



International
Association
of Oil & Gas
Producers

IOGP Technical Flash – INFO 51

GNSS Jamming and Spoofing – definitions, detection and defence

IOGP Webinar

23 September 2026

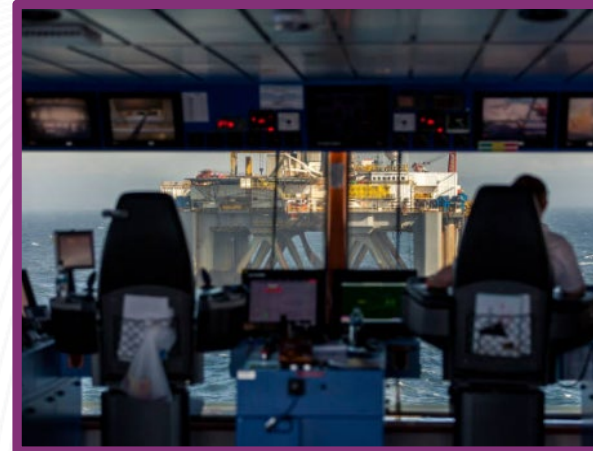
Walter Jardine, IOGP Vice Chair, Geomatics Committee

Elchin Teymurlu, Global Survey Technical Manager, bp



Agenda

1. Introduction to IOGP and the Geomatics Committee
2. Background & definitions: GNSS, jamming and spoofing
3. Defence & mitigation options
4. Case studies
5. Q&A and discussion



IOGP Geomatics Committee – who are we?



IOGP Contacts

Director:
Sajeev Menon

Managers:
Lucyna Kryla-Straszewska
Nicole Zhou

CHAIR
YEN PUASA



VICE-CHAIR
WALTER JARDINE

Independent

VICE-CHAIR
**SAIFUL NIZAM
B MUSTAFA**



VICE-CHAIR
**MONIKA
ZAKRZEWSKA**



5



SUBCOMMITTEES

- Geodesy
- Geo-Information
- Geophysical Operations
- Remote Sensing
- Surveying and Positioning

5



EXPERT GROUPS

- GeoRepository Support
- Drilling Hazard Site Survey Tech Notes Revision (DHSS)
- GIGS Support
- Seabed Survey Data Model Revision (SSDM)
- Global Navigation Satellite System Revision (GNSS)

5



PROJECT GROUPS

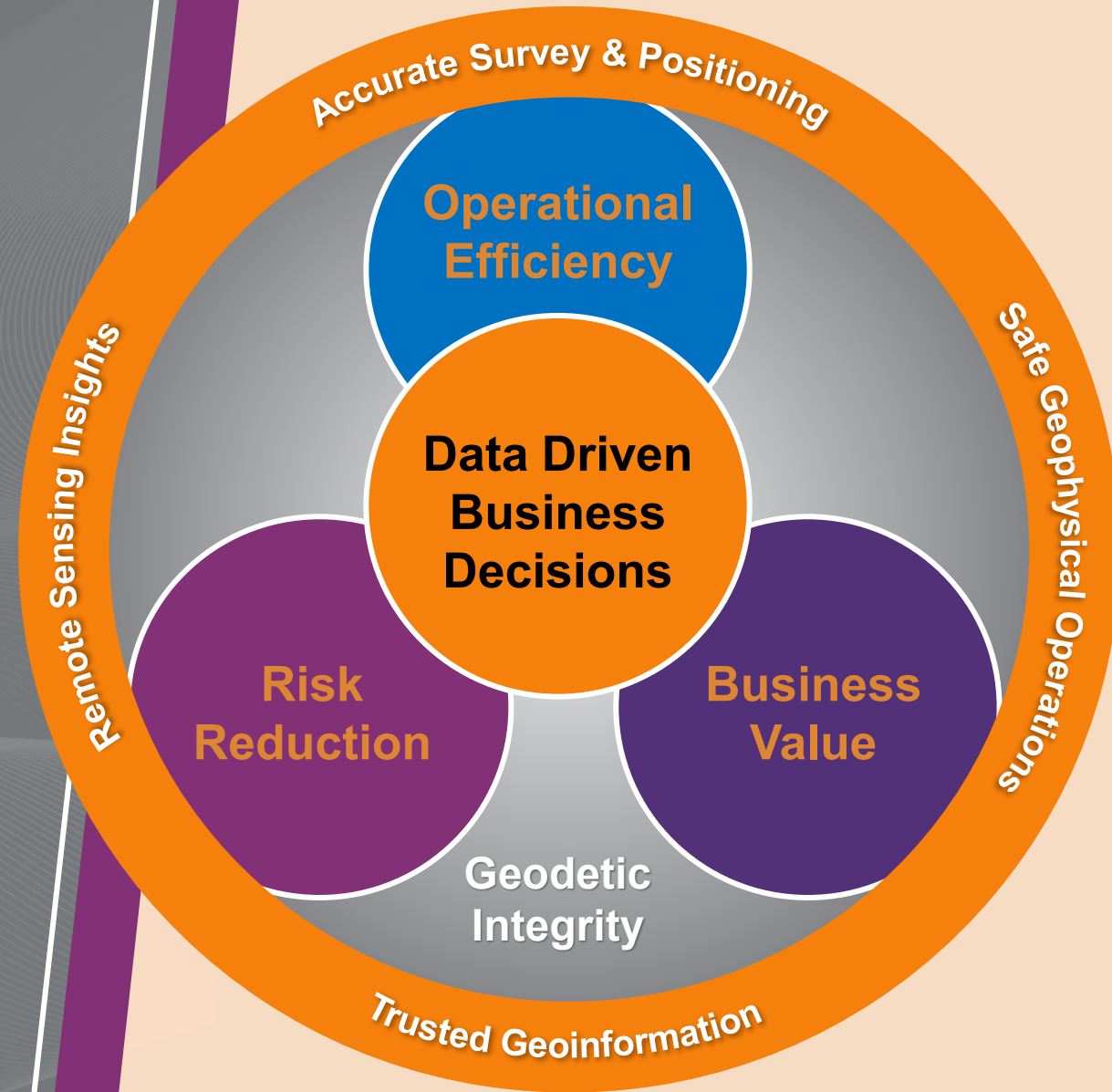
- 3D Point Clouds
- P formats Revision
- Remote Sensing Awareness
- Quality Control of Proposed Well Coordinates
- NATRF2022



International
Association
of Oil & Gas
Producers

The Geomatics Committee:

- Established in 2005 by the absorption into IOGP of the European Petroleum Survey Group (EPSG)
- We promote knowledge exchange
- We develop and drive good practices and sound geomatics principles for an efficient industry
- We engage with relevant stakeholders to identify and collaborate to solve common challenges related to geomatics activities
- We advocate the industry's position to address regulatory changes with geomatics activity implications





Technical Flash – GNSS interference, jamming and spoofing: definition, detection, and defence

