GNSS Jamming and Spoofing

Marine Operations in Practice – 22. April 2026

John Vint – Product Manager for Starfix Signals

Agenda

Presentation Scope

- Introduction.
- GNSS Cyber Security.
- What is Jamming and Spoofing.
- How can this be mitigated.
- Real life examples.
- Conclusions.

GNSS Cyber Security

Terminology

Intrusion

Jamming

Spoofing

GNSS Cyber Security

Security Risks

Intrusion (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.
Spoofing (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

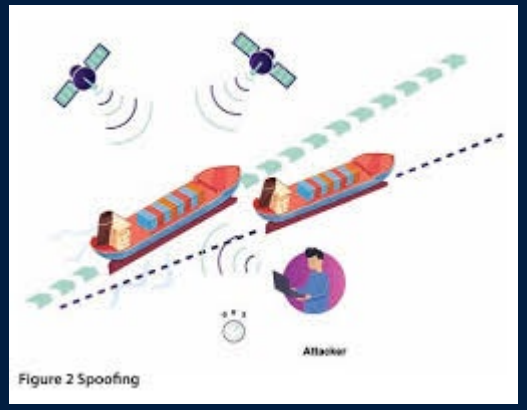
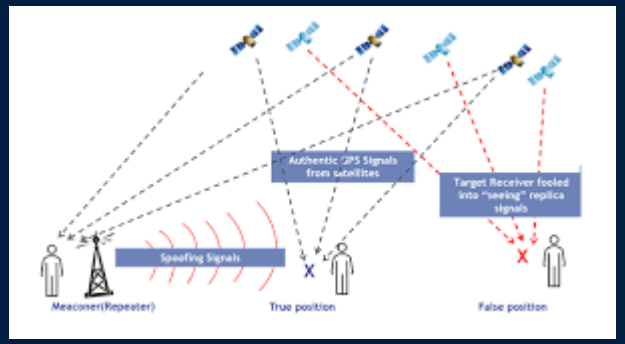


Figure 2 Spoofing

- 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

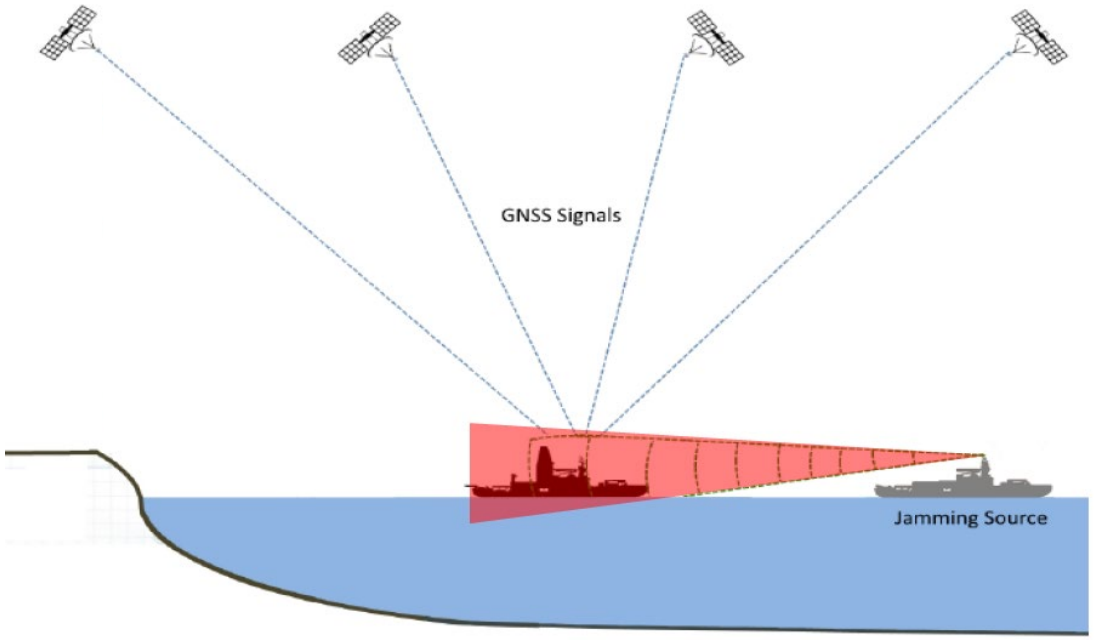


- Intercepting, amplifying and transmitting a GNSS receiver's signals, creating a false position for other receivers.
- All GNSS receivers receiving this signal will "move" to the location being transmitted.
- Uses a re-transmission of legitimate GNSS signals often at a higher power level than the original 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.

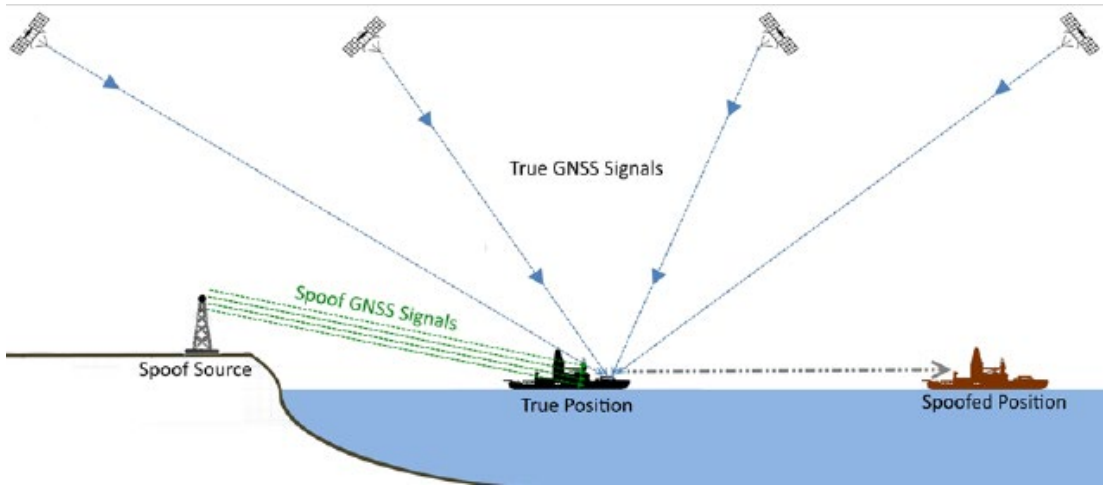
Jamming vs Spoofing

GNSS Cyber Security

Jamming



Spoofing



Signal Spoofing vs Meaconing

Spoofing

FUGRO SATGUARD™

Meaconing involves retransmitting real “captured” GNSS signals.

