septentrio
part of HEXAGON

CELEBRATING 25 YEARS
OF SECURE & ROBUST
GNSS POSITIONING

GNSS Jamming and Spoofing: Detection and Mitigation

Stefan Söderholm (stefan.soderholm@septentrio.com)

Director PNT Product Development

2 September 2025

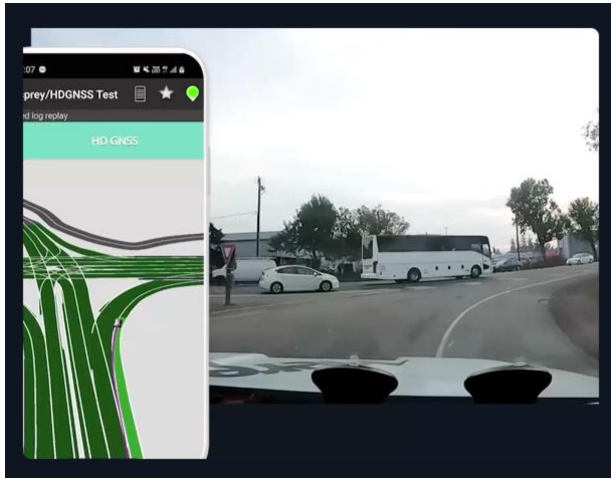
Agenda

- Introduction
- Jamming
  - Problem and Mitigation
  - Testing
  - Results (CW, Chirp, etc...)
- Spoofing
  - How
  - Detection and Mitigation
  - Results
- Take Away

Introduction

Work

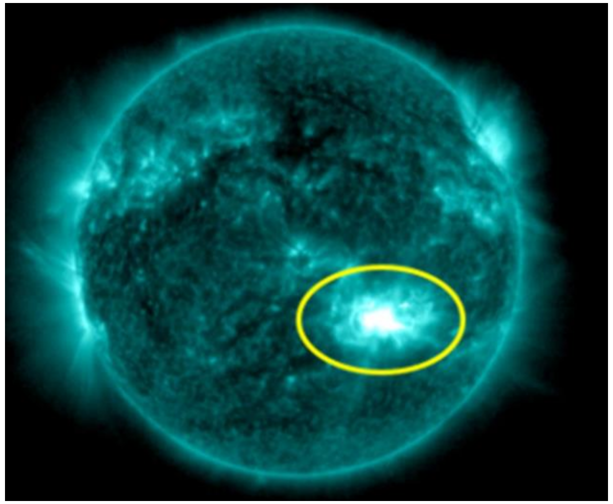
- Fastrax 2000-2013
  - Receivers for Suunto, Benefon, Nokia, etc
- uBlox 2013-2014
  - Automotive grade receiver
- Finnish Geospatial Research Institute (FGI) 2014-2018
  - High precision Positioning, new signals, jamming, spoofing
- HERE Technologies 2018-2020
  - High precision correctional service
- Septentrio 2020->
  - High precision receivers



septentrio
part of HEXAGON

R&D at Septentrio

- Currently working as:
  - General Manager, Septentrio Finland Oy
  - Team Leader, PE Integration
  - Director PNT Product Development
    - 4 teams: Chips, HW, DSP, PE, Integration Code
    - Not: WiFi, CAN, Cellular, Boxed receivers,...
- Activities:
  - Next gen Products (GreCo5 based) – AsteRx-m5, Mosaic-G5, Px6, ...
  - Innovation: RTK (3F-RTK), PPP-AR, tightly coupled INS
  - New signals: HAS, SAS, OSNMA, LEO-PNT
  - Performance: Iono mitigation, AJ/AS
  - Projects: Collaboration within Hexagon, EAKR, Timing, ...



Septentrio

Septentrio Finland,
Espoo, Finland

Septentrio HQ,
Leuven, Belgium

Septentrio Americas,
Los Angeles, USA

Septentrio China
Shanghai, PRC

Septentrio Japan
Tokyo, JP

Our markets

Machine Automation

Marine

Construction

Mining

Logistics

Agriculture

Autonomous driving

Survey and Mapping

Survey

GIS

Mobile Mapping

Unmanned Systems

Scientific/Reference

Reference Receivers

Timing Receivers

Space Weather

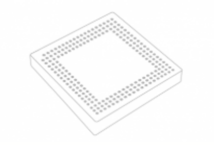
Aerospace/Defense

Aerospace

Defense

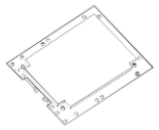
septentrio
part of HEXAGON

Our Products



Modules

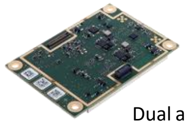
Our latest
Mosaic-x5



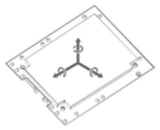
Boards

UAS models

Single antenna



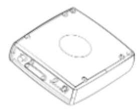
Dual antenna



GNSS/INS
boards

Non-tethered

tethered



Housed
receivers

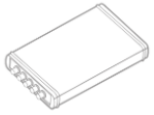
Single antenna

Dual antenna
Or GNSS-INS

Dual antenna

Smart
antenna

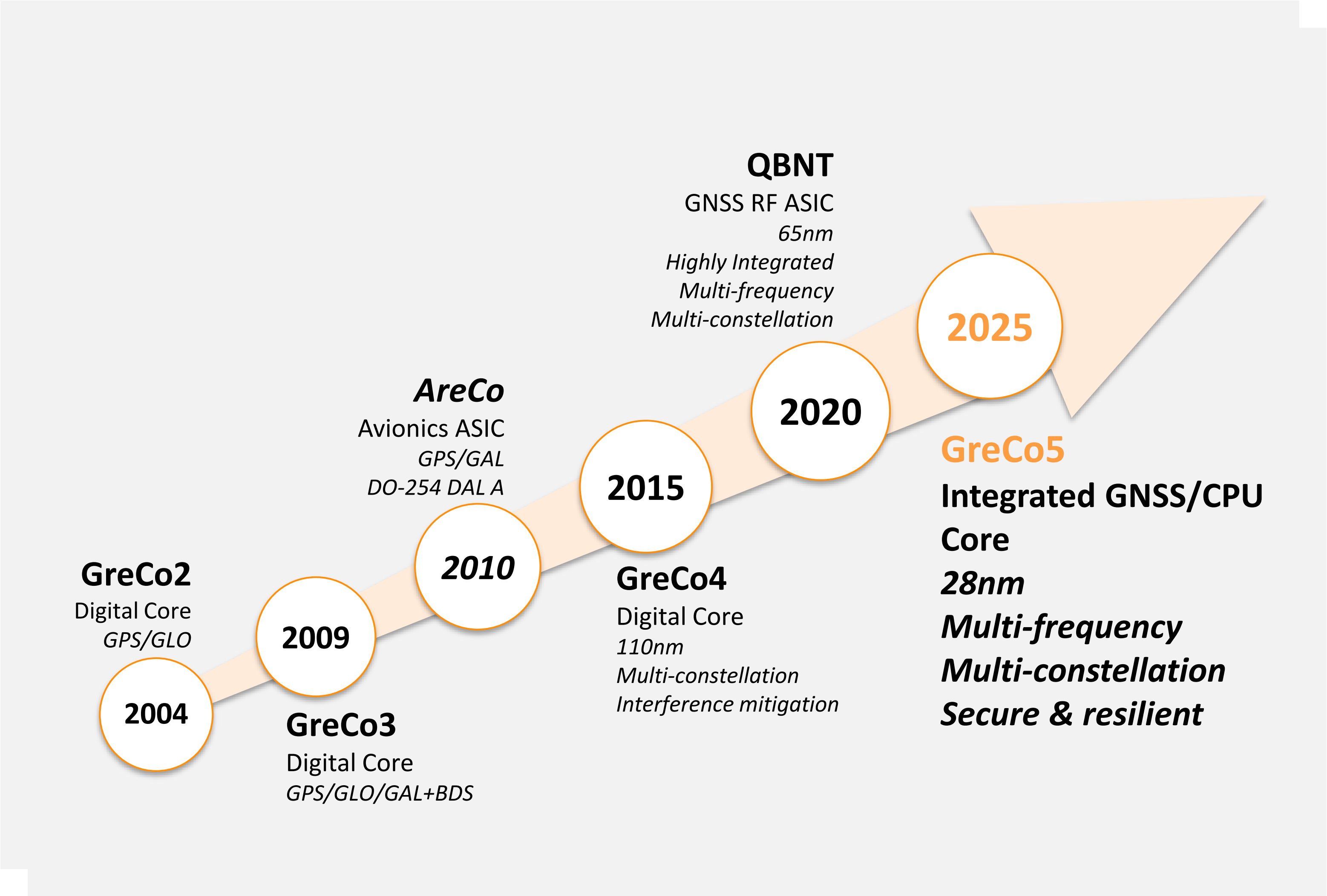
Flexible
Base & rover



Scientific
Receivers

Best measurements,
Timing or
Scintillation

Close up on mosaic-G5



2004

GreCo2
Digital Core
GPS/GLO

2009

GreCo3
Digital Core
GPS/GLO/GAL+BDS

2010

AreCo
Avionics ASIC
GPS/GAL
DO-254 DAL A

2015

GreCo4
Digital Core
110nm
Multi-constellation
Interference mitigation

2020

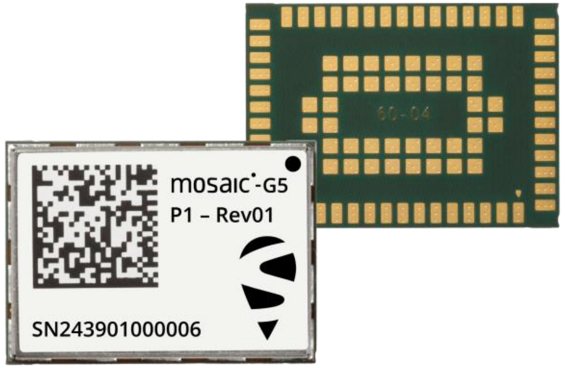
QBNT
GNSS RF ASIC
65nm
Highly Integrated
Multi-frequency
Multi-constellation

2025

GreCo5
Integrated GNSS/CPU Core
28nm
Multi-frequency
Multi-constellation
Secure & resilient

- Success deeply entrenched in our **unique chip design**
- **Unmatched innovation** combined with state-of-the-art software and resilience features
- Recognised **market leader** in high-end GNSS chips
- Setting **industry standards** for high precision performance

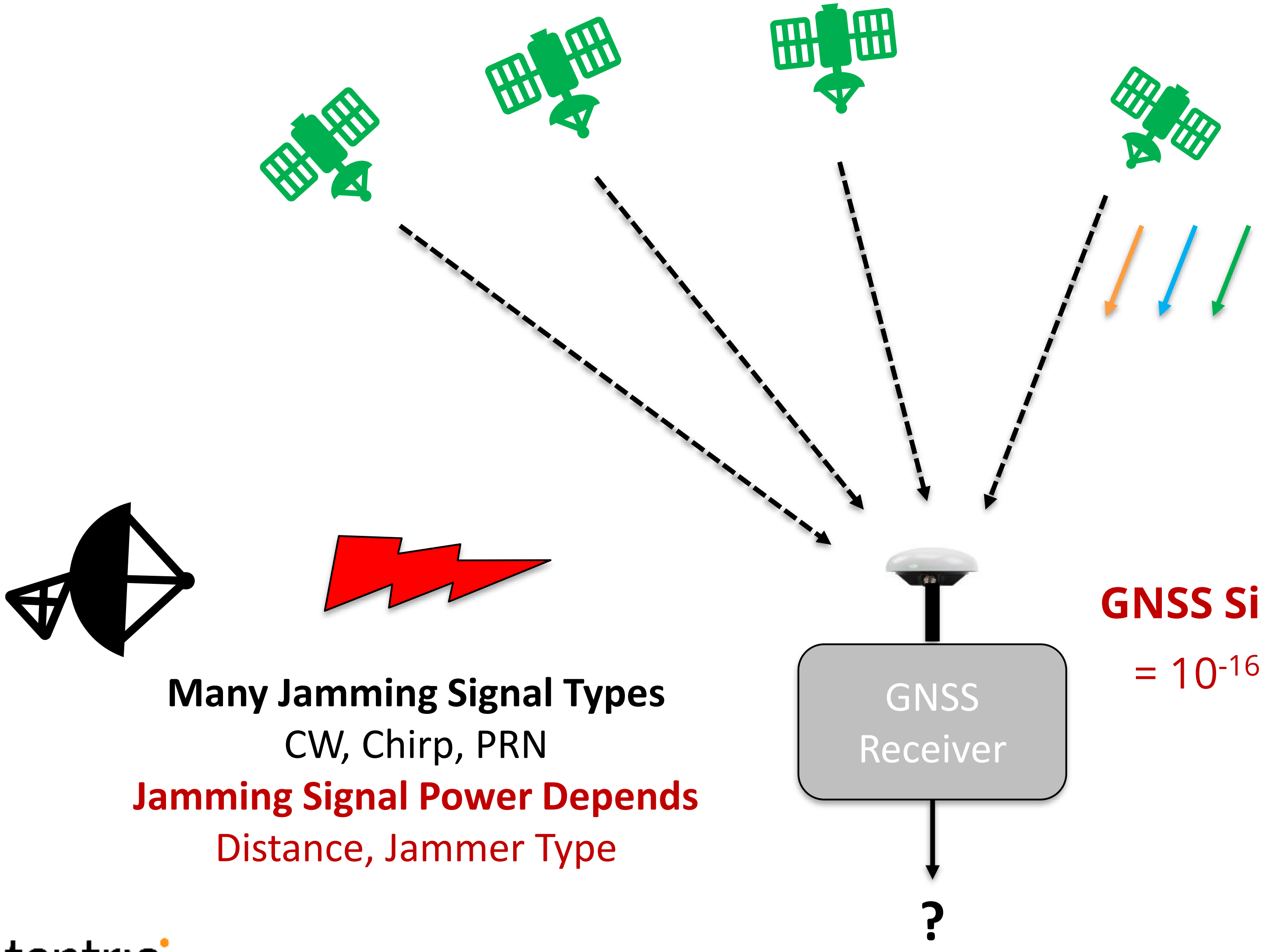
Close up on mosaic-G5



septentrio
part of HEXAGON

Jamming – Problem and mitigation

The Jamming Problem: Blocking the Receiver



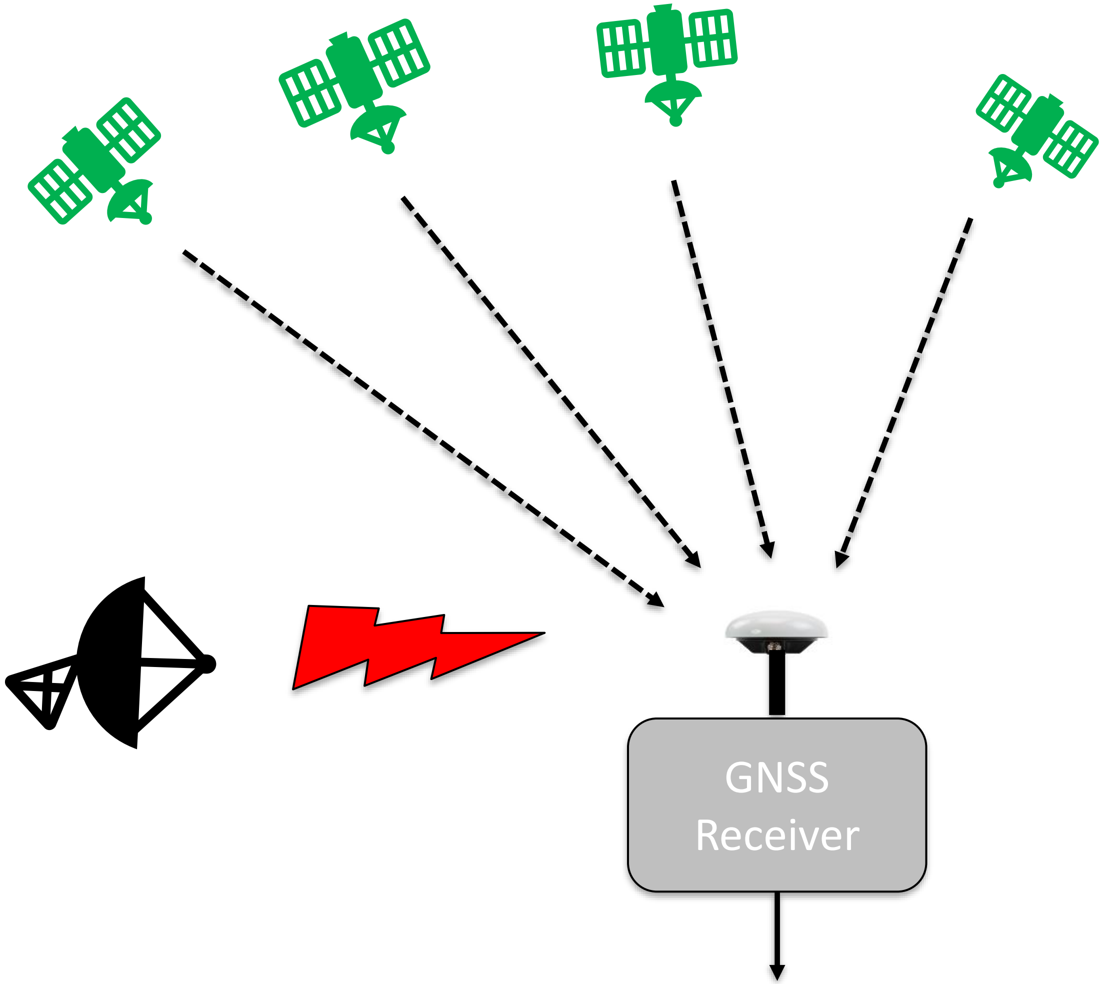
Variety of GNSS Signals
L1BC, E5a, E5b, E6

