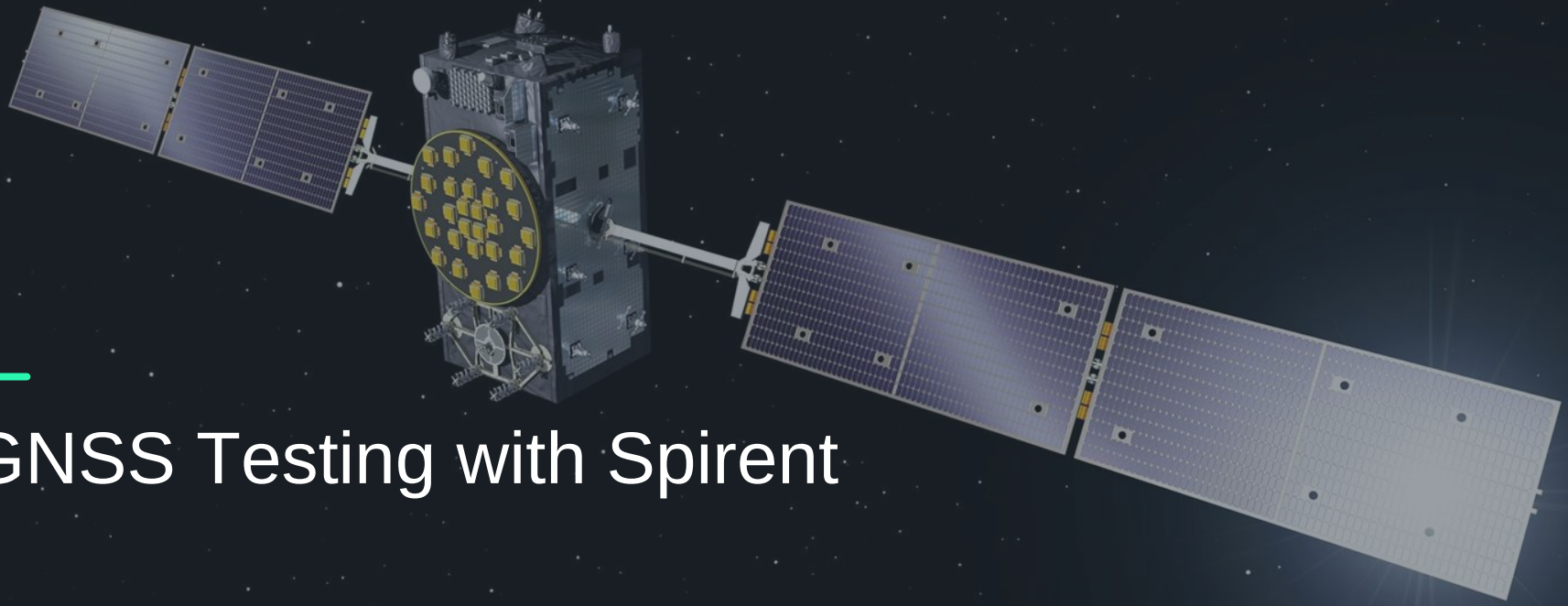
YOTTAVOLT TechDays

spirent™



GNSS Testing with Spirent

Who is Spirent?

Global leader of automated test and assurance solutions for PNT, wireless and wired networks.

1500+
Worldwide Customers

$474.3m
Revenue (2023)

20%
Revenue to R&D Yearly

10/10
Of the world's top Service Providers use Spirent

100%
Of the top Network & Device Vendors use Spirent

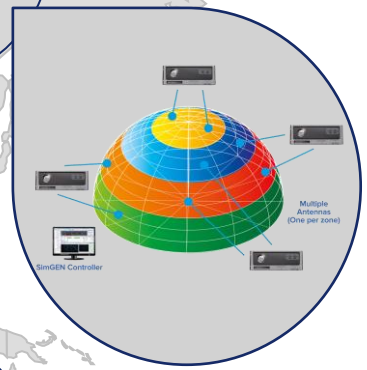
10/10
Of the world's largest tech & cloud companies use Spirent