IOGP Technical Flash



Phase	Recommended actions – selected and adjusted for environment and operations	Complexity	Interference	Jamming	Spoofing
Plan	Review risk level in area of operations. General GNSS status and jamming/spoofing hotspots can be checked using sites such as US Coastguard NAVCEN, NATO Shipping Centre, or GPSJAM website to check current status, risk areas, and recent incidents [see links further below].	Low		✓	✓
	Confirm anticipated external 'interference' sources (e.g., scintillation) or onboard 'interference' sources – e.g., multipath, signal leakage, proximal EMF signals, etc).	Low	✓		
	Breakdown operation, based on real-time positioning accuracy requirements for each phase, and investigate post-processing capabilities for data acquisition activities.	Low	✓	✓	✓
	Breakdown operation, based on navigation/positioning accuracy requirements, and create go/no go matrix that defines if activity can go ahead under certain levels of interference.	Medium	✓	✓	✓
	For higher risk areas, consider CRPA technology options to support identification and reduction/elimination of false GNSS signals, including tracking for encrypted authentication codes (NMA).	Medium		✓	✓
	For higher risk areas, consider closed coupled GNSS/INS systems.	Medium	✓	✓	✓
	For higher-risk areas, consider multi-constellation, multi-frequency GNSS, including signal-based protection and advanced digital filtering.	Low	✓	✓	✓
	Confirm suitable understanding of GNSS signals and minimal required experience for mobilized surveyors/dynamic positioning team.	Medium	✓	✓	✓
Some of these options, and others may be termed GAJT, collectively	Confirm suitable understanding and response for relevant personnel to cover GNSS interference incidents (natural and man-made) – consider requirements for scenario simulations, drills, etc.	Medium	✓	✓	✓

Do	Mobilize GNSS/GAJT systems as defined by planning process.	Medium	✓	✓	✓
	Monitor GNSS signal and system integrity – e.g., via reference and monitor stations and GNSS-supplier provided augmentation and NMA system.	Low	✓	✓	✓
	Monitor environmental factors.	Low	✓	✓	✓
	Monitor regional events.	Low	✓	✓	✓
	Use and manage relevant configuration/ antennas, etc., for required system accuracy, depending on operational task, as defined by planning process.	Low	✓	✓	✓
	If possible, monitor the heading at which disturbances are originating.	High	✓	✓	✓
	Fine tune the GNSS constellations, elevation masks, and frequencies used.	Low	✓	✓	✓
	Relocate GNSS antennas to set shields between disturbance source and hardware.	Medium	✓	✓	✓
	Where mobilized, switch to INS as primary system (for short periods only).	Low	✓	✓	✓
	Report jamming or spoofing issues to the US Coastguard Navigation Center (NAVCEN, at https://go.usa.gov/xQBaw or NATO Shipping Centre at https://shipping.nato.int/nscl).	Low		✓	✓
Learn	Rely on encrypted signals (OSNMA, e.g., Chimera).	Medium		✓	✓
	Segregate signal based on elevation and/or orientation.	High		✓	✓
	Apply digital filtering such as notch or band pass.	High		✓	✓
	When using CRPA antennas, apply space-time and space-frequency adaptive filtering.	High		✓	✓
	Where available, apply beam steering to increase power of real GNSS signals after beamforming.	High	✓	✓	✓



GNSS background – utilisation in the energy industry

Global Navigation Satellite Systems (GNSS), such as GPS, GLONASS, BEIDOU and Galileo, are critical to safe and efficient Oil & Gas operations, including :

- **marine and airborne navigation**, and **dynamic positioning** – tankers, PSVs, DSVs, FSVs, AHVs, DP rigs, construction & survey vessels, USVs etc. Fixed wing aircraft, helicopters, uncrewed aerial vehicles ('drones'). Indirectly it also affects subsea support systems such as ROVs and AUVs
- **vehicle tracking and navigation** – field vehicles, fleet systems (emergency response)
- land and marine **survey and positioning activities**
- **emergency response positioning and management** (common operating picture updates, response systems)
- **infrastructure and system time synchronization** (GPS time stamp accurate to 10^{-9} second) – data transfer, financials, network sync. etc.

GNSS incidents can have a critical impact on O&G operations, including:

- Safety risks to personnel and assets (e.g. marine vessel, aircraft or vehicle collision, drift or loss of control).
- Operational downtime & degraded performance (asset installation positioning, survey data acquisition, dynamic positioning (run-off / drive-off), time-based synchronization).
- Erosion of trust in GNSS-based systems and the need to strengthen operational resilience via e.g. redundancy and contingency plans.

GNSS signal background

- GNSS signals are transmitted from satellites ~20,000 km away, so by the time they reach Earth, they are **very weak**.



~-60 dBm

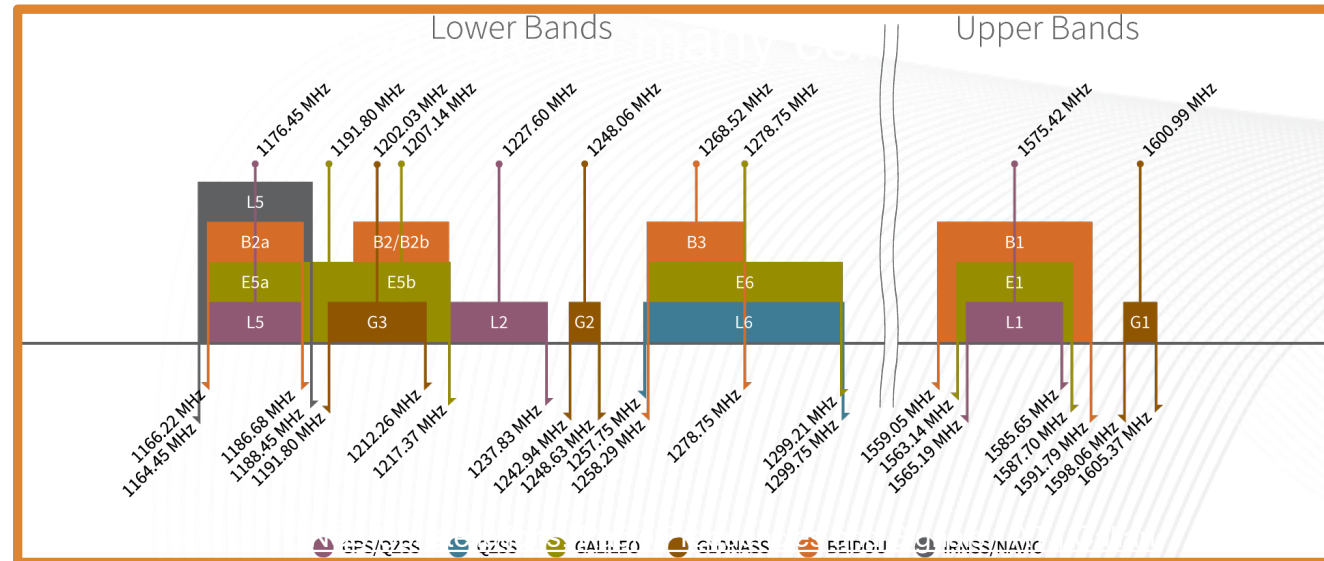


~-90 dBm



~-130 dBm

GNSS signal strength at receiver level 10^{-13} watts = 0.0000000000001 watts



GNSS interference definitions

Interference

Unintentional or accidental disturbances to GNSS signals
(from electronic equipment, radio transmitters or natural phenomena)



Degradation of carrier signal-to-noise ratio, loss of lock, positioning errors, and sporadic outages

Jamming

Deliberate emission of high-power signals on GNSS frequencies to disrupt reception



Partial or total loss of GNSS positioning, often without explicit system alerts. Impact zones may extend several kilometers.