GNSS Signal Power is Weak
= 10^{-16} Watt (0.1 femtoWatt)

Many Jamming Signal Types
CW, Chirp, PRN

Jamming Signal Power Depends
Distance, Jammer Type

Jamming Mitigation



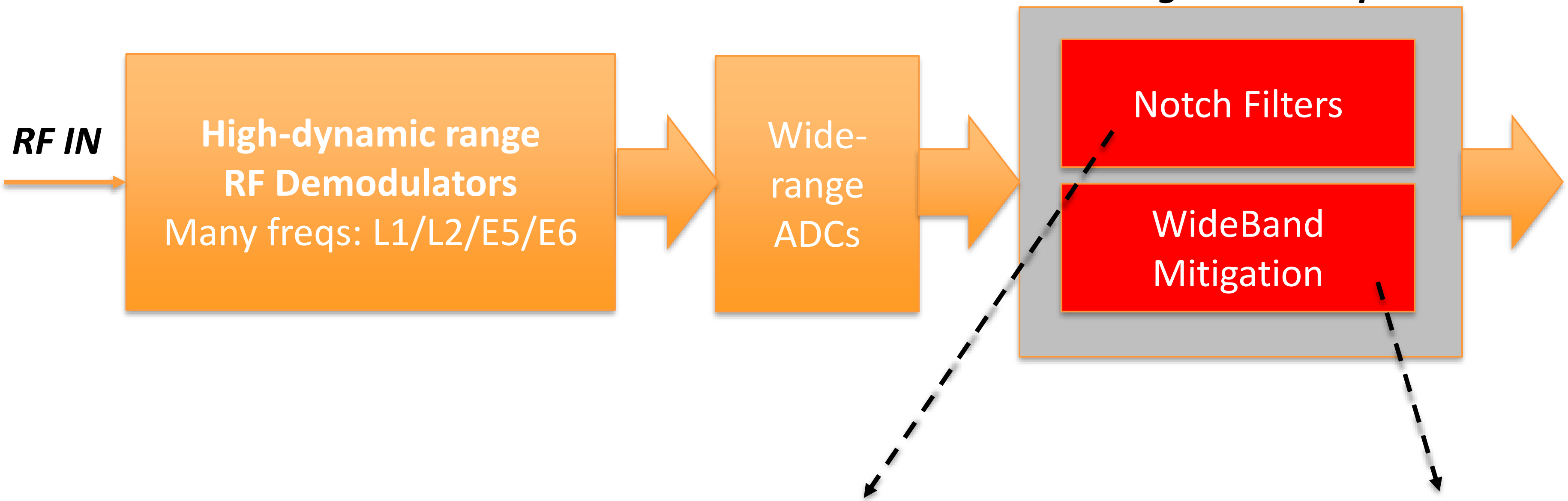
N50°50'54.87"E4°43'55.63"

Signal Level Mitigation
Some signals are more robust than others

Receiver Level Mitigation
Active Interference Rejection

Receiver Level Mitigation

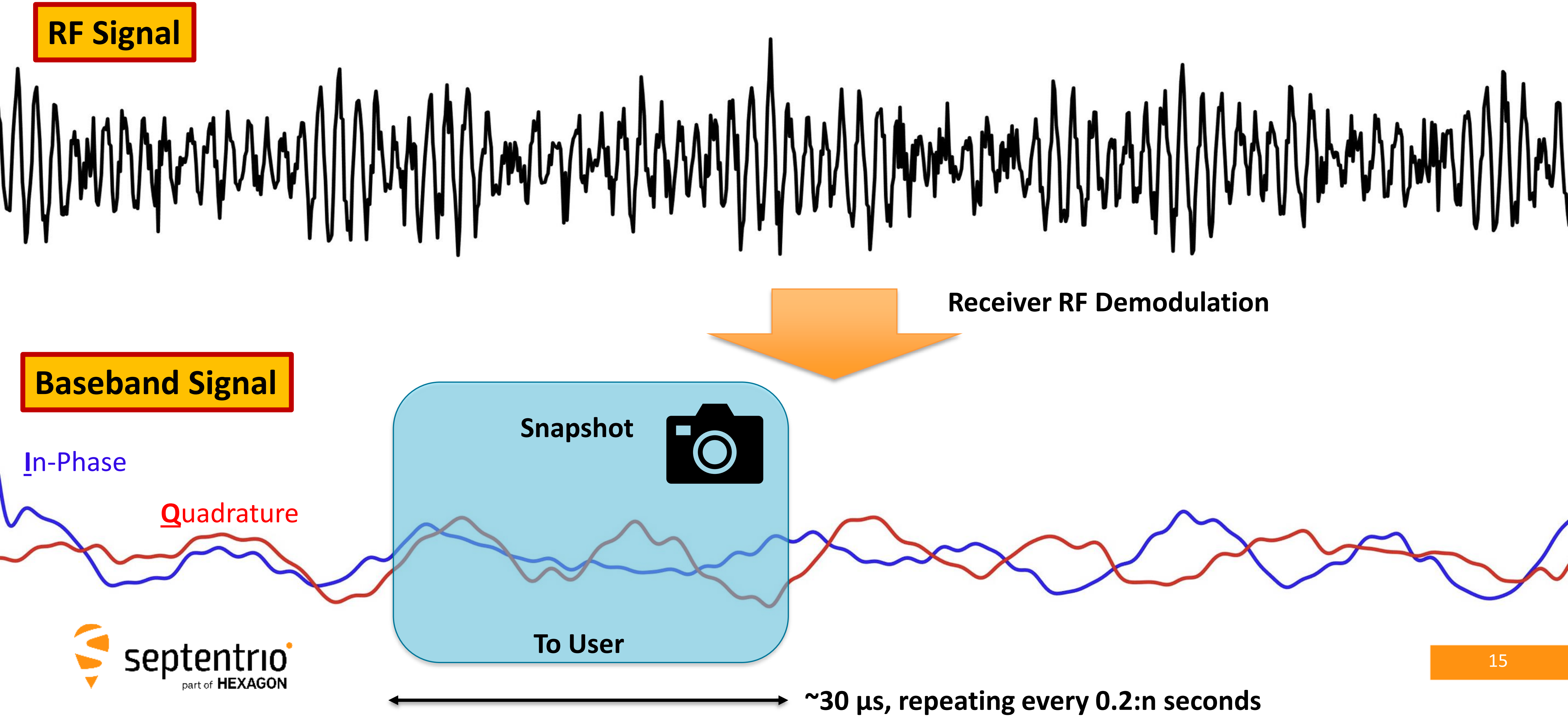
Anti-Jamming
Signal Cleanup



Removes Affected Spectrum
Automated operation without outages

Removes Chirp Jammers
Automated operation without outages
Advanced digital circuit

Raw Signal Awareness: Baseband Samples



RF Signal

Receiver RF Demodulation

Baseband Signal

In-Phase

Quadrature

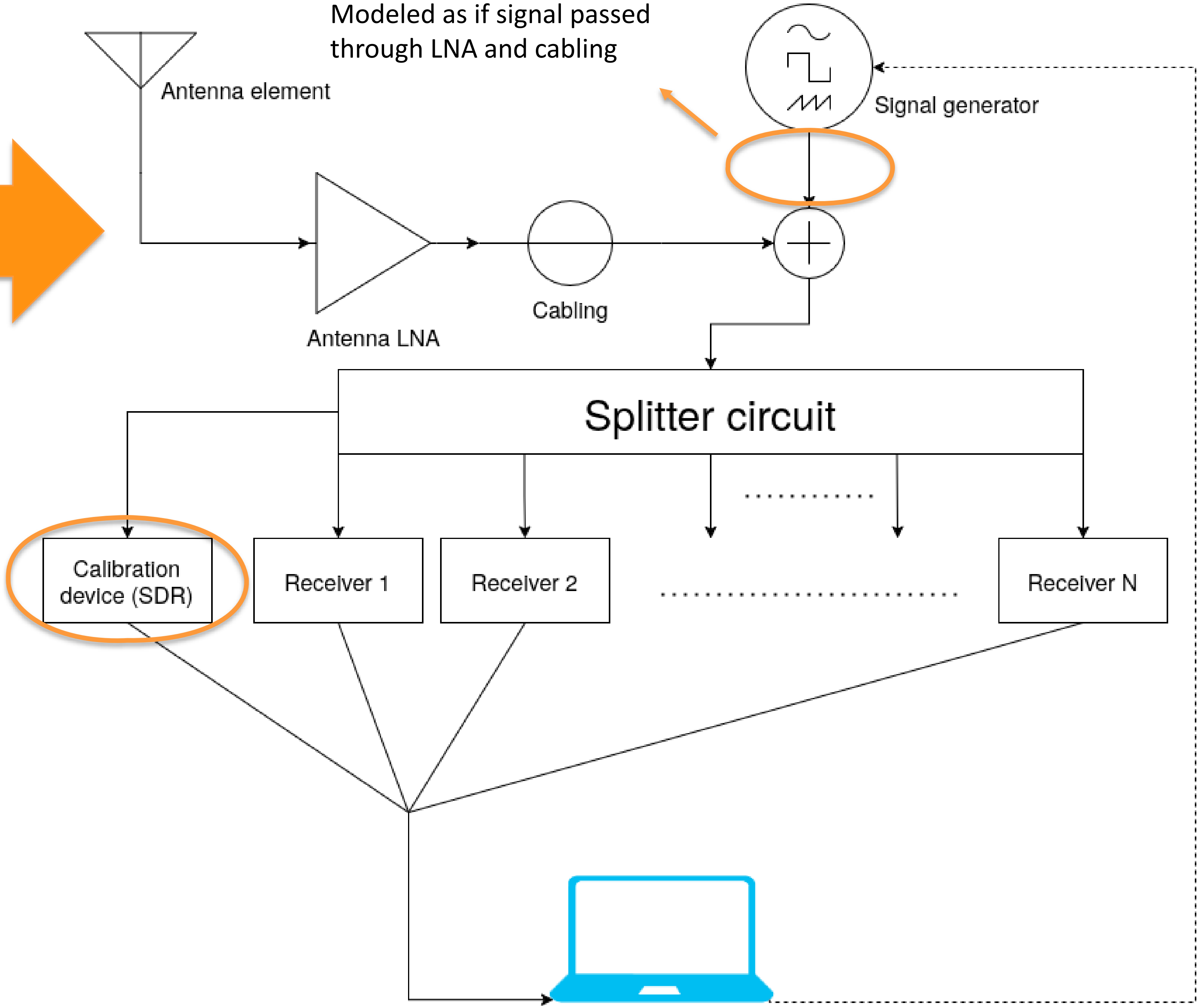
Snapshot

To User

~30 µs, repeating every 0.2:n seconds

Jamming - Testing

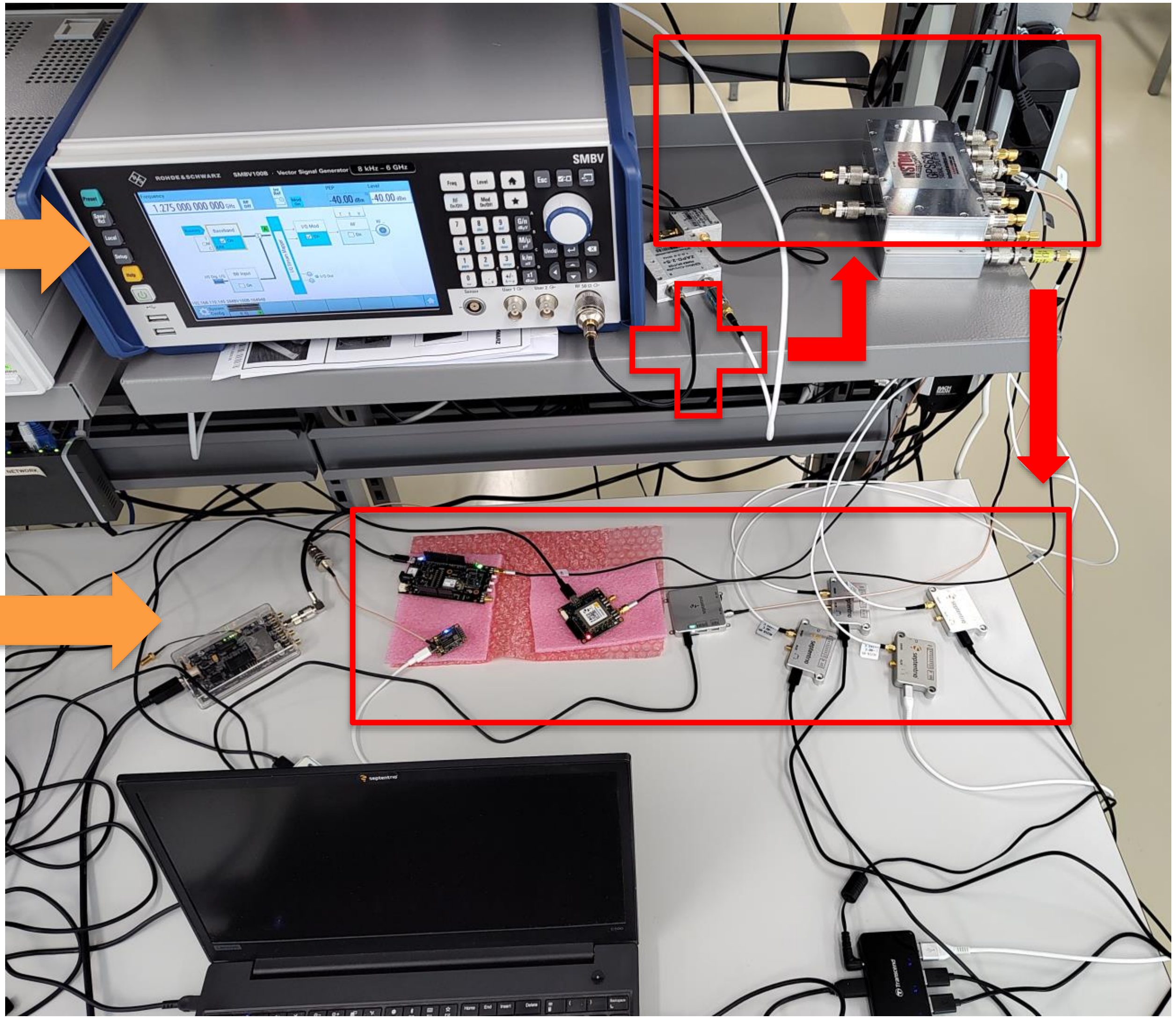
Test Setup



Interference reference point

Modeled as if signal passed through LNA and cabling

Test Setup



Arbitrary Waveform RF Signal Generator (500 MHz Tx Bandwidth)

Calibration device (SDR)

Splitter circuit

Combiner

Receivers

Norway Jammertest

- **Advanced outdoor jamming & spoofing tests**
  - Very remote location avoids impact
  - Multi-constellation, multi-frequency spoofing!
  - Large variety of jamming and spoofing scenarios
- **Organized by Norwegian Governmental Agencies**

Statens vegvesen

Justervesenet

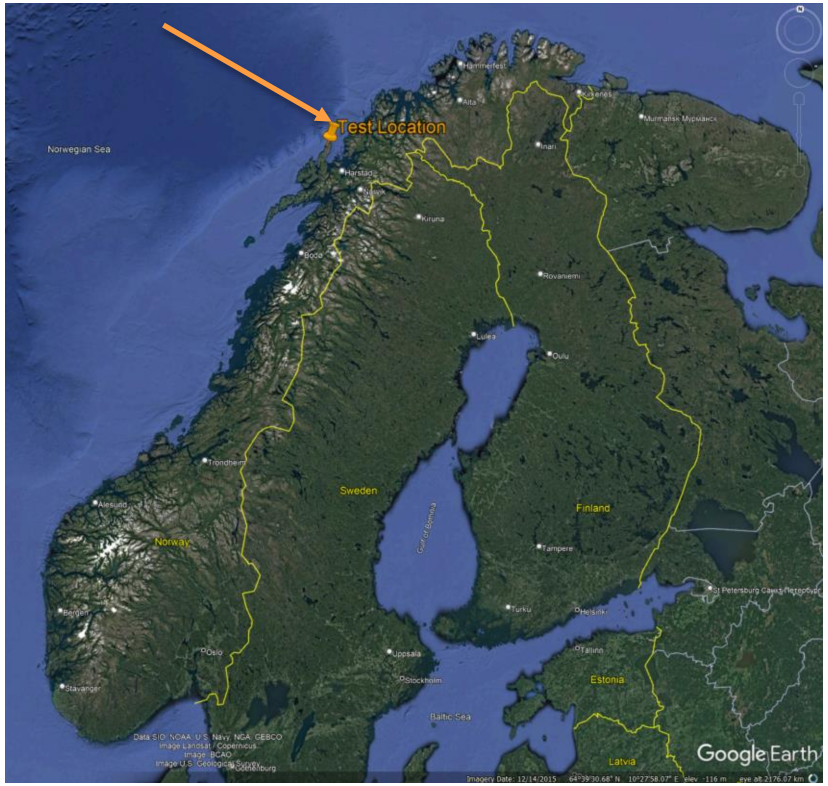
Norsk Romsenter
Norwegian Space Agency

NKOM
Nasjonal
kommunikasjons-
myndighet

FFI Forsvarets
forskningsinstitutt
Norwegian Defence Research Establishment

TESTNOR

- **Participants:**
  - Authorities
  - Industry
  - Academia



Septentrio at Jammertest 2023

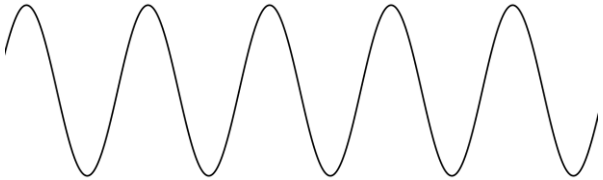
- Three Heros
- Static and dynamic setups
- Many antenna and receiver types