Spirent's Positioning Technologies (PNT) Division at a Glance

40
Years of PNT Excellence

1,700
Employees Globally

>15
Number of PNT test Patents



>400
PNT customers served in 2023

25+
Offices globally; 6 in Europe

6
ISO Accreditations

Test
& Assurance Focus

GNSS Overview

What is GNSS and the need for test

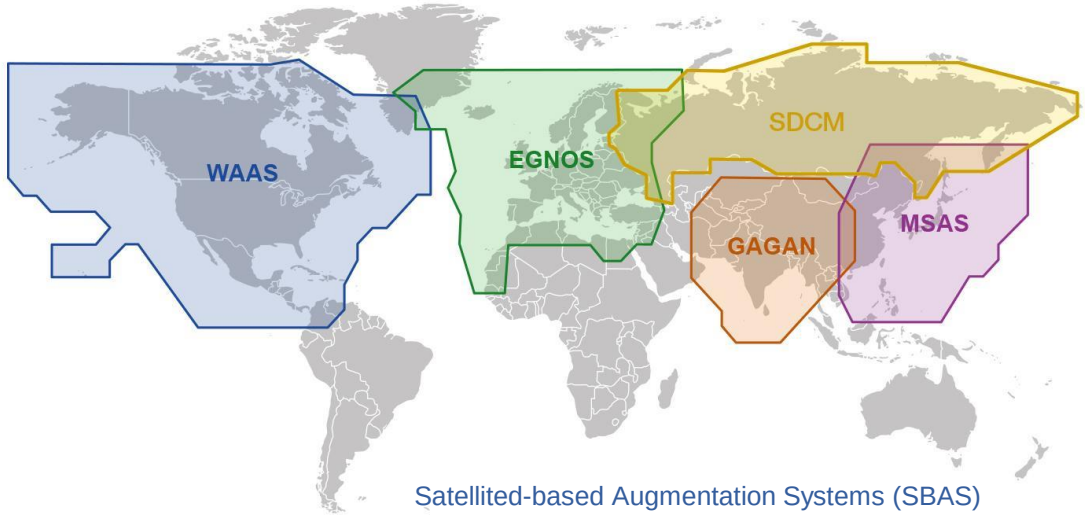
GNSS – A General Overview

- What is the Global Navigation Satellite System (GNSS)?

Frequencies / Signals

Beidou B1I	Galileo E1	GLONASS L1OF
Beidou B2I	Galileo E5	GLONASS L2OF
Beidou B3I	Galileo E6	GLONASS L1OC
Beidou B1C		GLONASS L2OC
Beidou B2a		GLONASS L3OC
Beidou B2b		

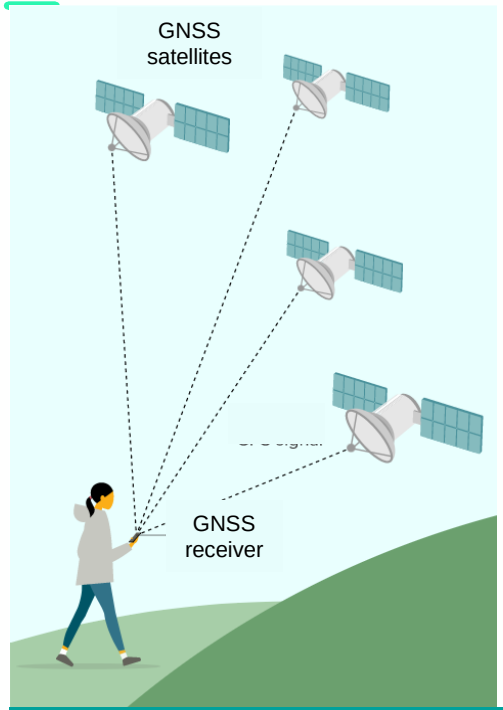
GPS L1	NavIC L1	QZSS L1
GPS L2	NavIC L5	QZSS L2
GPS L5	NavIC S-band	QZSS L5
		QZSS L6



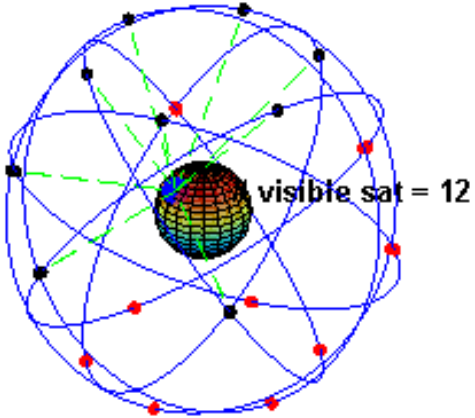
Satellited-based Augmentation Systems (SBAS)

There are 6 billion GNSS devices in use in 2024.
That number is expected to reach 9 billion by 2033.

Satellite navigation – the importance of having at least 4 satellites in line-of-sight



GNSS satellites are constantly in orbit, meaning that the number of satellites in view of a GNSS receiver is always changing



