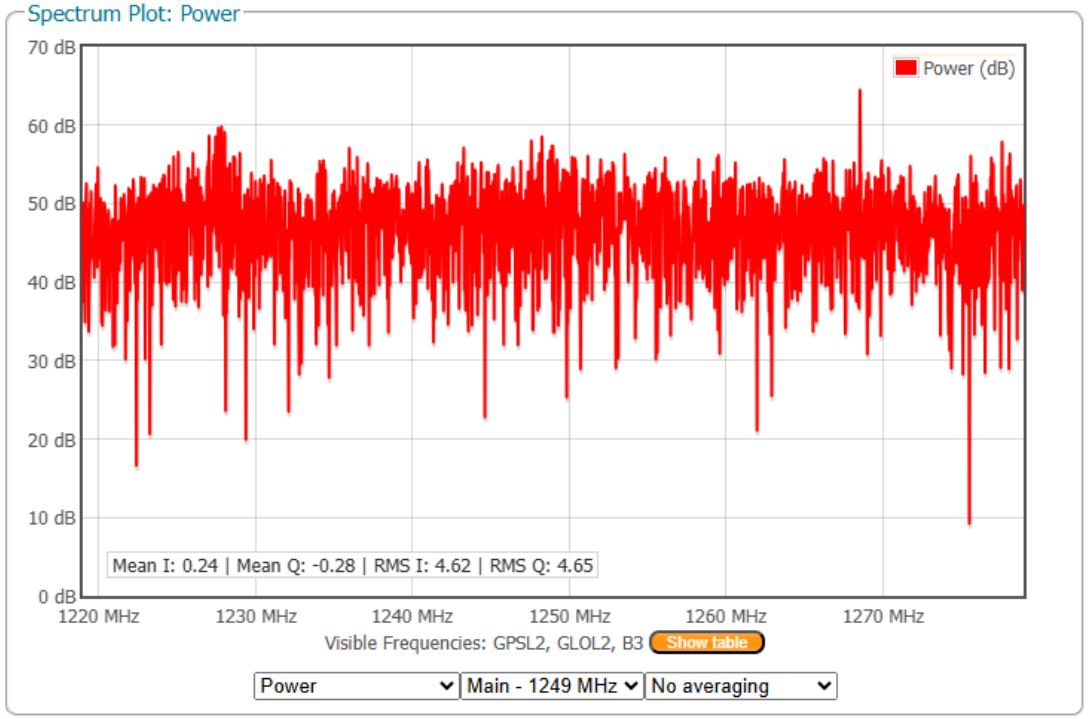
Starfix X5

Modern GNSS Receiver

- Septentrio Mosaic X5 GNSS Card.
- Supported GNSS Frequencies:
  - GPS L1C/A, L2C, L5.
  - GLONASS L1C/A, L2C/A, L3CDMA.
  - Galileo E1, E5A, E5B, E5AltBOC, E6.
  - BeiDou B1, B2, B3.
- Raw data available for analysis.

Starfix X5

Modern GNSS Receiver



Spectrum Analyser

Advanced Interference Mitigation (AIM+)

Baseband Sampling Configuration

Baseband sampling mode ◉ BeforeIM ○ AfterIM

Notch Filters

	Notch1	Notch2	Notch3
Mode	auto	auto	auto
Center frequency	1100.000 MHz	1100.000 MHz	1100.000 MHz
Double-sided bandwidth	30 kHz	30 kHz	30 kHz

Wideband Interference Mitigation

Enable WBI mitigation ○ off ◉ on

AGC Mode

	L1	B3E6	L2	L5	LBand
Mode	auto	auto	auto	auto	auto
Gain	35 dB	35 dB	35 dB	35 dB	35 dB