YOUR NEXT GENERATION GPS IS TESTED HERE
SEPTENTRIO PRECISE POSITIONING
septentrio

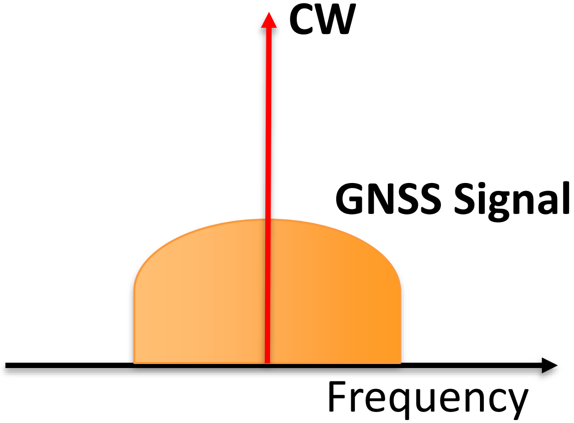
Jamming - Results

Continuous Wave (CW)

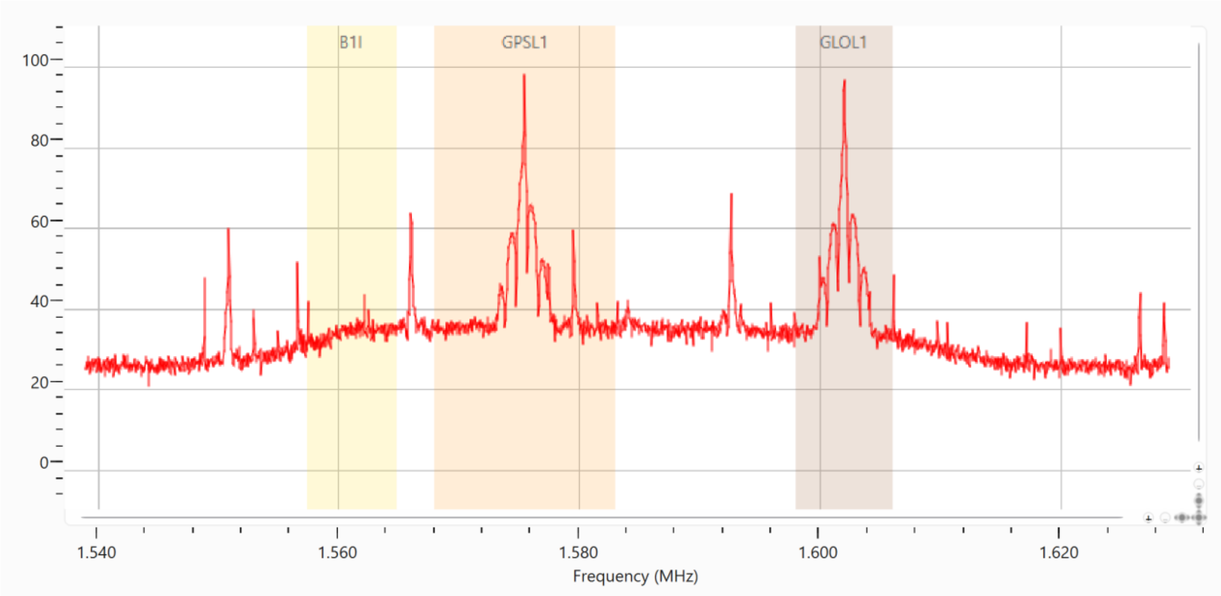
- **Plain Sine Wave**



- **At Center Frequency of Targeted Signal Band**
  - Classical way of jamming
    - Norway Test, Middle East,…

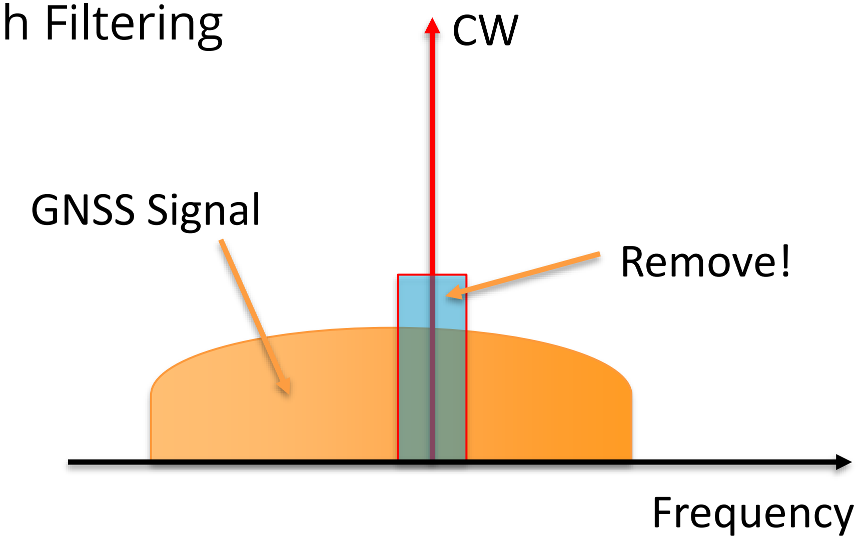


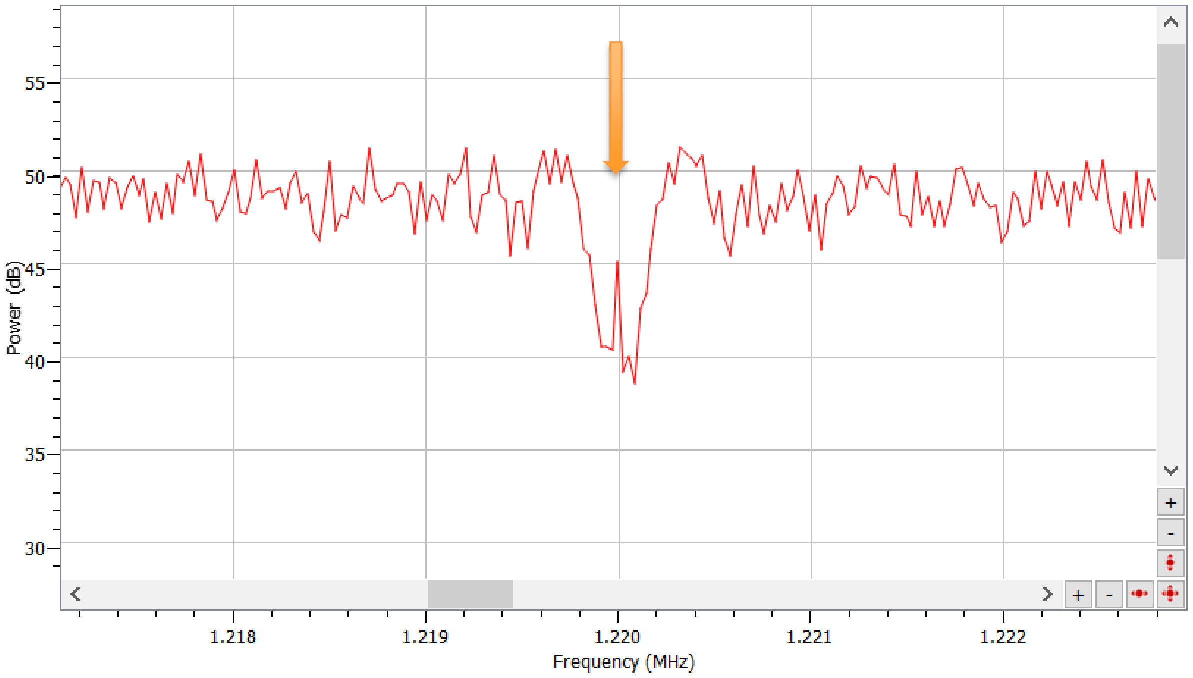
Example from Norway Jammertest



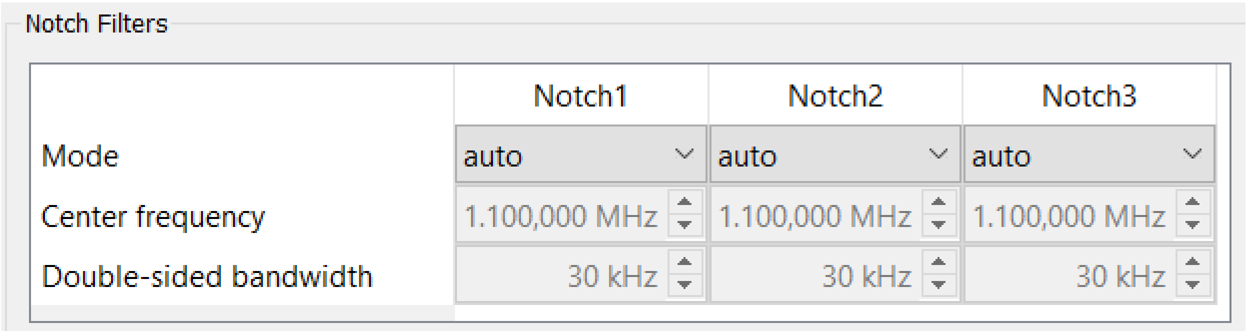
Mitigation Techniques for CW Jamming

- Notch Filtering



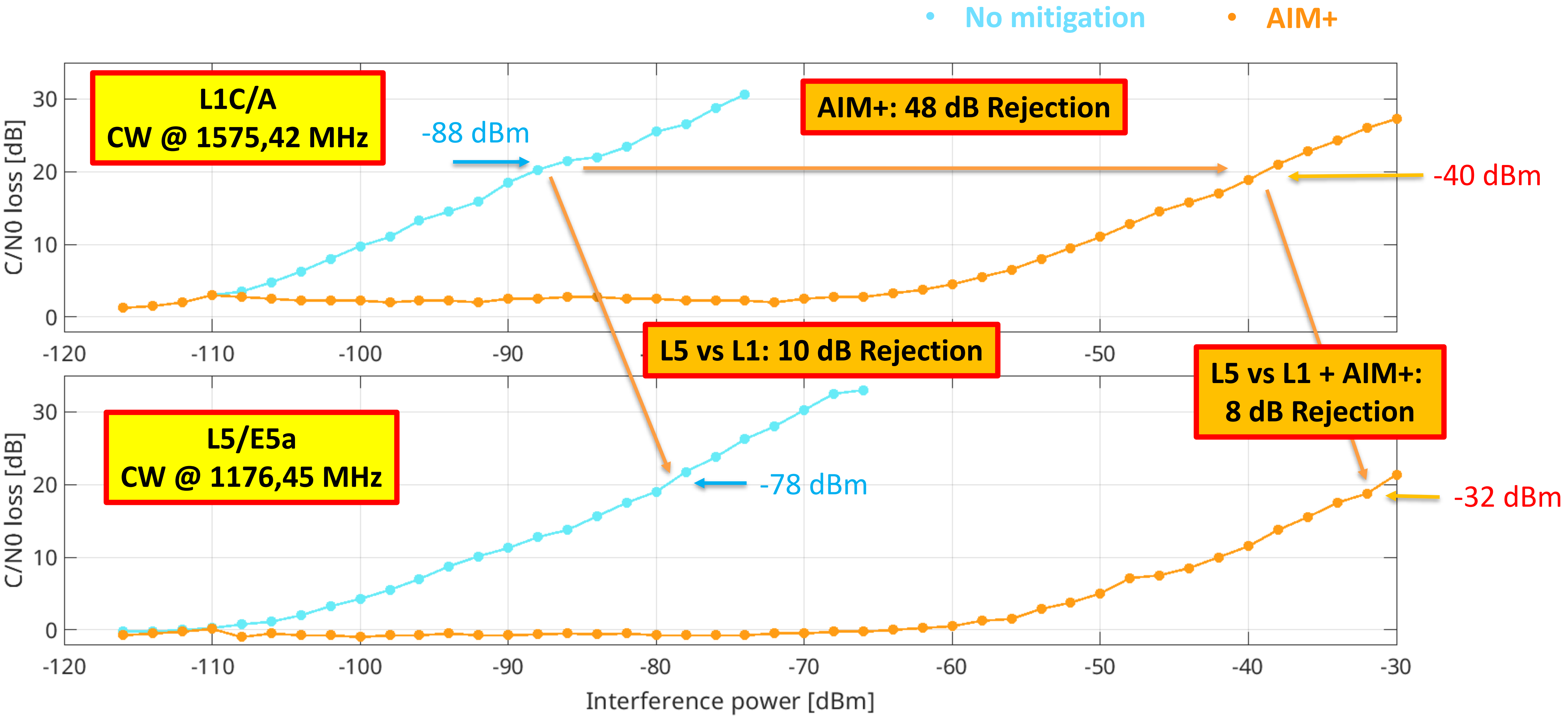


- Digital Implementation
- Dynamic Range Matters → Multi-Bit ADCs
- Septentrio: 45 dB rejection


Notch Filters

	Notch1	Notch2	Notch3
Mode	auto	auto	auto
Center frequency	1.100,000 MHz	1.100,000 MHz	1.100,000 MHz
Double-sided bandwidth	30 kHz	30 kHz	30 kHz

Continuous Wave (CW), L1 vs L5



L1C/A
CW @ 1575,42 MHz

AIM+: 48 dB Rejection

L5 vs L1: 10 dB Rejection

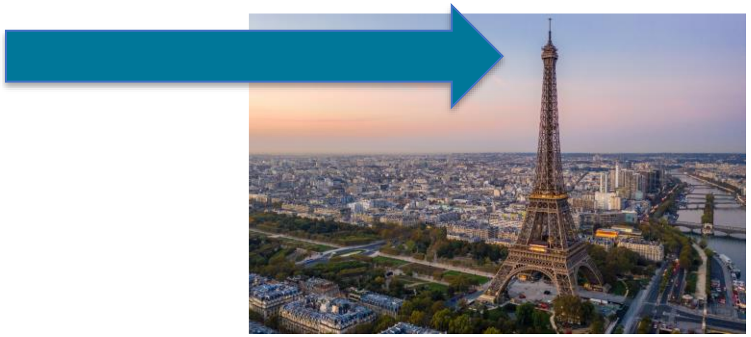
L5 vs L1 + AIM+:
8 dB Rejection

L5/E5a
CW @ 1176,45 MHz

CW Jamming from Eiffel tower

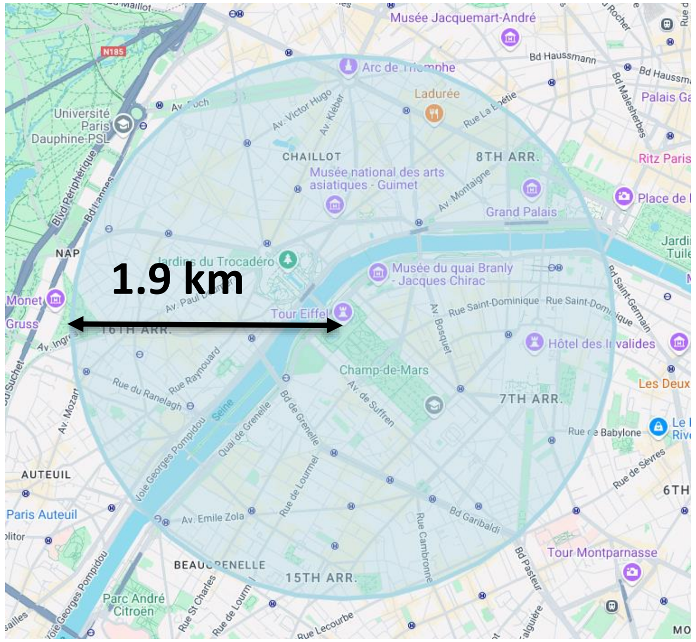
- **1 Watt Carrier at Every Center Frequency**
  - Free space propagation
  - Configuration: GPS+GALILEO+BEIDOU

➔ Area where position fix is lost:

