Timing Performance of LEO PNT in a GNSS-Denied Environment

WSTS 2026

Bellevue WA
May 2026

Charlie Meyer
Senior Technical Director
Commercial Position, Navigation & Timing Division

iridium®

Legal Disclosures

Statements made in this Presentation are not warranties, and IRIDIUM EXPRESSLY DISCLAIMS ALL WARRANTIES, IMPLIED WARRANTIES, WARRANTIES OF MERCHANTABILITY AND WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, except as expressly set forth in the relevant Iridium Limited Warranty and the Iridium Product Sales Terms and Conditions.

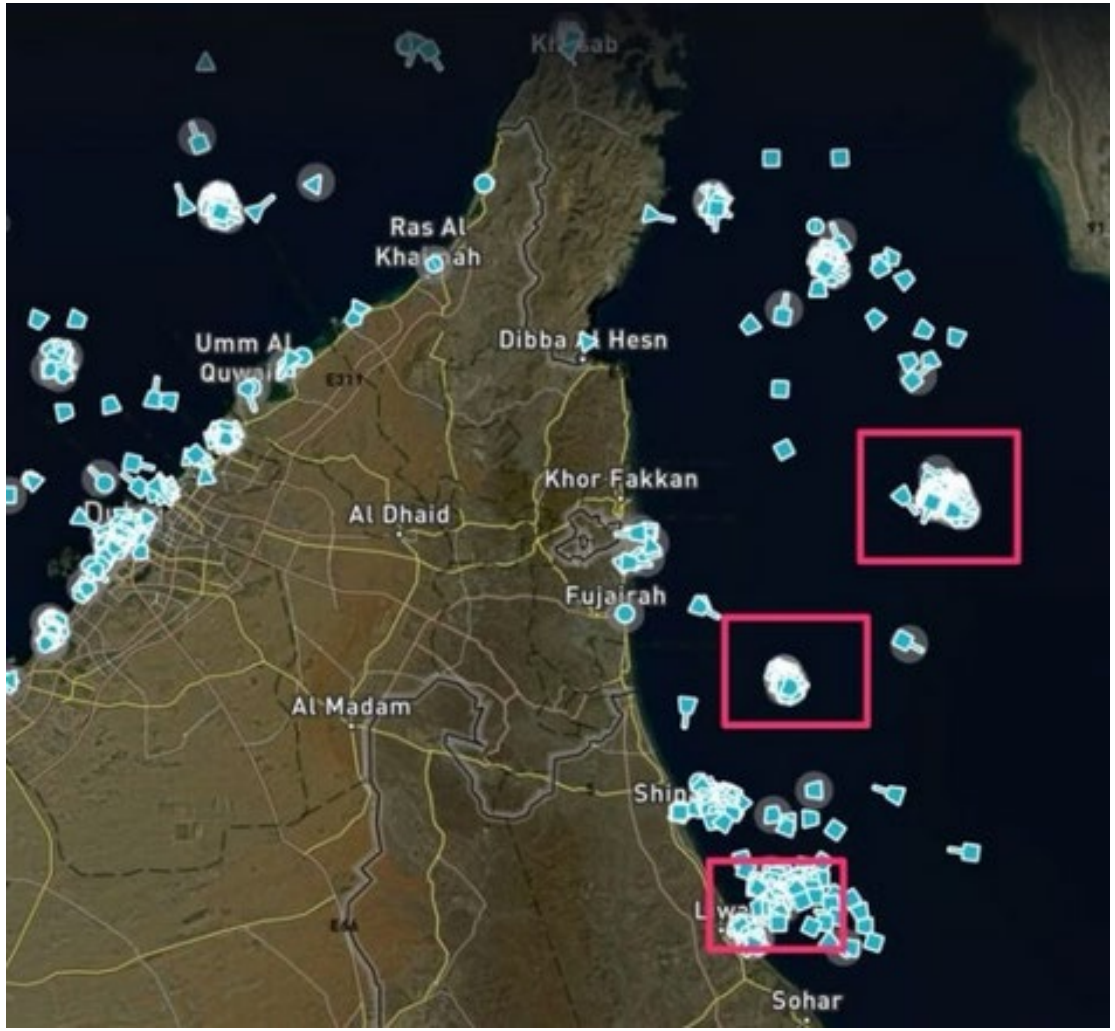
The views and opinions expressed in this Presentation are solely those of the presenter and do not necessarily represent those of Iridium which makes no warranty as to accuracy or completeness of the information provided or the views or opinions presented. The information in this Presentation is subject to change without notice.

Read and understand the Iridium User Manual and the safety warnings and information contained in that Manual before using any Iridium product.

Recent GPS Jamming/Spoofing in Gulf of Oman

March 7th, 2026:
GPS jamming and spoofing affected more than 1,650 ships in the Middle East Gulf, up 55% from the previous week, erroneously placing vessels across land and sea in Kuwait, Iran, Saudi Arabia, Oman, and the United Arab Emirates.

14 tankers and an oil rig have been attacked or hit by missiles or drones, with the Joint Maritime Information Center confirming 11 events. Eleven crew members have been killed.

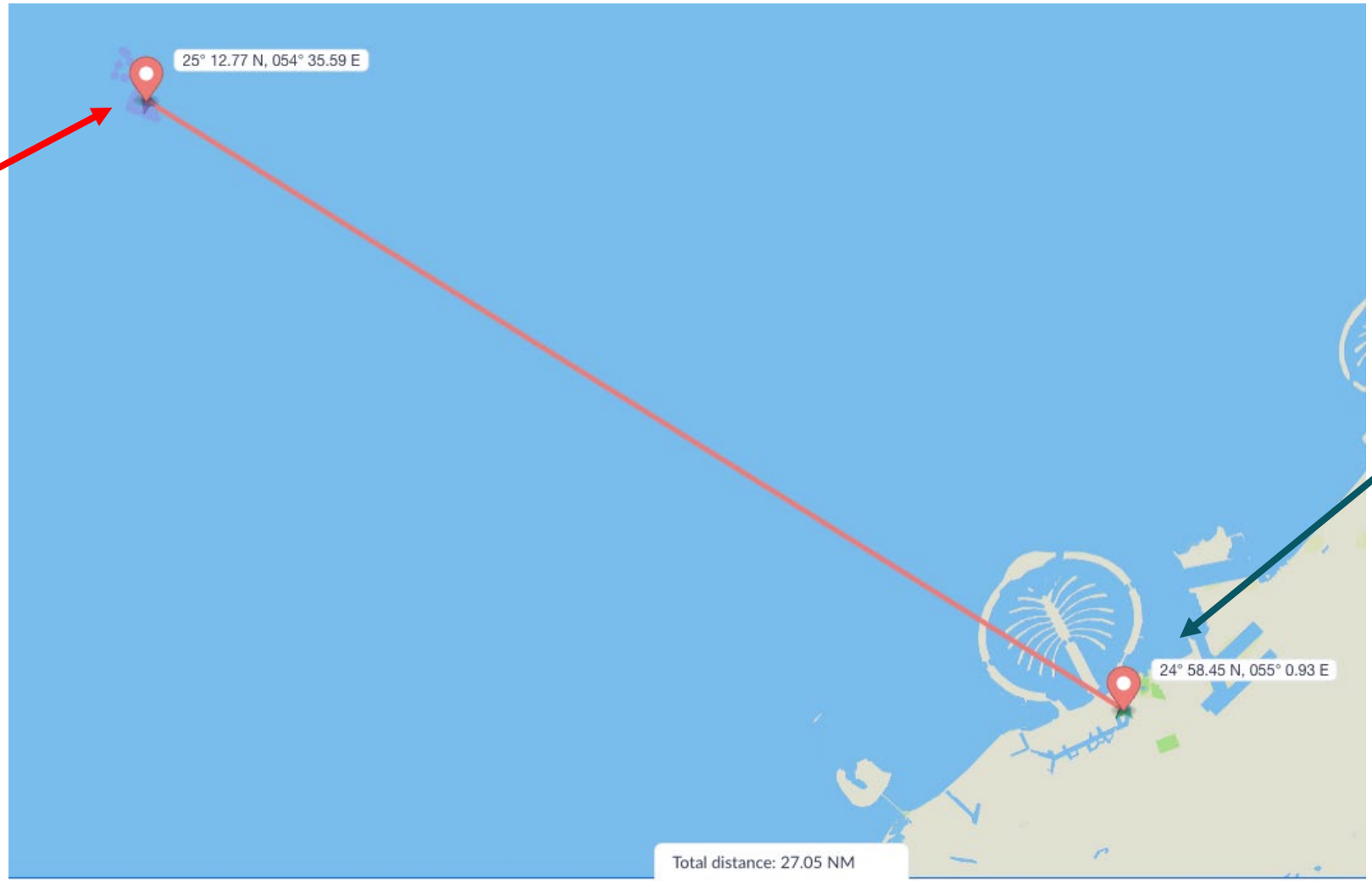


Boxes mark clusters of false locations reported from hundreds of ships

Data and Image courtesy of WINDWARD

Example of 50 km GNSS spoof, Dubai, March 2026
Iridium LEO PNT showed the true ship location

