# GNSS: Mitigating the Threats of Interference, Jamming & Spoofing

Eddie Milne, Technical Manager

30, May, 2018

HEXAGON
POSITIONING INTELLIGENCE

veripos

# Agenda

1

## Introduction and Overview

Overview of interference, jamming and spoofing and their effects on GNSS reliability and accuracy

2

## Real World Examples

Real world examples showing the impact of GNSS denial

3

## Mitigation

Exploring how to mitigate the threats by looking at the technology available

# Introduction and Overview

Overview of interference, jamming and spoofing and their effects on GNSS reliability and accuracy

HEXAGON
POSITIONING INTELLIGENCE

veripos

# Terminology

- Interference - is the unintentional transmission of signals stopping the reception of the GNSS signals. Can be In-band or Out-Band interference.
- 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.

# Interference - In-band

- Typically caused by GNSS receivers themselves!
- Re-radiate the local oscillator from the receiver
  - Faulty antenna
  - Breakdown in shielding of coaxial cable
- Continuity lost between antenna and receiver
- Coaxial cable acts as antenna for local oscillator
  - Picked up by other GNSS receivers causing loss of lock
- Can be caused by
  - Water ingress and corrosion
  - In-correctly terminated cables
- Symptoms can be intermittent

# Interference - In-band Systems

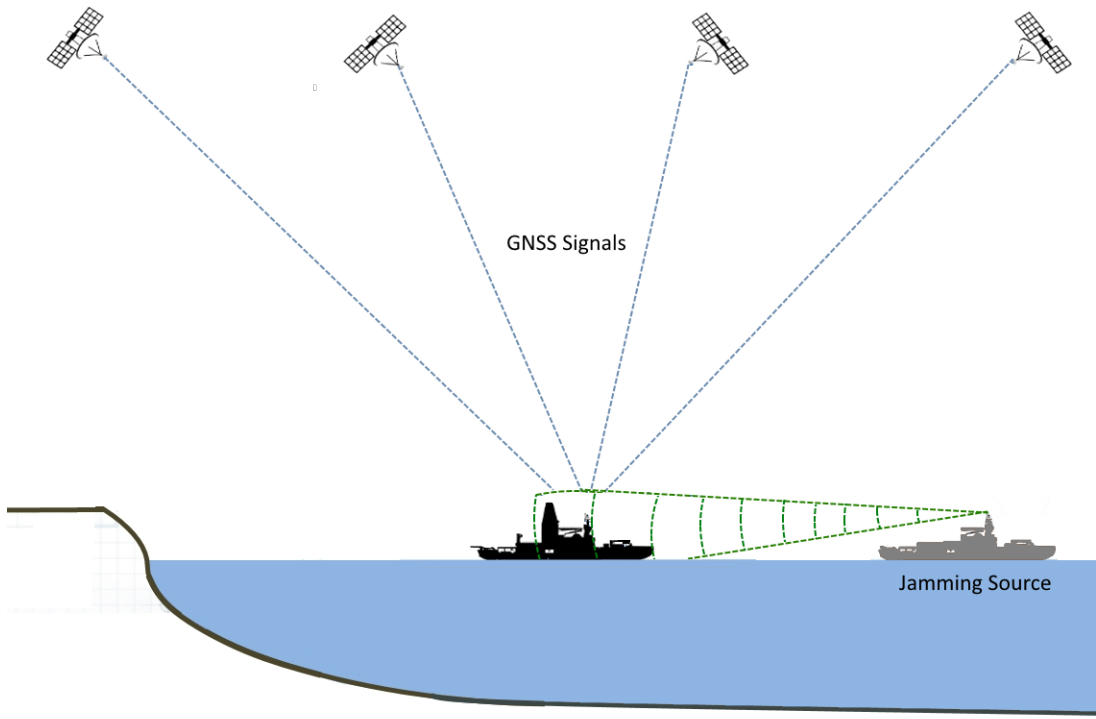
- General navigation receivers
  - Ships GMDSS equipment e.g. Furuno, Thrane & Thrane, Leica, JRC etc.
- Communications domes using GNSS receivers for orientation
  - Inmarsat, (B, C and BGAN) from Thrane & Thrane, NERA and Furuno etc., KU and C Band V-Sat, and TV systems from Caprock, Schlumberger-DMS etc.
- Doppler speed logs such as SatLog etc.
- Automatic Identification Systems (AIS)
- GPS Heading Sensors
- Plotter systems or ECDIS with integrated GNSS
- High Accuracy commercial augmentation services
- GNSS receivers integrated into a vessel DP system
- Survey & seismic receivers inc. Heading Sensors and Tailbuoy Tracking
- Precision timing equipment used to time survey systems