Spoofing involves generation and transmitting false GNSS signals.

FUGRO

GNSS Interference Resolution

Fugro Solutions

FUGRO SATGUARD™

AJT – Anti Jamming Technology

NMA – Navigation Message Authentication

SIA – Spatial Integrity Analysis

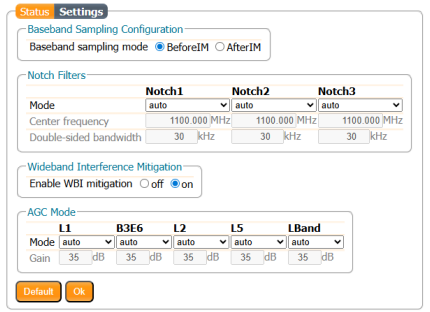
FUGRO

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

AJU Terminology

CRPA / GAJT Antenna

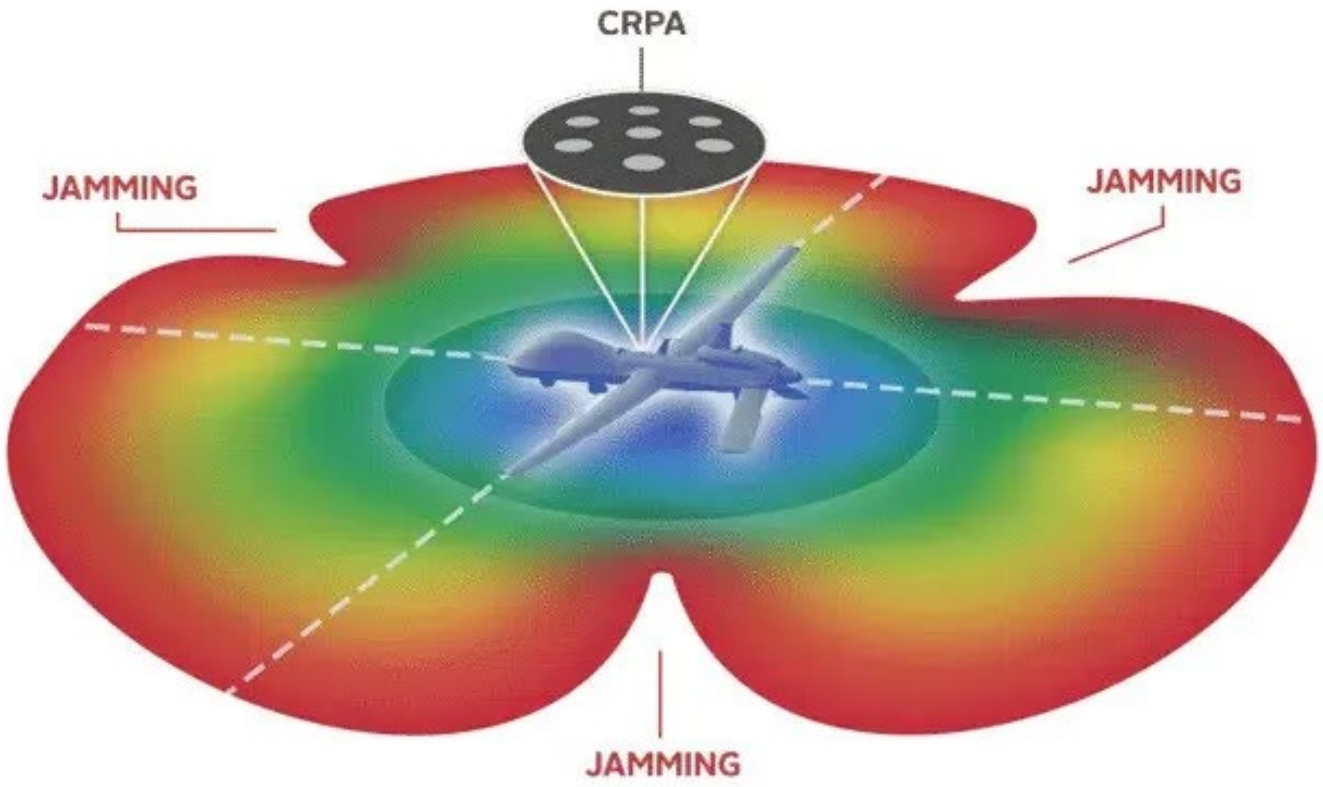
Controlled Reception Pattern Antenna

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 expensive – new cheaper technology ?
- Subject to export control – lengthy process ?

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 a particular direction.
- “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 ✓