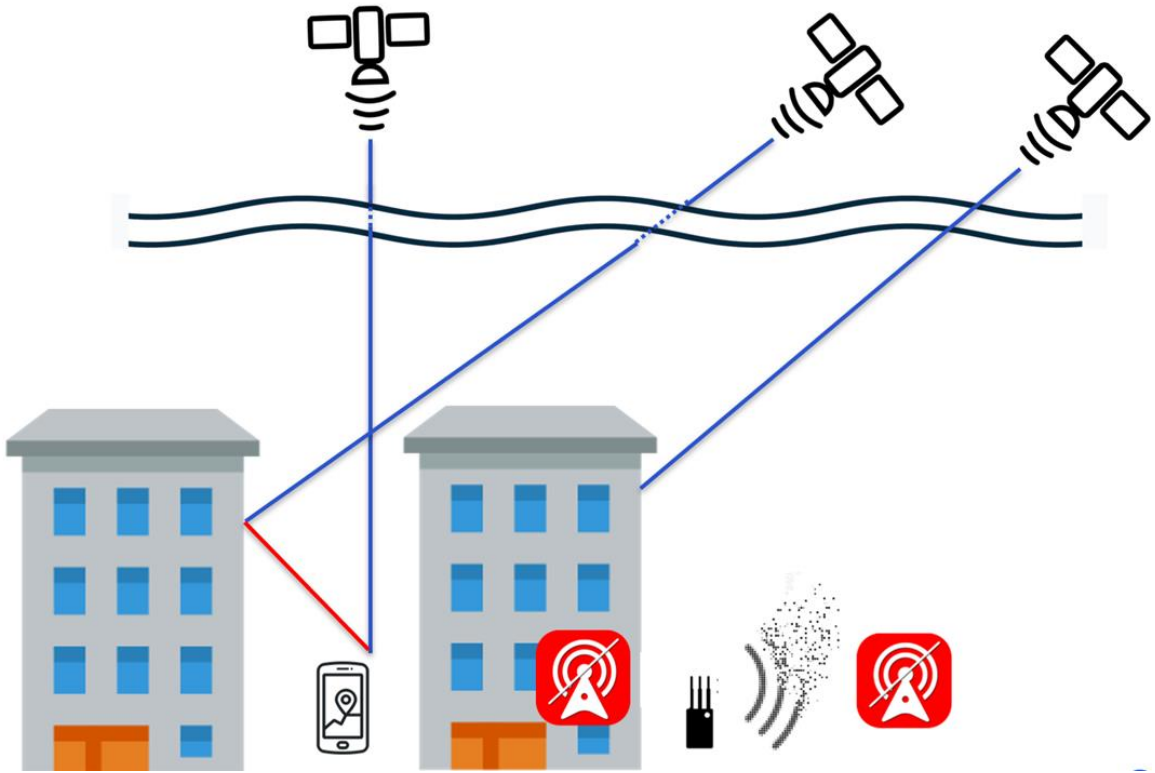
GNSS signals are very weak…the equivalent of a 40W light bulb from space (-130dBm on earth). This makes GNSS very vulnerable to interference

GNSS receivers in devices continuously track Radio Frequency (RF) signals from GNSS satellites via an antenna and measure Time of Arrival of the signal to calculate PNT

The factors that affect performance

Factors that affect performance can be split into four areas

- Errors from the Space segment
- Errors as the signal travels to the receiver
- Signal Processing errors in the receiver
- Signal Interference (Jamming/Spoofing)



What is a GNSS simulator?

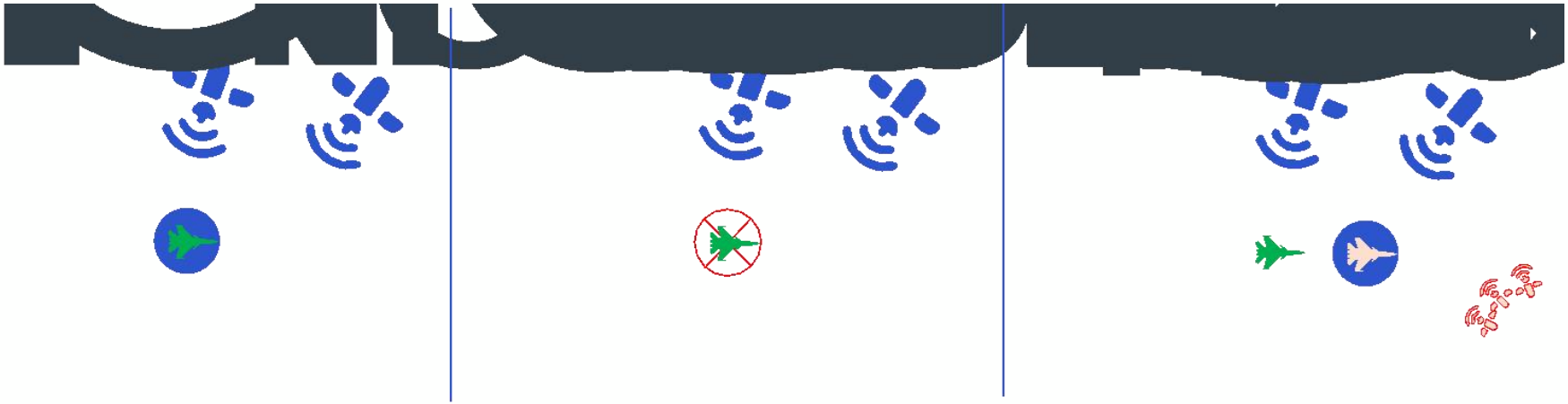
- A GNSS simulator **emulates the environment of a GNSS receiver** by modelling vehicle and satellite motion, signal characteristics, atmospheric and other effects, causing the receiver to navigate according to the parameters of the test scenario.
- The GNSS receiver will process the simulated signals **in exactly the same way** as it would those from actual GNSS satellites.
- A GNSS simulator provides a **superior alternative for testing**, compared to using actual GNSS signals in a live environment.
- Unlike live-sky testing, testing with simulators provides **full control** of the simulated satellite signals, both current and future signals, and the simulated environmental conditions.