# Interference - Out-band

- Interferer outside GNSS band cause interference
- Typically a stronger signal swamps the antenna & drives the antenna LNA into saturation thus blocking the GNSS signals
- This can be cause by several devices:
  - Microwave data links
  - Radar systems
  - TV antenna amplifiers or transmitters
  - Communications Systems
  - Telemetry Systems (data or video)
- Systematically test systems to find cause of interference (or change vessel heading)

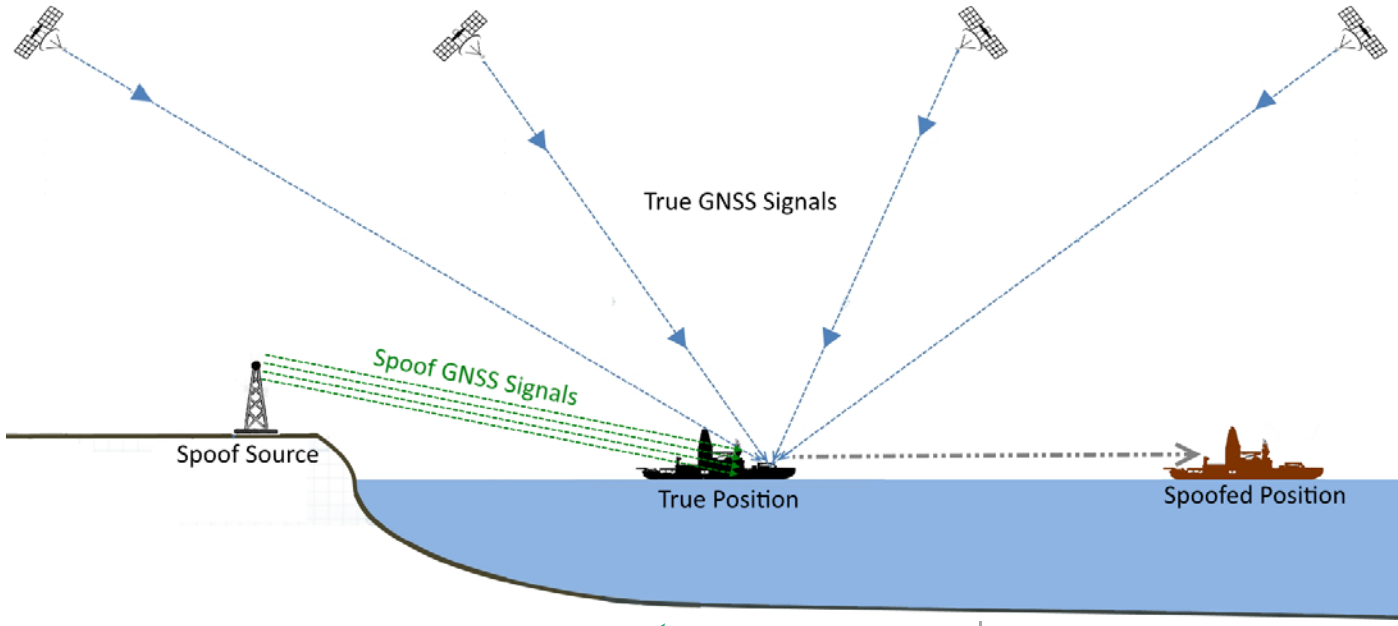
# Jamming

- Intentional jamming of GNSS signals
- Technology commercially available to anyone
- Generally In-band Interference
- Effective range depends on power of transmitter
  - Range from metres to kilometres
- Can be Land, Sea or Air based



# Spoofing

- Using false GNSS signal to supplant real GNSS signal
- Attacker broadcasts signals with same structure and frequency as GNSS signals
- The spoofed message is changed so receiver calculates incorrect position or time
- Spoofing GNSS signals is complicated and requires sophisticated equipment