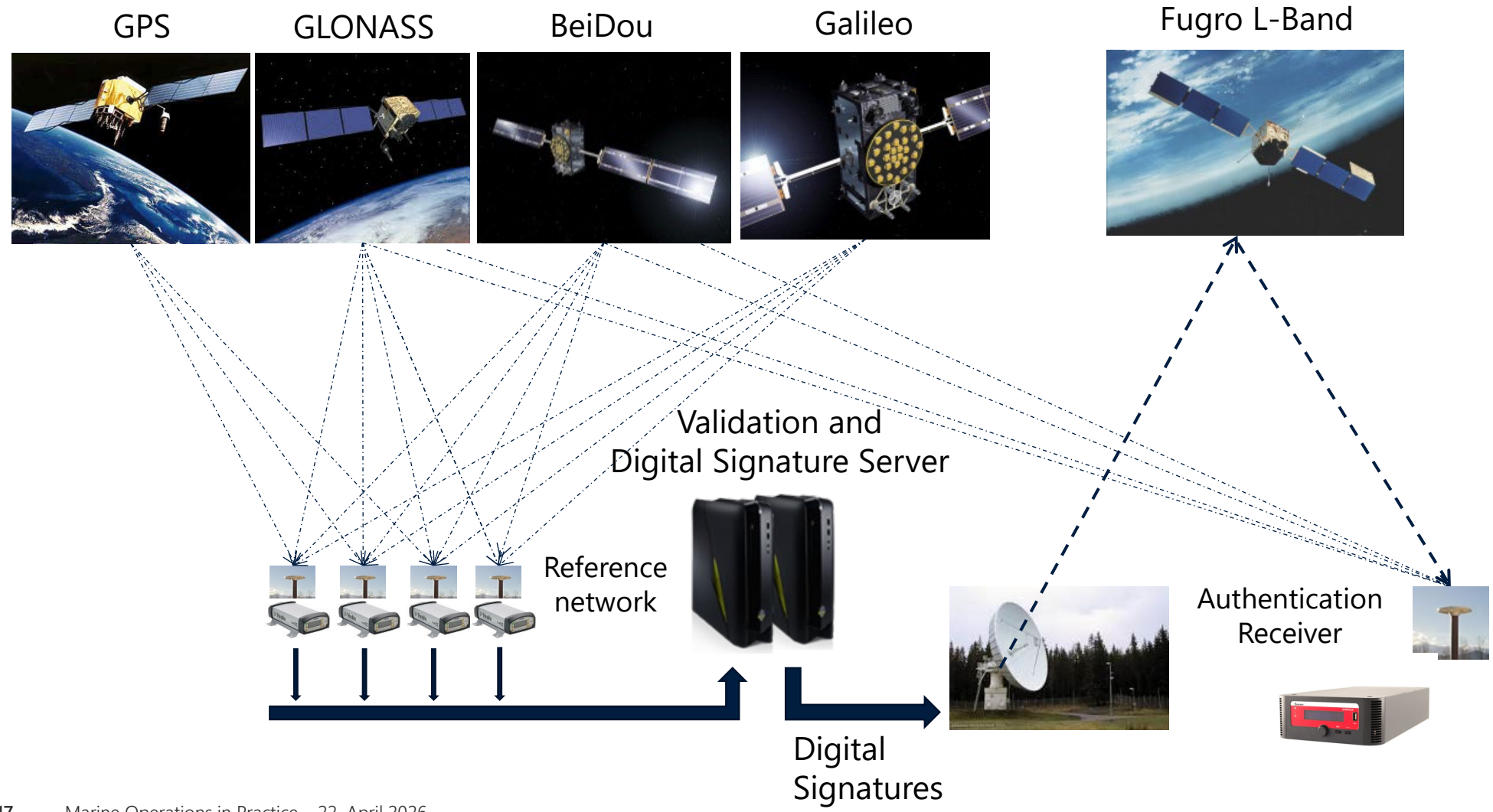
Signature distributed ✓

FUGRO

FUGRO

GNSS Authentication Infrastructure

Navigation Message Authentication



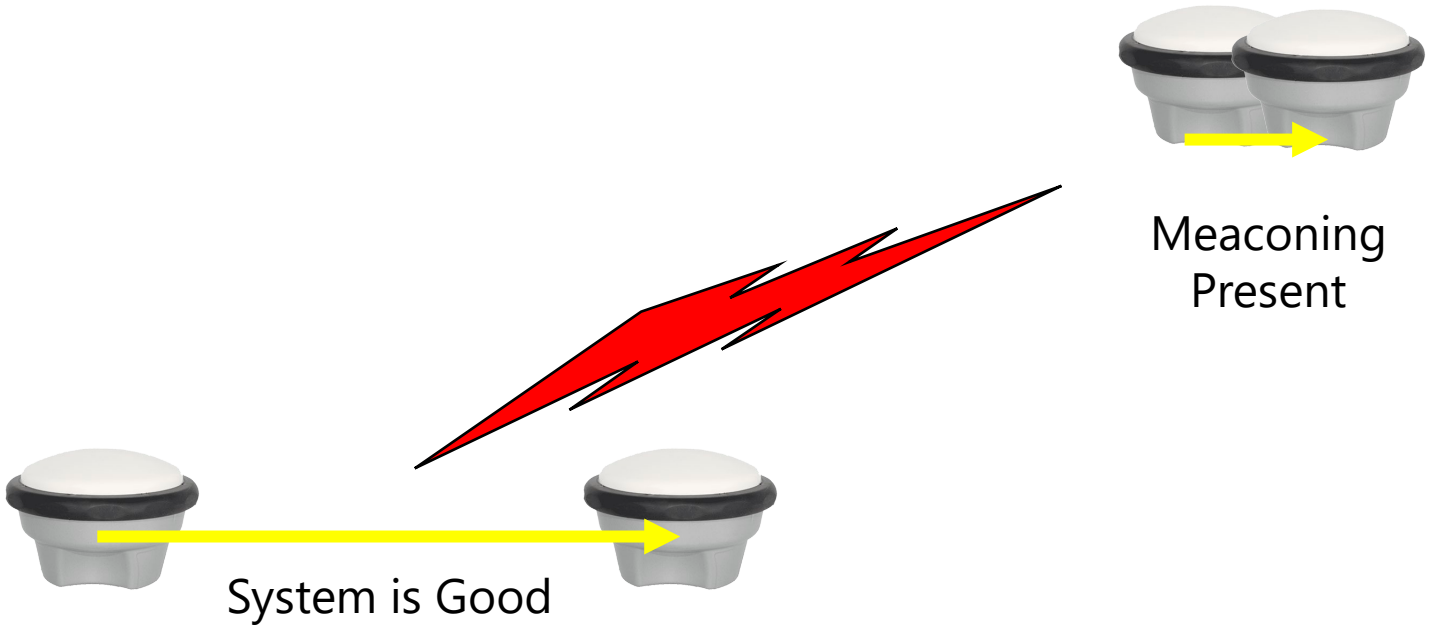
Strict Mode

Mitigating Spoofing

- Navigation Message Authentication – detects and warns of spoofing.
- New algorithms built into Fugro products – SatGuard “Strict Mode”.
- These facilitate the removal of spoofed satellites observations from the solution.
- Result – stable and useable solution.