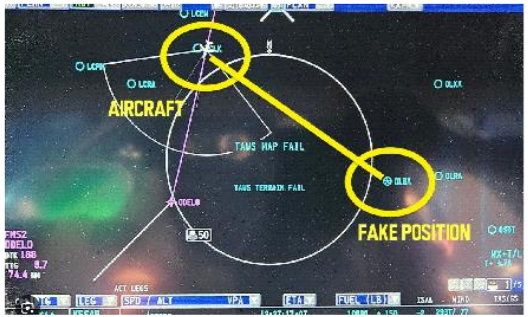
Examples of Spirent's GNSS simulators: the PNT X (top) and GSS7000 (below)

Typical Types of GNSS Testing

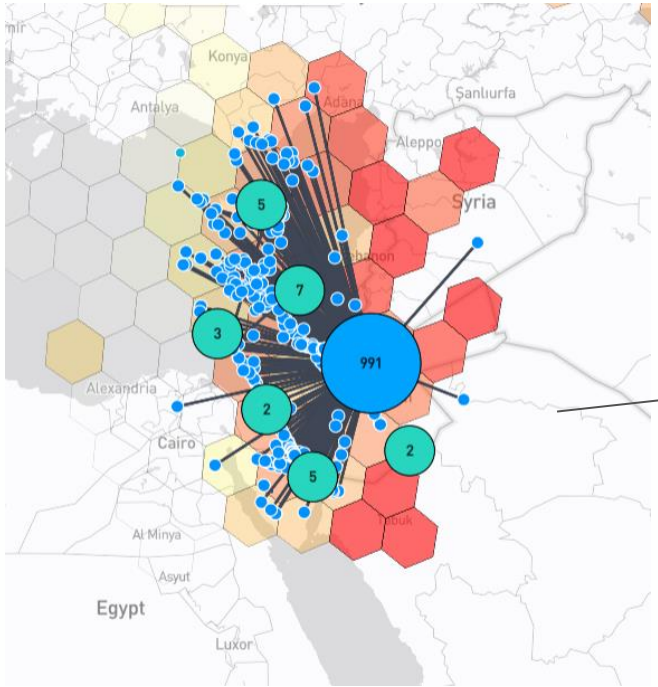
Test Type	Possible with Spirent's Portfolio?
1. Fundamental Performance	✓
2. Multi-constellation, Multi-frequency	✓
3. Dynamics Vehicles and Operations	✓
4. Multipath and Obscuration	✓
5. Hardware-in-the-loop (HIL)	✓
6. Embedded GPS/INS (EGI) & Inertial Measurement Unit (IMU) Simulation	✓
7. Correction and Augmentation	✓
8. Spoofing	✓
9. Jamming	✓
10. Atmospheric Conditions	✓