Incorrect Location reported from GNSS receiver



Correct Location reported from Iridium LEO PNT receiver

iridium

Jammertest 2025

iridium

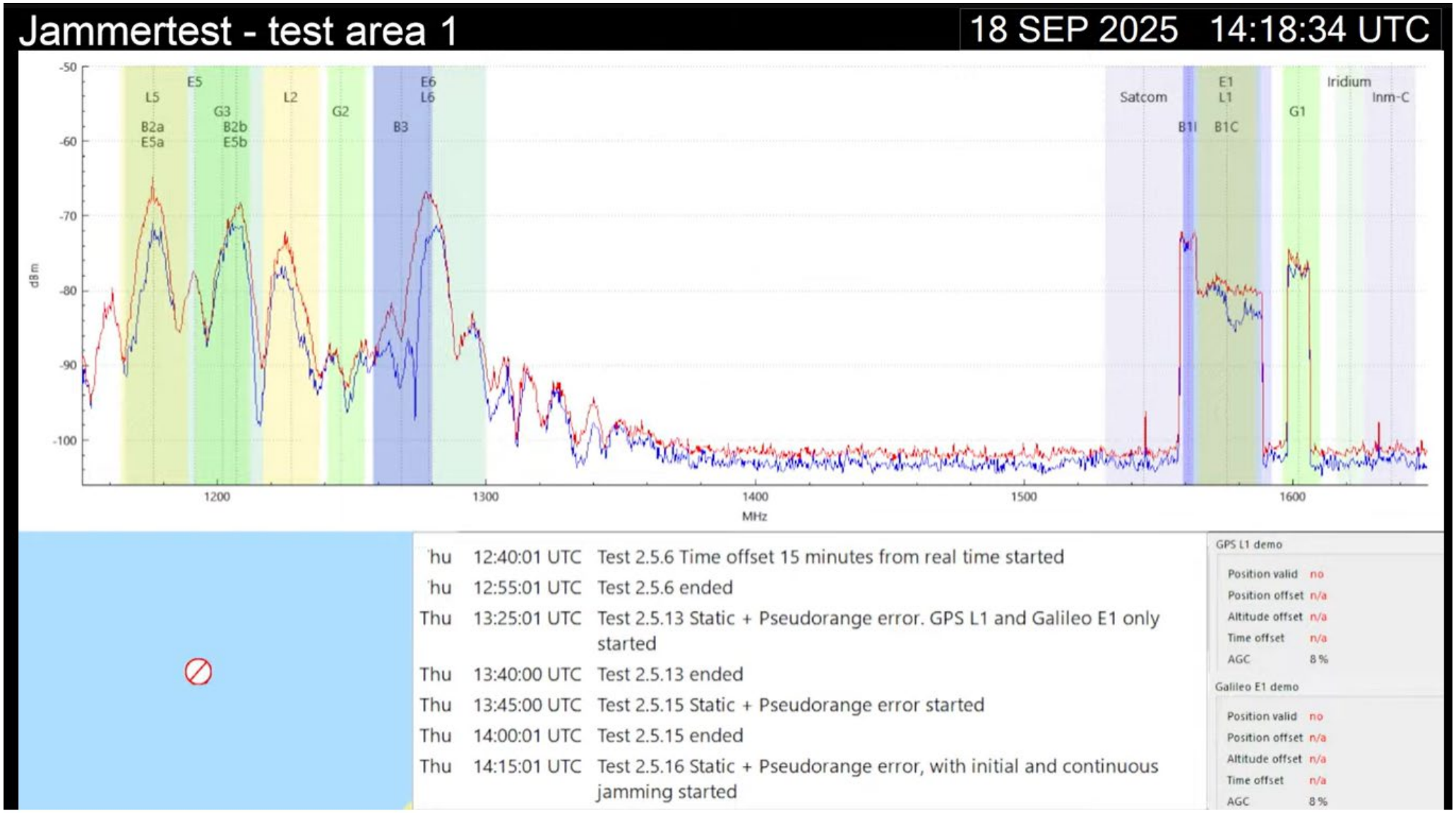
Jammertest 2025

Jammertest is a Norwegian government initiative, open to international participation, where six Norwegian authorities have come together to create an environment where **GNSS jamming, spoofing, and meaconing are present under controlled conditions** in a live, real-world outdoor environment.

Jammertest 2025 was held in Bleik, Norway, September 15-19, 2025.

iridium

All GNSS Signals Were Attacked, Often Simultaneously



Test Locations

Vehicle and Maritime Harbor Testing

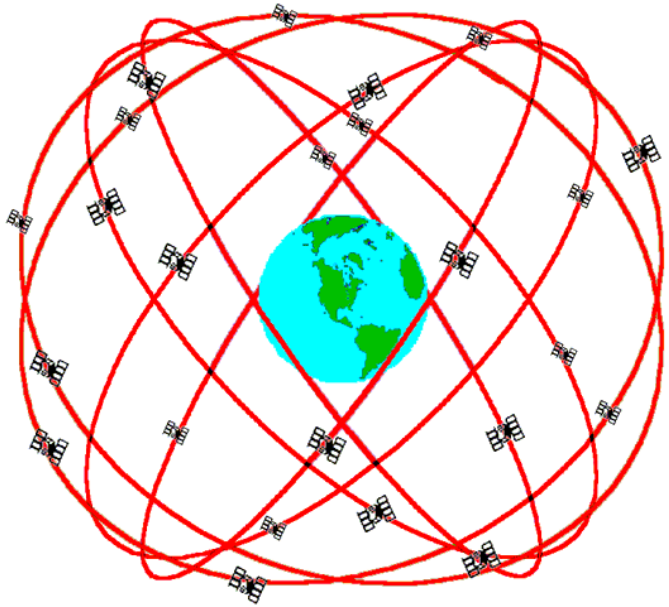
Timing Test Lab

8

Iridium® PNT

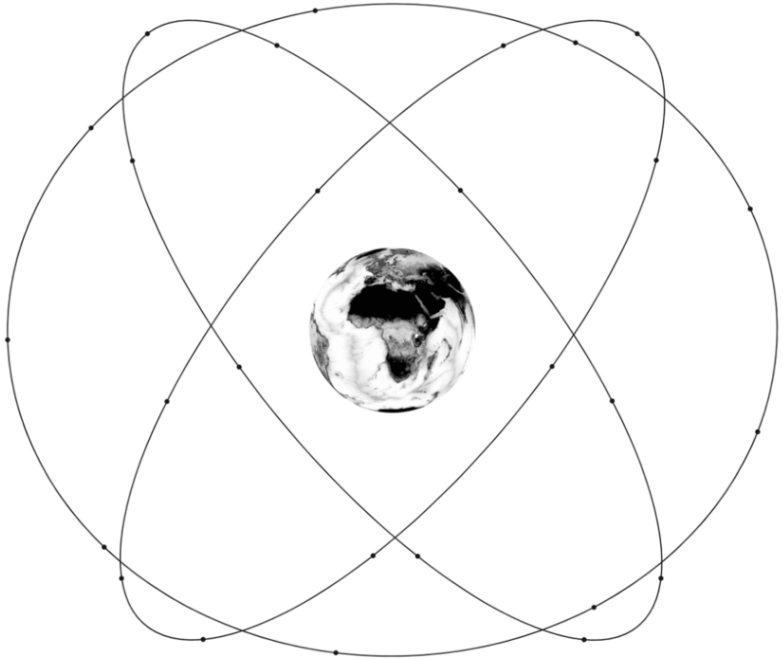
iridium®

GPS/Galileo MEO vs Iridium LEO Constellations



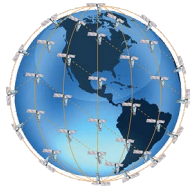
GPS MEO Constellation

24+ Satellites in 6 Orbital Planes
4 Satellites in Each Plane
20,180 km Altitude, 55 Degree Inclinations
Orbital Speed 14,000 km/hr (9k mph/mach 12)
Orbital Period 12 Hours (2x/day)
Different Satellite in Each Plane Every 3 Hours