Spatial Integrity Analysis

Spatial integrity analysis for meaconing detection

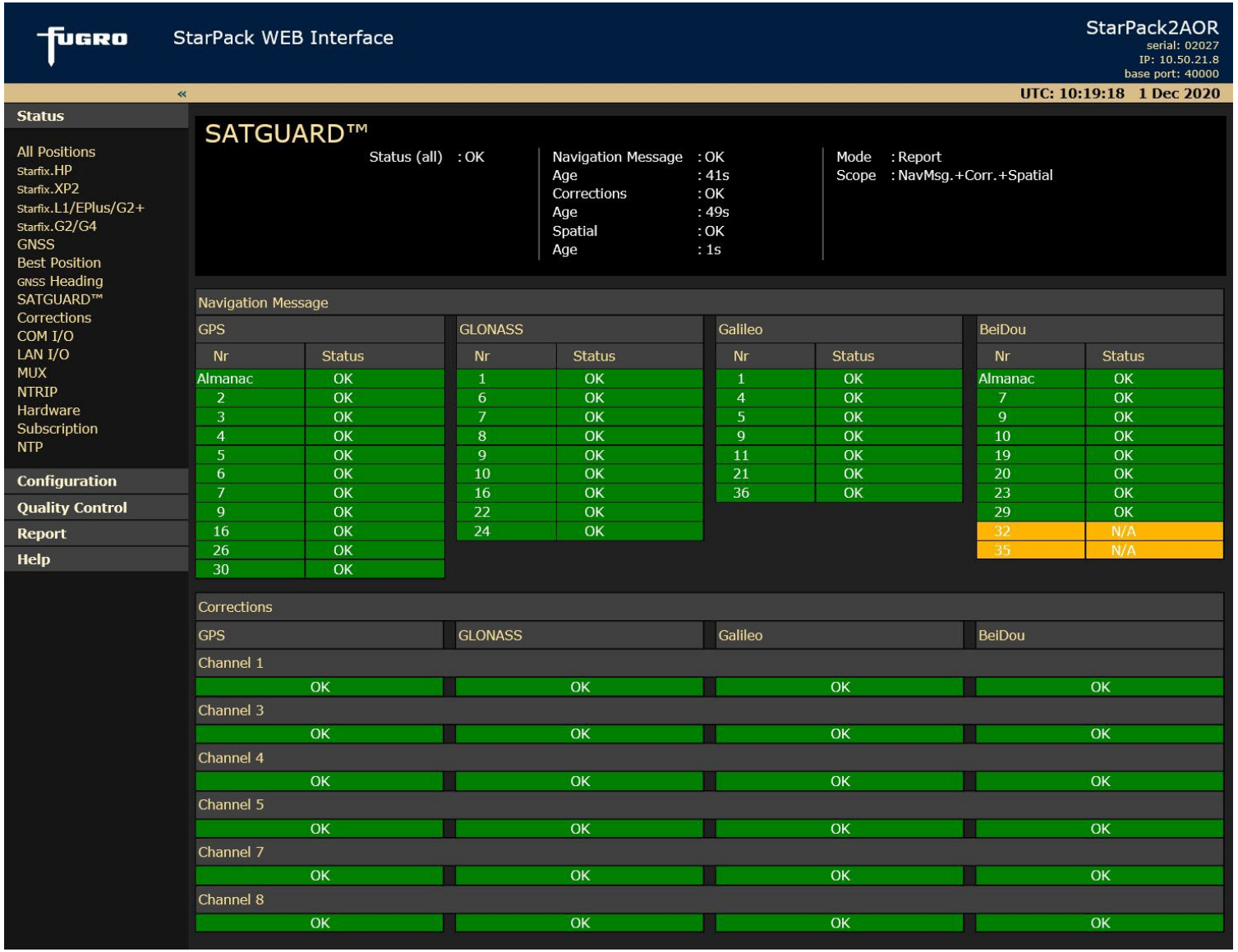


- When Meaconing is present all antennas will have the same position.
- The offset between two antennas on a vessel less the 2cm meaconing could be present.

Fugro NMA

Implemented in StarPack 2

FUGRO SATGUARD™



FUGRO

CRPA Performance

Kobi Ruegg, Mediterranean, June 2025

Technical Details

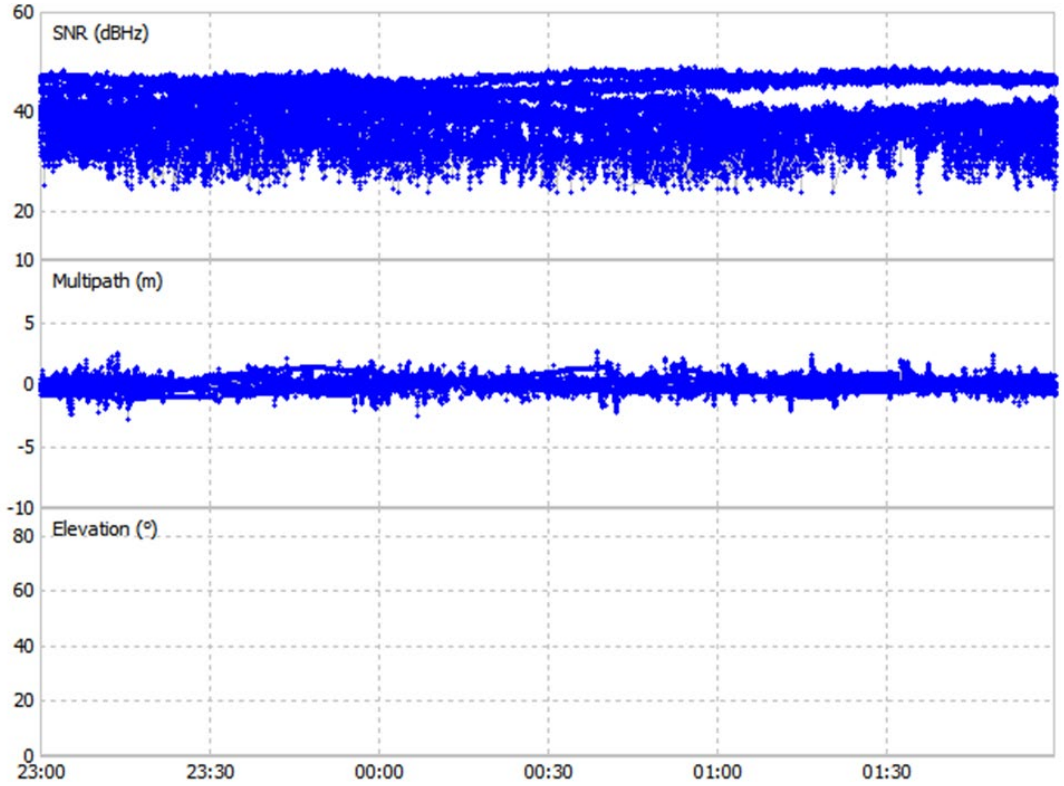
Hexagon GAJT-710MS

- GPS L1/L2, Galileo E1.
- StarPack cannot use Galileo E5.
- 7 array elements.
- 6 simultaneous independent nulling directions.