Spoofing

Transmission of counterfeit GNSS signals to deceive the receiver about its position or time
Includes 'meaconing'



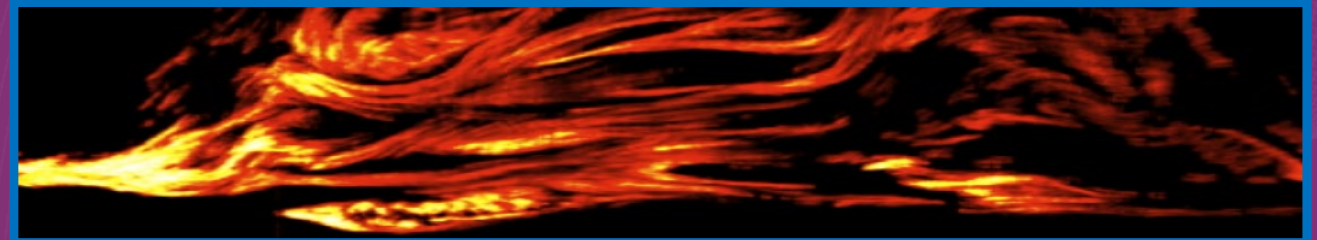
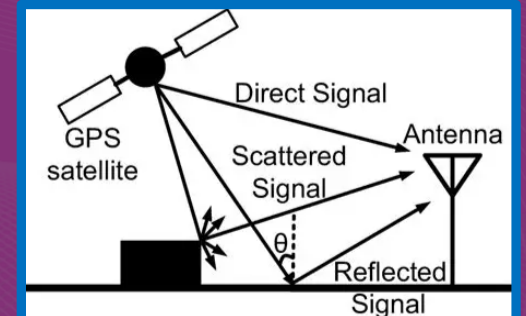
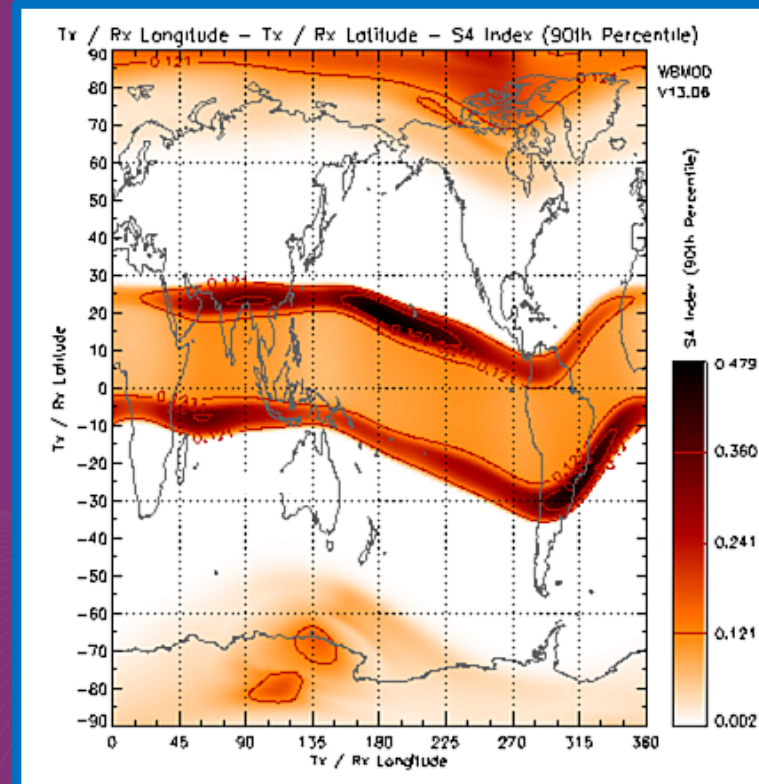
Erroneous position/time, gradual or abrupt drift, risk of undetected "silent failure". Spoofing can be precluded by a period of jamming.

Unintentional or natural interference can look very similar to jamming or spoofing

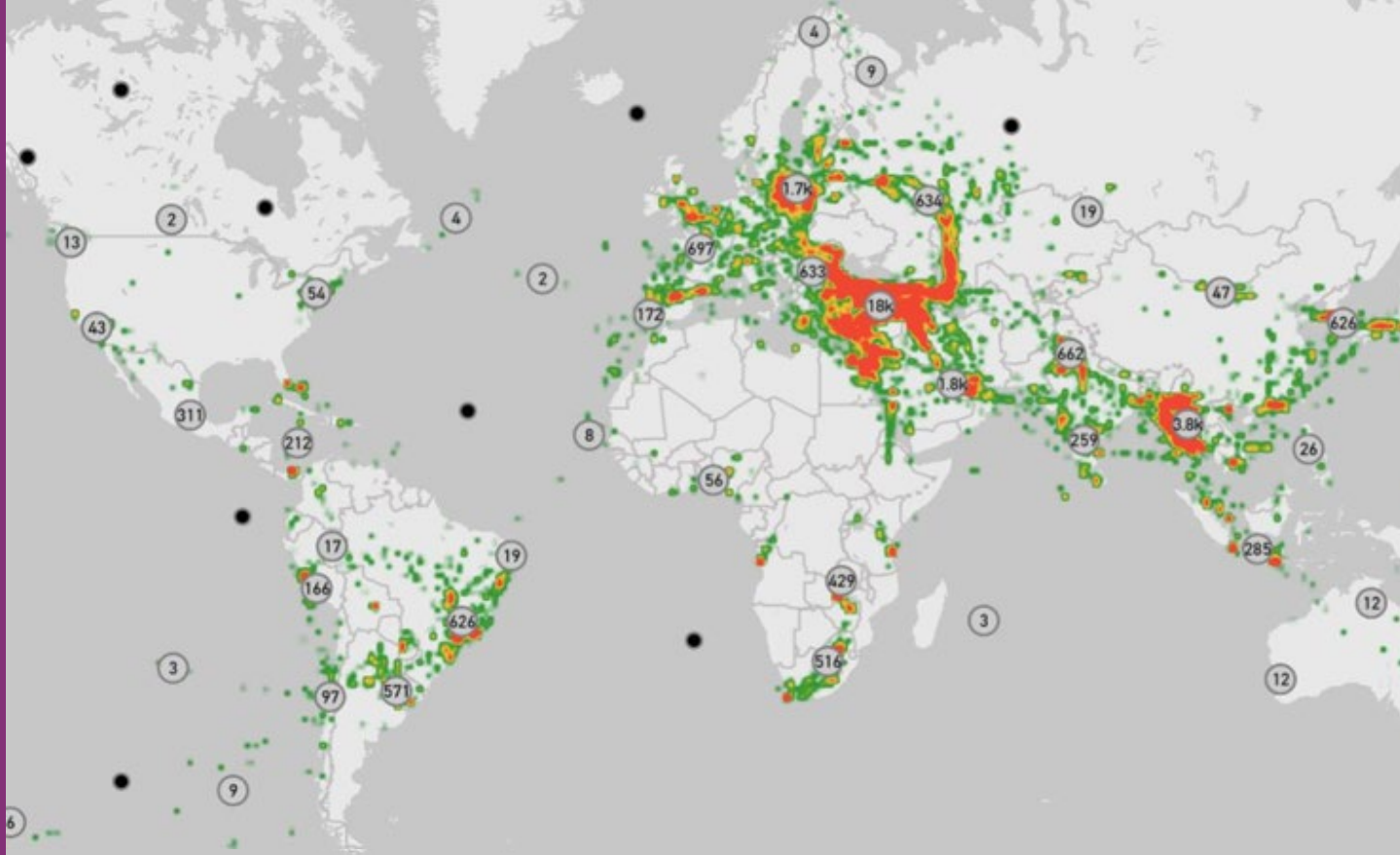
Scintillation, ray bending and multipath – not good for GNSS ☹