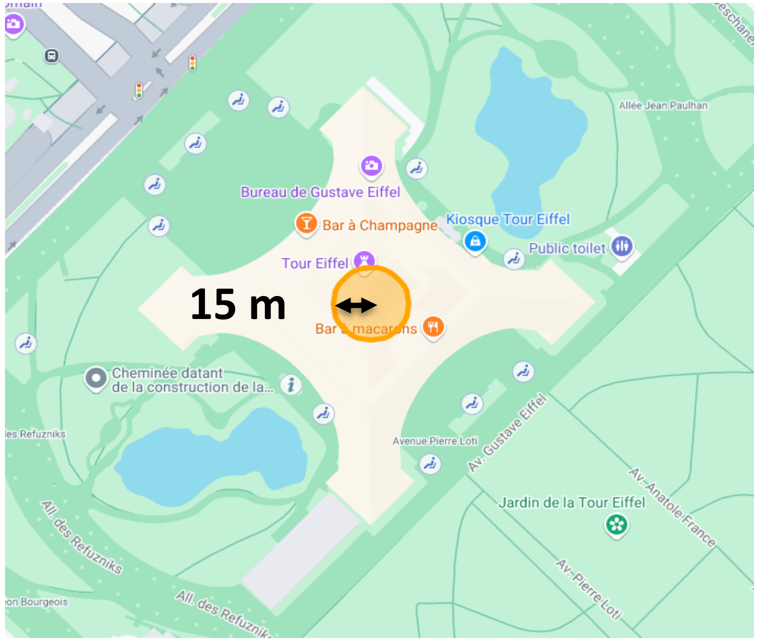


$$\mathrm{FSPL} = \left(\frac{4\pi d}{\lambda}\right)^2$$

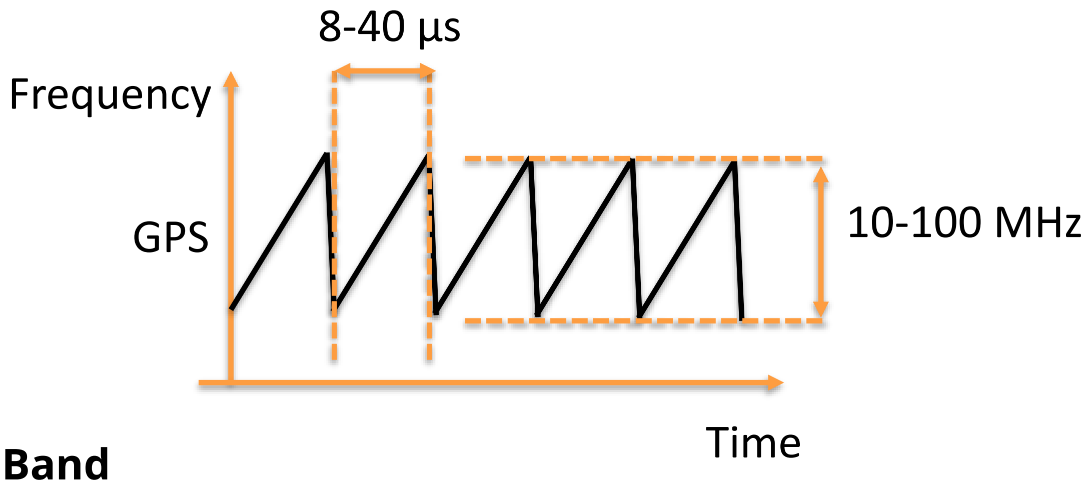
No Mitigation



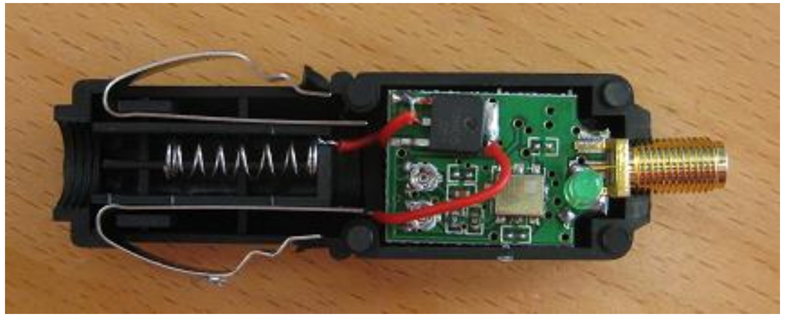
AIM+ Interference Mitigation

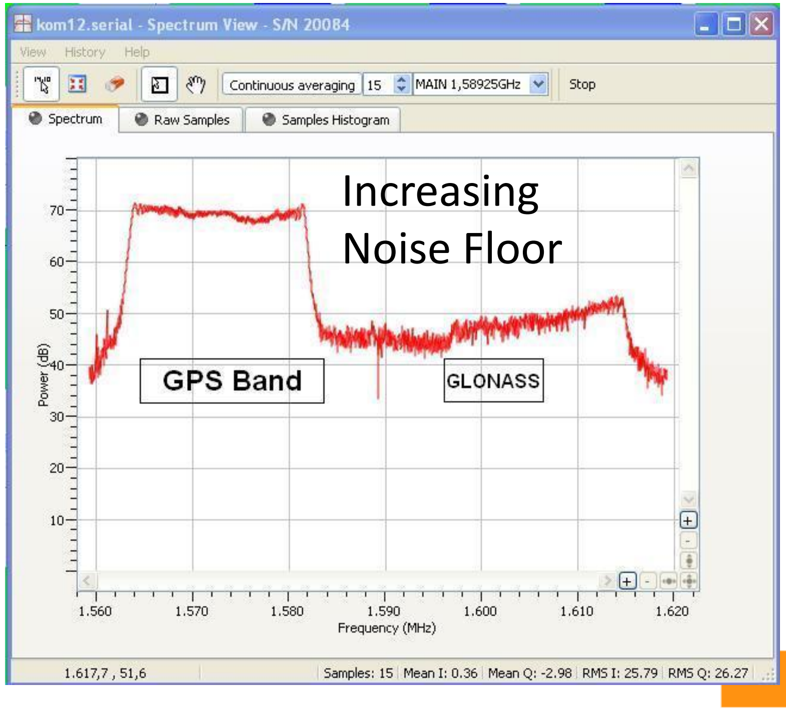


Chirp Jamming



- **Sine Wave Frequency Cycling in Target Band**
  - Simple Way to “Wipe-out” Frequency Band
  - Dominant Design for Personal Protection Devices
- **Center Frequency = Center Frequency of Targeted Signal Band**
  - Typical parametrization:
    - 20 MHz wide, 10 µs sweep time





kom12.serial - Spectrum View - S/N 20084

Continuous averaging 15 MAIN 1,58925GHz

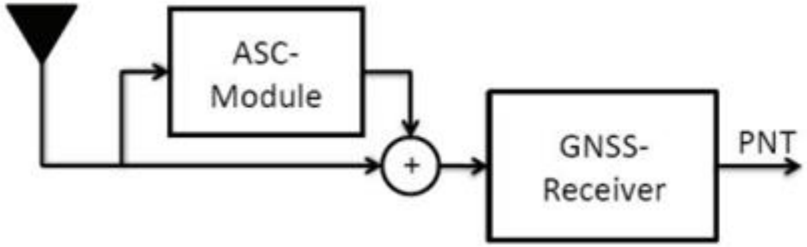
1.617,7 , 51,6 | Samples: 15 | Mean I: 0.36 | Mean Q: -2.98 | RMS I: 25.79 | RMS Q: 26.27

Increasing Noise Floor

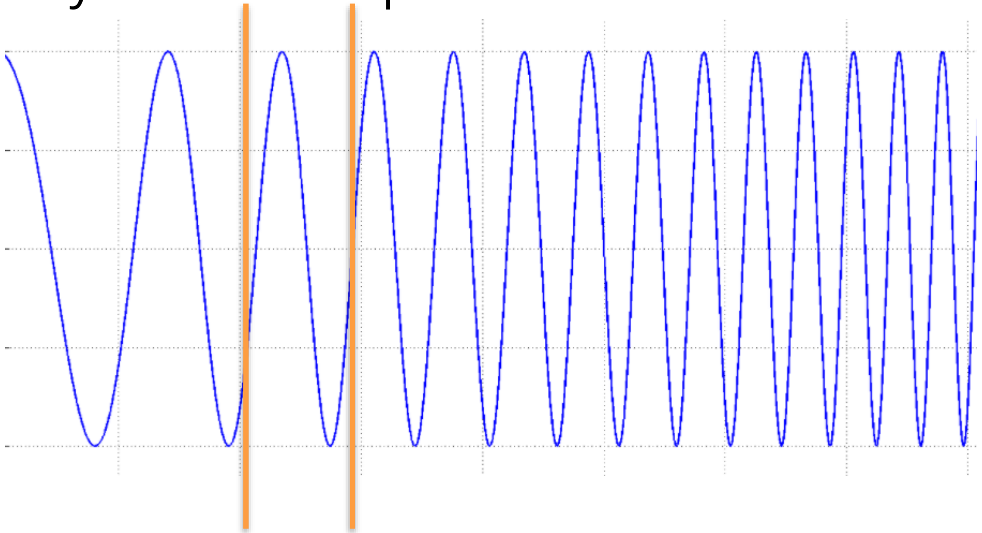
Mitigation Techniques for Chirp Jamming

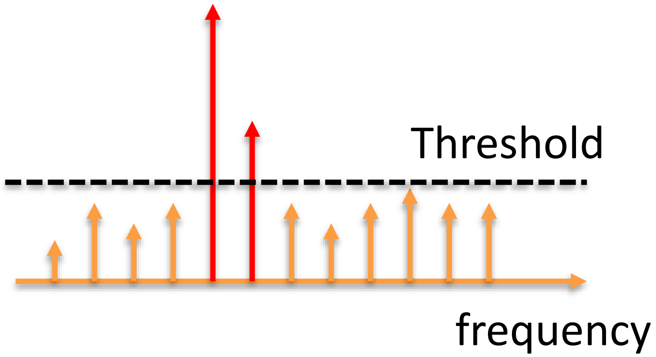
- Method 1: Mimick the signal, and subtract
  - Parameter estimation: frequency-range, chirp-rate, phase
  - Problem: can't deal well with reflections

Active Signal Cancellation



- Method 2: FFT – set peaks to zero - IFFT
  - = FDAF: Frequency Domain Adaptive Filter

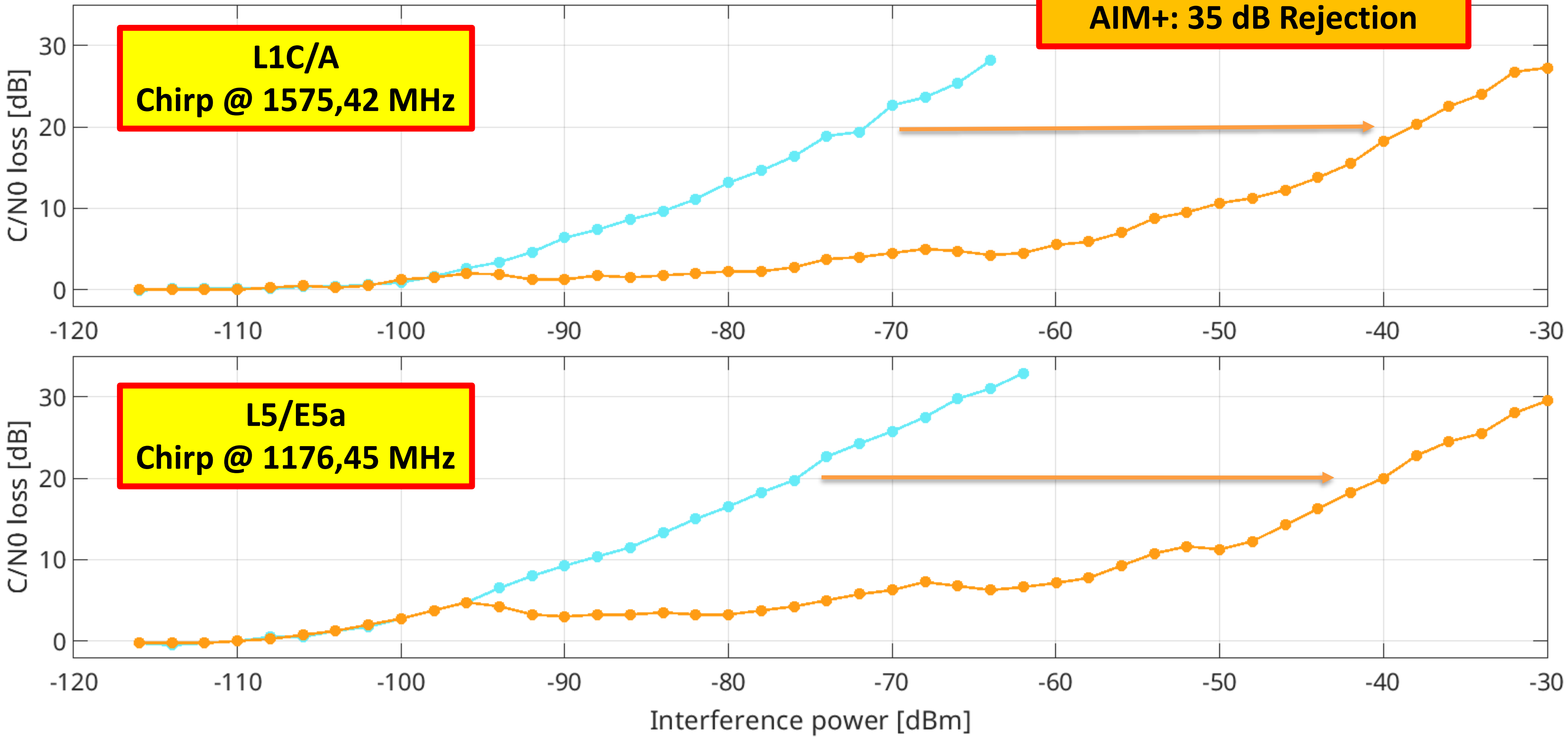




Chirp, 20 MHz, 10 µs Sweep Time

- No mitigation
- AIM+

Similar Impact at L1 and L5
AIM+: 35 dB Rejection



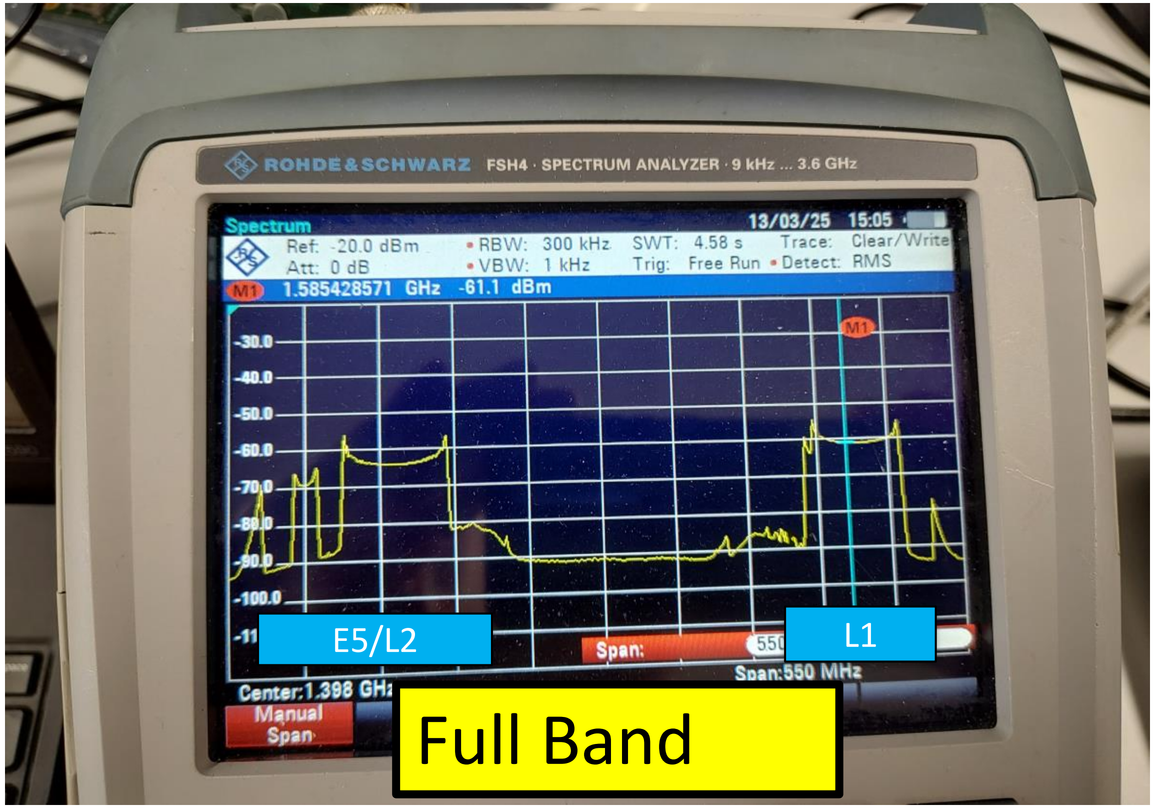
L1C/A
Chirp @ 1575,42 MHz

L5/E5a
Chirp @ 1176,45 MHz

Advanced Multi-Frequency Chirp Jammer

- **Commercial High-Power Jammer from Norway Jammertest Arsenal**
  - Replicated on our test system following description in Test Catalogue

165 Watt!



Ref: -20.0 dBm
Att: 0 dB
RBW: 300 kHz
VBW: 1 kHz
SWT: 4.58 s
Trig: Free Run
Trace: Clear/Write
Detect: RMS
M1 1.585428571 GHz -61.1 dBm
Center:1.398 GHz
Span:550 MHz