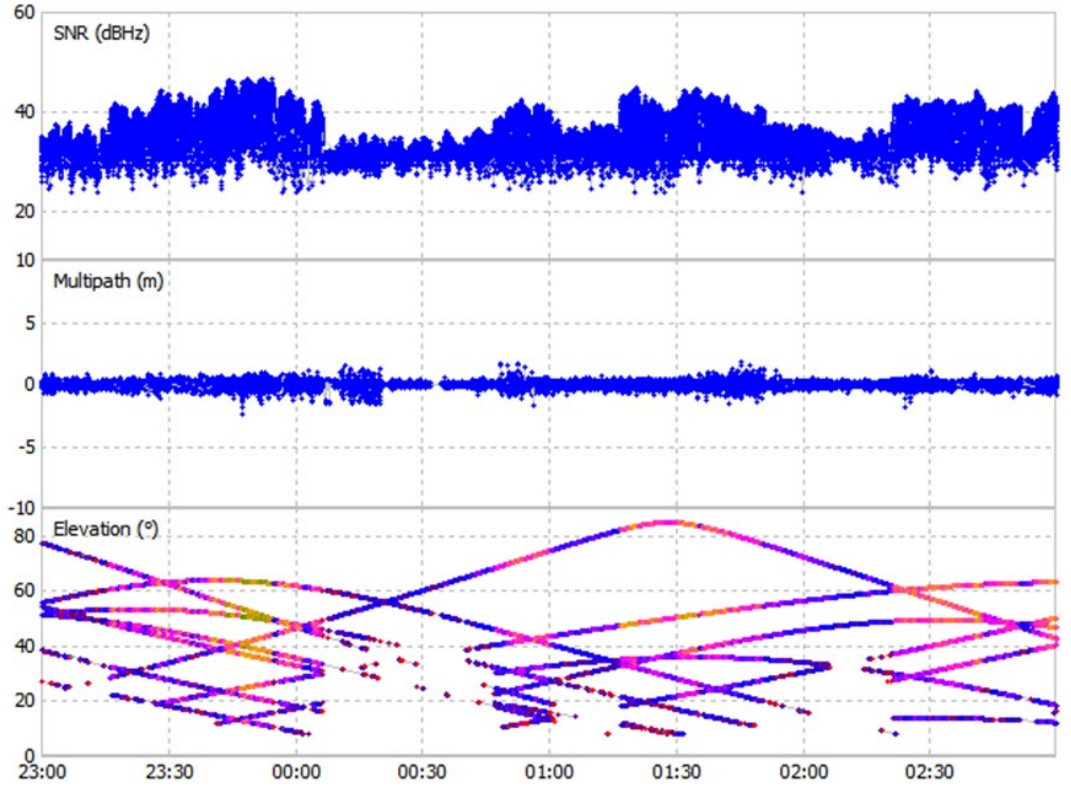
GPS L1 Tracking

CRPA Performance

GPS L1 with CRPA Antenna



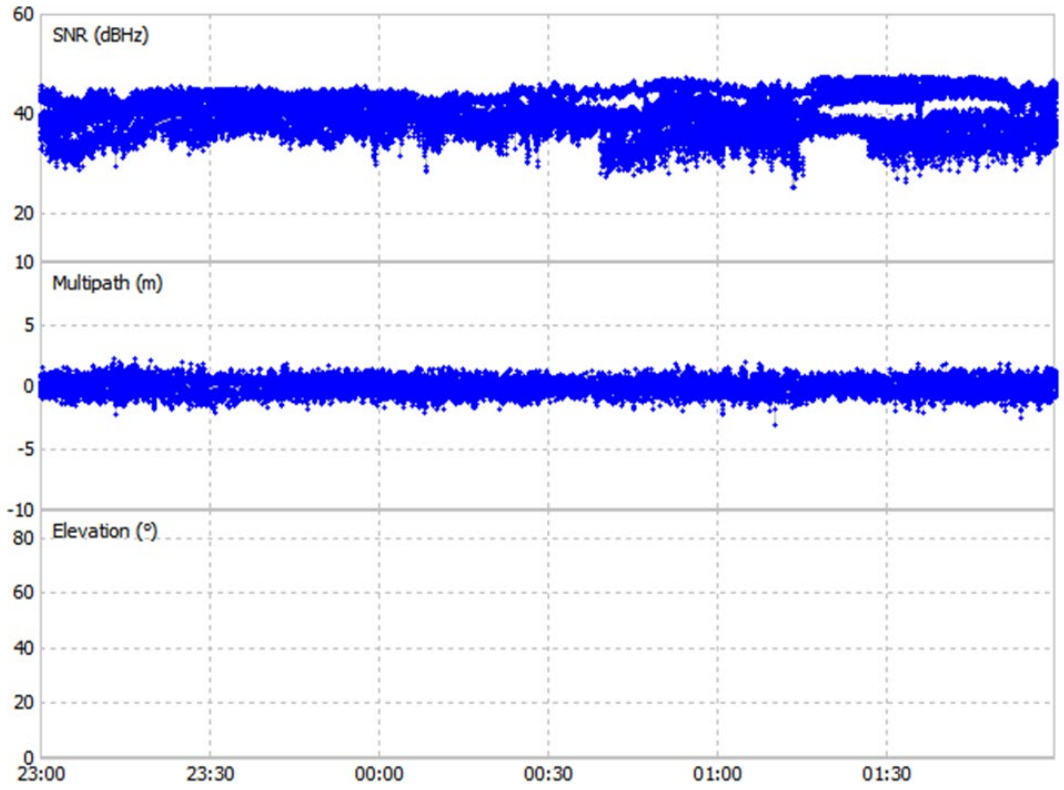
GPS L1 without CRPA Antenna



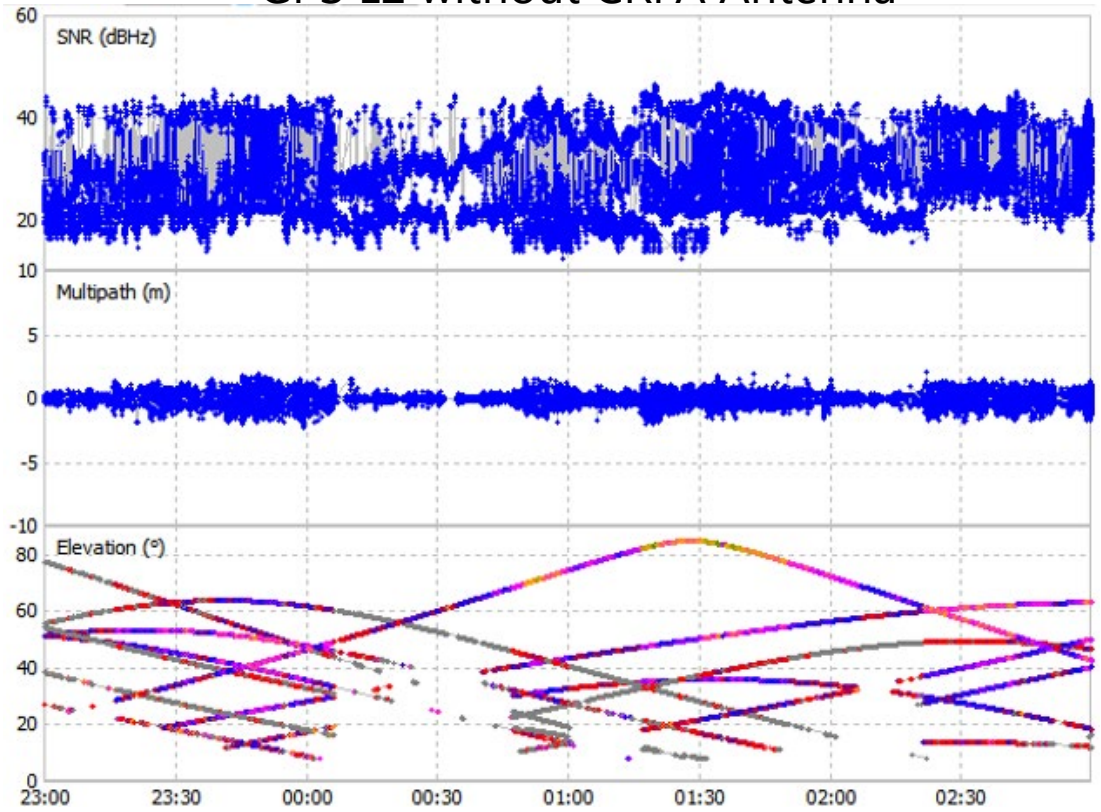
GPS L2 Tracking

CRPA Performance

GPS L2 with CRPA Antenna



GPS L2 without CRPA Antenna



Real Jamming Events / Mitigation

Fugro Project, Qatar, April 2026

Vessel Configuration

Jamming and Spoofing Mitigation

- System #1 – CRPA Antenna with Fugro 9410 - “Strick Mode” enabled.
- System #2 – Standard Antenna with Fugro StarPack – No “Strick Mode”.
- System #3 – Standard Antenna with Fugro StarPack – No “Strick Mode”.