Galileo MEO Constellation

24+ Satellites in 3 Orbital Planes
8 Satellites in Each Plane
23,222 km Altitude, 56 Degree Inclinations
Orbital Speed 13,200 km/hr (8k mph)
Orbital Period 14 hours (~2x/day)
Different Satellite in Each Plane Every ~1.5 Hours



Iridium® LEO Constellation

66 Satellites in 6 Orbital Planes
11 Satellites in Each Orbital Plane, Spaced 30° Apart
781 km Altitude, Polar Orbits (86.4 Degrees)
Orbital Speed 27,000 km/hr (17k mph/mach22)
Orbital Period 100 Minutes (14x/day)
Different Satellite in Each Plane Every 9 Min

LEO PNT from the Iridium Satellite Network

66 Active Satellites

- 6 orbital planes of 11 satellites each
- Plus in-orbit spares

Low-Earth Orbit (LEO)

- Nominal 30 dB stronger than GNSS
- Doppler-assisted ranging

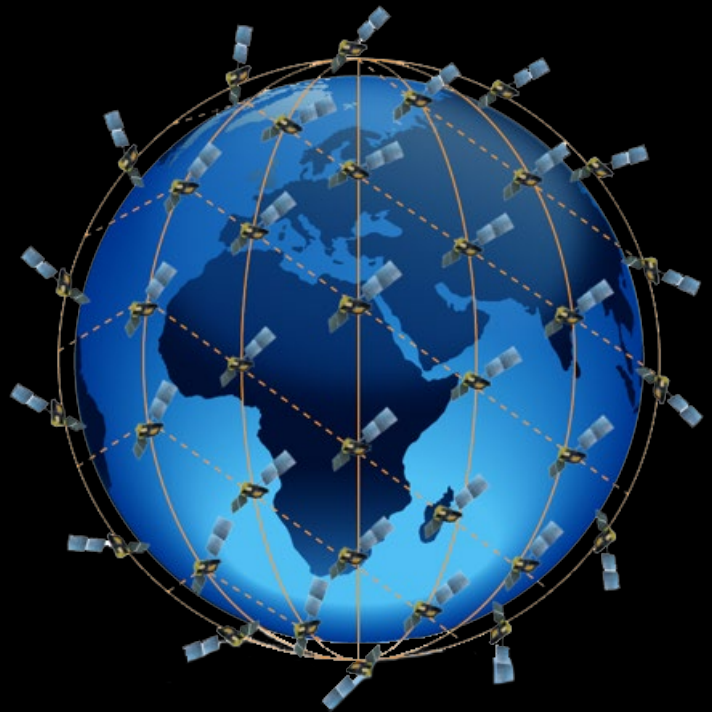
L-Band System

- Smaller receivers and antennas
- Works even in adverse weather

Satellite Crosslinks

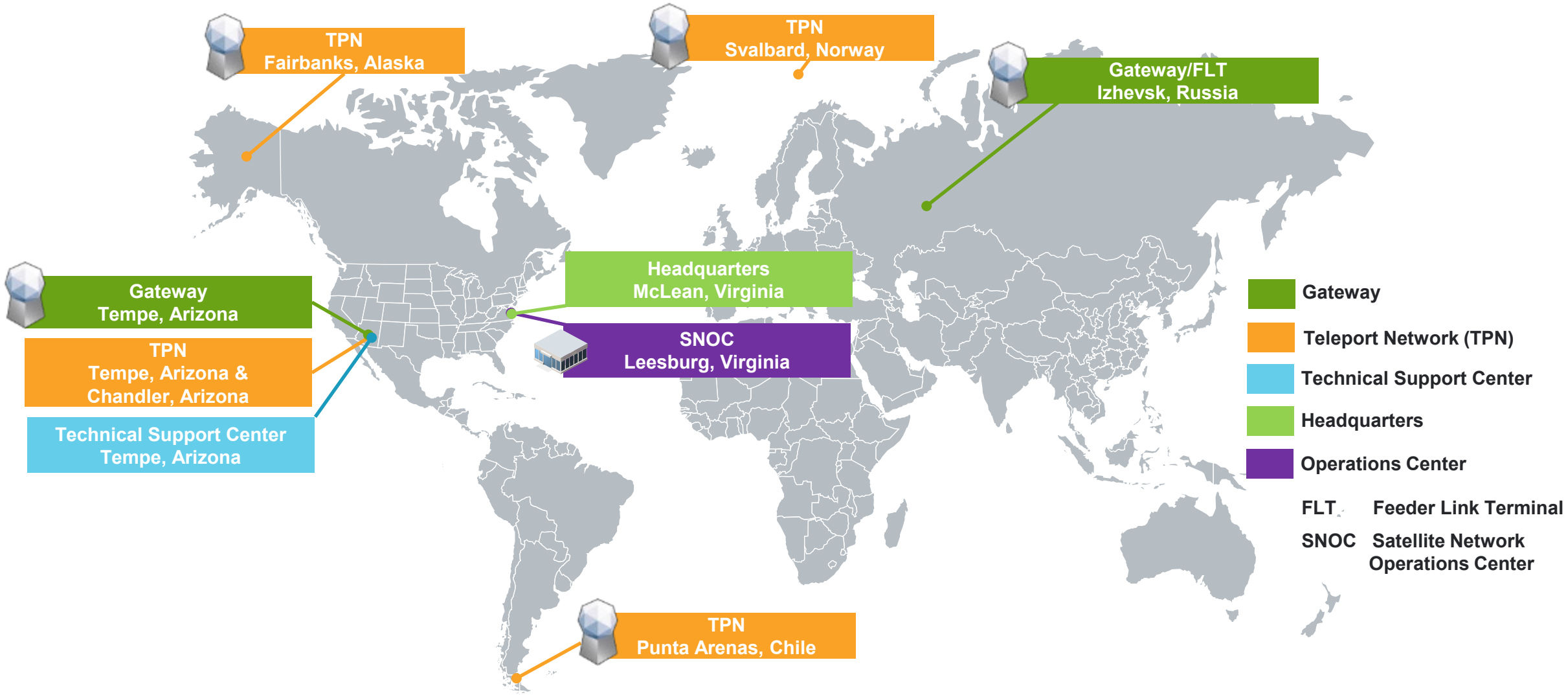
- Creates low-latency, resilient connections

Iridium's constellation provides
Global PNT service



The Iridium PNT signal is Traceable to UTC(USNO), UTC(NIST), and UTC(IT)