Difference between Jamming and Spoofing

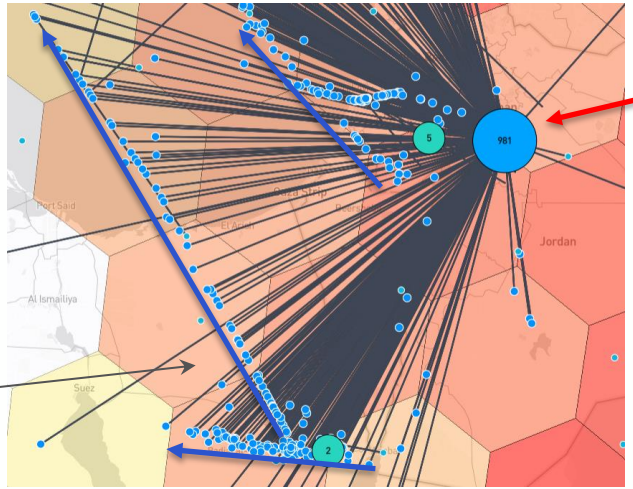




Jamming and Spoofing – Cases 09/11/2024 - 12/11/2024



Actual flight part



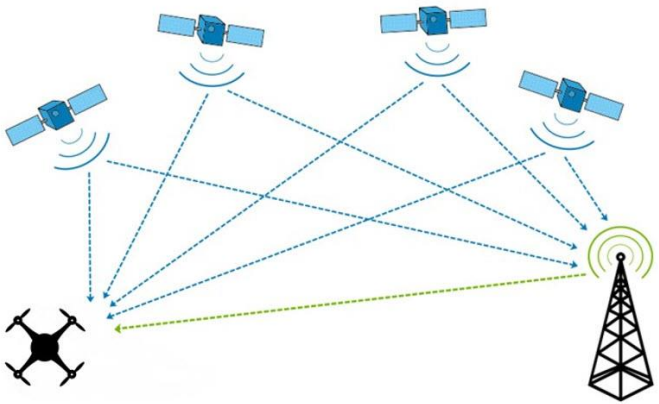
Position reported by FMS

https://spoofing.skai-data-services.com/

GNSS spoofing attacks - 1

Meaconing

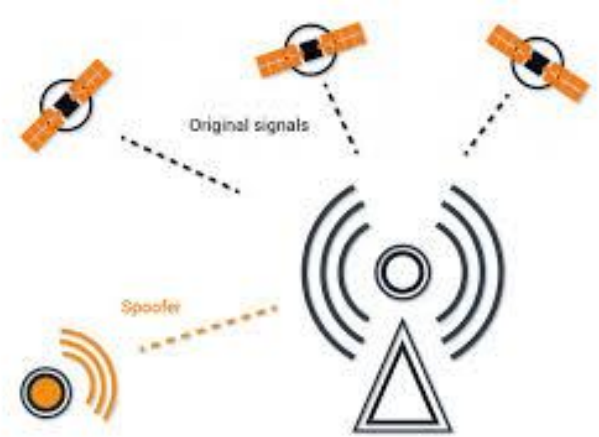
- The re-transmission of the authentic GNSS signals to a target receiver
- Meaconing attacks on GNSS can have significant impact and is one of the easiest
- If Spoofed, the GNSS receiver will think its location is the same as the location of the Spoofer antenna
- Harder for the GNSS receiver to distinguish between the real and fake signals as the navigation message is the same and all satellites in view may be spoofed.
- As the signal is only delayed, the Encryption algorithm may not detect the signal is re-broadcast

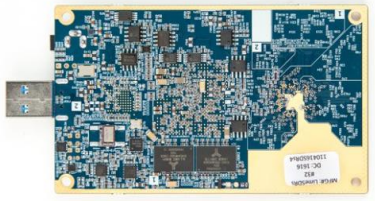


GNSS spoofing attacks - 2

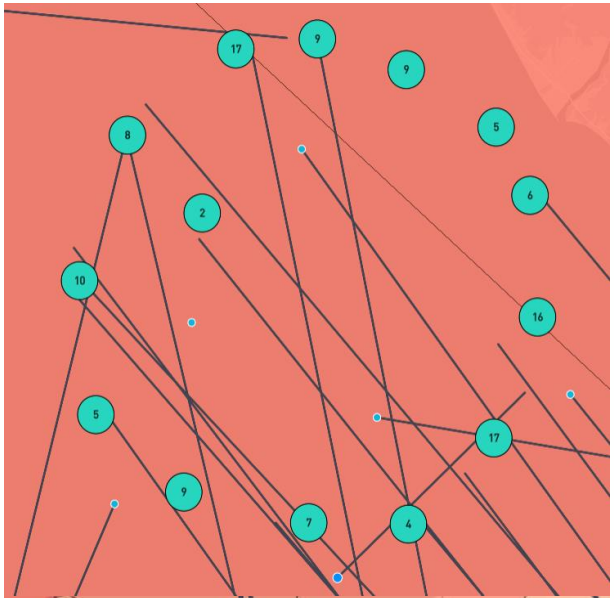
Transmission of a fake signal

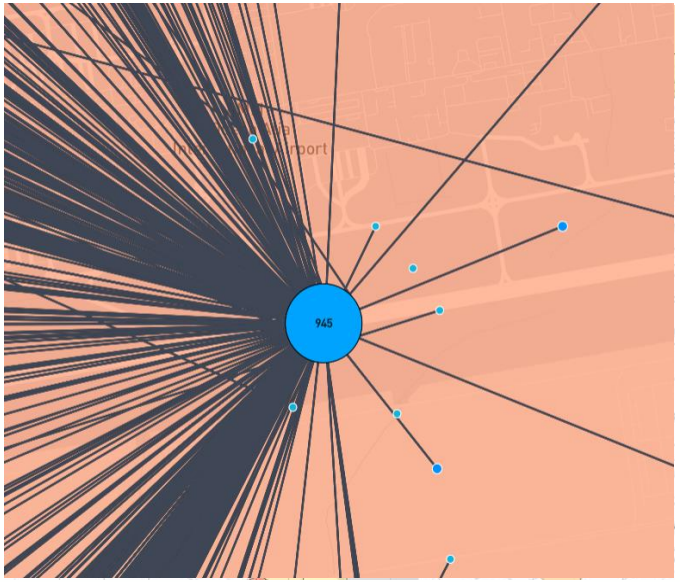
- Generation and broadcast of a fake GNSS Signal. The attacker replicates GNSS signals using an RF signal generator
- The aim is to manipulate the power, code and carrier phase of the replica signals to take control of the target receiver tracking loops
- Attacks can vary in sophistication but have the potential to have very high impact
- Spoofed Position or Time could now be anywhere the attacker wishes
- Significantly harder than meaconing especially when Multi-Constellation and Multiple Frequencies are being tracked





Jamming and Spoofing – Cases 09/11/2024 - 12/11/2024





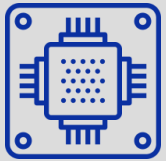
https://spoofing.skai-data-services.com/

Common techniques in commercial receivers to counter spoofing threats

Detection of spoofing

- Antenna (Ax)-aided techniques (1)
  - AoA detection w/ multiple Ax
  - Beamforming techniques
- Signal power monitoring techniques (2)
  - AGC power monitoring
  - Noise floor increase
- Correlation properties evaluation (3)
  - Correlation function shape
- Navigation message checks (4)
  - Nav data forecasting
- PVT consistency checks (5)
  - Jumps in position / time
  - Unreal acceleration / velocity
  - Doppler frequency, code phase & range consistency
  - RAIM
  - Cross GNSS system checks
  - Consistency with other sensors