AJU Terminology

CRPA / GAJT Antenna

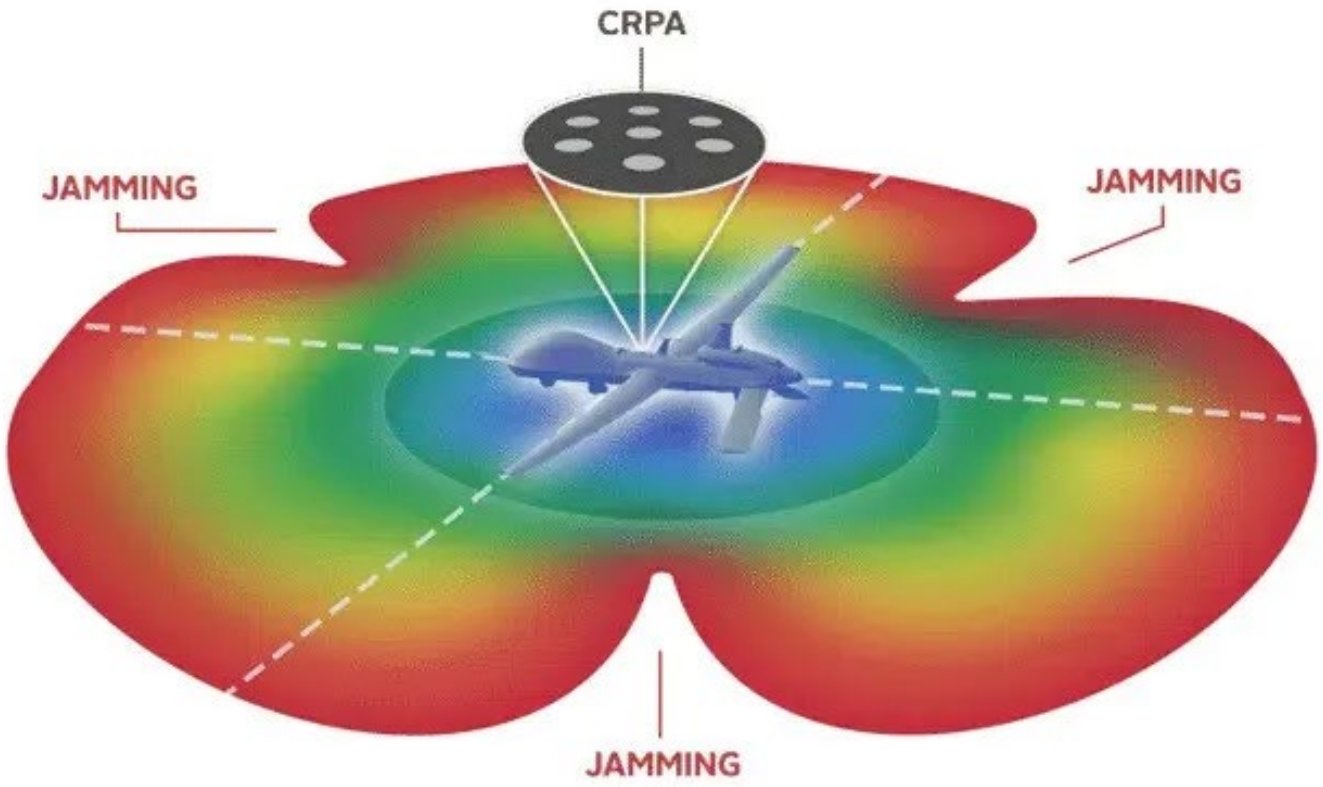
Controlled Reception Pattern Antenna

GNSS Anti-Jam Technology

GAJT ⇔ CRPA

Anti-jamming Units

CRPA / GAJT Antenna



- Use nulling and/or beam forming to mitigate the effects of interfering signals.
- Provide protected RF signals to any GNSS receiver.
- Anti-Jamming Units are relatively expensive – prices reducing ?
- Subject to export control – subject to change later this year ?

Beam Forming

CRPA / GAJT Antenna

- Exploit spatial diversity – satellite signals and the jamming signals arrive from different directions.
- Create spatial filter - removes signals that arrive from particular directions.
- “Steer” maximum overall antenna gain towards that GNSS satellite and away from jamming source.
- This is typically what is meant when we refer to “beam forming”.