HEXAGON
POSITIONING INTELLIGENCE

veripos

# Real World Examples

Real world examples showing the impact of GNSS denial

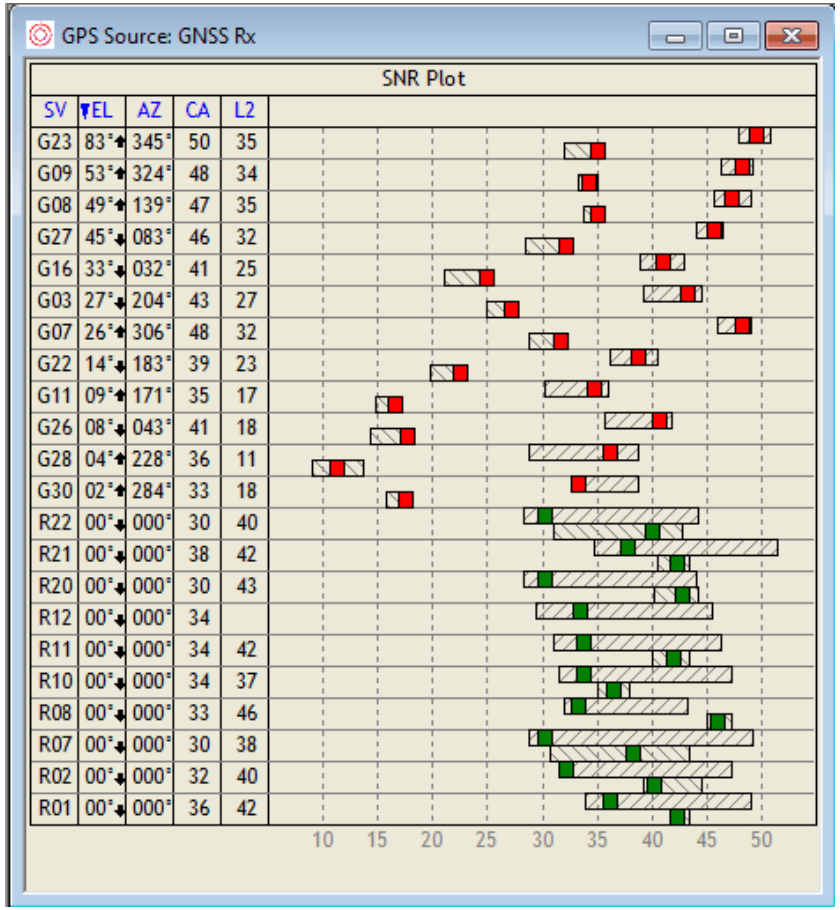
=

HEXAGON
POSITIONING INTELLIGENCE

veripos

# Unintentional In-Band Interference - August 2017

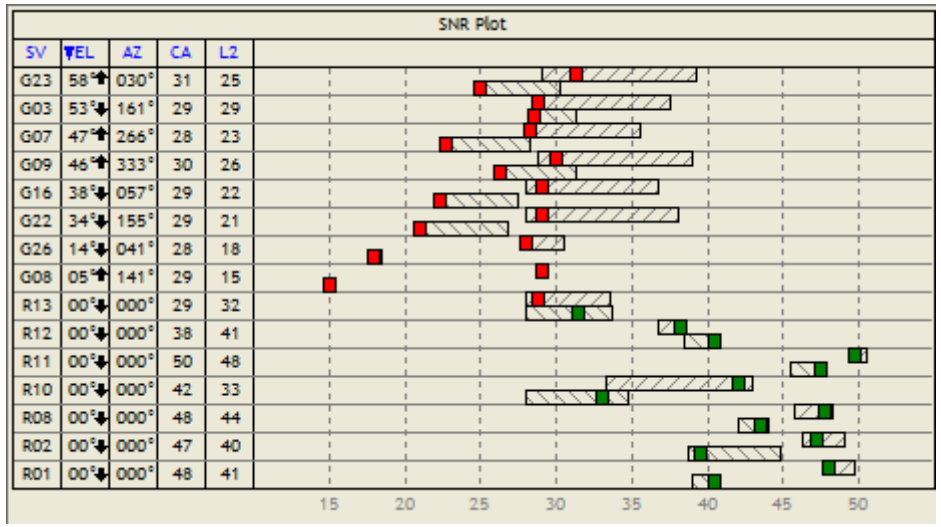
- Incident 24th August 2017
- All GNSS Systems onboard vessel lost positioning - **Except 1?**
  - “GPS1, GPS2 and GPS4 dropped Out.  GPS3 did not drop out. GPS1 was off only momentarily.  GPS2 and GPS4 were in and out for about 1 hour.  Satellites would be in and out.”
- When issue recurred shutdown working system and other systems recovered.
- Issue found to be triggered by faulty inline connector causing GNSS re-radiation