Natural or unintentional GNSS effect examples:

- **Scintillation** : rapid modification of radio-frequency signal phase and/or amplitude as the signal passes through ionosphere
- **Ray bending** : bending / delay of radio-frequency signal as it passes through the ionosphere / troposphere.
- **Multipath** : reception of delayed radio-frequency signal as it is reflected or scattered, typically by a hard / reflective surface near the antenna



Challenges and risks - GNSS 'interference' levels increasing

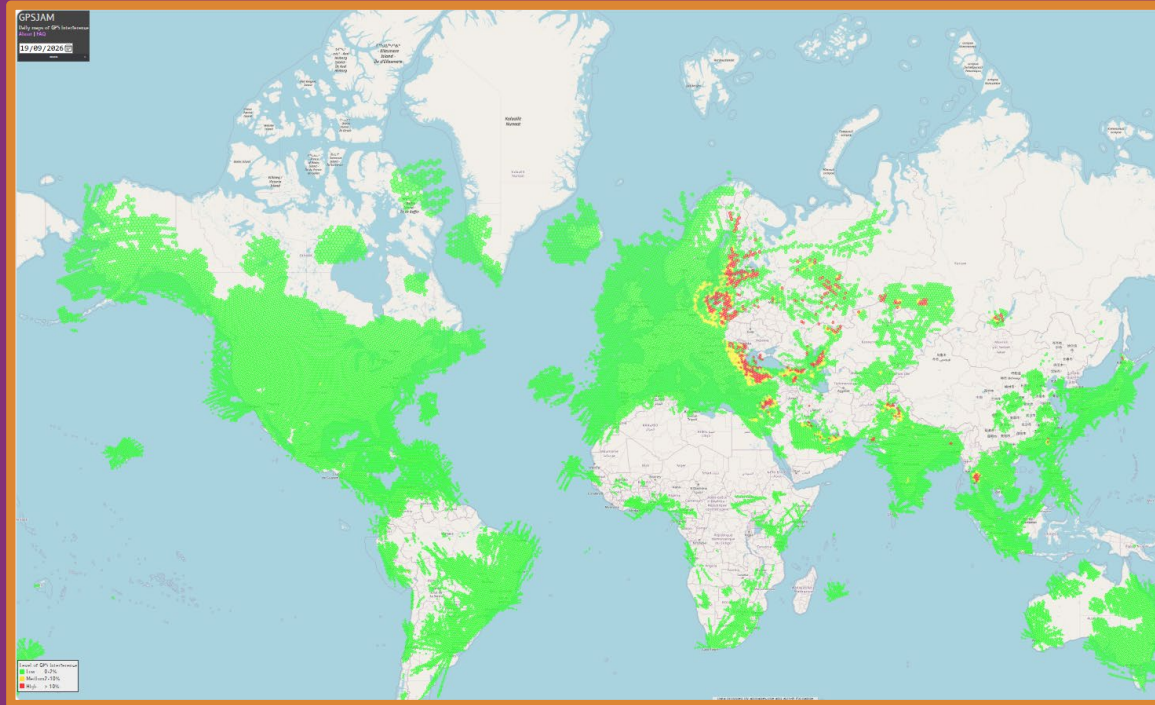


Threat evolution: the availability of portable jammers (Software Defined Radio (SDR) based “GPS jammers”) and open-source spoofing tools make GNSS attacks more accessible to ‘non-state actors’.

This increases the risk of intentional interference and also potentially accidental interference from faulty equipment, ‘cheap’ receivers or cables, poor cable runs (e.g. lack of electrical insulation) and connections etc.

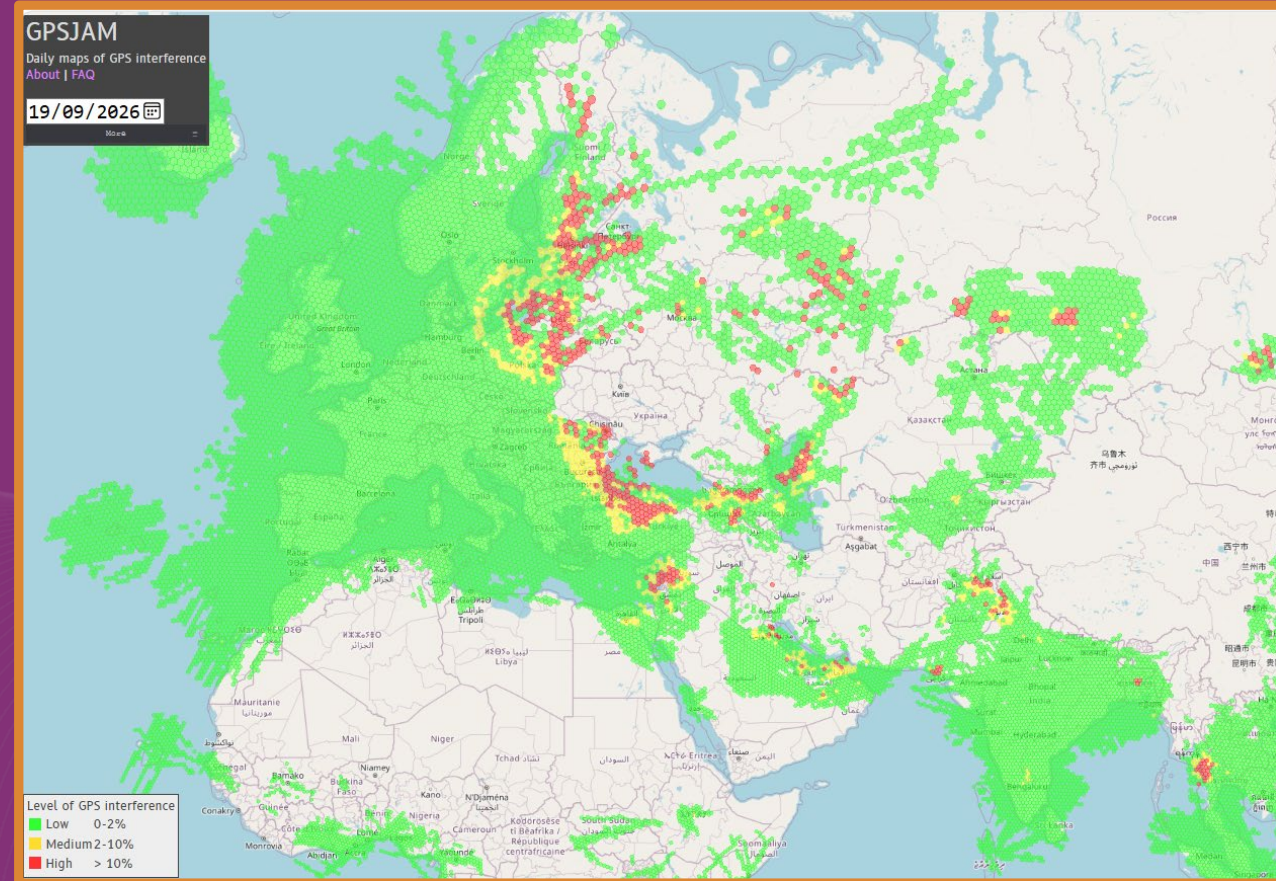
Recorded events 2022, 2023, 2024, 2025 (Jan – Jun)