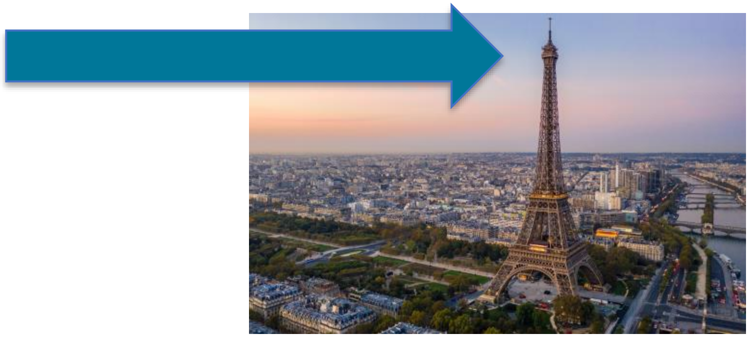
E5/L2

L1

Full Band

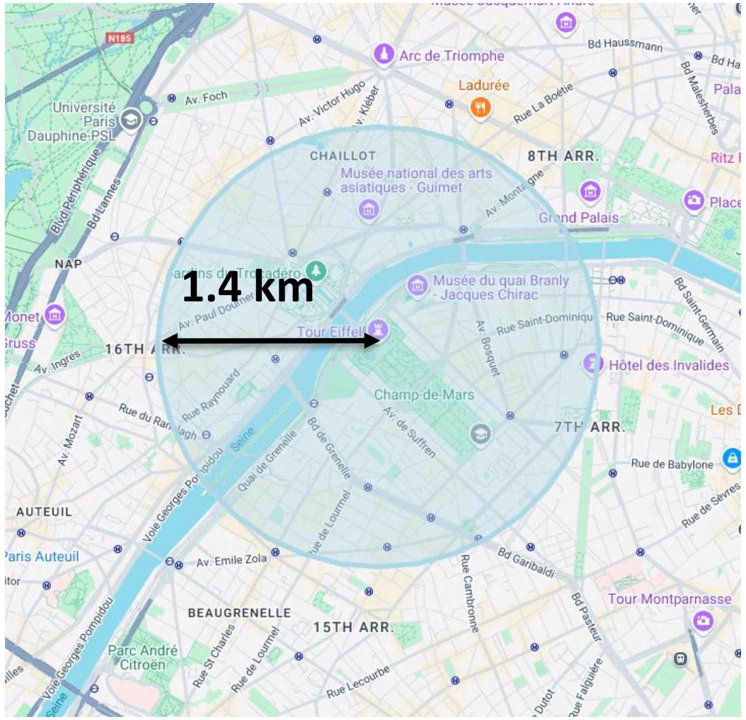
Output of our Test System

Jamming at 165 W from Eiffel tower

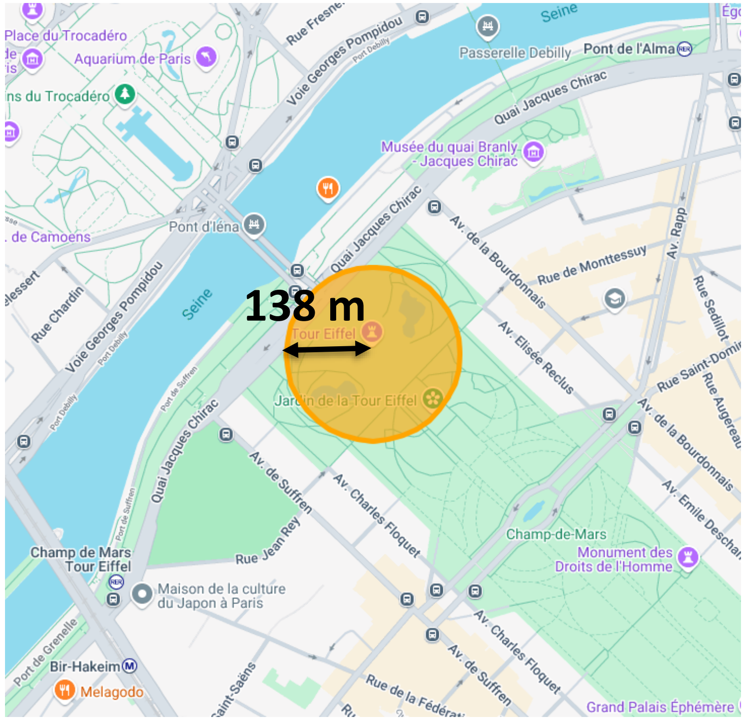


- Simulating precise receiver exposure vs distance
  - Free space propagation
  - Configuration: GPS+GALILEO+BEIDOU
- **Area where position fix is lost:**

Without AIM+

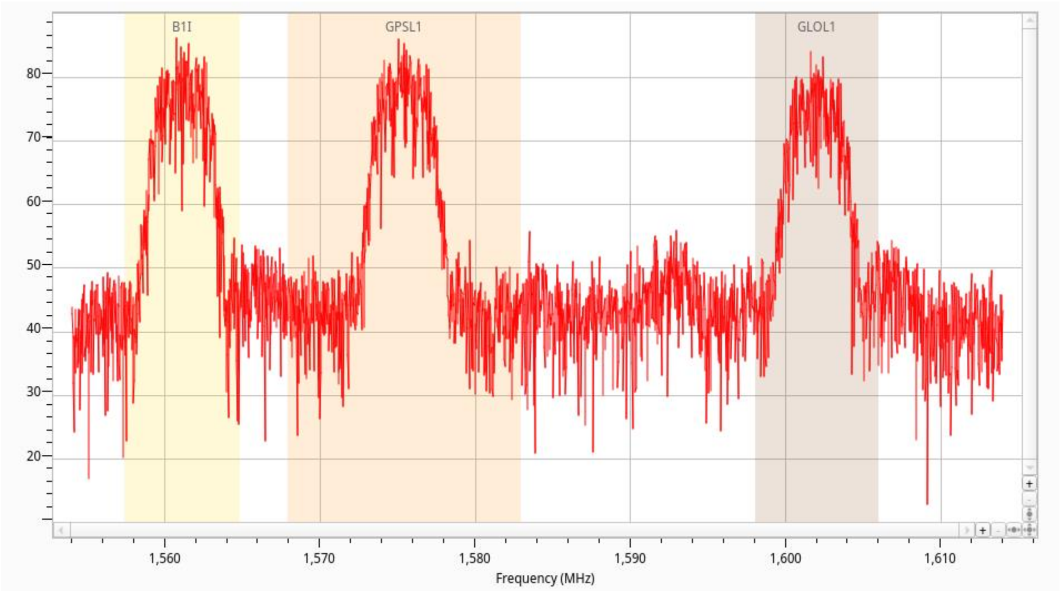


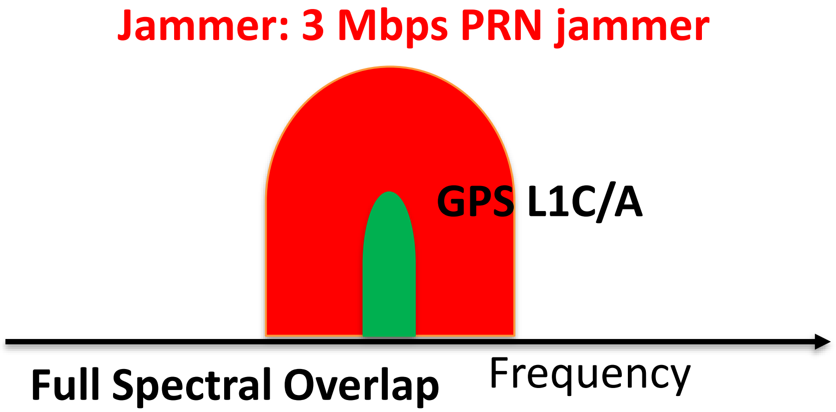
With AIM+

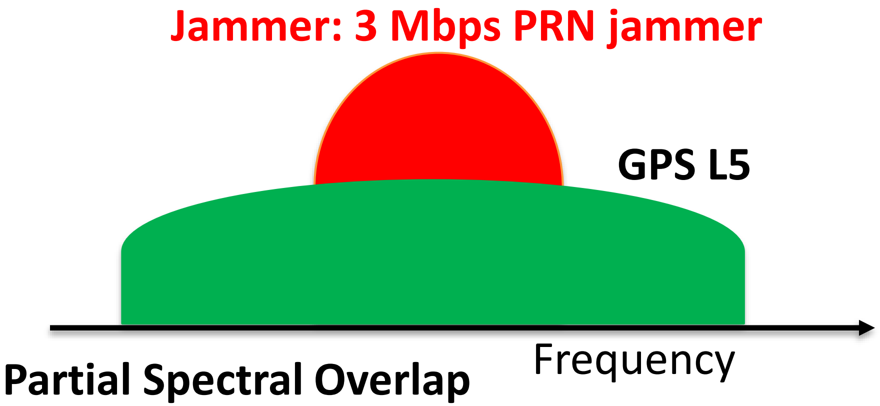


PRN Jamming

- **Typical Military Jamming Technique**
- **Worst Jammer from Norway Jammertest**
  - 3 Mbps BPSK at all Carrier Frequencies
  - Replicated in our Test System



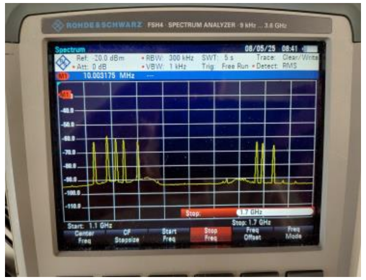


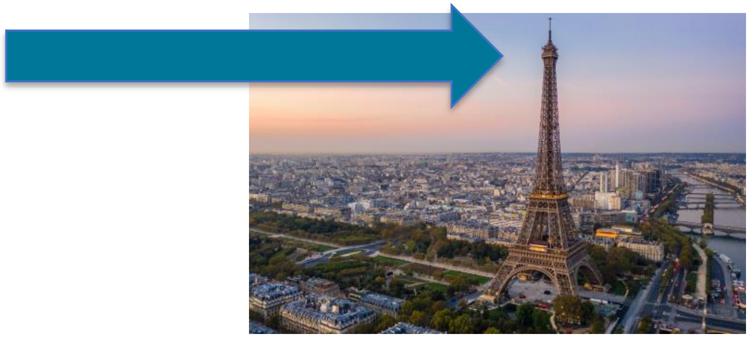


→ Mitigated with Band-Stop Filter!

septentrio part of HEXAGON

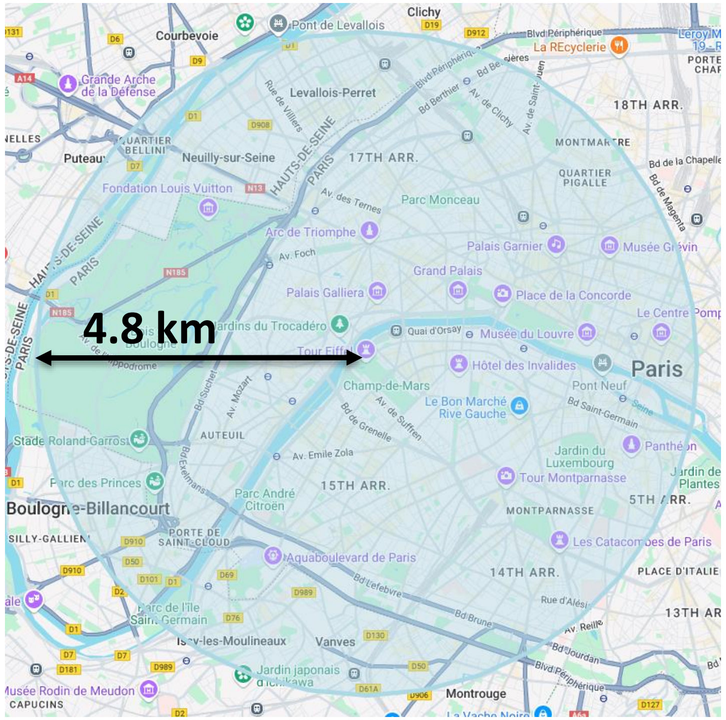
50W PRN jamming from Eiffel tower



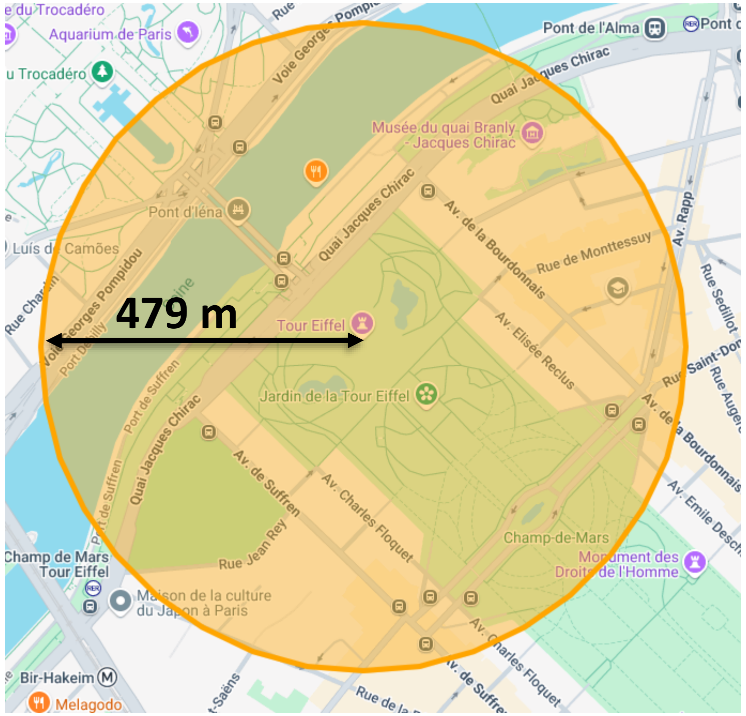


- Simulating precise receiver exposure vs distance
  - Free space propagation
  - Configuration: GPS+GALILEO+BEIDOU+GLONASS+SBAS
- **Area where position fix is lost:**

Without AIM+



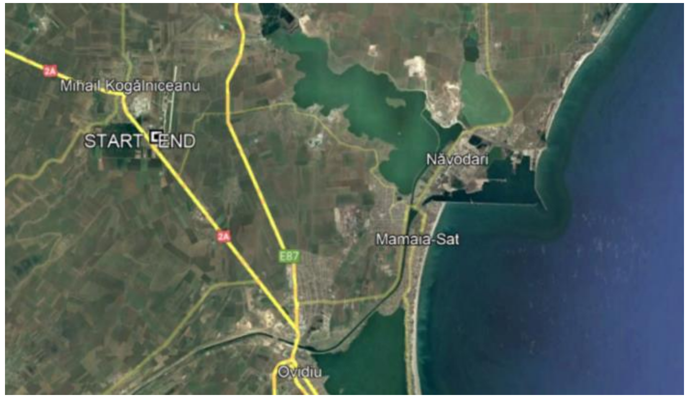
With AIM+



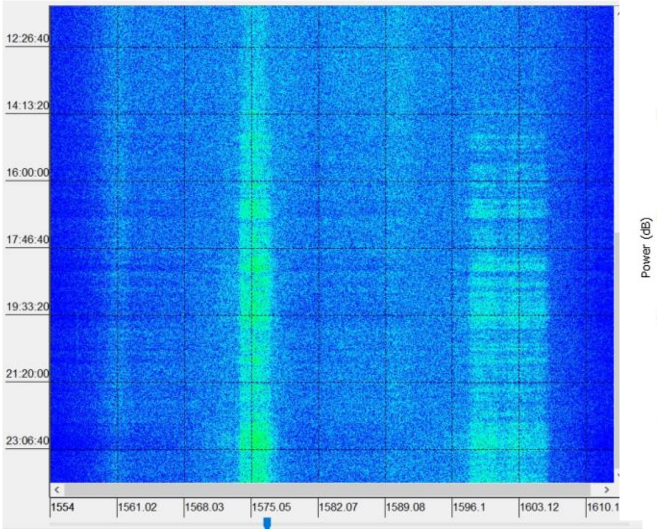
septentrio
part of HEXAGON

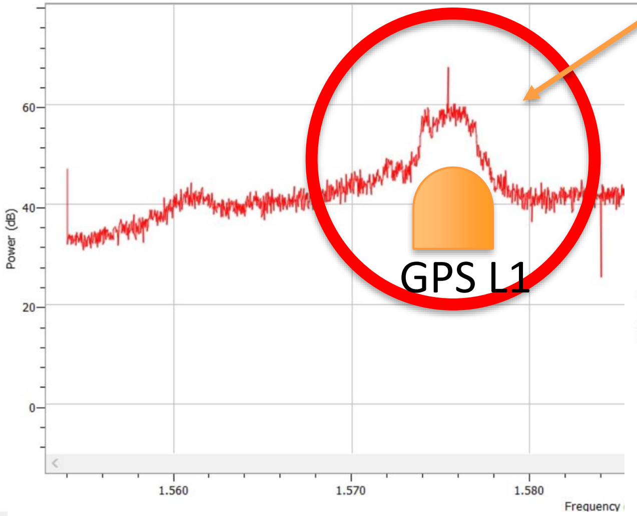
Military Theaters: High Entropy Interference

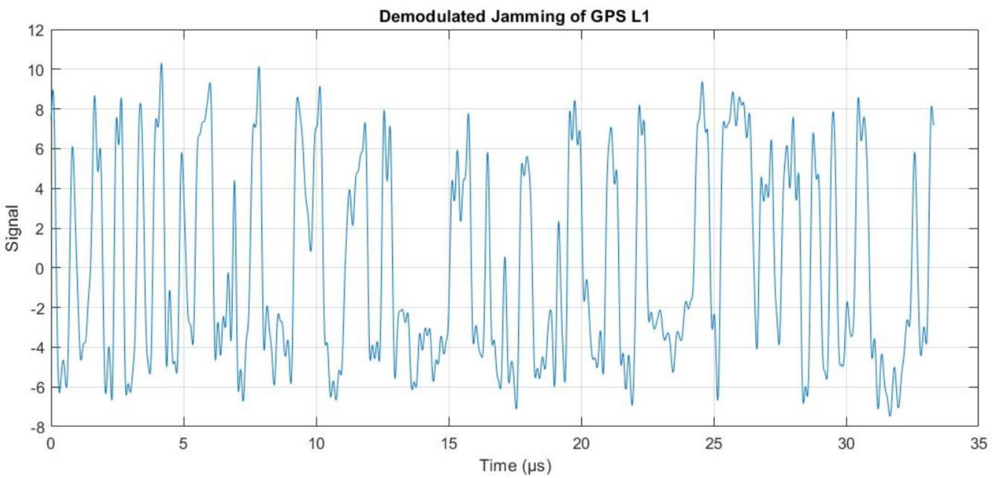
- **Black Sea, Romania, June 2022**
  - Interference recorded by PolaRx CORS receiver
  - Baseband samples → Enabling Demodulation
    - Wide band BPSK @ 1575,42 MHz
    - Pseudo-random