HEXAGON POSITIONING INTELLIGENCE | veripos

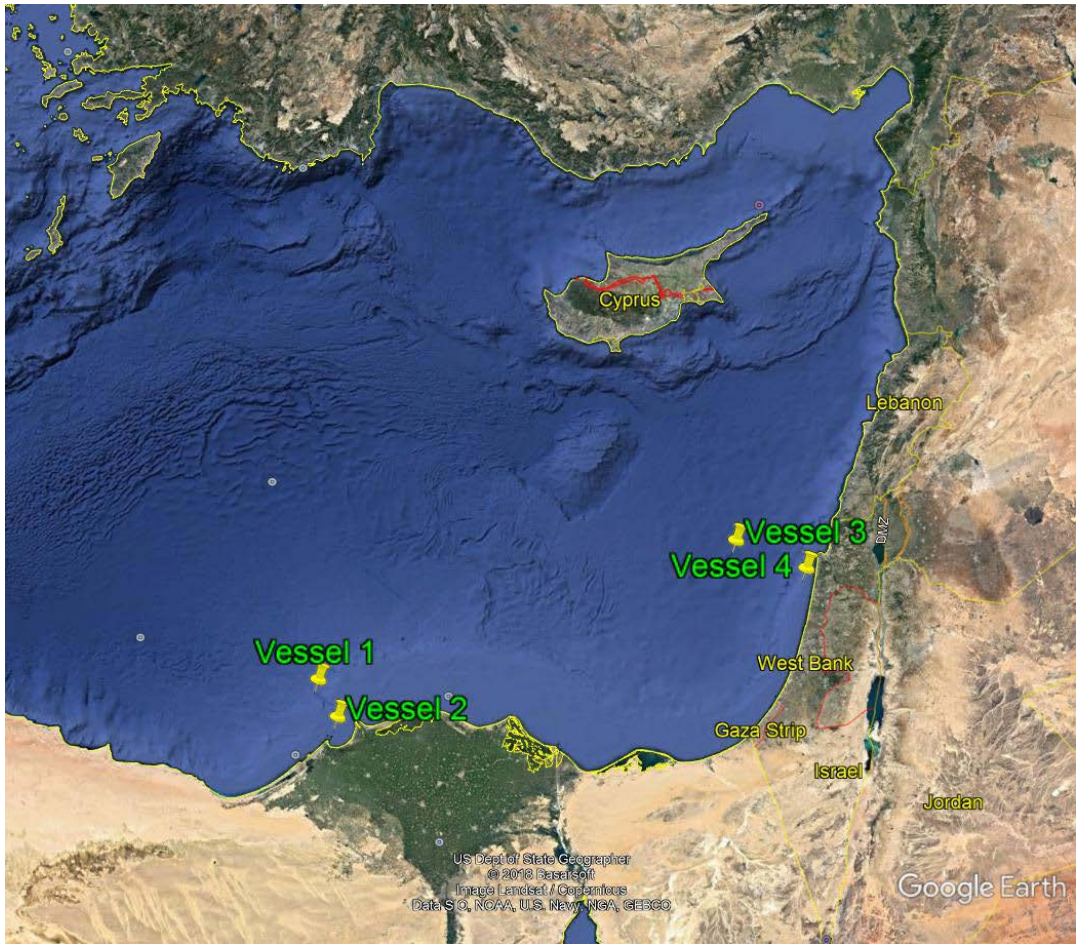
# Suspect Jamming - October 2016

- Incident Persian Gulf 26th October 2016
- 6 vessels reported issue with Positioning
- 40Km Range
- Lasted approximately 30 minutes and returned 16 hours later
- All GPS signals lost on all systems
- Source Unknown