Navigation Message Authentication

FUGRO SATGUARD™

Authenticity of messages ✓

Digital signature produced ✓

Signature distributed ✓

FUGRO

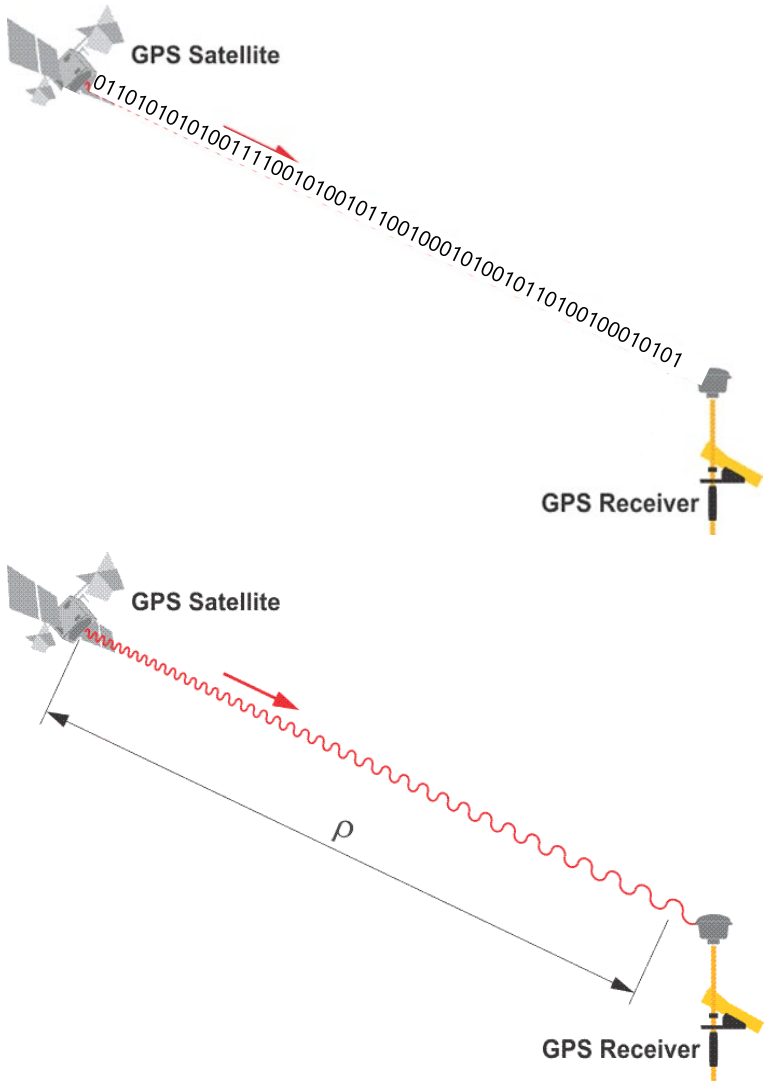
FUGRO

What is GNSS Authentication

Navigation Message Authentication

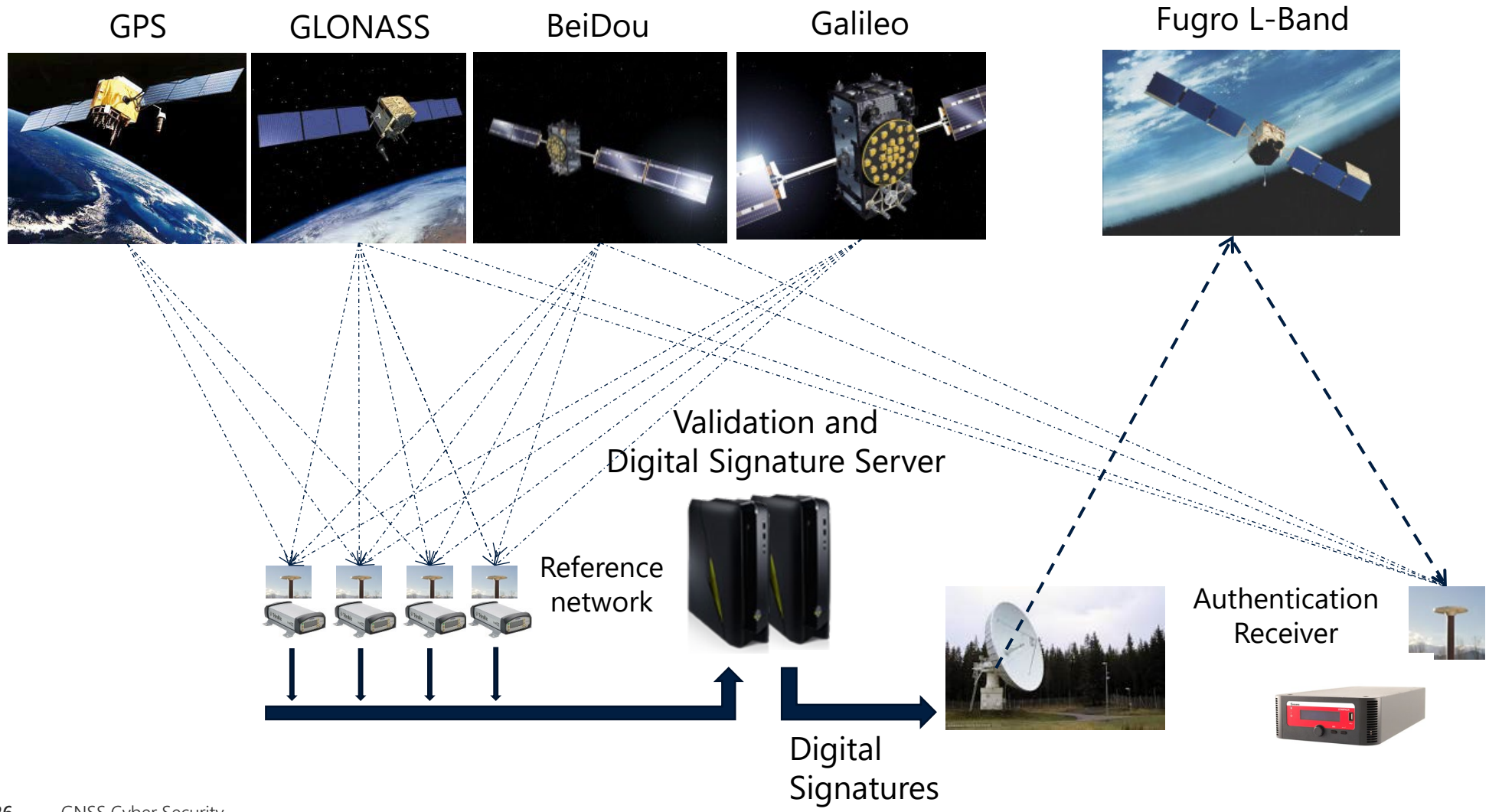
- There are two parts of GNSS authentication:
  1. Navigation Message Authentication (NMA)
  2. Signal (pseudo-range) authentication

- Both parts are essential:
  - Then the position is authenticated, determined using only the original GNSS signals



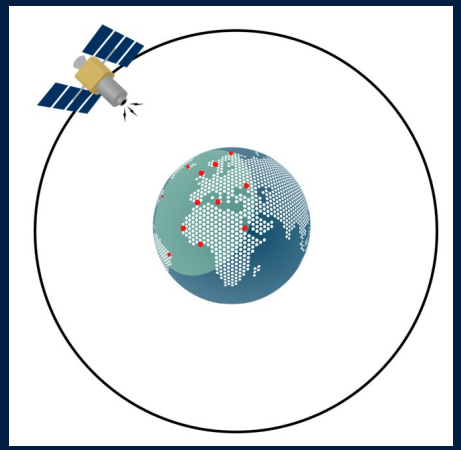
GNSS Authentication Infrastructure

Navigation Message Authentication



SATGUARD

Navigation Message Authentication



- Fugro has no direct access to original Navigation Messages.
- The Navigation Messages are collected and proven as authentic:
  - Observe in global network*
  - All sites with the satellite in view shall receive the same message*
  - No site outside the area of visibility should report the satellite*
  - Navigation Message contents is validated against known information*

Difficulties for a spoofer:

- Synchronise an attack at many sites.
- Need concurrent presence over multiple continents.