Challenges and risks – GPS Interference Maps and Alerts



GPSJAM GPS/GNSS Interference Map

19 Sept 2026



Mitigation

- **Understand level of risk** in your operational area – both natural and man-made. Incorporate into RA processes
- **Define positional accuracy requirements** for each task and options if/when positioning is degraded
- **Seek professional advice** – e.g. from internal Geomatics Team and/or Survey & Positioning, GNSS solution, Marine or Dynamic Positioning suppliers
- **Utilise competent suppliers** – marine, aviation, survey & positioning, GNSS services that understand:
 - antenna system – type, location/s & installation. Cabling and cable run integrity etc.
 - receiver system – type, dual / multi-frequency, channels etc.
 - redundancy – multi-constellation, dual / tertiary GNSS options
 - online GNSS signal monitoring and alarms
 - integrated and backup positioning system options:
 - Inertial Navigation Systems, Doppler Velocity Log, Attitude and Heading Reference Systems, independent GNSS solutions. backup acoustic positioning systems
 - **GNSS Anti-Jamming Technology (GAJT) options** – controlled reception pattern antennas (CRPA), beam-steering, null-forming antennas, encryption, notch and band pass filtering, Navigation Message Authentication etc
- **Report incidents** e.g. US Coastguard Navigation Center (NAVCEN), NATO Shipping Centre, positioning supplier



Information sources:

- GNSS service suppliers
- GNSS equipment suppliers
- Trade bodies - IOGP & IMCA technical flashes
- Institutes & Authorities: RIN, RICS, EASA, IATA, FAA
- Online services: GPSJam, Flightradar, GPS World etc



Information Note

IN 1436 – GNSS interference, jamming and spoofing

Information Note Published on 10 April 2019

1. Introduction

This Information Note provides a brief overview of global navigation satellite system (GNSS) interference, jamming and spoofing.

- **Interference** is the unintentional transmission of signals stopping the reception of the GNSS signals.
- **Jamming** is the intentional interference of the GNSS signal reception to deny the receiver GNSS signals.
- **Spoofing** is the practice of tricking a GNSS receiver into reporting an incorrect position or time.

2. Interference

In general, technical issues with the GNSS receivers themselves or the associated cabling are likely to be a causal factor in the majority of problems caused by interference. Antennas may be faulty, or there may be a failure in the shielding or the continuity of the cabling, or there could be water ingress causing electrical leakage. Cables can sometimes themselves act as antennas, with unpredictable consequences. Symptoms may be intermittent and thus difficult for engineers to isolate and fix.

Interference might also be caused by other, stronger radio frequency transmissions on similar frequencies such as microwave data links, radars, and satellite communications systems.

3. Jamming

The signals used by GNSS equipment are in general very weak radio signals. Jamming relies on stronger transmission on the same frequencies as GNSS, in order to drown the relatively weak GNSS signals. The technology to jam GNSS signals over short distances is widely available to anyone at relatively modest cost. To jam GNSS signals over longer distances (that is, greater than line of sight), requires more sophisticated and more easily detectable equipment.

4. Spoofing

Unlike jamming a GNSS signal, which involves swamping existing weak signals, spoofing involves deliberately superimposing real signal data with false data and tricking a GNSS receiver into reporting an incorrect position or time. The spoofing attack will broadcast signals with the same structure and frequency as GNSS

IMCA Contact:



Richard Purser
Technical Advisor – Marine



Jennifer Evans
Technical Advisor – Marine



Roger Moore
Technical Advisor – ROV

Original IMCA author:



Nicholas Hough
Consultant – Safety & Security

Committees:

Marine – DP (Dynamic Positioning)

Offshore Survey

Topic:

#Marine



IMPACTS OF GNSS INTERFERENCE ON MARITIME SAFETY

A special report by the RIN Maritime GNSS Interference Working Group

Digital Report Published January 2026

ROYAL INSTITUTE OF NAVIGATION

The RIN Maritime Report v1.2



Type search term

Find a member About RICS Contact

Profession & Standards Regulation Get Involved Careers Training & Events News & Insight Dispute Resolution Service Candidates & Assessment

Home > News & Insights > GNSS Spoofing and mitigation in the Arabian Gulf



News and insight

GNSS Spoofing and mitigation in the Arabian Gulf

26 March 2026

Geospatial Professional Practice Update & Latest Regional Developments (as of March 24th 2026)

By RICS Geospatial Expert Group



International Association of Oil & Gas Producers

INFO SHEET
INFO51

MARCH
2026



Technical Flash – GNSS interference, jamming and spoofing: definition, detection, and defence

Phase	Recommended actions – selected and adjusted for environment and operations	Complexity	Interference	Jamming	Spoofing
Plan	Review risk level in area of operations. General GNSS status and jamming/spoofing hotspots can be checked using sites such as US Coastguard NAVCEN, NATO Shipping Centre, or GPSJAM website to check current status, risk areas, and recent incidents (see links further below).	Low		✓	✓
	Confirm anticipated external 'interference' sources (e.g., scintillation) or onboard 'interference' sources – e.g., multipath, signal leakage, proximal EMF signals, etc).	Low	✓		
Some of these options, and others may be termed GAJT, collectively	Breakdown operation, based on real-time positioning accuracy requirements for each phase, and investigate post-processing capabilities for data acquisition activities.	Low	✓	✓	✓
	Breakdown operation, based on navigation/positioning accuracy requirements, and create go/no go matrix that defines if activity can go ahead under certain levels of interference.	Medium	✓	✓	✓
	For higher risk areas, consider CRPA technology options to support identification and reduction/elimination of false GNSS signals, including tracking for encrypted authentication codes (NMA).	Medium		✓	✓
	For higher risk areas, consider closed coupled GNSS/INS systems.	Medium	✓	✓	✓
	For higher-risk areas, consider multi-constellation, multi-frequency GNSS, including signal-based protection and advanced digital filtering.	Low	✓	✓	✓
	Confirm suitable understanding of GNSS signals and minimal required experience for mobilized surveyors/dynamic positioning team.	Medium	✓	✓	✓
	Confirm suitable understanding and response for relevant personnel to cover GNSS interference incidents (natural and man-made) – consider requirements for scenario simulations, drills, etc.	Medium	✓	✓	✓