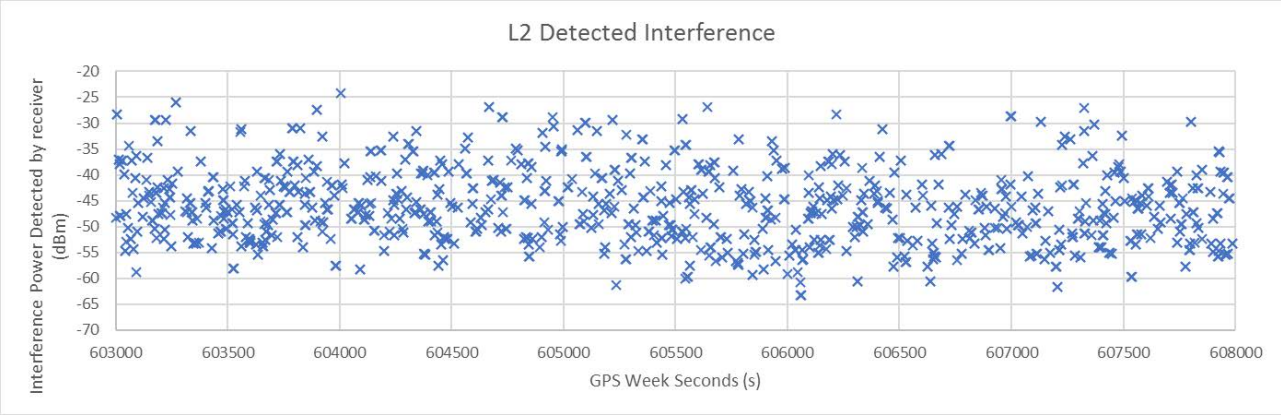

# Suspect Jamming - Ongoing

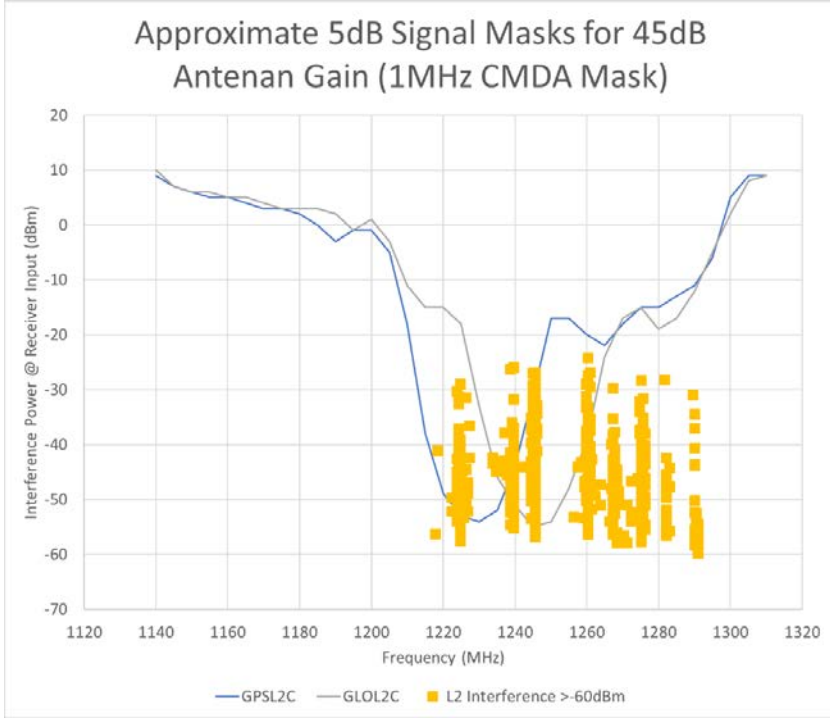
- Incident Eastern Mediterranean
- First report 18th March - has continued for over 70 days
- Multiple vessels affected
- 250 Nautical Mile range
- Duration ranged from a few minutes to hours
- Affects ranged from reduced usable satellites on specific constellations to a complete loss of satellite tracking (GNSS and L-Band Corrections)
- Source Unknown
- Result - vessels were unable to operate using GNSS alone