Once authenticated by the server:

- NMs are signed
- Signatures broadcast

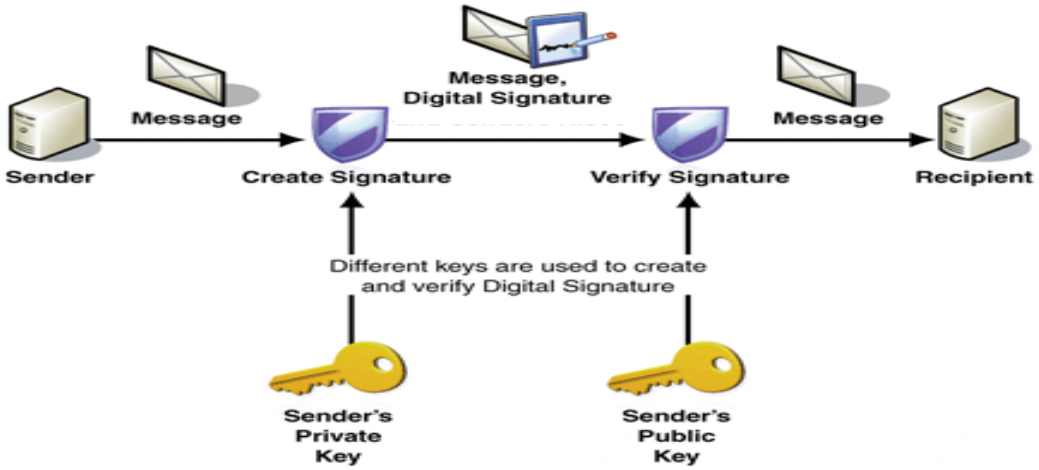
* Patented

Digital Signatures

Navigation Message Authentication

- Each Navigation Message summarised in a unique hash.
- Hashes are broadcast in signed messages.
- Fugro has a private key used to sign the message.
- The user has the public key.
- The public key can be used to verify that the signature is made from a combination of the Navigation Messages and Fugro's private key.
- Specially developed efficient protocol*