Iridium Gateway & Ground Station Locations

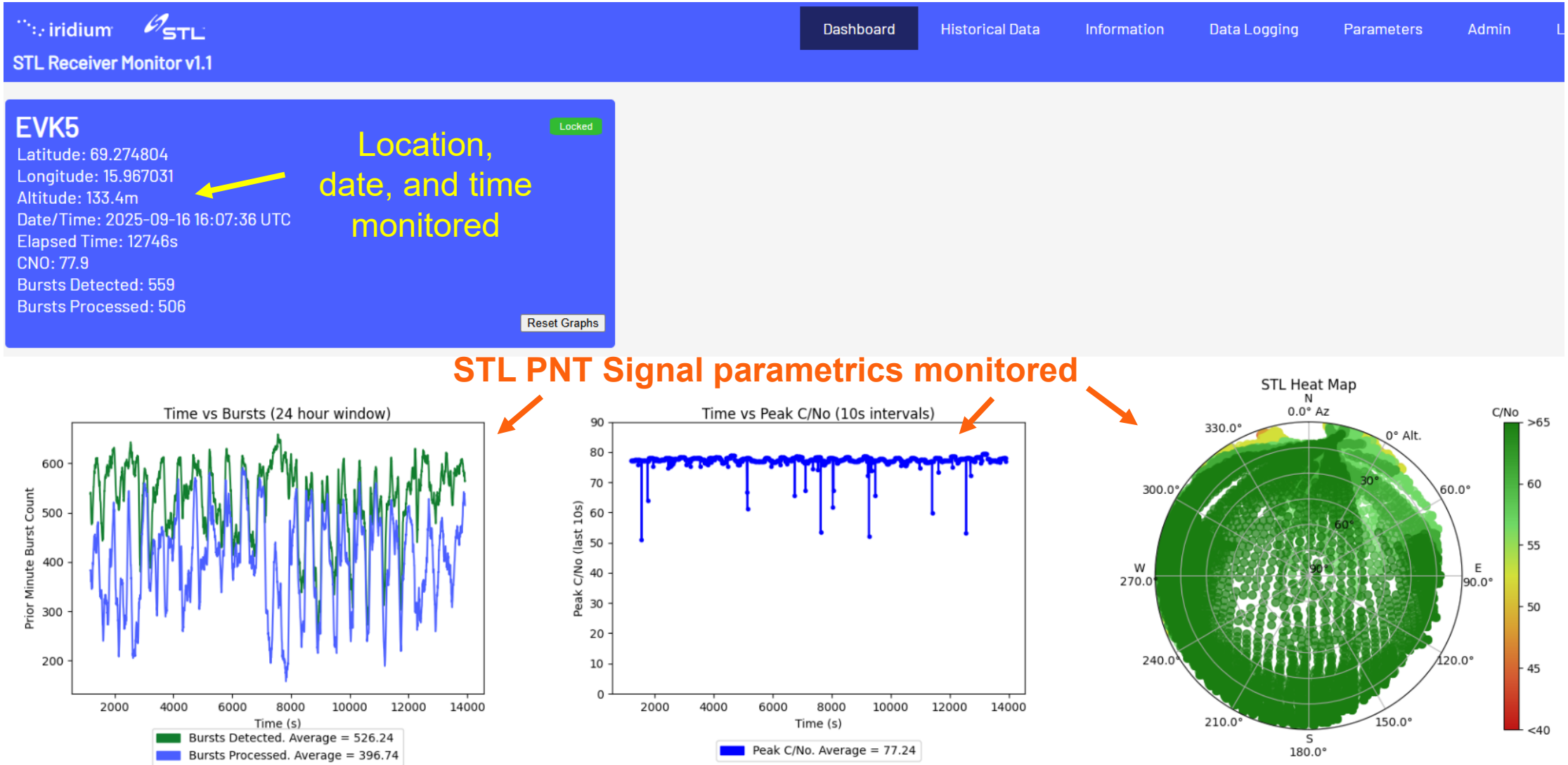


iridium

Iridium PNT LEO Facts

- Iridium PNT is a commercially available LEO PNT (satnav) service with a signal that is deliberately engineered to transmit cryptographically protected **almanac and ephemeris**. It is purpose-built for PNT and NOT a noncooperative signal of opportunity.
- **Time is linear** (no leap seconds) and **UTC traceable** to multiple national standards: currently UTC(USNO) and UTC(NIST) in the U.S., UTC(IT) in Italy, and others being planned.
- **Location is per WGS-84** for compatibility with existing GPS/GNSS mapping services.
- Iridium PNT uses **independent satellite resources** to broadcast a signal that is **receive-only on the ground**. It does not rely on or use the Iridium communications channels or services (i.e., it is satnav not satcom). It is a native, end-to-end Iridium service rather than a capability provided via a hosted payload.
- Satellite timing is **managed by the ground network**; the satellites do not receive, use, or reuse, signals from GNSS satellites in MEO.
- Iridium's **full-size satellites** also have superior maneuverability and larger fuel reserves that, compared to other commercial satellites, enable station-keeping capabilities that can easily and quickly reposition to counter the effects of orbital drag.

Iridium PNT (STL®) Signal Monitor



Vehicle Testing

iridium

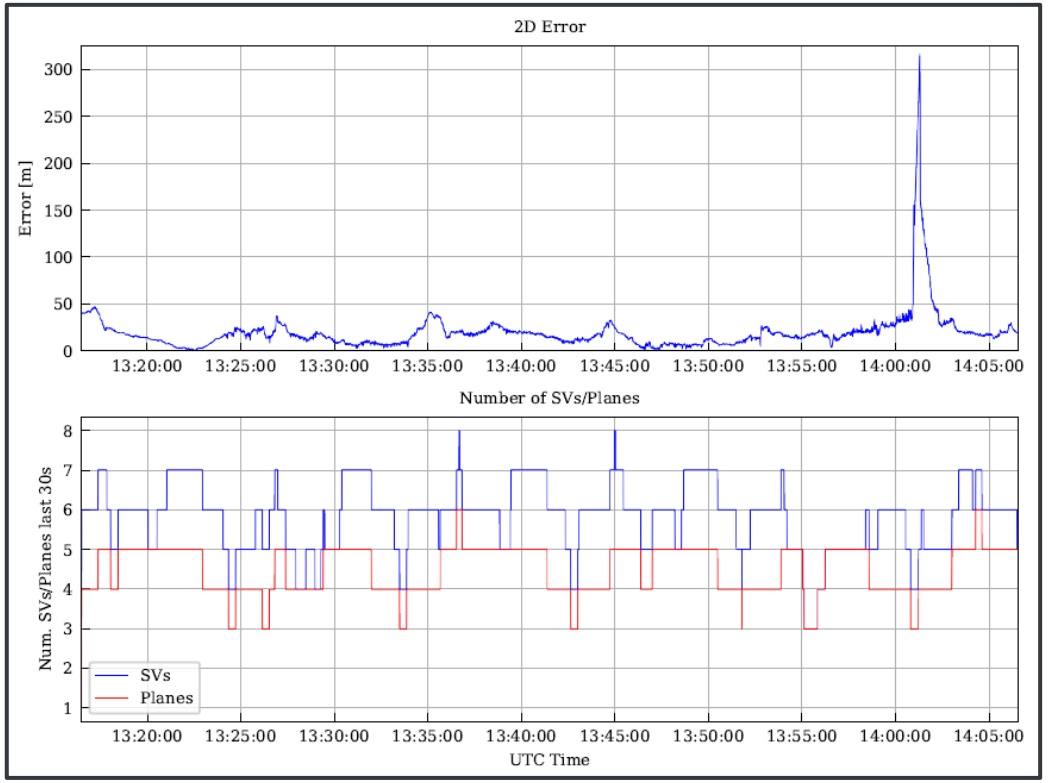
Benign Vehicle Performance

Data collected with Iridium® PNT ASIC

Vehicle Speeds Up to 100 kmh Andøya, Norway

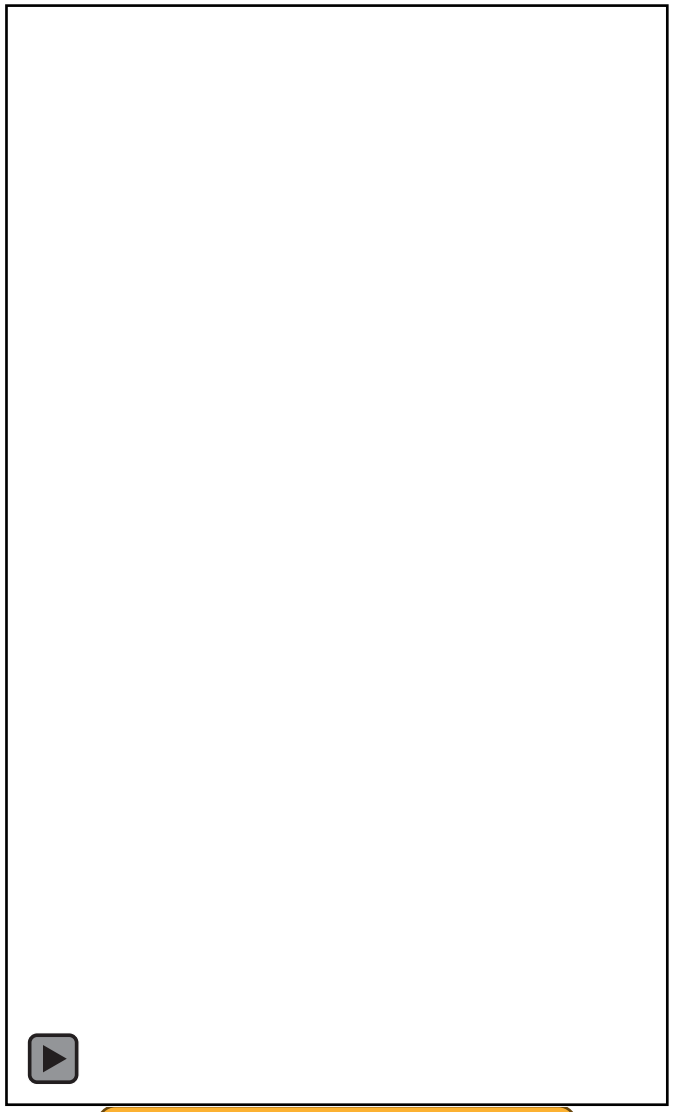
Horizontal Error (m)	
Median	16 m
Mean	19 m
Std Dev	22 m
95th %	39 m