# Suspect Jamming- Ongoing - Data Analysis

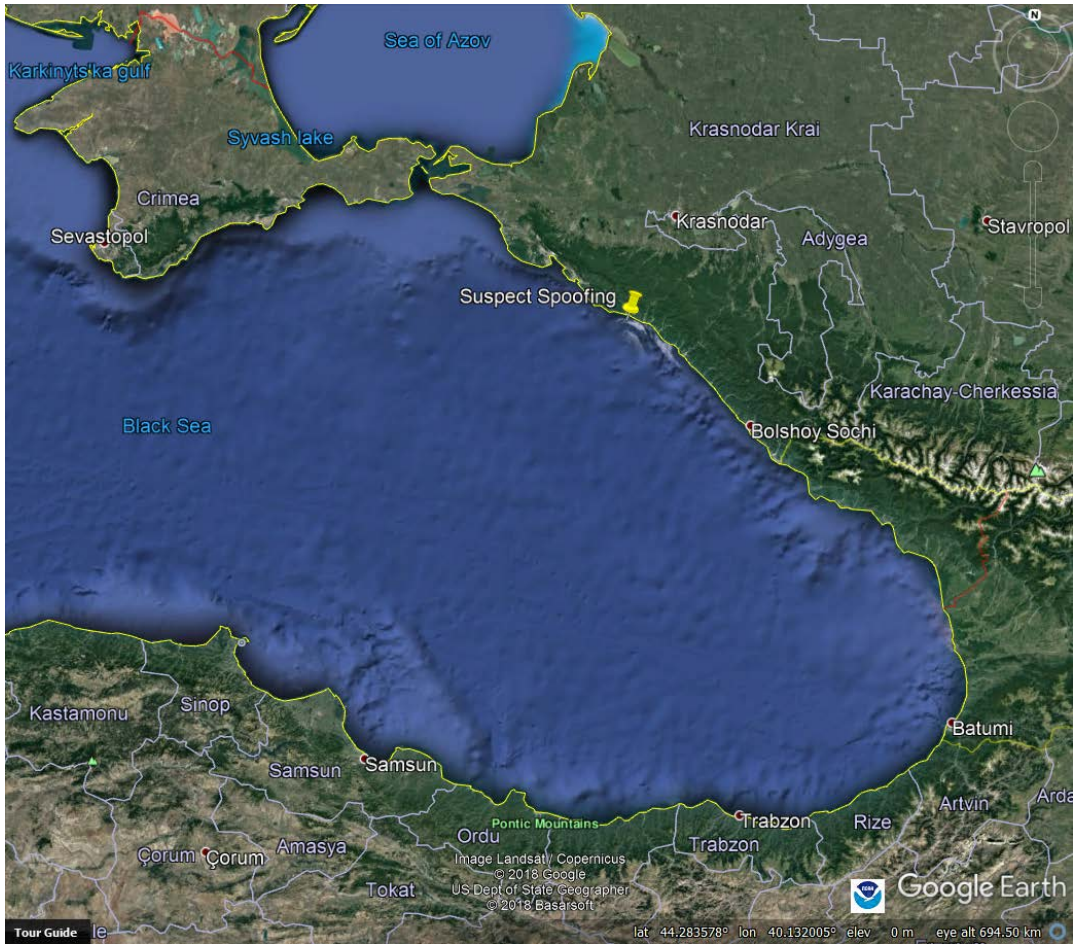
- Severity of interference observed varies greatly
- One data set analysed observed:
  - Strong interference on L2 signals
  - Varying by 40dB over time



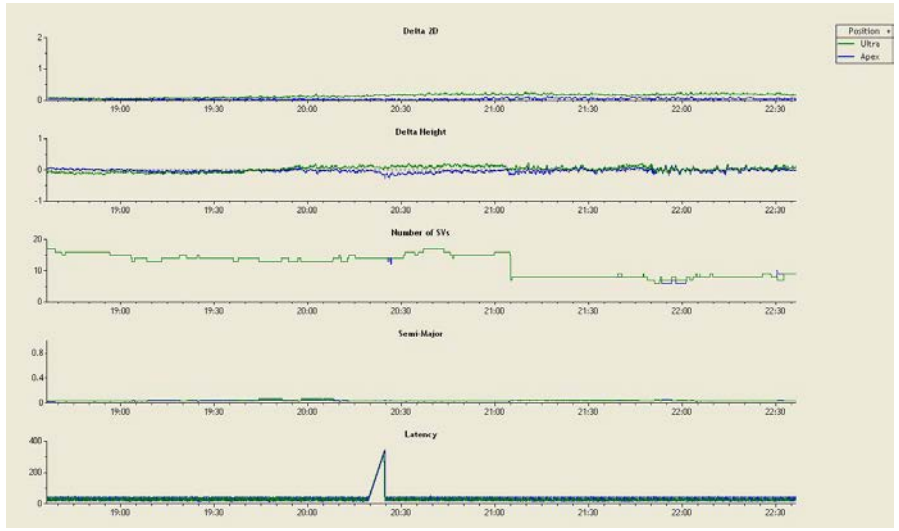
# Suspect Spoofing

- Incident reported by vessels operating in the Black Sea
- Between 22nd and 24th June 2017 -
  - However some reports state it was still ongoing into October 2017
- Reported anomalies with their GPS-derived positions
- Reported to be located at an airport
- Receivers affected appear to be Single Frequency GPS Only with Standalone positioning
- Debate whether this issue is Spoofing or GNSS re-radiation.



# Constellation Issue - GLONASS Event 2014

- Occurred on 01 April 2014, just after 21:00 UTC
- Each satellite reported ‘Illegal Ephemeris’ or ‘Failure (URE>75m)’
- Entire constellation un-usable
- Resulted in no GLONASS and in some cases a problem with the position computation
- GLONASS only solution displayed low residuals but horizontal position was 50km out
- Compared ephemeris received with the previously received ephemeris was in the order of 100,000m difference