Full Spectral Overlap, Pseudo-Noise

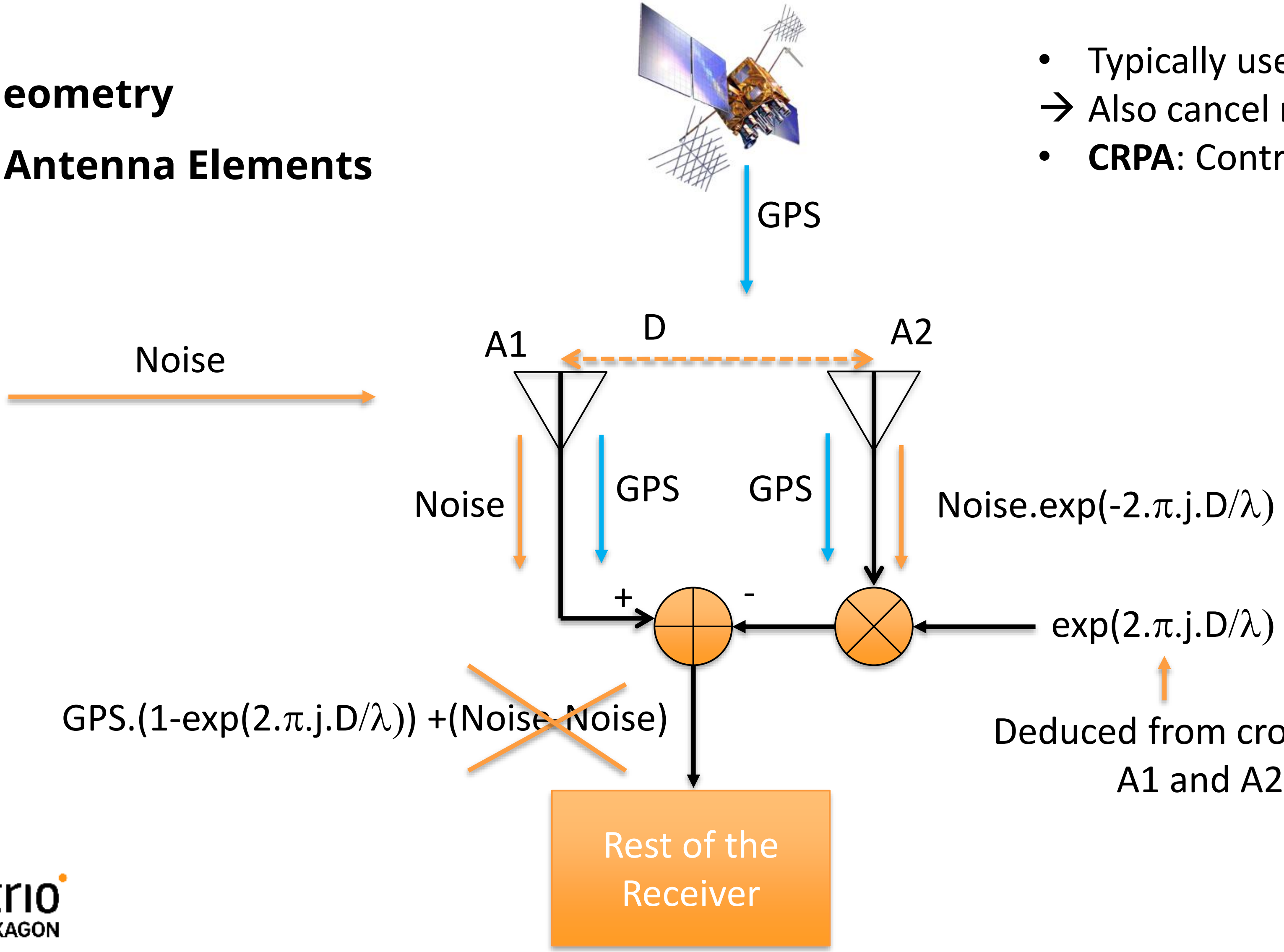






Military Grade Anti-Jamming: Beam Forming

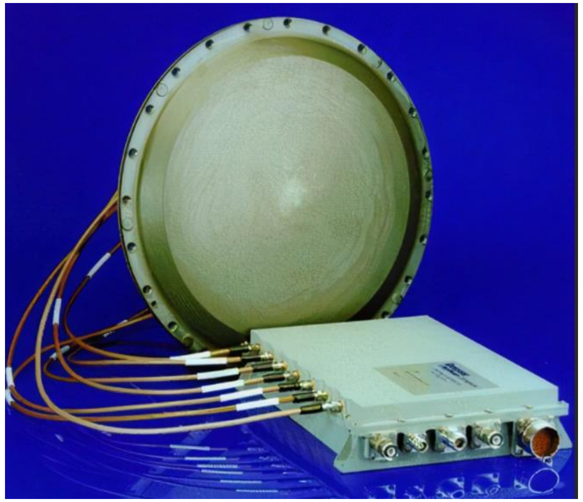
- **Exploit Geometry**
- **Multiple Antenna Elements**


GPS
D
A1
A2
Noise
Noise
GPS
GPS
Noise.exp(-2.π.j.D/λ)
+
-
exp(2.π.j.D/λ)
$\text{GPS.}(1-\exp(2.\pi.j.D/\lambda)) + (\cancel{\text{Noise-Noise}})$
Deduced from cross-correlation
A1 and A2 signal
Rest of the Receiver

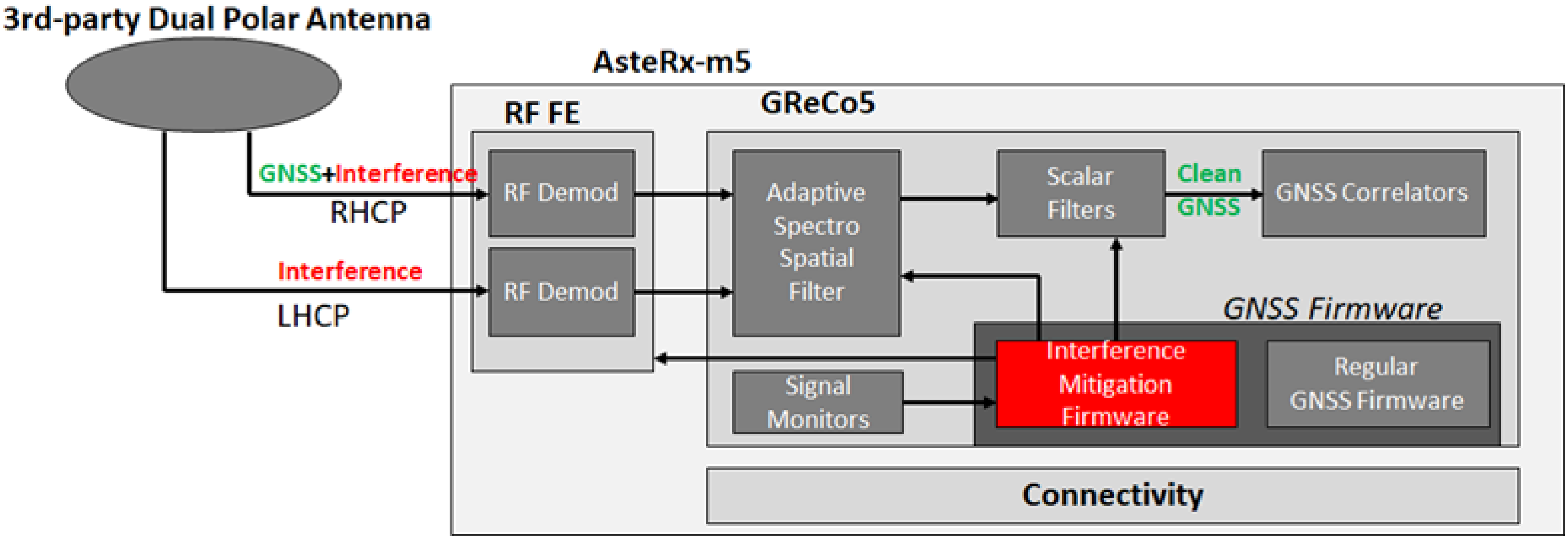
- Typically uses 4 to 7 antena elements

→ Also cancel reflections of jamming

- **CRPA**: Controlled Radiation Pattern Antenna



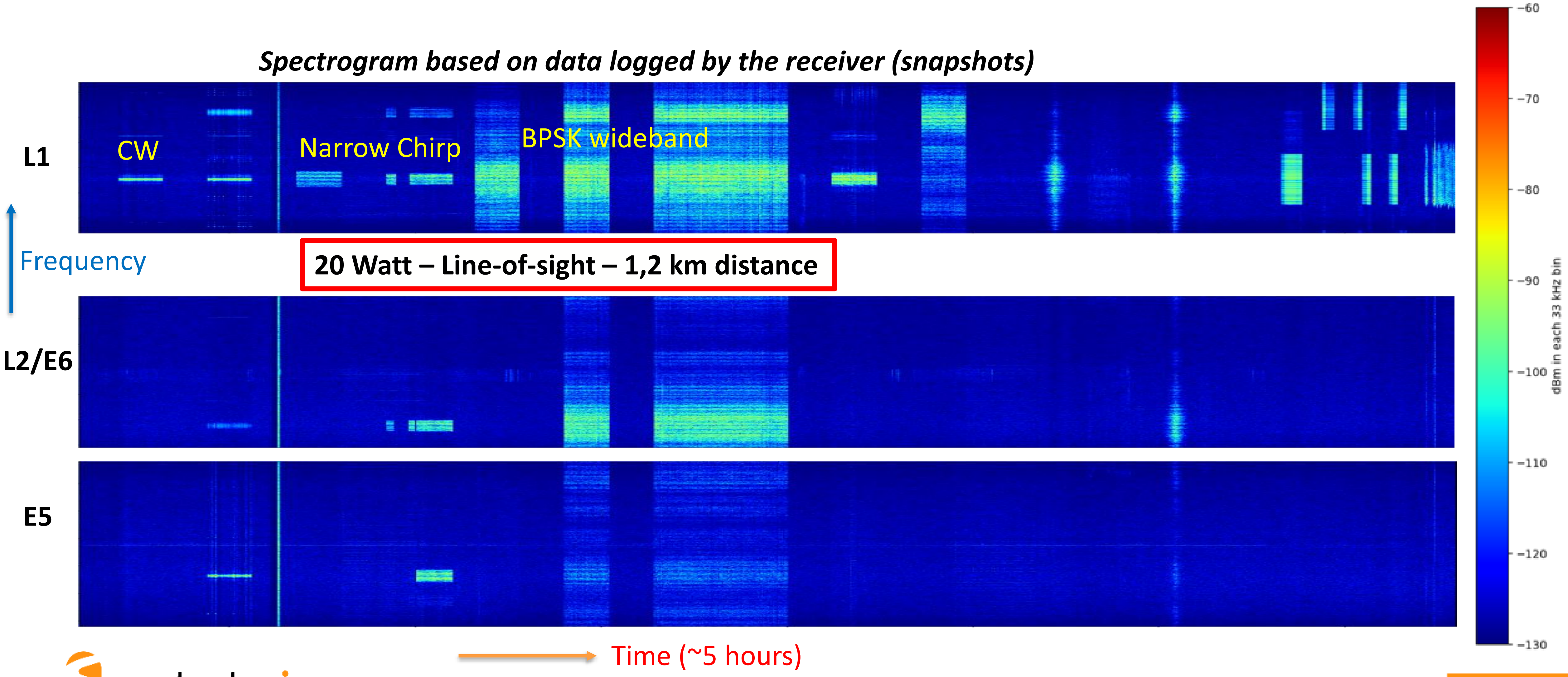
Firmware Support for Dual Input Adaptive Null Steering



septentrio part of HEXAGON

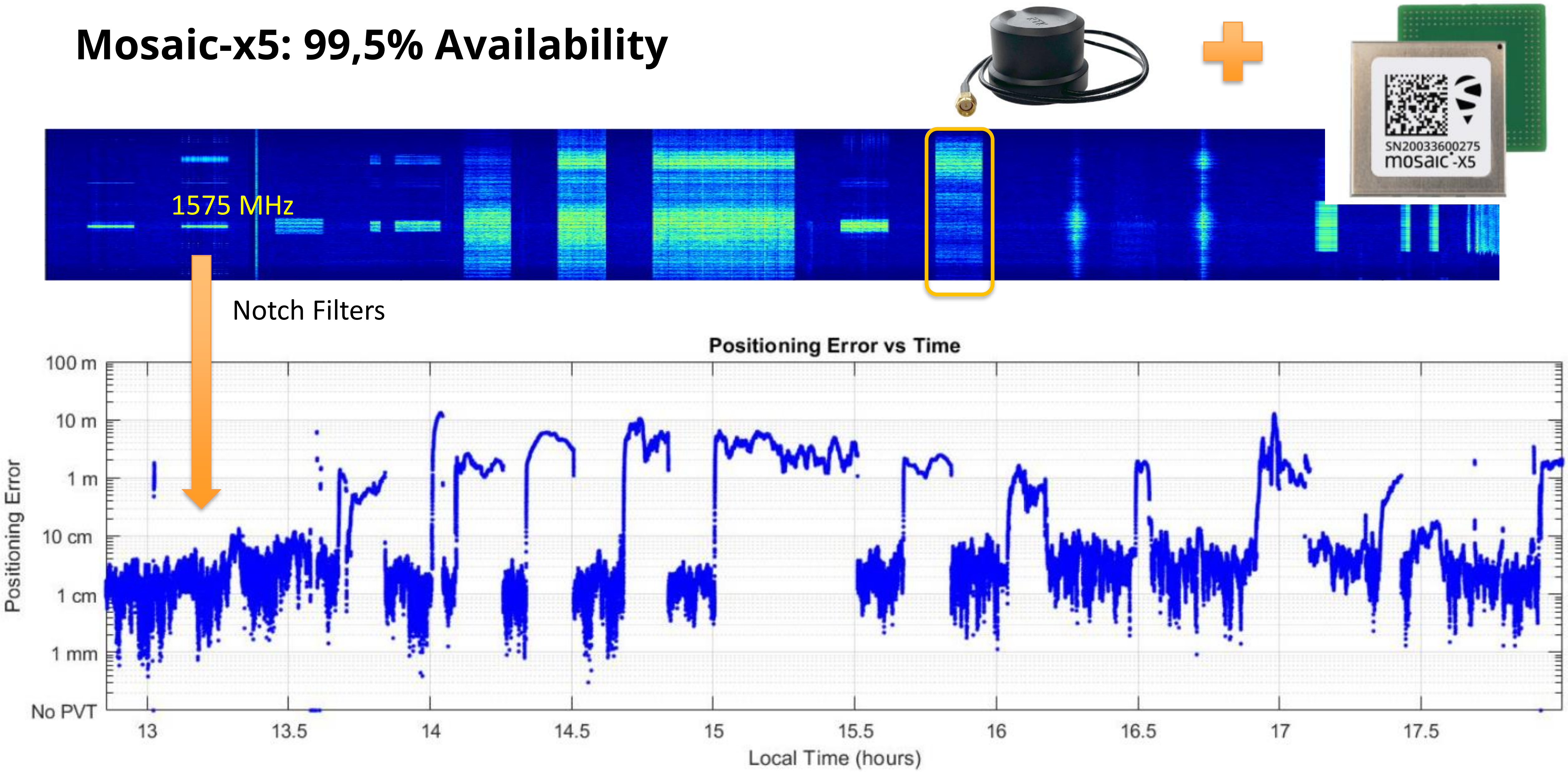
Day 1 Norway 2023: Applying all flavours of jamming waveforms

Spectrogram based on data logged by the receiver (snapshots)



20 Watt – Line-of-sight – 1,2 km distance

Mosaic-x5: 99,5% Availability



1575 MHz

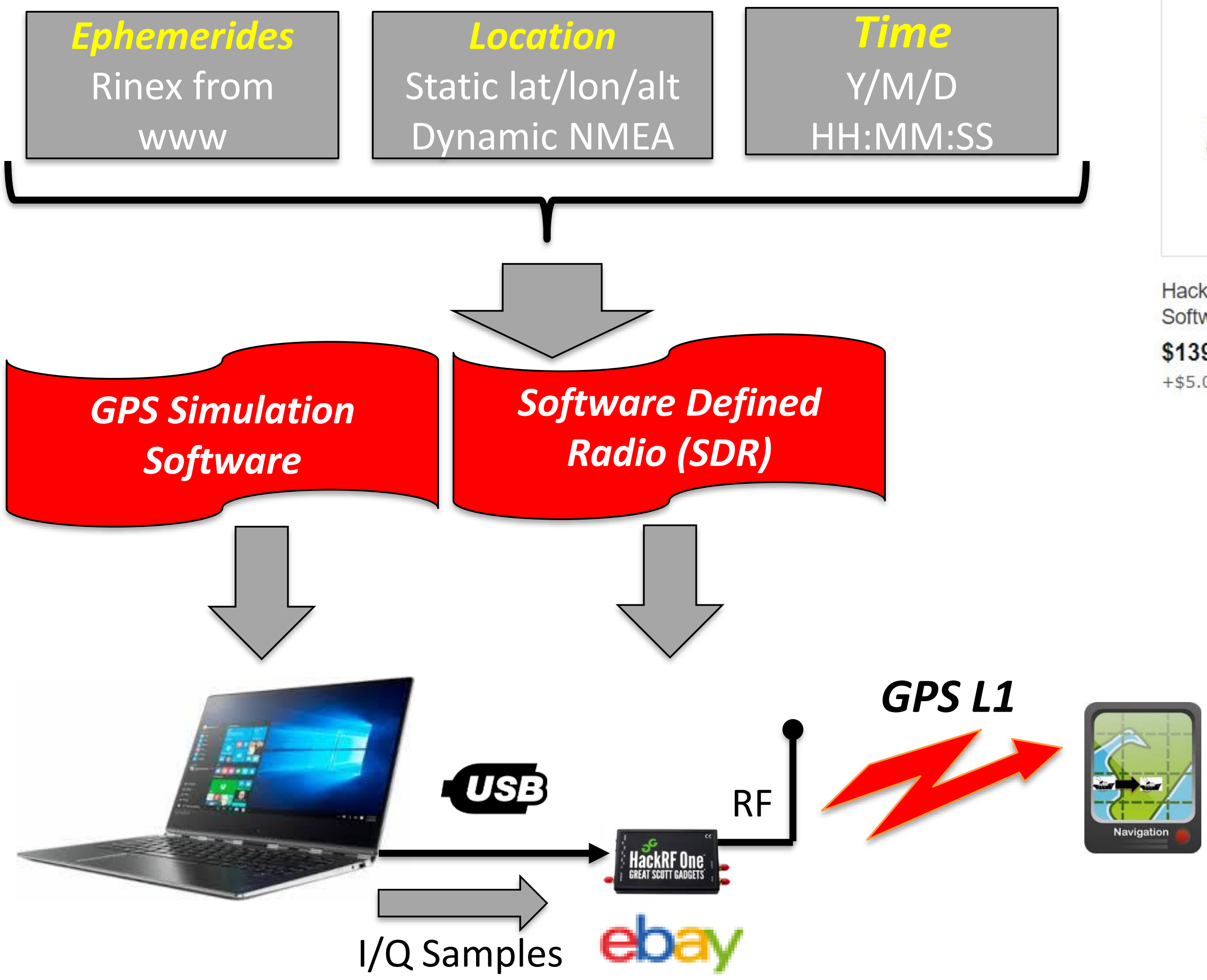
Notch Filters

septentrio part of HEXAGON

Spoofing

How is it done ?