Mean BPM: 398
Mean C/N_0 : 61 dB-Hz

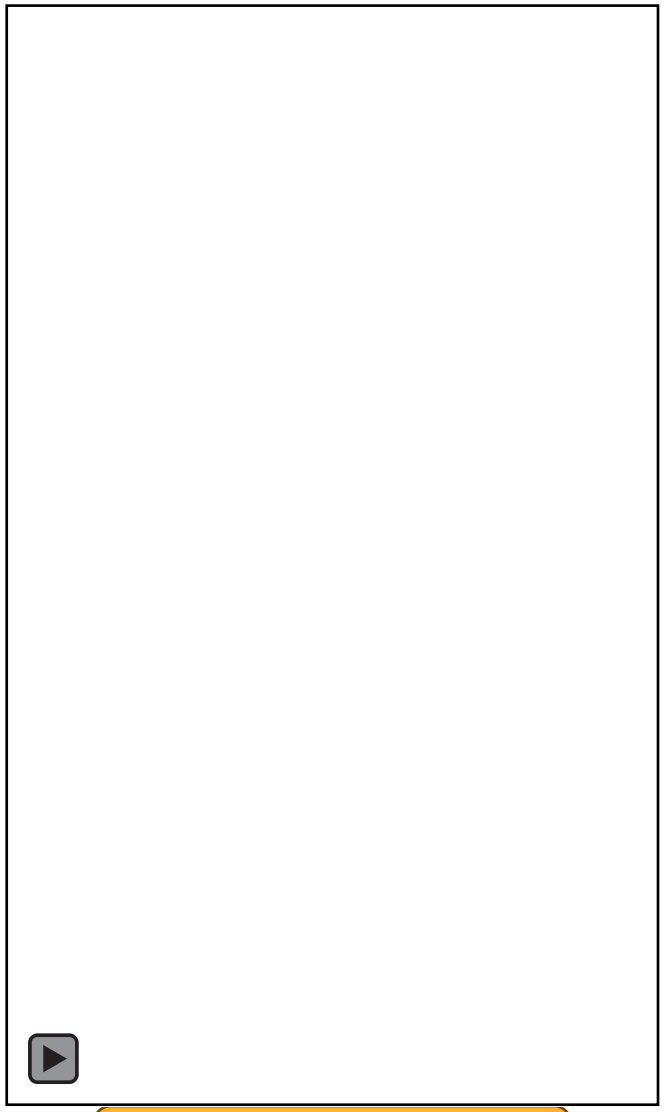


iridium

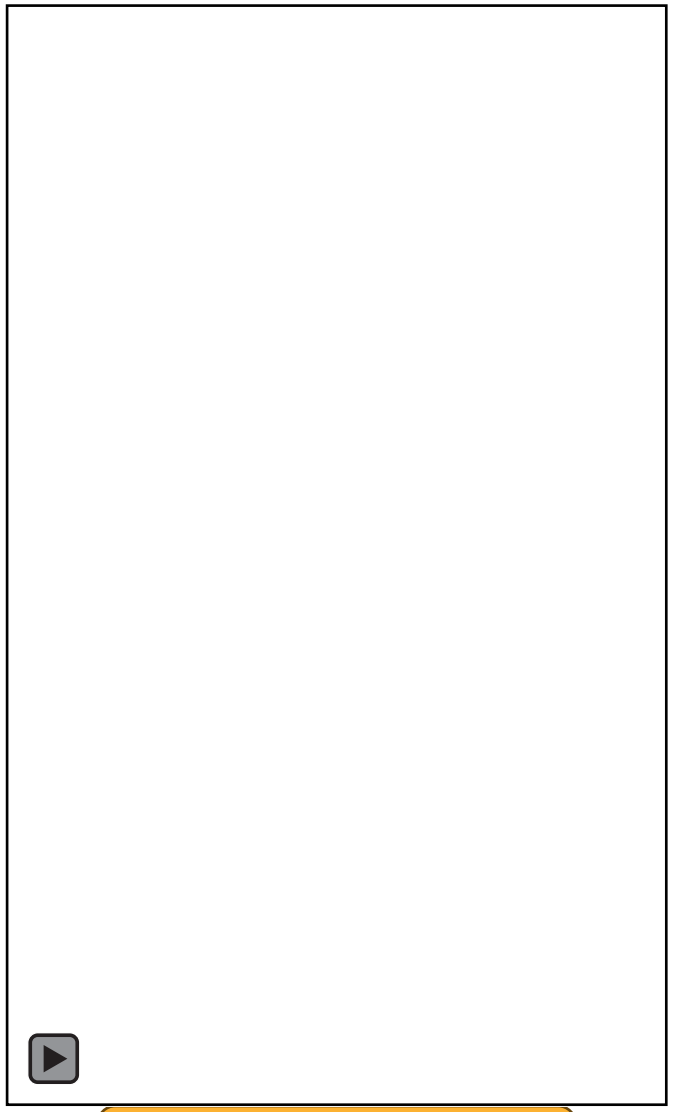
Mobile GNSS Spoof – Test Area 3 (video)