Positioning Engine



Mitigation of spoofing

1. Signal authentication
   - SIS hash-type encryptions
2. Alarms and thresholds
   - Appropriate alarm thresholds
3. Alternative navigation sensors handover
   - Augmentation systems, e.g. IMU or DR
   - Alternate location systems, e.g. WIFI
   - Stable handover clocks for timing applications

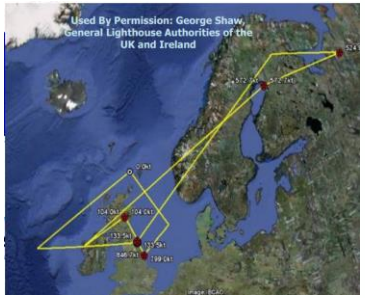
Which form of detection and mitigation should I use?

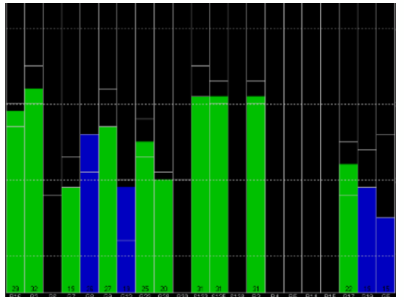
- **Cost** – Angle of arrival antennas are very expensive and may be export controlled

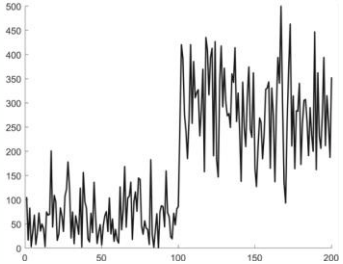
- **Encrypted Signals** A GNSS receiver that can track encrypted codes such as Galileo OSNMA may struggle to with a meaconing attack

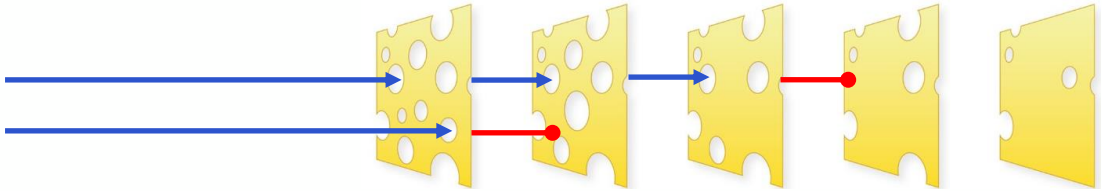
- **A-RAIM** Effective, but only when some satellites are spoofed
- **Cross GNSS** system checks. Cost effective but a meaconing attack may re-broadcast everything in view

- **No perfect solution exists. The more layers of protection the better the resilience**