* Patented

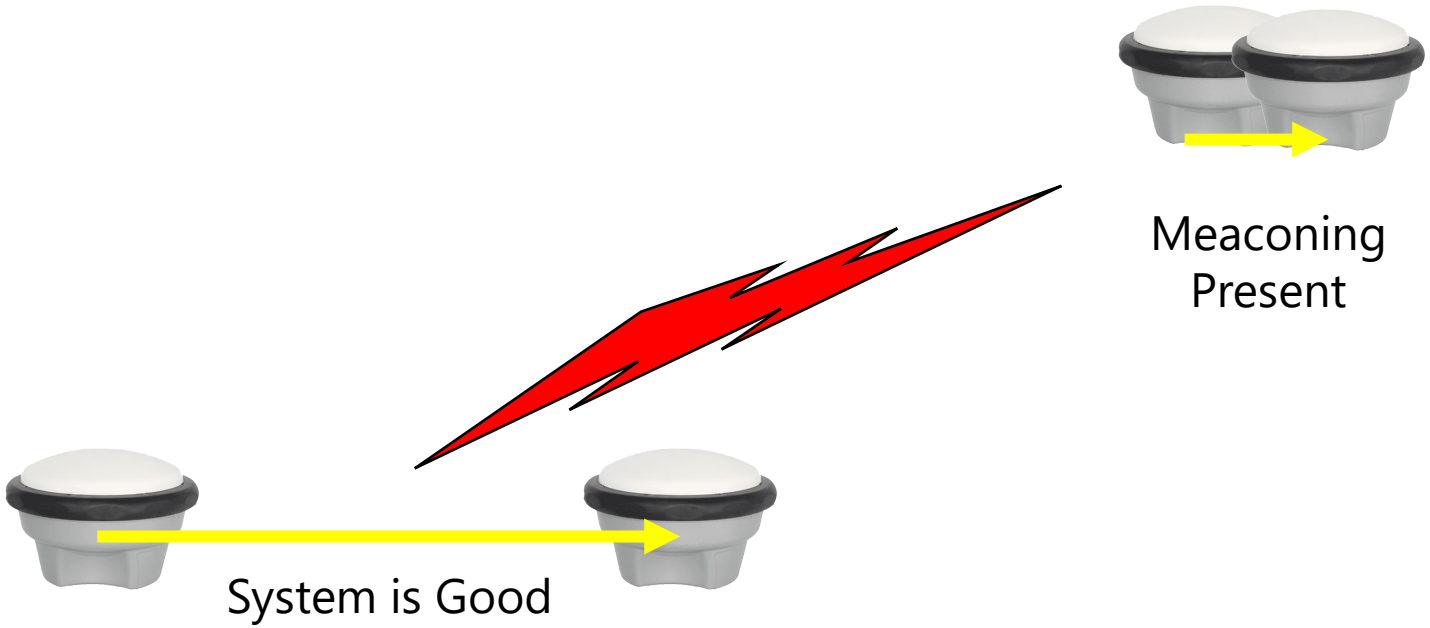


Message authentication system with a private and public key pair

- Number generator for internet banking.
- used to authenticate you and ensure the information sent to the bank is secure.
- The number and your password represents your private key.

Spatial Integrity Analysis

Spatial integrity analysis for meaconing detection

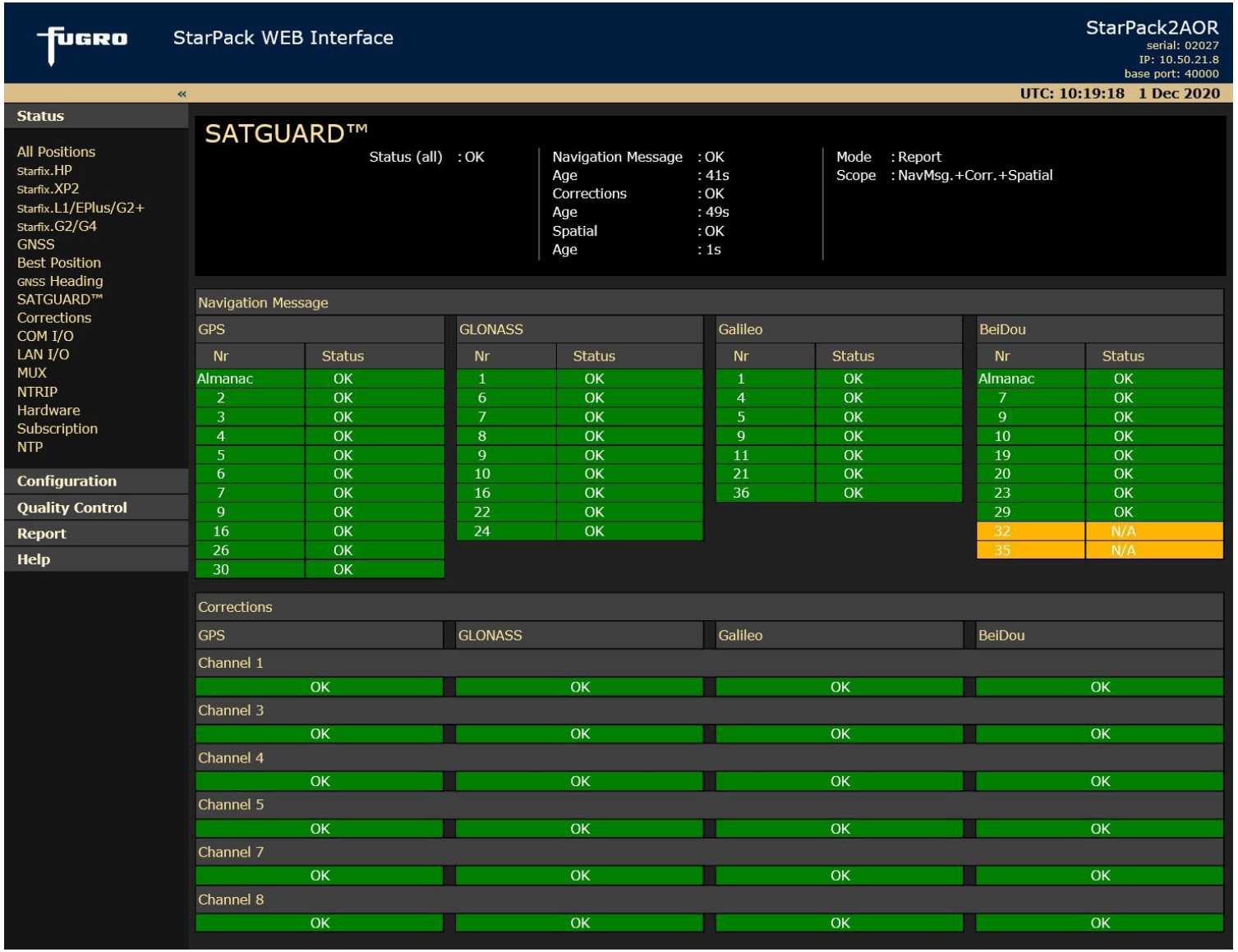


- When Meaconing is present all antennas will have the same position.
- The offset between two antennas on a vessel less the 2cm meaconing could be present.