Scenario 2.6.3



Scenario 2.6.4



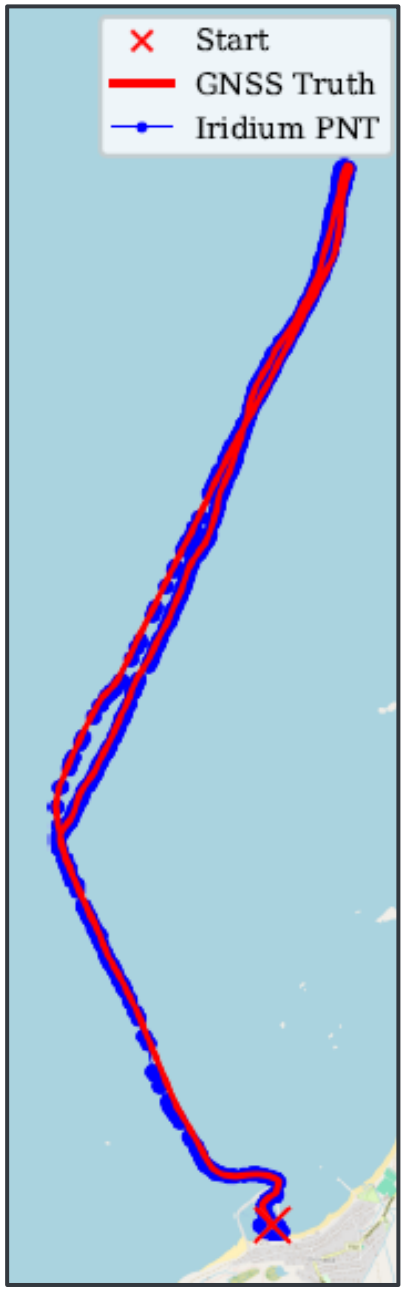
Scenario 2.6.5

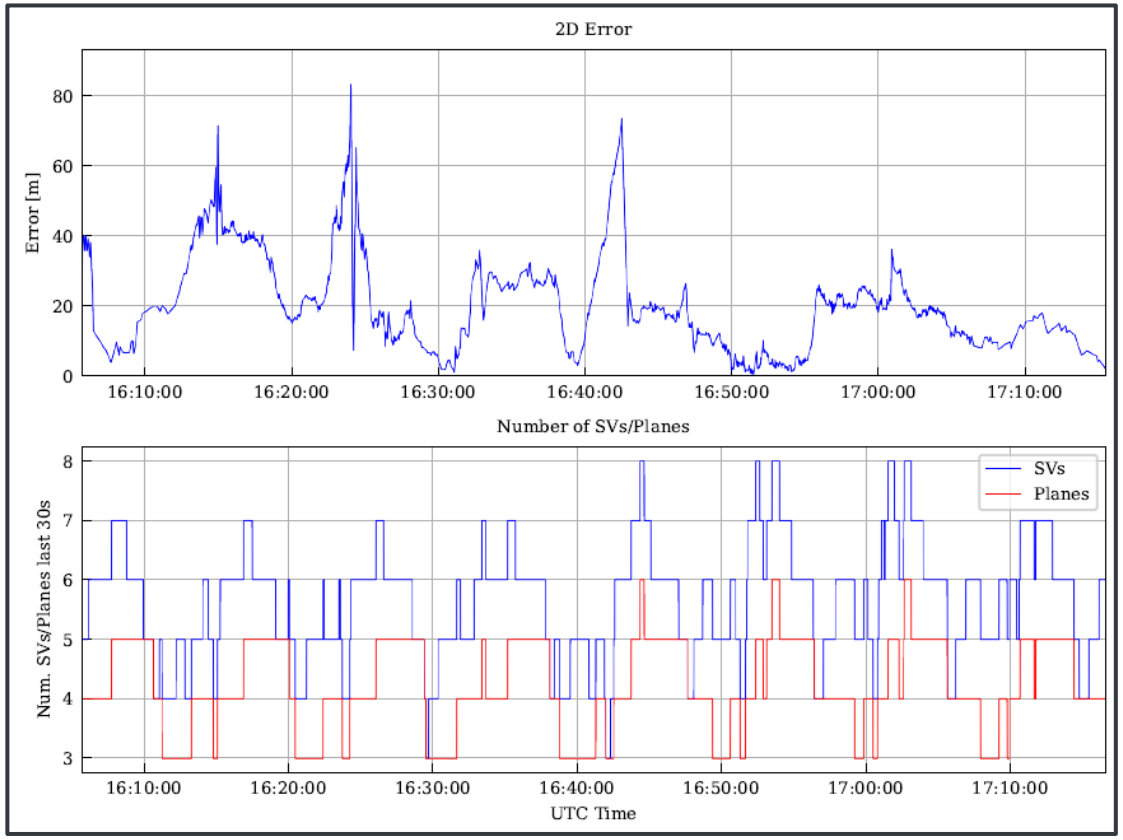
Maritime Testing

iridium

Benign Maritime Performance

Data collected with Iridium PNT ASIC





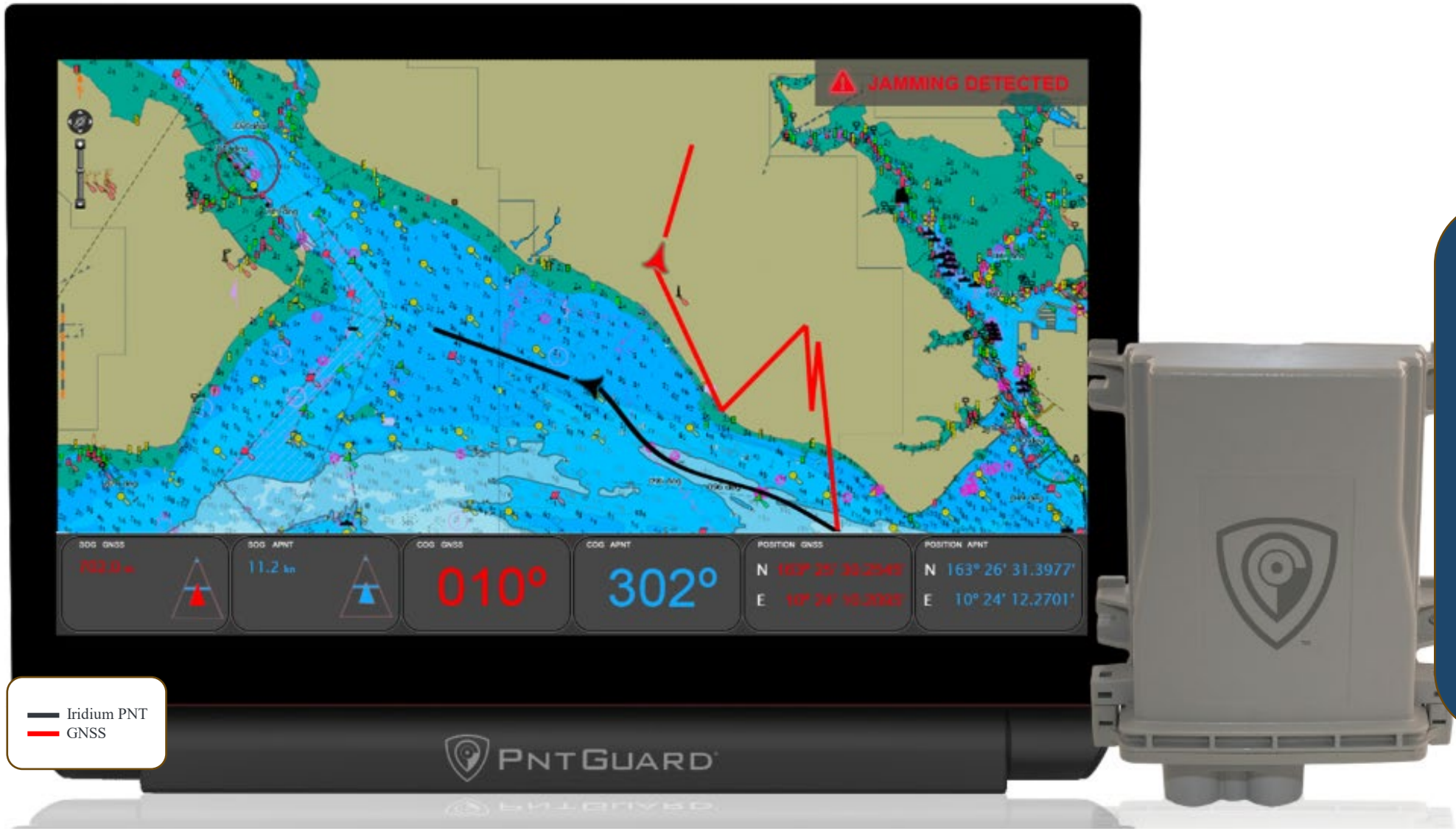
Maritime
Up to 20 knots
Bleik, Norway

Horizontal Error (m)	
Median	19 m
Mean	21 m
Std Dev	13 m
95th %	44 m

Mean BPM: 371
Mean C/N_0 : 57 dB-Hz

iridium

Maritime GNSS Spoofing



Our partner, NAL Research, tested their new maritime-security solution

The device used Iridium PNT to maintain accurate PNT during a GNSS spoof scenario