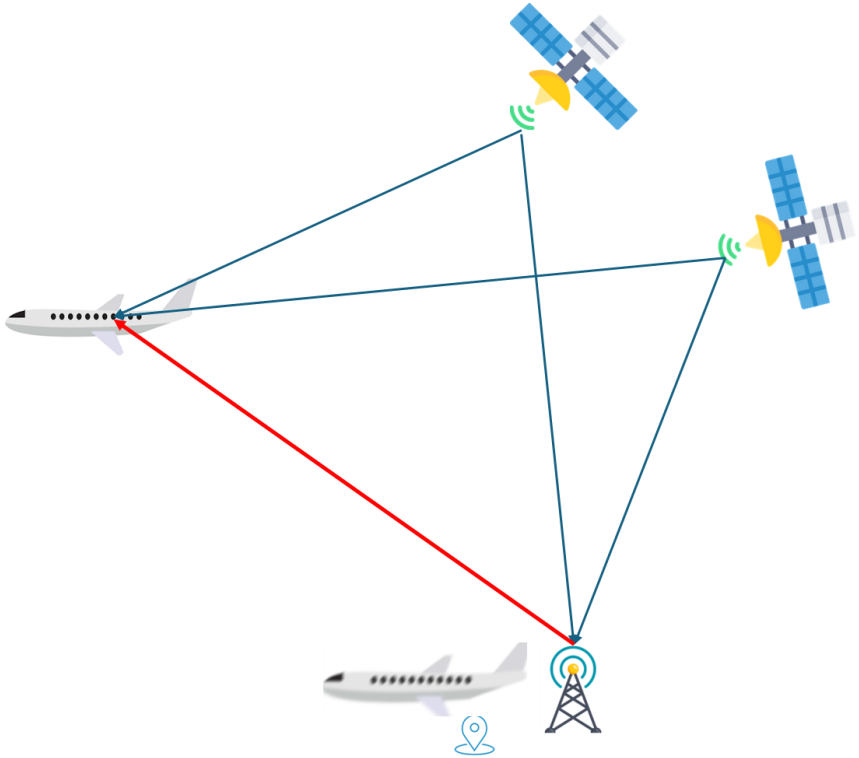




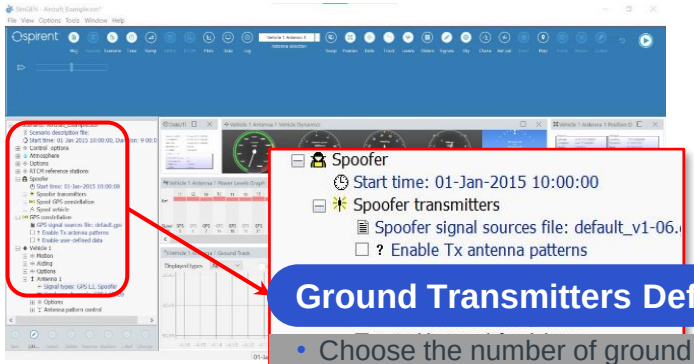


Realism is important in Simualtion!

- To test the receiver mitigation, you must correctly simulate the attack
- Appropriate factors must be modelled and automatically controlled in the simulation:
  - Angles of arrival
  - Delays
  - Doppler changes
  - Noise
  - Signal phase
- Spoofing signals where the spoofer is in the sky is not realistic

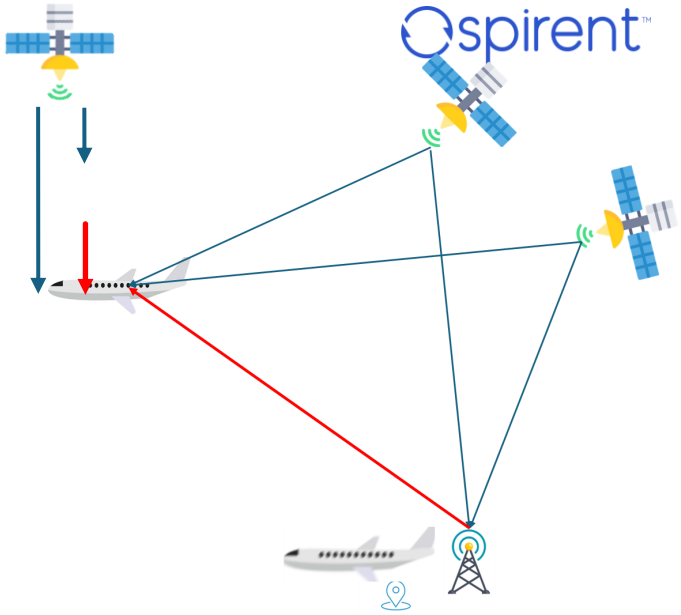


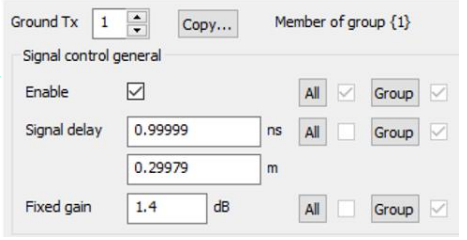
Meaconing Simulation

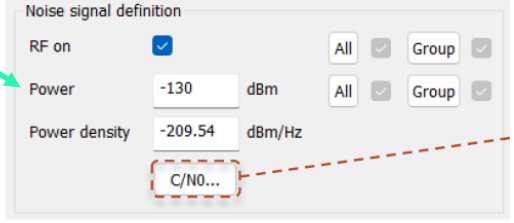


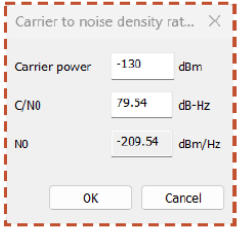
Ground Transmitters Definition

- Choose the number of ground transmitters and their location (absolute or vehicle relative)
- Choose modelled or fixed transmit power levels
- Add Antenna patterns to the Spoofer (Receive and Transmit)
- Apply motion to transmitters either pre-defined or in real time
- Apply processing delays of the signal through the spoofer
- Propagation delays to the DUT are modelled including Doppler and Power
- Add Noise to the Spoofer signal to mimic a Low noise Amplifier





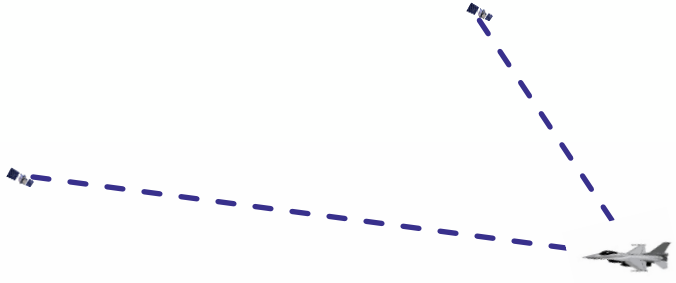




Terrain Modelling PNT X

3D Realism for Jamming and Spoofing Scenarios

- **3D visualisation** of static and dynamic jammers and spoofers.
- Real-time calculation of **obscuration** and **multipath** effects on interference signals, alongside GNSS.
- Single software and hardware solution to support all types of scenarios.