# Mitigation

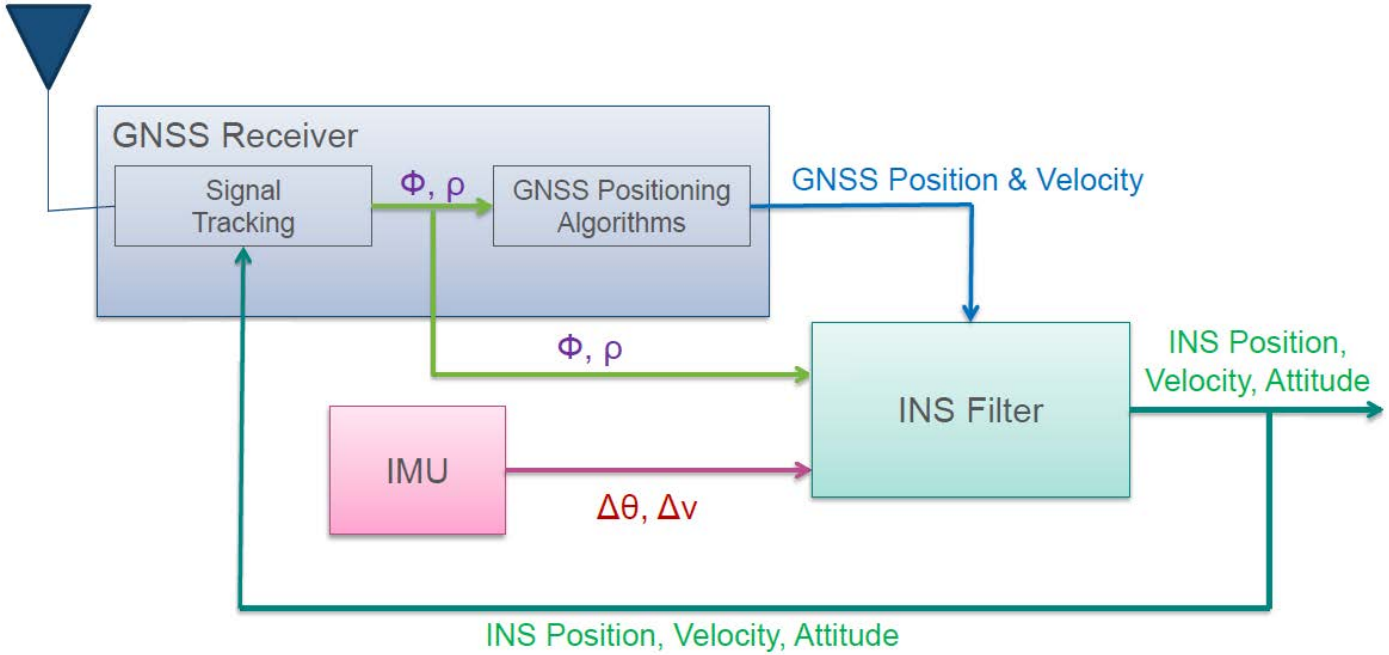
Exploring how to mitigate the threats by looking at the technology available

HEXAGON
POSITIONING INTELLIGENCE

veripos

# Mitigation - GNSS / INS integration

- Can continue to provide position through short periods (few minutes) of GNSS denial through Interference or Jamming
- Can detect and remove large jumps in measurements and position from the GNSS receiver during Spoofing attack
- However longer periods of GNSS denial shall still experience exponential drifting and spoofing is still achievable using small incremental changes

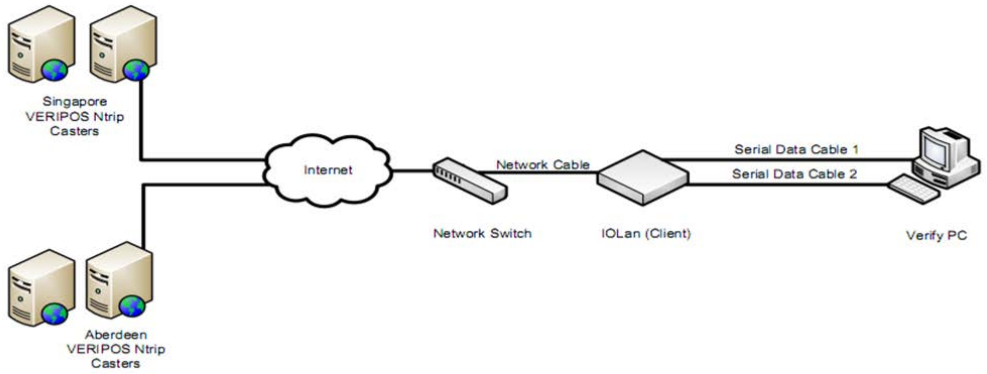


# Mitigation - Augmentation Services

- Augmentation signals provide an integrity check on the GNSS measurements
- During Glonass Event 2014 standalone positions shifted 50km where augmented positions rejected Glonass constellation