<https://www.imca-int.com/resources/technical-library/>



International Association of Oil & Gas Producers

GNSS Spoofing and mitigation in the Arabian Gulf

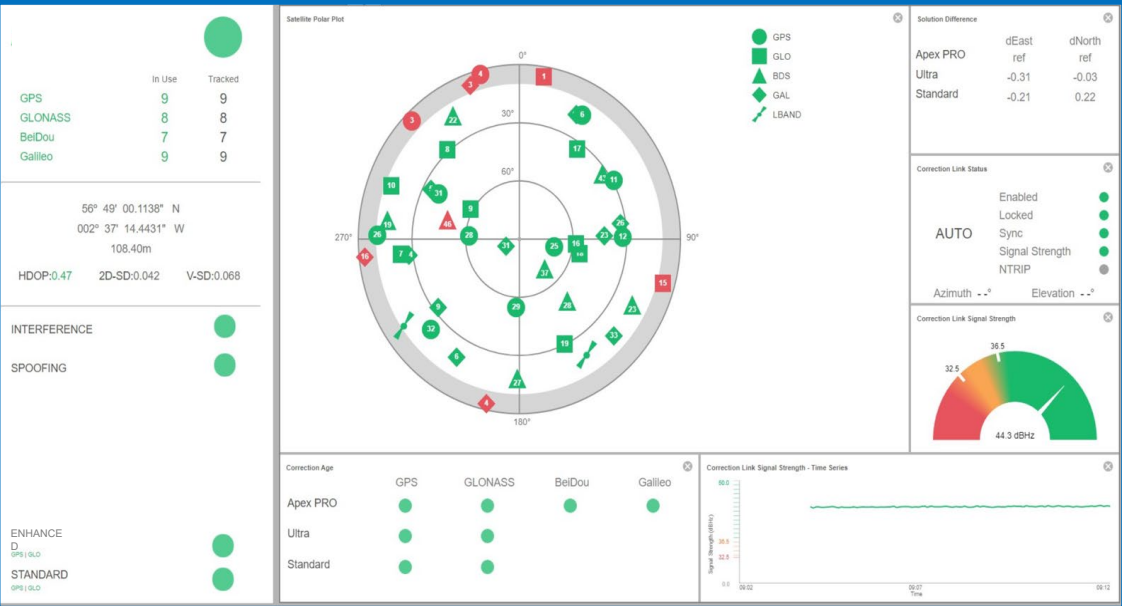
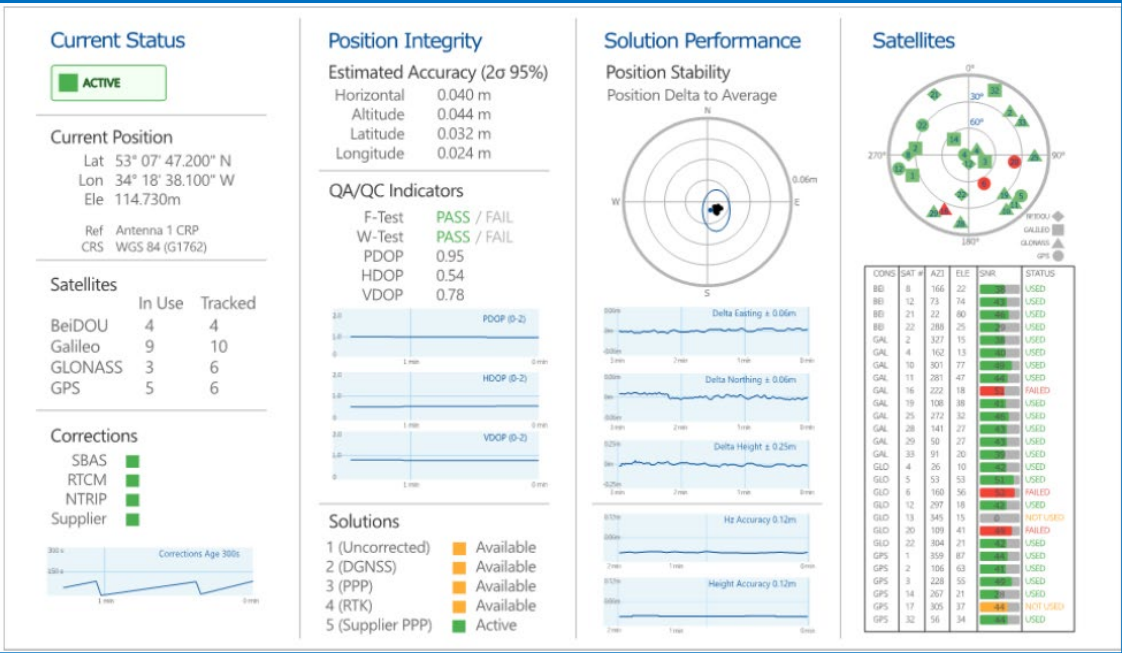
Online system monitoring

Professional survey & positioning and GNSS suppliers should provide high-quality live system monitoring software – both onboard the vessel, and via their own independent GNSS monitoring or reference stations