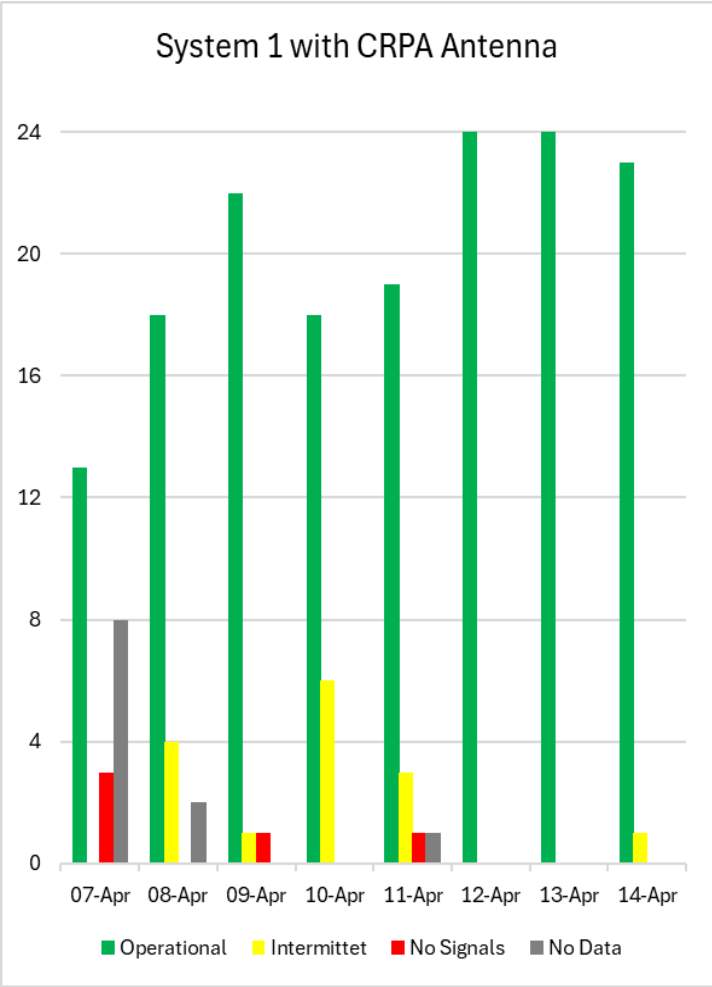
Technical Details

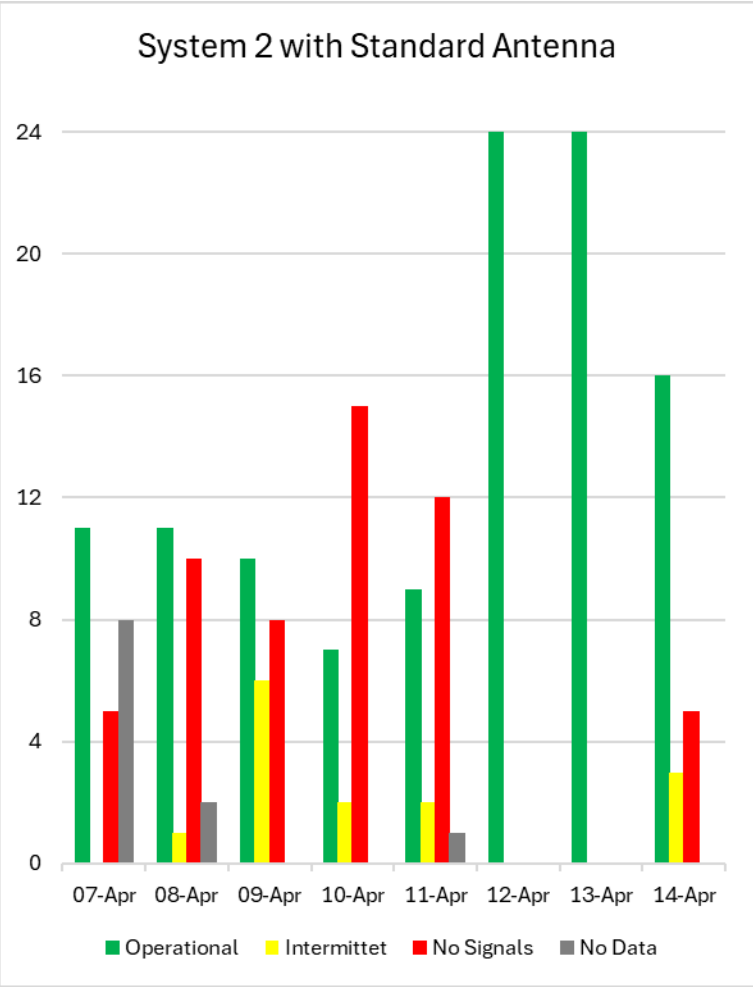
Tualcom TUALAJ 8300-D

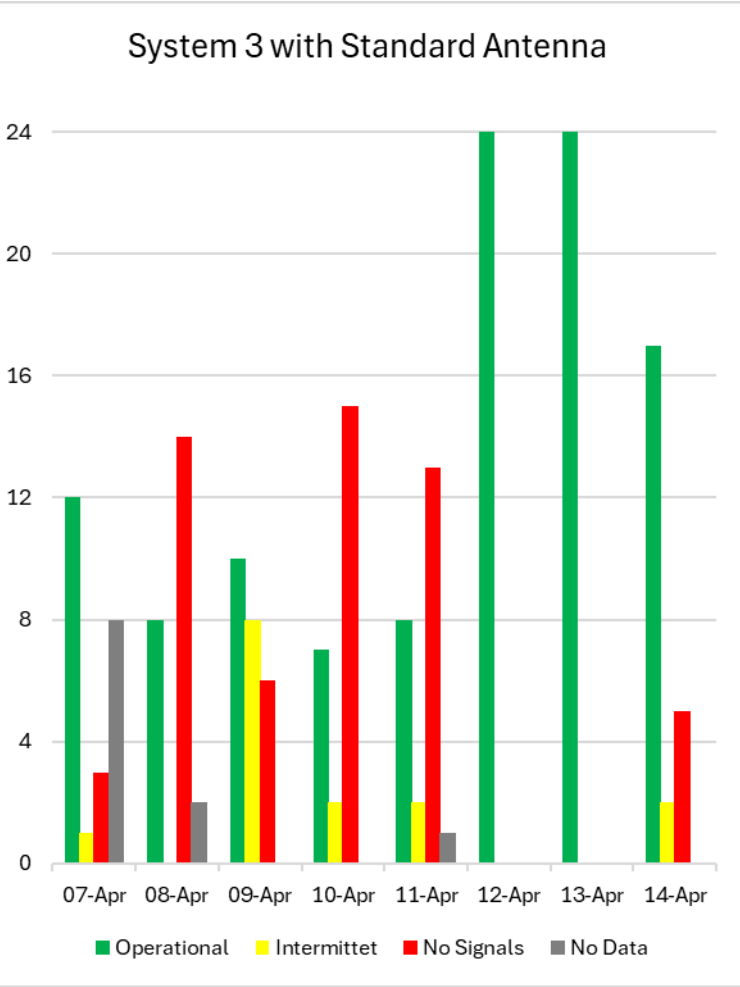
- GPS L1/L2/L5, GLONASS L1/L2, Galileo E1/E5a/E5b, BeiDou B1
- 8 array elements
- 7 simultaneous independent nulling directions