Maritime Navigation During Dynamic Position Spoof

GNSS position was spoofed (**green traces**) and **not usable**

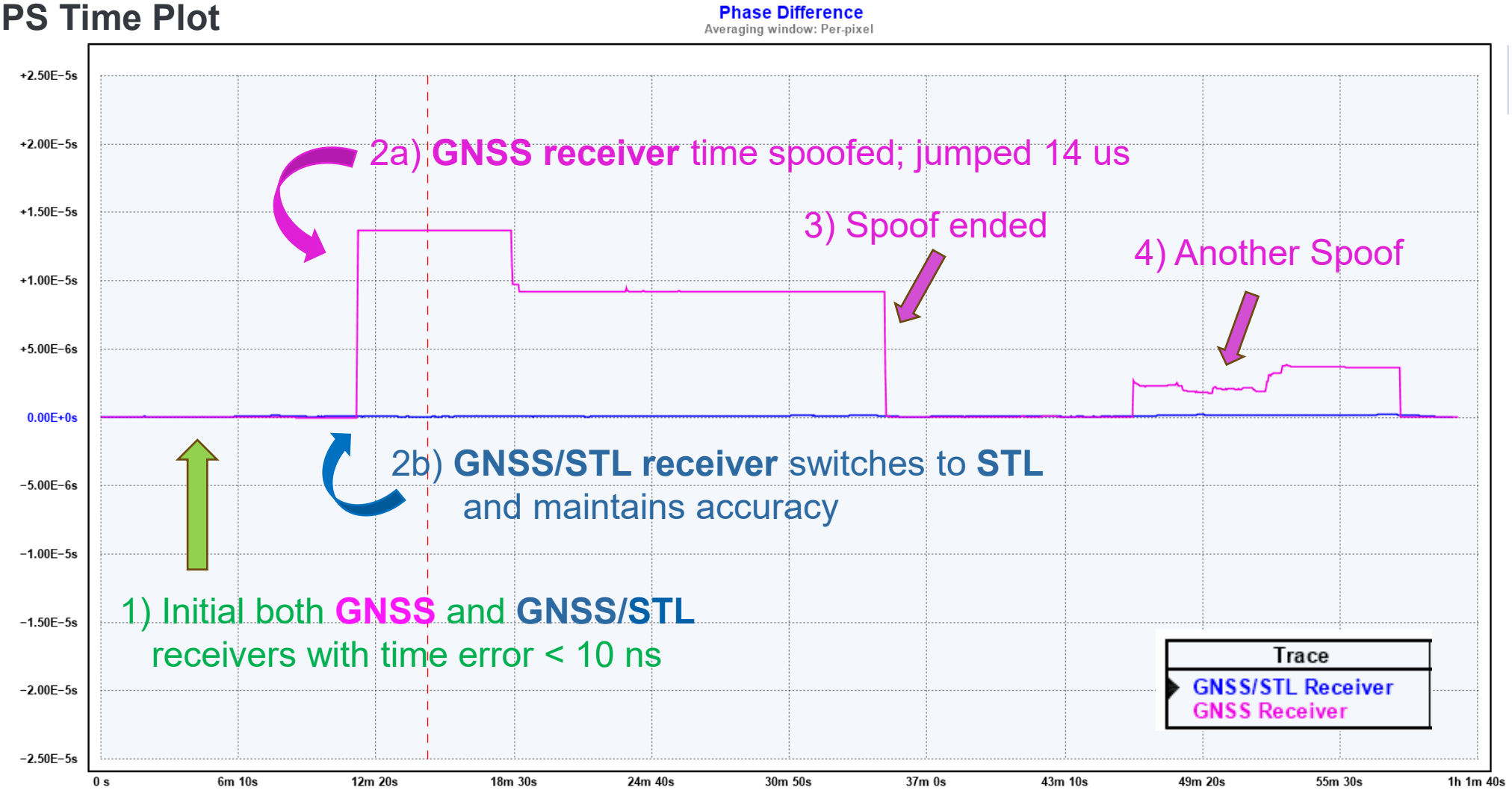
STL PNT (**blue trace**) was used to safely navigate the boat back into the harbor and dock

Timing Results

iridium

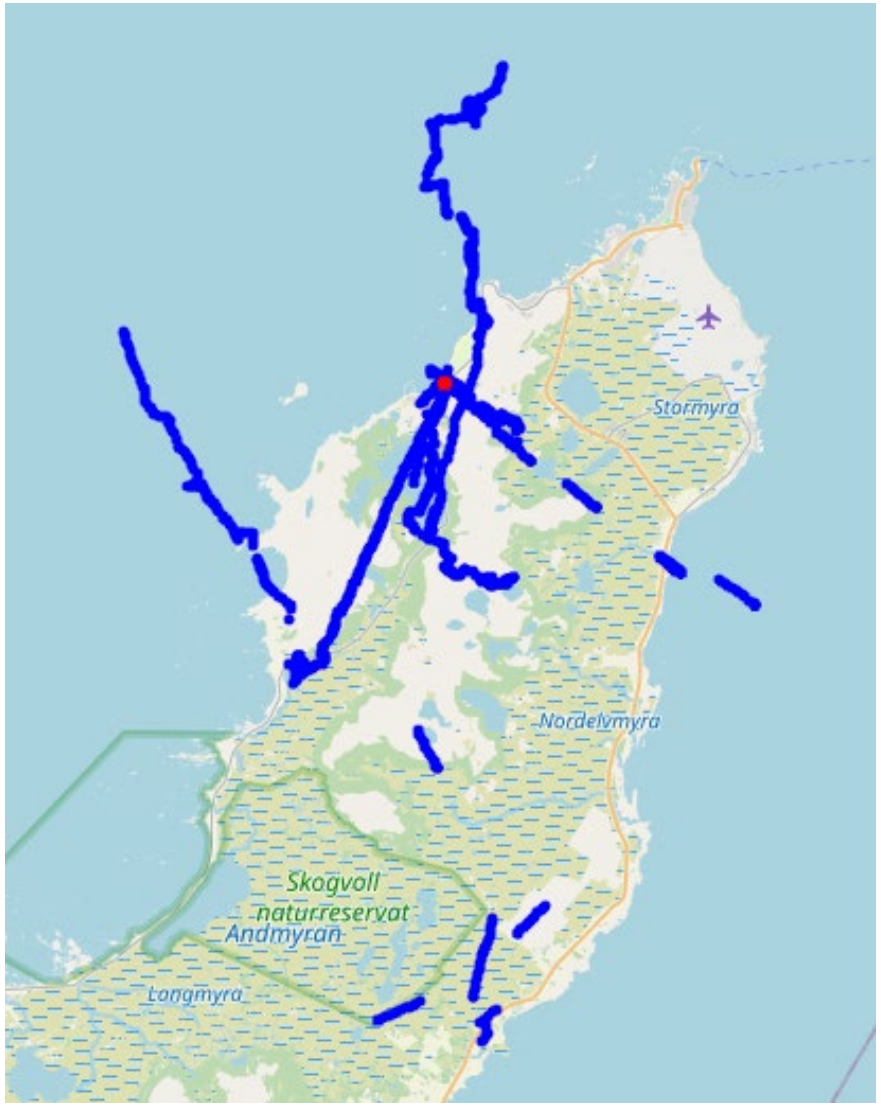
Example of Timing Spoof (Test 3.2.7)

1PPS Time Plot



Trace	Notes	Input Freq	Sample Interval	Phase at 14m 38s	Duration	Elapsed	Acquired	Instrument
EVK5 GNSS/STL	3.2.7	1.0 Hz	1.000 s	6.47E−8s	100 d	1h 0m 31s	3631 pts	TAPR TIC
GNSS	3.2.7	1.0 Hz	1.000 s	1.37E−5s	100 d	1h 0m 46s	3646 pts	TAPR TIC