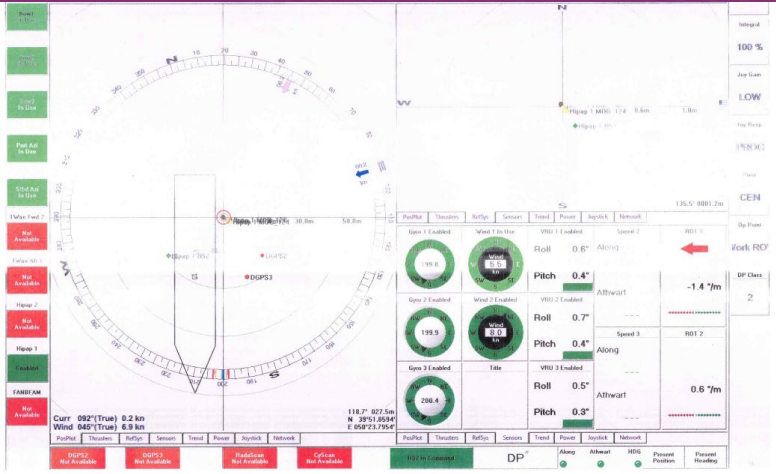
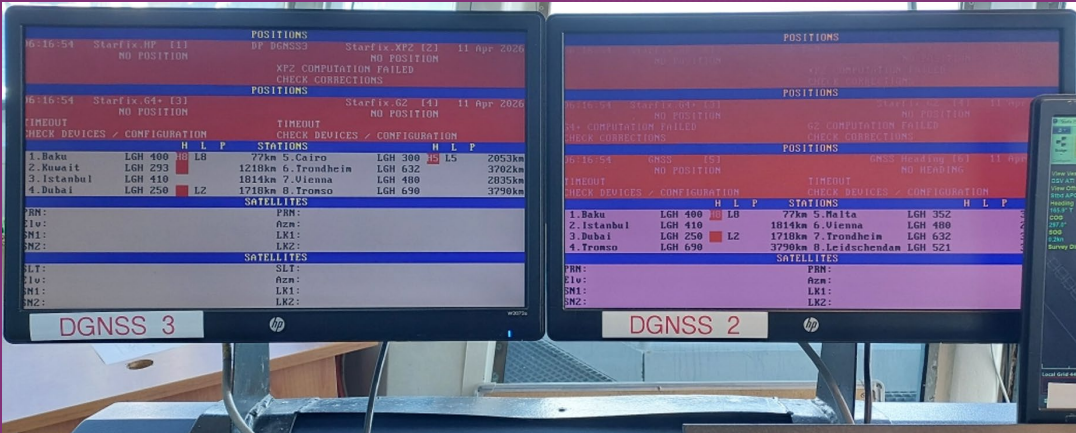
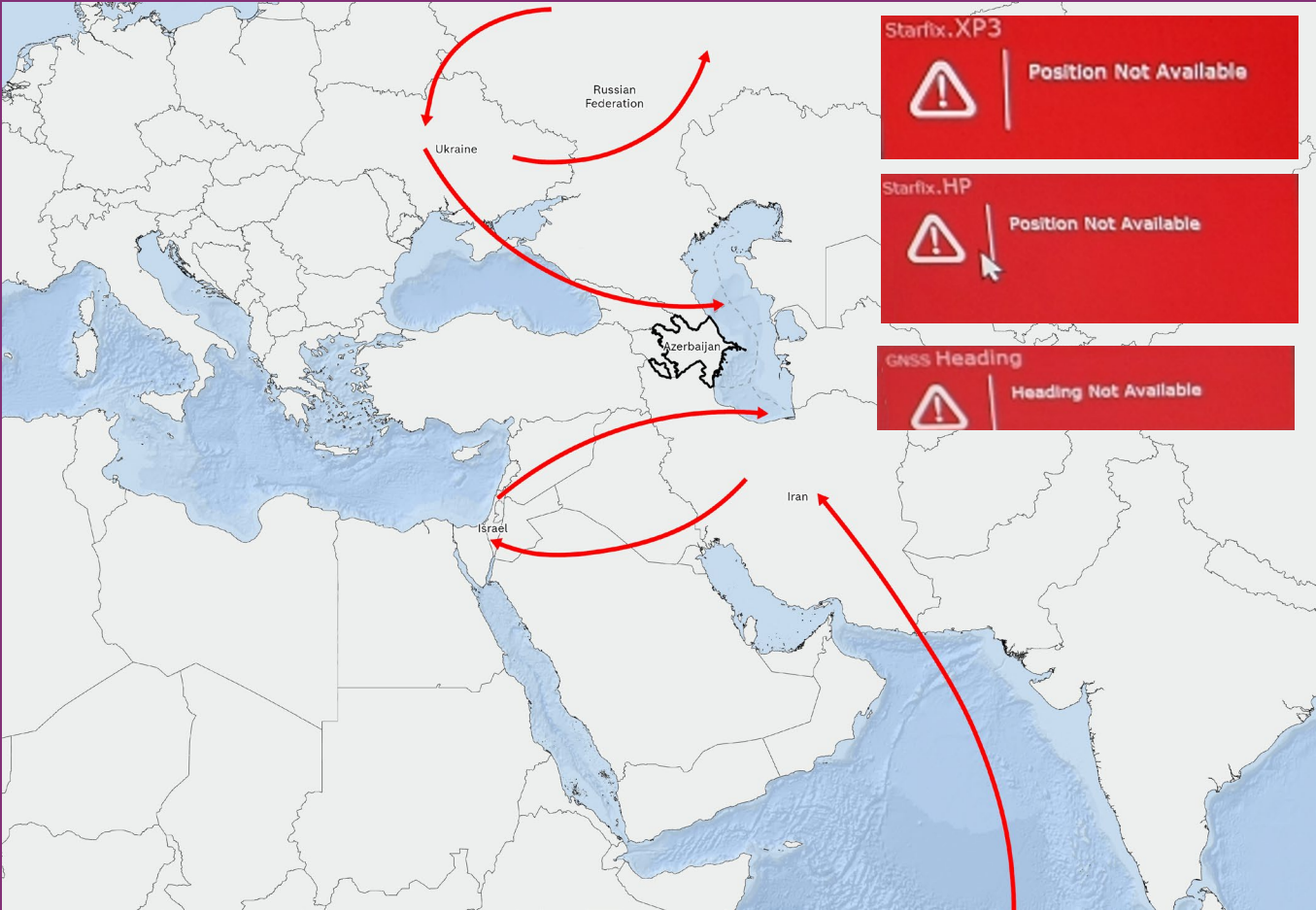
Navigation Message Authentication – NMAs

Galileo OSNMA (Open Service Navigation Message Authentication):

Designed to provide users with a means to verify the integrity and authenticity of received Galileo navigation data



Case study 1: Caspian Sea



Case study 1: Caspian Sea

Sent: Saturday, April 11, 2026 10:46 AM
Subject: Unstable DGPS signal

Good morning,

I would like to inform you that today, over the past hour, we've encountered another problem with GPS instability. The signal is extremely unstable and at times disappears completely. I'd like to add that not only the ship's GPS, but also the GPS used by survey team is also losing signal. We've tried altered the vessel's course several times, but the result is the same. Please find attached images and print screens. Please note that until the signal is restored and stable, we will be unable to continue operations, as the vessel is currently in the open sea over underwater assets. We are unable to use alternative reference systems, and are solely relying on DGPS and HIPAP. Please assist us in resolving this issue.

I will keep you updated.

02:26	02:34	00:08		Survey and Vessel report DGPS lost
-------	-------	-------	--	------------------------------------

09:19	11:25	02:06		Survey and Vessel report DGPS lost
-------	-------	-------	--	------------------------------------

Time (AZT)	Event	1 September 2025
04:08	Survey team observed unstable GNSS signals. Investigation with nearby vessels suggested GPS/GNSS jamming .	
04:10	Rig move operations stopped.	
04:10 – 07:25	Rig move on standby awaiting GNSS recovery.	
07:25	GNSS signal returned. Positioning systems on rig and AHTs back online.	
08:00 – 09:55	Tug Management System (TMS) synchronization issues caused by GNSS outage were troubleshoot and resolved	

Persistent discrepancies (up to 1.5m) and instability in the Seastar GNSS system experienced on rig. Contractor suspects jamming during the 8 November military parade.

Time (AZT)	Event	2 September 2025
02:25	Survey team detected unstable GNSS signal. GPS/GNSS believed jammed.	
02:26	Rig move operations stopped.	
02:26 – 05:40	Standby awaiting GNSS recovery.	
05:40	Management discussion held; decision made to continue limited activities.	
09:10	GNSS fully restored and positioning systems back online.	
09:10 – 11:48	TMS synchronization issues resolved.	