- gps-sdr-sim
  - Open Source @ GitHub
  - Easy to Set Up



Ephemerides
Rinex from
www

Location
Static lat/lon/alt
Dynamic NMEA

Time
Y/M/D
HH:MM:SS

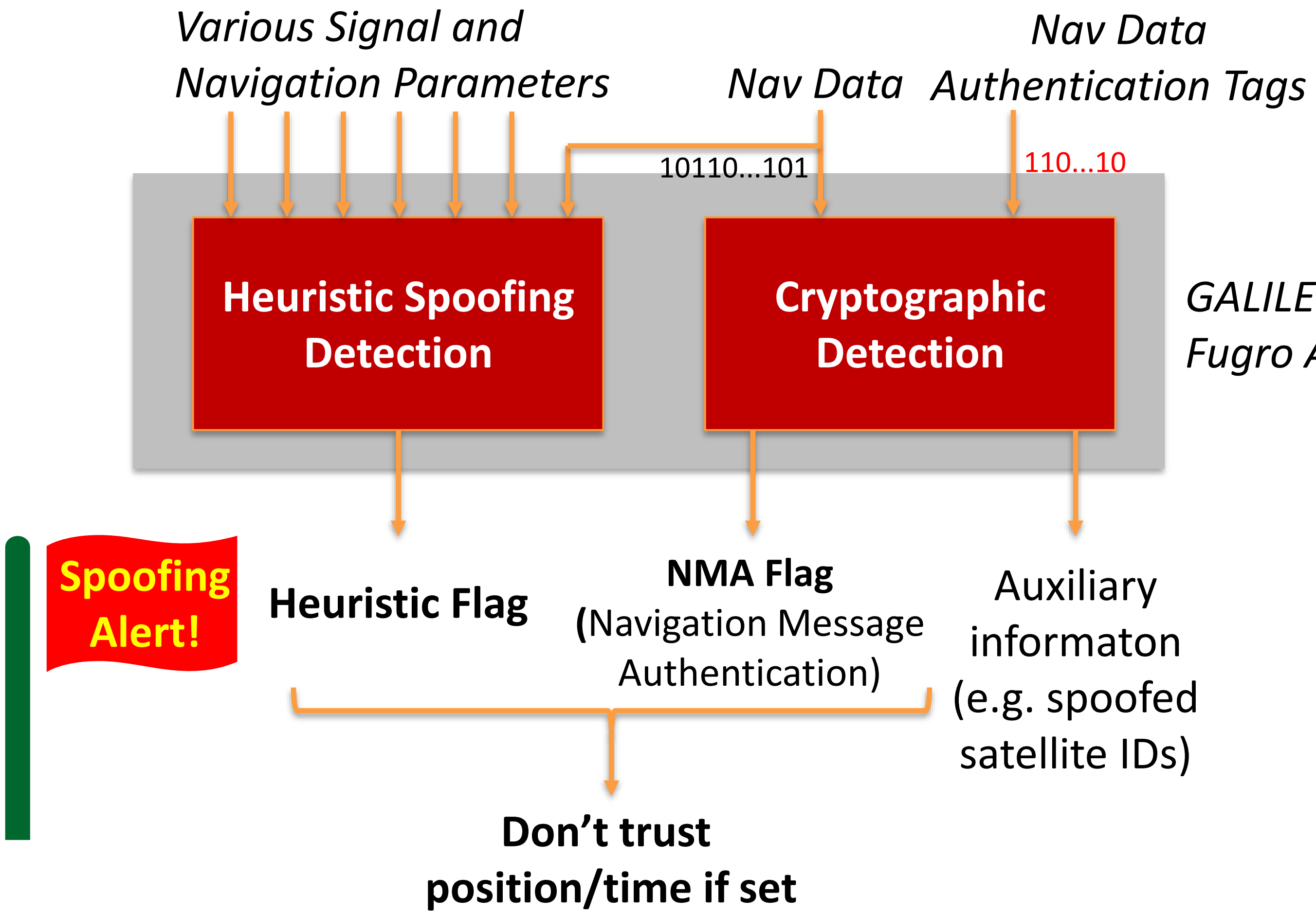
GPS Simulation Software

Software Defined Radio (SDR)

I/Q Samples

HackRF One 1-6GHz Open Source Software Defined Radio Platform…
$139.81
+$5.00 shipping

Spoofing mitigation



Various Signal and Navigation Parameters

Nav Data

Nav Data Authentication Tags

10110...101

110...10

Heuristic Spoofing Detection

Cryptographic Detection

Spoofing Alert!

Heuristic Flag

NMA Flag (Navigation Message Authentication)

Auxiliary informaton (e.g. spoofed satellite IDs)

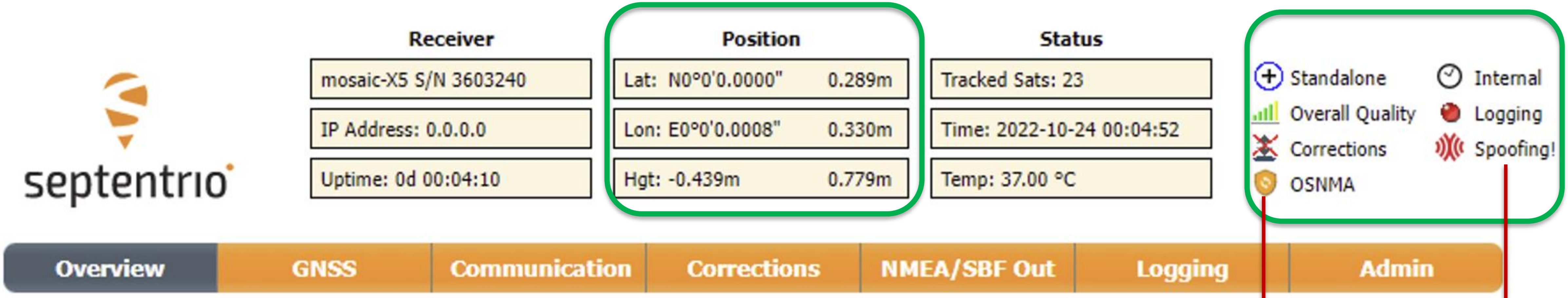
Don’t trust position/time if set

GALILEO OSNMA (mosaic-x5/H/T)
Fugro AtomiChron (mosaic-T)

No Calibration Required – Working out-of-the-box

Spoofing Detection

Spoofed Coordinate → User Informed



Receiver	Position	Status
mosaic-X5 S/N 3603240	Lat: N0°0'0.0000" 0.289m	Tracked Sats: 23
IP Address: 0.0.0.0	Lon: E0°0'0.0008" 0.330m	Time: 2022-10-24 00:04:52
Uptime: 0d 00:04:10	Hgt: -0.439m 0.779m	Temp: 37.00 °C

Authentication of GALILEO L1 Signal Failed!
Cryptographic method to authenticate NavData
Network Time Protocol (NTP) for anti-replay

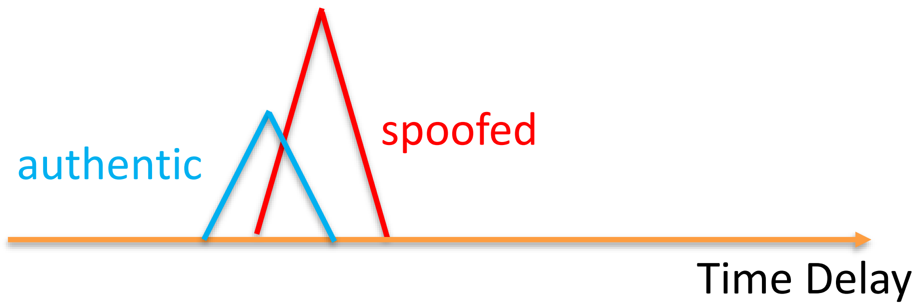
Spoofing Detected with Heuristic Methods:
Waveform Anomalies, NavData Analomalies,
Inconsistencies,...

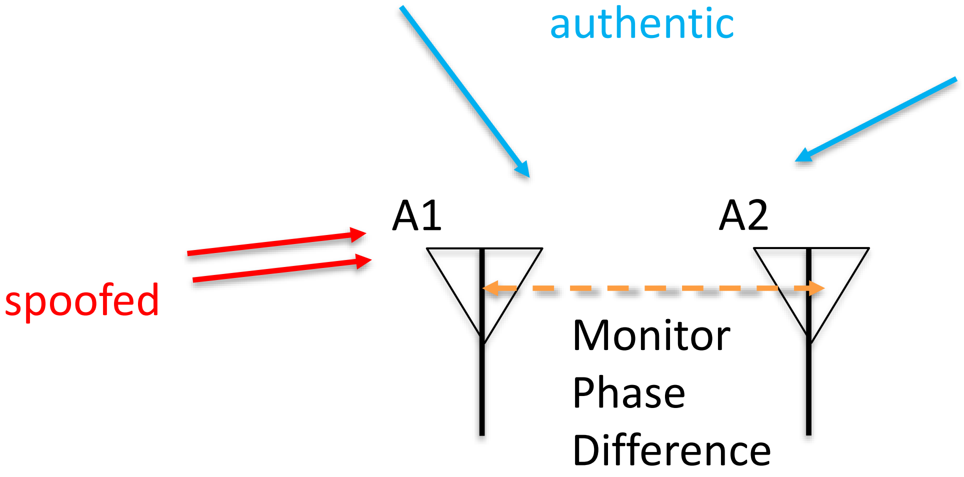
septentrio part of HEXAGON

Heuristic Approach

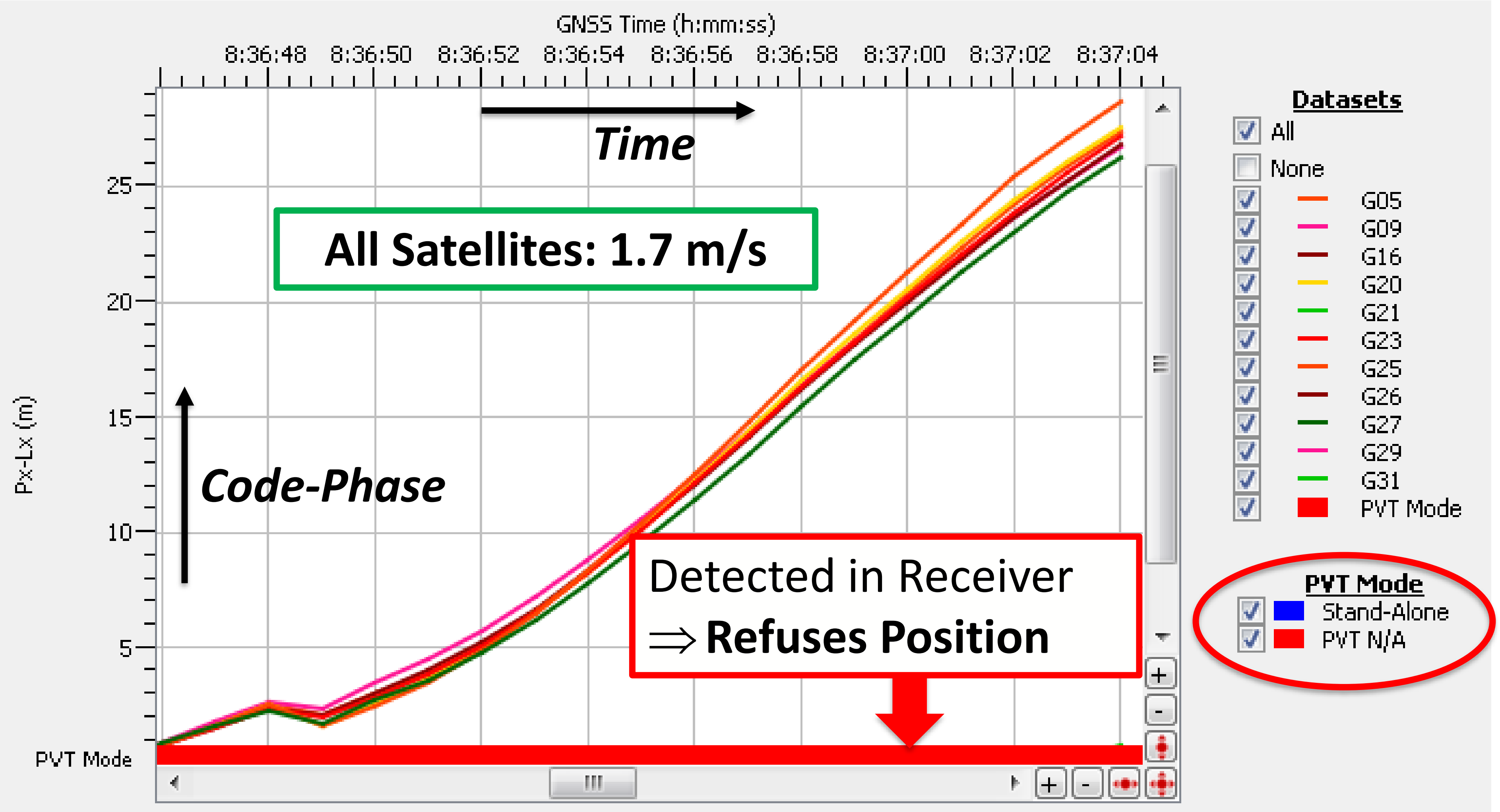
- **<u>Signal Parameter Anomalies</u>**
  - Maximize Detection of Spoofing
  - Minimize False Positives

- Example Techniques:
  - Detect excessive power
    - But can also come from high-gain antenna…
  - Detect correlation profile deformation
    - But can also come from multipath…
  - Detect divergence
    - But can also come from ionospheric scintillation…
  - Detect wrong angle-of-arrival (2 antenna-receivers)
    - But can be reflection….