Jammer/Spoofer

Jammer/Spoofer

Jamming can be performed in a similar way either externally or in band interference

Spirent's PNT Product Portfolio

For **high-end and mil/gov R&D** customers

PNT X

PNT X is a revolutionary simulation system that addresses the increasing complexity of the PNT environment. This all-in-one solution generates all GNSS constellations, RF threats, and signals of opportunity available for comprehensive test coverage and high realism.

For **high-end** civil and **integrators** customers

GSS7000

GSS7000 delivers every current and planned signal via 256 channels and two independent RF outputs.

Create the most precise and realistic test environments – with comprehensive control over signals generated, power levels and scenario dynamics.

For **field testing**

Portable Simulator

Multi-frequency, multi-constellation capability with up to 36 channels easily configured in the field.

Easily portable and can be run using an external battery pack.

For **field** and **lab** testing

GSS6450

The GSS6450 record & playback system brings the real world into the lab in dynamic detail, for high fidelity testing using real-world signal environments.

Tailored Solutions for CRPA

Test the full antenna in an Over-the-Air chamber

Test the Antenna electronics in conducted mode

The Spirent Academia Program

Building the future of resilient PNT technologies through university partnerships

Spirent ACADEMIA PROGRAM

- Teaching & Lab Support
- Research & Innovation
- Knowledge Transfer

Spirent

UKRI Innovate UK

THE ROYAL SOCIETY

Royal Academy of Engineering

Research and Innovation in emerging technology

Core Segments	Emerging Segments	Product Improvement
Aviation, AI, Automotive, Handheld Devices, GNSS Receivers, Maritime, Space Weather	Space Weather, New Space, Robotics, AI, Sensor Fusion, LEO, Autonomous Vehicles, Non Terrestrial Networks	User Experience, Efficient Data compression

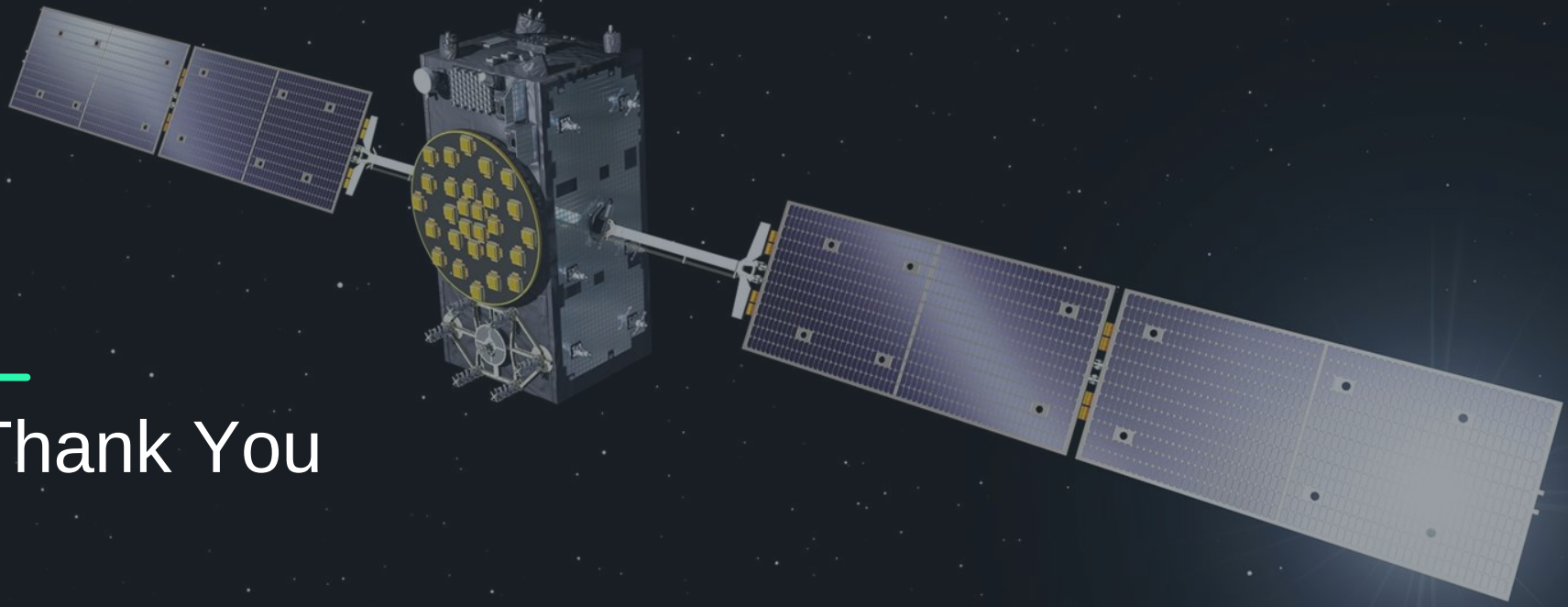
Labs and teaching material

Your research partner

>30 Engaged Universities Globally

YOTTAVOLT TechDays

Spirent™



Thank You