Case study 2: Eastern Mediterranean pipelay operations

Date	Time	DGPS#1 Anti-jam antenna A	DGPS#2 Anti-jam antenna B	DGPS#3 Anti-jam antenna C	DGPS#4 Anti-jam antenna D	DGPS#5 Standard antenna	Comment
8th May	10:36			X	X	X	DGPS# 3,4,5 Drop Out
	12:00						DGPS# 3,4,5 Back in
	13:17	X	X	X	X	X	All GPS Drop out
	15:15						Positions improving, converging
	18:10						All GPS Back in
	23:33				X		Veripos 1 Lost
9th May	22:50						Veripos 1 Back
	17:01				X		DGPS# 3,4,5 Drop Out
	17:30			X	X	X	DGPS# 3,4,5 Drop Out
	21:39	X	X	X	X	X	Not recorded when all back in
10th May	21:45						All DGPS out, RDV to sit on seabed
	10:12	X	X	X	X	X	All DGPS back in
	10:15		X	X		X	All GPS Drop out
11th May	10:35						DGPS#1 and 4 Back in
	14:00		X	X			All DGPS back in
	14:01						DGPS# 2,3 Drop Out
	14:20	X	X	X	X	X	DGPS# 2,3 Back in
	14:25	X	X	X	X	X	All GPS Drop out
	14:29			X			DGPS 1,2,3,4 Improving, DGPS# 2 No data
	14:31	X	X	X	X	X	DGPS# 2 Back in
	14:43	X	X	X	X	X	DGPS#1,2,4,5 Back in Converging, DGPS#3 No Data
	14:45	X	X	X	X	X	All GPS Drop out
	15:20						DGPS 1,2,4,5 Improving, DGPS# 3 No data
	20:20	X	X	X	X	X	All DGPS back in
	20:27						All GPS Drop Out
	20:27					X	DGPS 1 to 4 Back
	20:27						DGPS 2 Not Working
12th May	06:40		X				DGPS# 2 Drop Out
	06:47						DGPS# 2 Back In
	07:50		X				DGPS# 2 Drop Out
	20:14	X				X	DGPS# 1,5 Drop Out
	20:45	X	X	X		X	DGPS# 1,2,3,5 Drop Out
	21:50	X				X	DGPS# 1,5 Converging
	22:19						All DGPS back in

Date	Time	DGPS#1 Anti-jam antenna A	DGPS#2 Anti-jam antenna B	DGPS#3 Anti-jam antenna C	DGPS#4 Anti-jam antenna D	DGPS#5 Standard antenna	Comment
13th May	10:08			X			DGPS# 3 Drop Out
	11:51		X				DGPS# 3 Back In, GPS#2 Drop Out
14th May	08:40					X	DGPS# 5 Drop Out
	05:25		X	X			DGPS# 2,3 Drop Out
	05:48		X	X	X		DGPS# 2,3,4 Drop Out
	07:20						All DGPS back in
	10:34			X			DGPS# 3 Drop Out
	11:59						All DGPS back in
	14:02	X					DGPS# 1 Drop Out
	14:10	X					DGPS# 1 Converging
15th May							
16th May	13:55	X					DGPS# 1 Drop Out
	15:48	X	X	X	X	X	All GPS Drop Out
	15:53	X	X	X	X	X	All DGPS back in but converging
	16:24						All DGPS back in
	22:50	X				X	DGPS# 1,5 Drop Out
17th May	03:48					X	DGPS# 5 Drop Out
18th May	11:35	X					DGPS# 1 Drop Out
	11:40						All DGPS back in
19th May	05:52		X	X			DGPS# 2,3, Drop Out
	05:55	X	X	X		X	DGPS# 1,2,3,5 Drop Out
	06:02						DGPS# 5 Back in
	06:07						All DGPS back in
	07:06		X	X			DGPS# 2,3, Drop Out
	07:14						All DGPS back in
	10:55		X	X			DGPS# 2,3, Drop Out
	10:59						All DGPS back in
	13:02		X				DGPS# 2 Drop Out
	13:10		X	X			DGPS# 2,3, Drop Out
	13:36						All DGPS back in
20th May	14:03		X	X			DGPS# 2,3, Drop Out
	16:10		X	X			DGPS# 2,3, Drop Out
	19:00			X		X	DGPS# 3,5 Drop Out
	19:05						All DGPS back in
	05:40	X	X	X		X	DGPS# 1,2,3,4 Drop Out
	05:56						All DGPS back in

Case study 2: mitigation details

Situation:

- DP pipelay vessel GNSS drop-out during pre-lay – all GNSS positions lost for mins to hours on multiple occasions over several days (see example).
- Issued traced to ‘security jamming’ from nearby FPSO. Downtime amounted to >30 hours over 60-day full operational period (~2.1% of project time)
- Pipelay vessel has INS aided USBL acoustic position reference system option (PRS) but water depth too deep for extended and accurate DP operations. INS aiding does allow short / low risk DP operations using acoustic PRS (USBL on own not suitable as DP reference)
- Once pipelay starts – no realistic option to stop the operation, so any GNSS jamming risk has to be fully mitigated before commencing pipelay

Mitigation:

- Upgraded GAJT GNSS antenna and additional differential correction systems were pre-installed (quicker recovery period) due to known risk
- Pipelay ‘critical periods’ to be monitored closely. DP alert system to be activated according to status
- USBL transponders installed at route critical points – additional PRS if necessary, over short periods
- Use ROV ‘garage’ with USBL transponder positioned under vessel – if DGNSS is lost, transponder released and DP switches to acoustic PRS. Drills conducted to test suitability – switch over timing and acoustic footprint acceptable for short periods
- Longer layback to be implemented during non-critical lay periods – allows more lateral vessel movement
- Acoustic PRS implemented during pipelay stationary operations (e.g. tie-in)
- Where DP loses all GNSS PRS, and system reverts to ‘model control’, closer monitoring of exit angle of pipe and layback distance (using ROV)



For more information please contact:

Lucyna Kryla-Straszewska, ls@iogp.org
Principle Manager – Digital and Geomatics

Nicole Zhou, nzh@iogp.org
Manager – Geomatics

Credits and sources:

1. iStock images (slides 1, 2, 5, 6 and 10)
2. IATA GNSS RF Interference Safety Risk Assessment – map series (slide 11)
<https://ic.iata.org>
3. GPSJam data (slide 12):
<https://gpsjam.org>
4. Royal Institute of Navigation (slide 14):
https://cdn.ymaws.com/rin.org.uk/resource/resmgr/maritime_report/the_rin_maritime_report_v1.2.pdf
5. Royal Institute of Chartered Surveyors (slide 14):
<https://www.rics.org/news-insights/gnss-spoofing-and-mitigation-in-the-arabian-gulf>
6. International Marine Contractor's Association (slide 14):
<https://www.imca-int.com/resources/technical-library/>

IOGP Headquarters

www.iogp.org

3 Moorgate Place
London EC2R 6EA
United Kingdom
T: +44 20 4570 6879
E: reception@iogp.org

IOGP Europe

www.iogpeurope.org

Avenue de Tervueren 188A
B-1150 Brussels
Belgium
T: +32 2 882 16 53
E: reception-europe@iogp.org