Fugro NMA

Implemented in StarPack 2

FUGRO SATGUARD™



FUGRO

SATGUARD OUTPUT

From StarPack 2

FUGRO SATGUARD™

$PFUG,SGD,1,172814.00,R,2*0E

Table B.38: PFUG,SGD Message Description

Parameter	Description
1	Message version
172814.00	UTC time of report, 17:28:14.00
R	Mode: R – Report – when SATGUARD status is not tied to a particular solution but rather reports on the authentication or integrity status of various components that are used as input data to positioning solutions in the unit F – Flag (reserved, not used) D – Detect (reserved, not used) U – Use only (reserved, not used)
2	Global status: 0 / empty – Unknown or N/A 1 – OK 2 – Alert 3+ - reserved
	Checksum

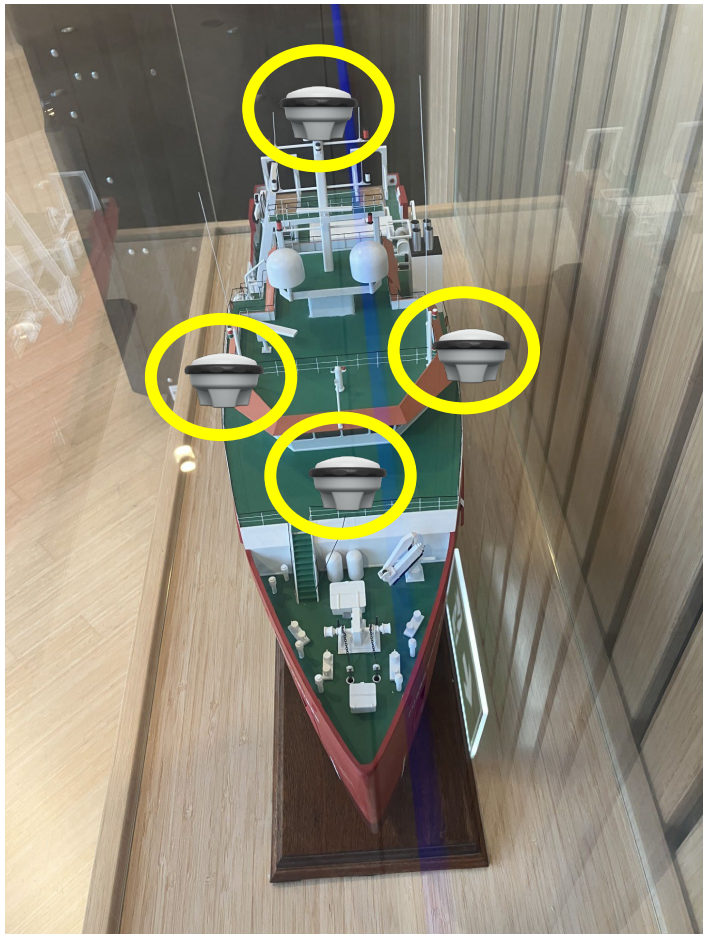
FUGRO

Rounding Off

Ideas and Summary

Novel Ideas

Thinking out of the box



Ship as
Shield

Chat GPT

Seen Offshore

Summary

Reflection on Today's Situation

- For many years GNSS has been like a "black box" – simply performed well.
- New challenges have arisen "in the light of" jamming and spoofing.
- Knowledge of modern receiver interfaces and analysis techniques required.
- There are solutions to jamming and spoofing, but we need to stay one step of the "intruder".
- GNSS antennas assume ground-based jamming and spoofing – drones create a different situation.
- New tests undertaken in Andøya 2025.

FUGRO

Unlocking **Insights**
from **Geo-data**