Example of Static Position Spoof



GNSS position was spoofed (**blue dots**) and **not usable**

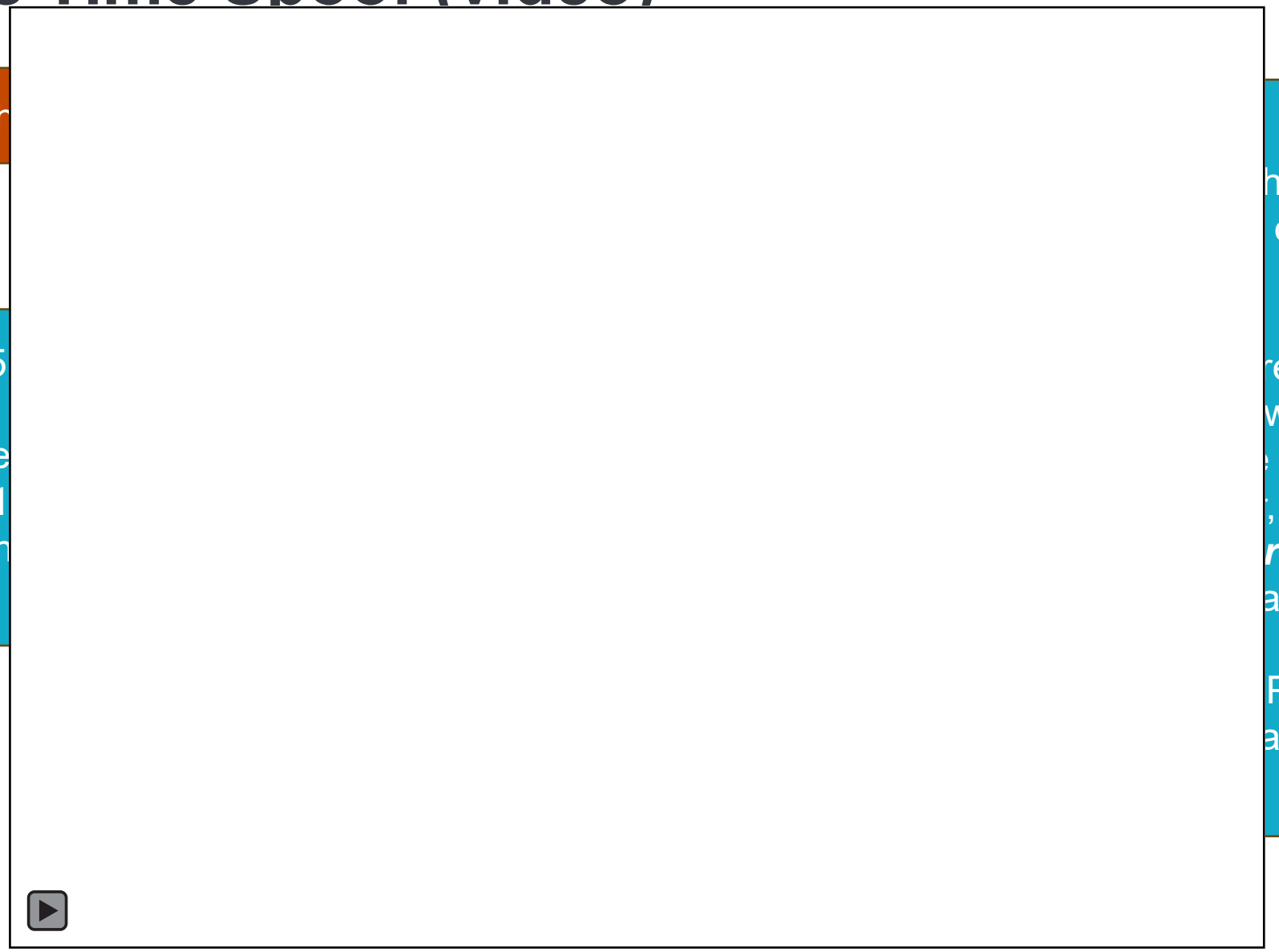
STL PNT (red dot) showed the true (static) location

Dynamic Time Spoof (video)

Watch th

Scenario 2.5

GNSS receive
spoofed to 1
minutes in th
future

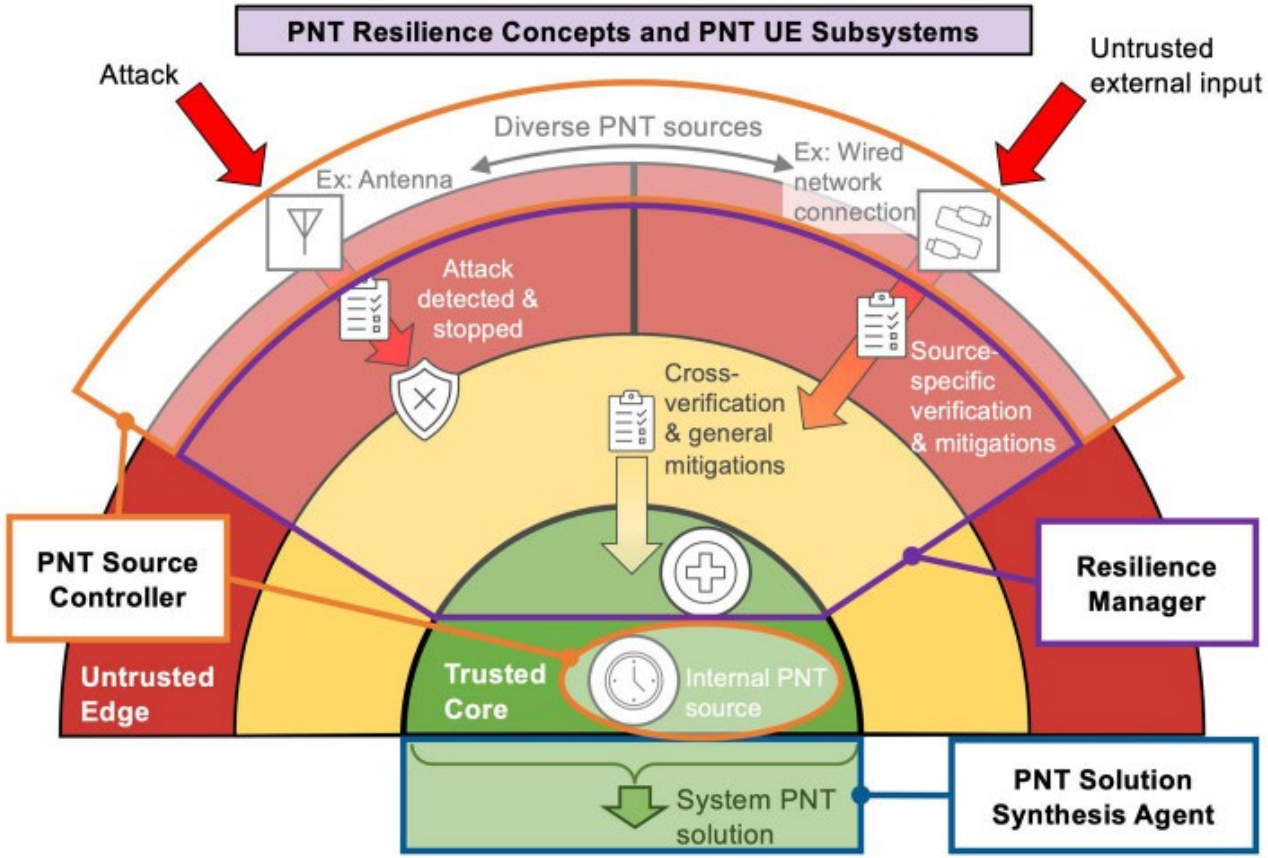


hicle begins
of contested

receiver **time**
when it comes
proximity to the
, and ***does not***
r after leaving
a

PNT continues
ate as normal

IEEE-1952 Resilience Levels 4 and 5 require a Resilience Manager and a PNT Source Controller



The PNT Source Controller organizes the input and output from multiple, diverse PNT sources. Some PNT sources receive untrusted external input from different signals and services and occupy the untrusted edge of the device.

The Resilience Manager implements resilient functions. It brings external input from the untrusted edge to the trusted core through different techniques to build trustworthiness. It identifies untrustworthy PNT information and prevents it from propagating to the trusted core. It also executes mitigation and recovery processes when appropriate.

From U.S DHS Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture, Ver 1.0

Resilience Manager and a PNT Source Controller

An Iridium EVK5 employed a **resilience manager and PNT source controller** algorithm *that continuously monitored and compared the GNSS vs Iridium PNT (STL) information, alarms and output signals*

- **This was highly effective to detect spoofing and meaconing attacks, especially when the GNSS receiver did not detect them**

- **Examples of Geo-fence & Chrono-fence parameters used:**
  - GNSS vs STL **Time of Day** (integer seconds) disagree ≥ **2 seconds**
  - GNSS vs STL **1PPS** disagree ≥ **300 ns** + 3*sum of combined uncertainties
  - GNSS vs STL **position** disagree ≥ **100 meters** + 3*RSS of combined uncertainties
  - GNSS vs STL **velocity vectors** disagree ≥ **1.0 m/sec** + 3*RSS of combined uncertainties (all devices were static, STL uncertainty=0)

  Note: Large errors were allowed so we could "observe" the solution walk off when spoofed

Summary

1) All **Iridium PNT (STL)** receivers **operated properly** throughout the testing (no loss of lock or degradation)

2) When the GNSS/STL receivers **detected** GNSS jamming, spoofing, or meaconing, they **switched to STL** and maintained an accurate PNT solution

3) Some GNSS/STL receivers **did not detect that the GNSS signal was spoofed** and so were not aware they needed to switch to STL

4) **Comparing GNSS to STL** (geo/chrono-fence) was very effective to detect GNSS spoofing/meaconing and to maintain an accurate PNT solution

5) Having **multiple sources of PNT** creates a highly resilient solution

Questions?

iridium