System Comparisons

CRPA vs Standard Antenna Performance

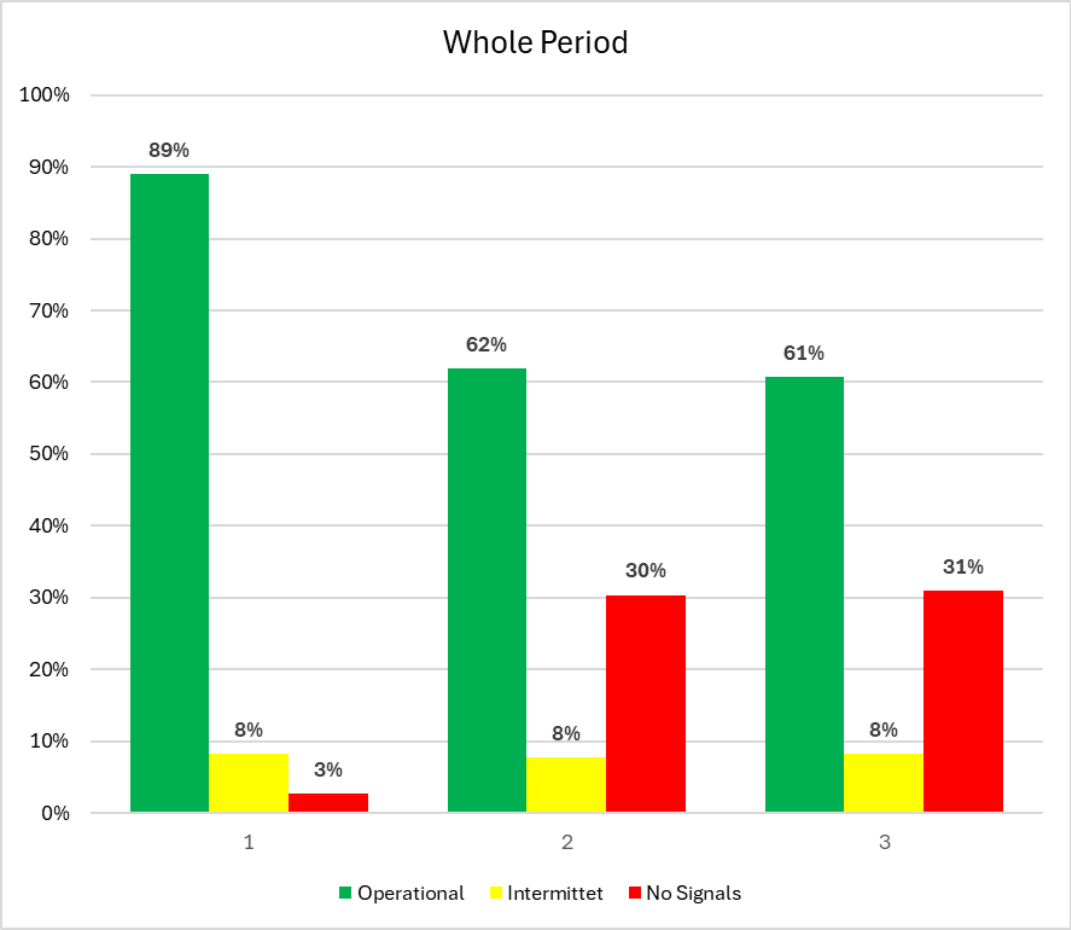


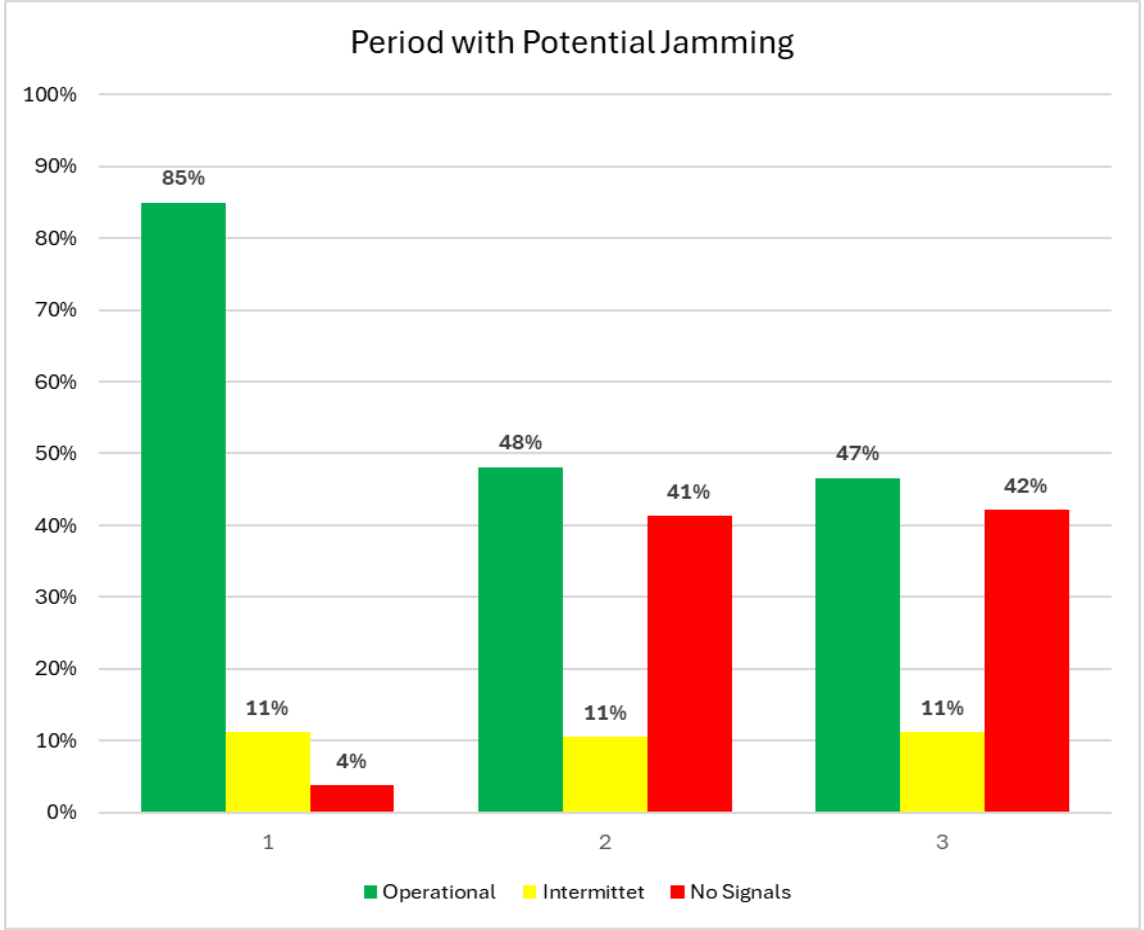




Performance Summary

CRPA vs Standard Antenna Performance





Conclusions

GNSS Cyber Security

- During recent times, the Geopolitical Situation in the world has led to increased geographical spread of Jamming and Spoofing.
- Primary aim in mitigation is to protect the GNSS receiver such that it receives usable GNSS Signals.
- A CRPA antenna is essential for this protection task.
- Fugro's SatGuard "Strict Mode" algorithms will protect against Spoofing.
- Extreme High-Power Jammers can still be a challenge.

Thank You

Questions ?

John Vint
Product Manager for Starfix Signals
Email: j.vint@fugro.com

FUGRO

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