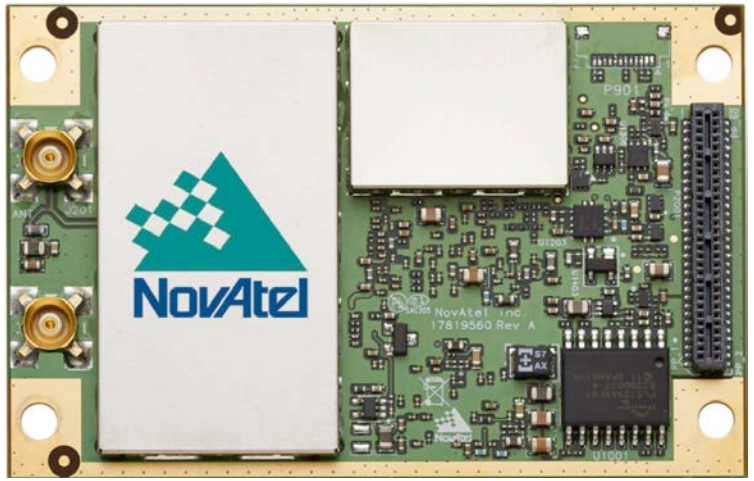
## Interference / Jamming

- Diverse Communications systems - L-Band and NTRIP
  - Utilising different communications systems to receive Augmentation Services
  - L-Band Demodulator and NTRIP Correction sources
  - Inmarsat - V-SAT - Iridium



# Mitigation - New Generation GNSS receivers

- Utilising Multiple Constellations and Frequencies -
  - More satellites in computation with diverse frequency bands and modulation techniques
- Improved tracking capabilities and interference rejection
- Improved resilience against Spoofing - Multi Constellation & Frequencies
- Have been deployed in strong interference environment and shown improved performance over legacy equipment



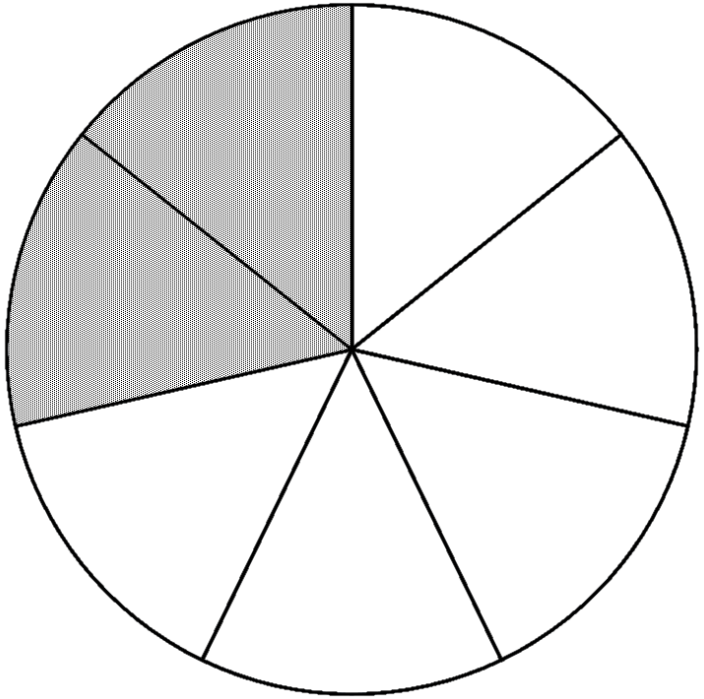
# Mitigation - Interference Toolkits

- Interference Toolkits - available on certain New Generation GNSS receivers
- Ability to detect, display, profile and mitigate interference
- Notch Filters
- Bandpass Filters


- Cannot mitigate interference on the GNSS frequency as required signal would also be filtered

# Mitigation - Anti-jam Antenna

- CRPA (Controlled Reception Pattern Antennas)
- Mitigates In-Band and Out-Band Interference
- Creates nulls in the antenna gain pattern in the direction of jammers
- Providing significant anti-jam protection even in dynamic multi-jammer scenarios
- Compatible with legacy GPS receivers




HEXAGON
POSITIONING INTELLIGENCE

veripos

# Summary

- Unintentional and international interference an increasing risk
- Recent Events show increasing duration and severity of suspect jamming
- Local interference still causing issues
- Utilising multiple constellations, frequencies and diverse communication links improve resilience
- New technology currently available to mitigate Interference, Spoofing and Jamming


HEXAGON
POSITIONING INTELLIGENCE
veripos