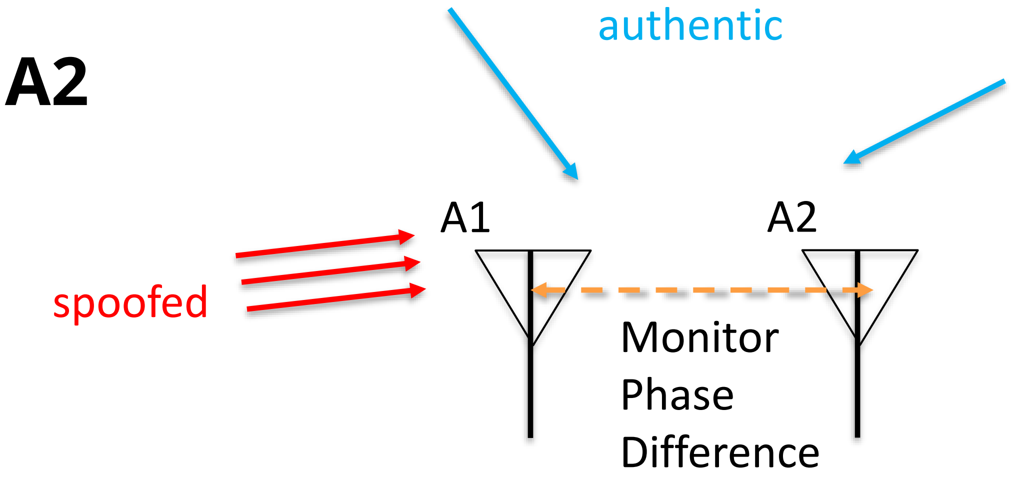
Most SDRs: Huge Code-Carrier Divergence

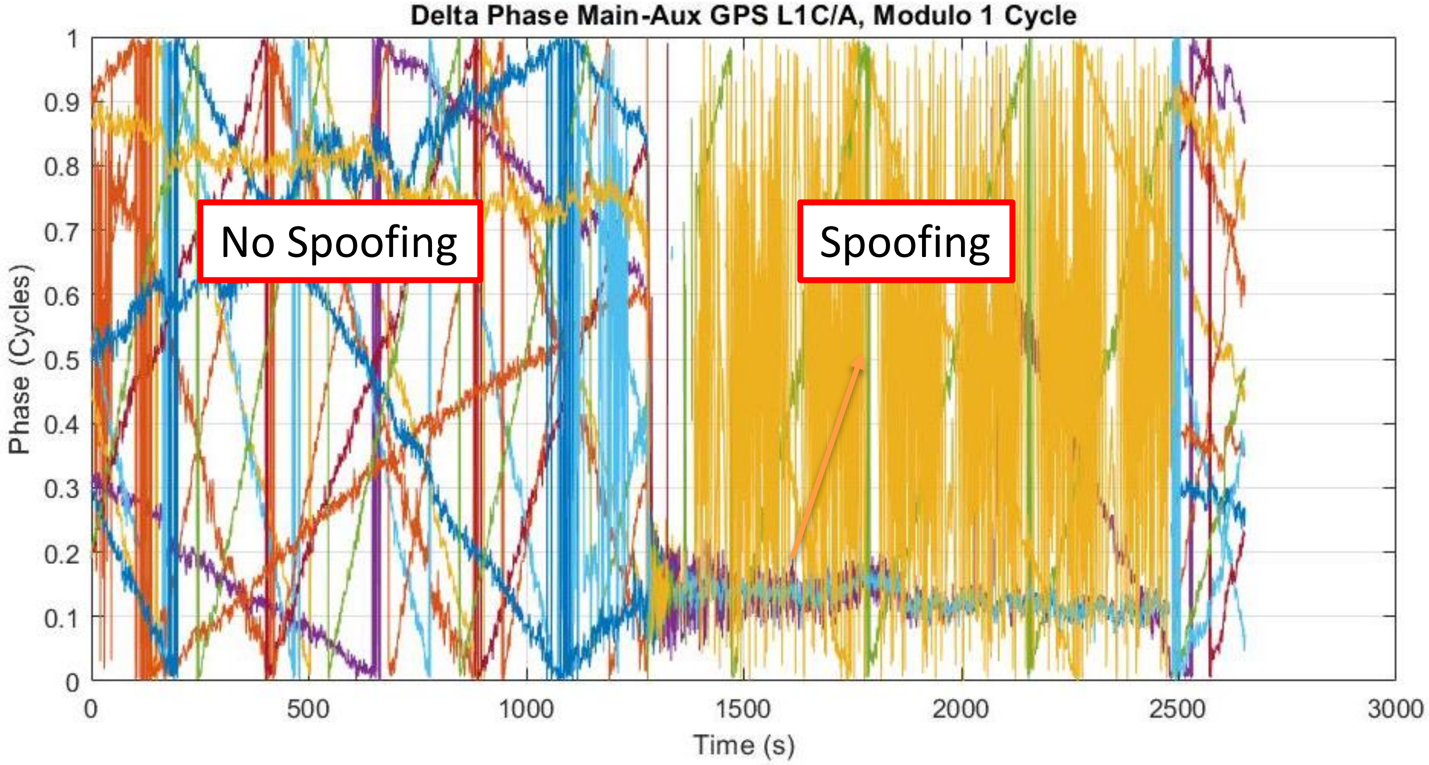


All Satellites: 1.7 m/s

Detected in Receiver
⇒ **Refuses Position**

Single Difference Phase A1 – A2

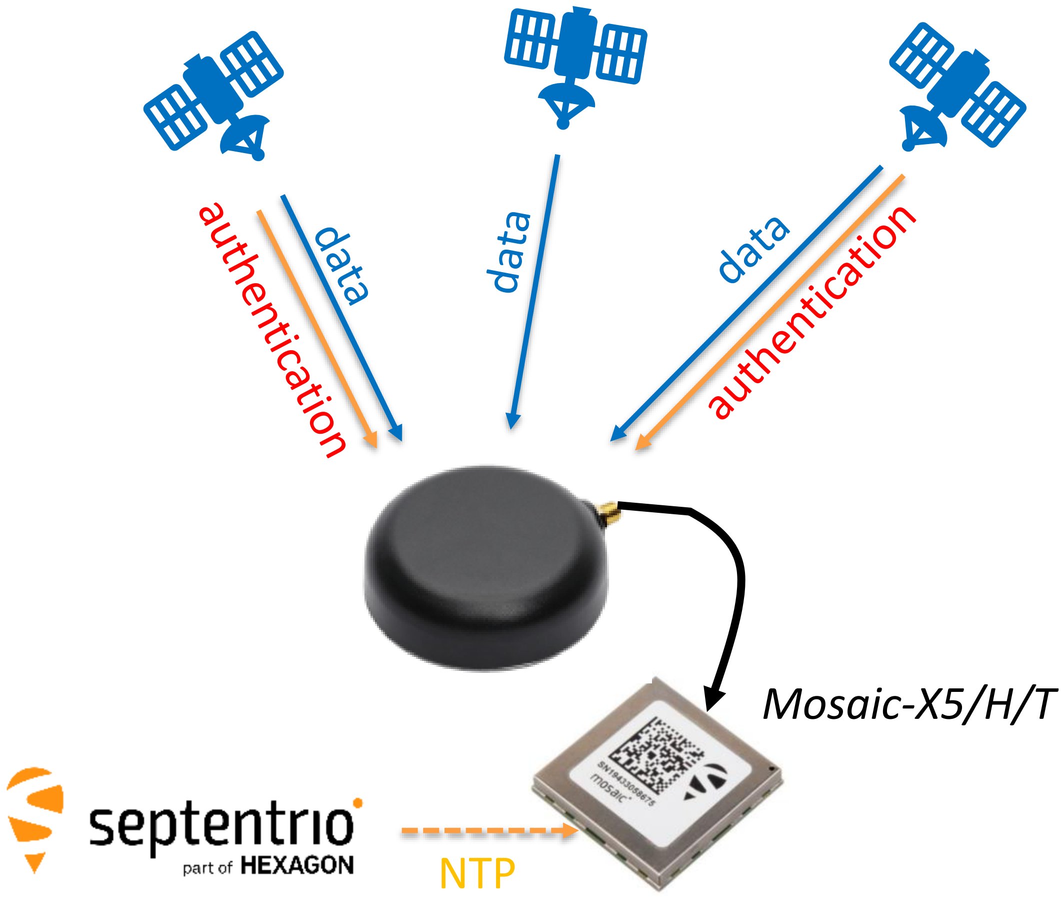


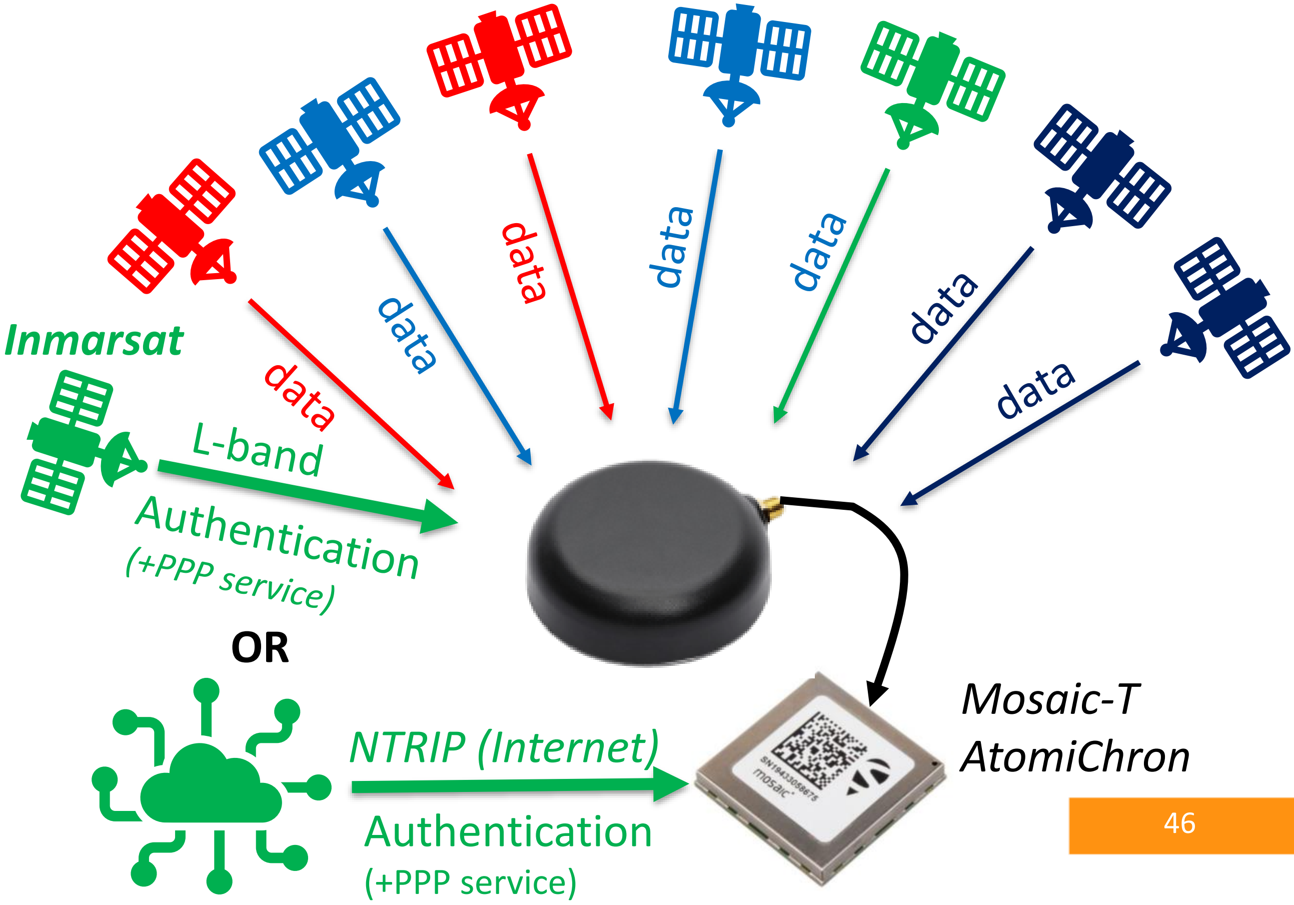


Navigation Message Authentication (NMA) Flavors

Open Service NMA (OSNMA)
Freely available on GALILEO L1BC
Authentication of GALILEO I/NAV

AtomiChron NMA
Part of PPP timing subscription service
Authentication of GPS, GALILEO, BDS, GLONASS

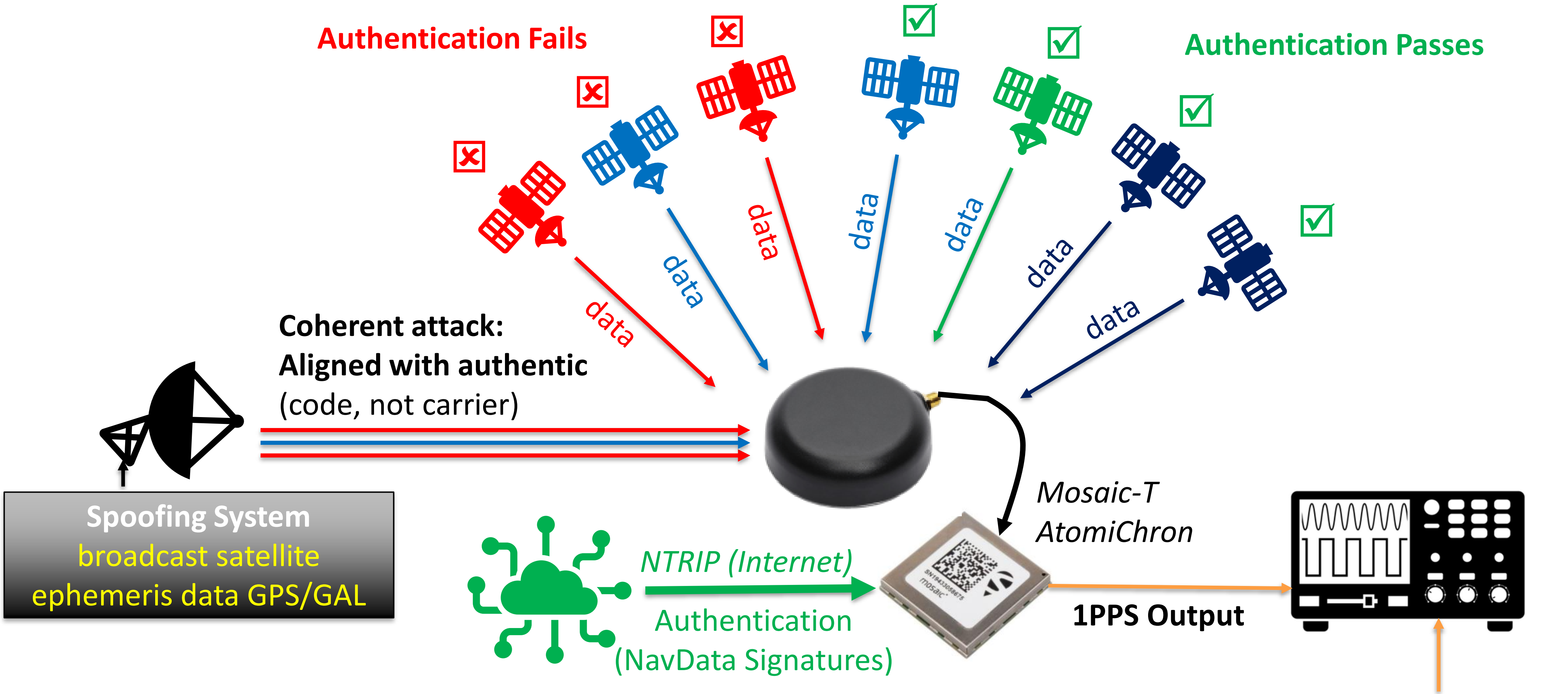




All Five Days 2023: Statistics

Parameter	Result
Heuristic Flag Availability During Spoofing	91%
OSNMA Flag Availability During Spoofing	55%
Positioning Error Bound (99.9%, all five days, approved epochs)	10 m
Average Time to Spoofed Outlier (>10 m) Detection	8 seconds
Maximal Time to Spoofed Outlier (>10 m) Detection	34 seconds

AtomiChron Receiver Setup



Authentication Fails

Authentication Passes

Coherent attack:
Aligned with authentic
(code, not carrier)

Spoofing System
broadcast satellite
ephemeris data GPS/GAL

NTRIP (Internet)

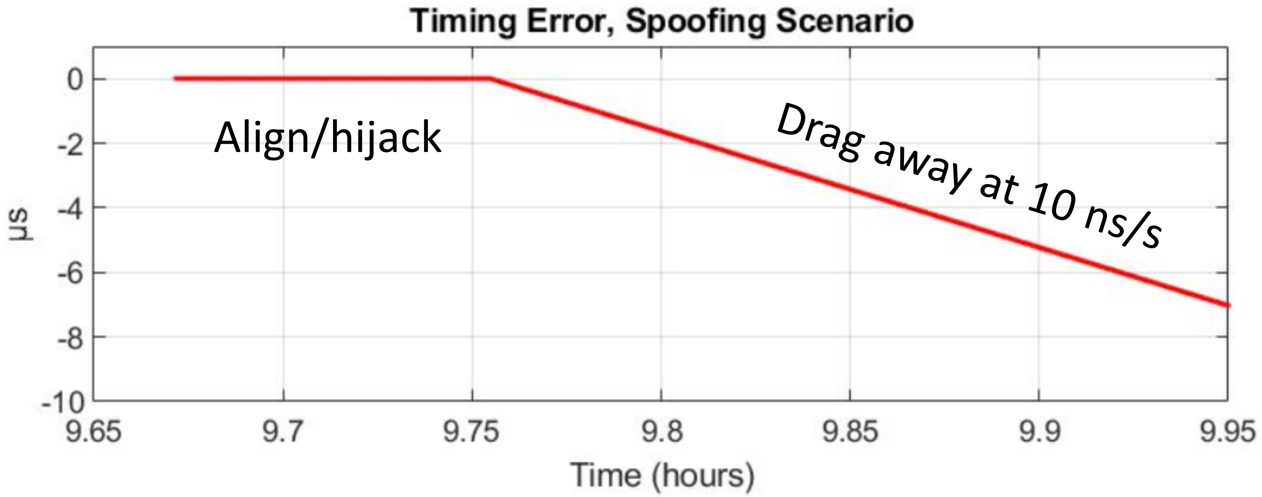
Authentication
(NavData Signatures)

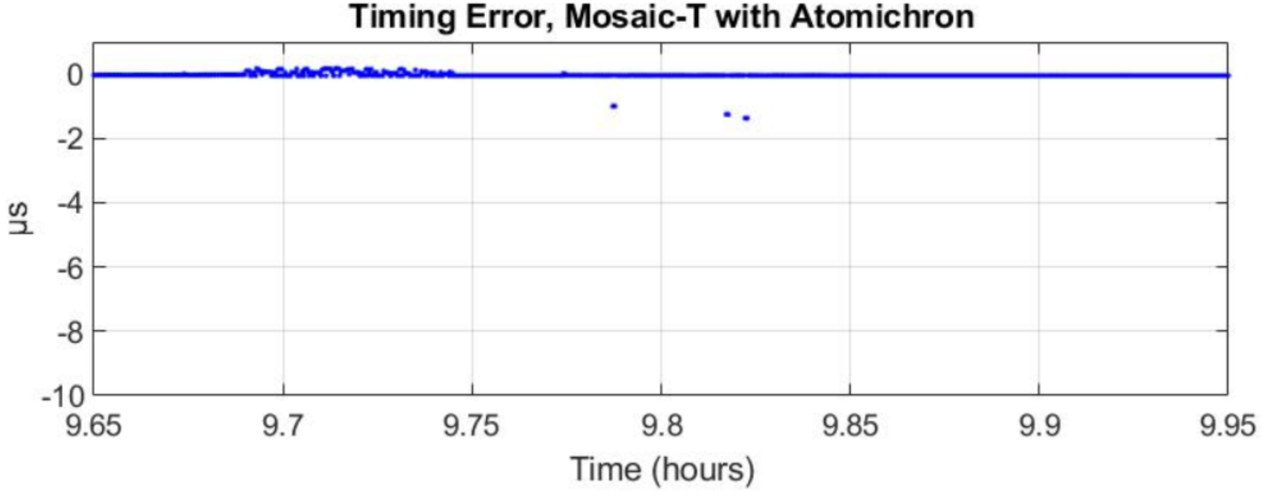
Mosaic-T
AtomiChron

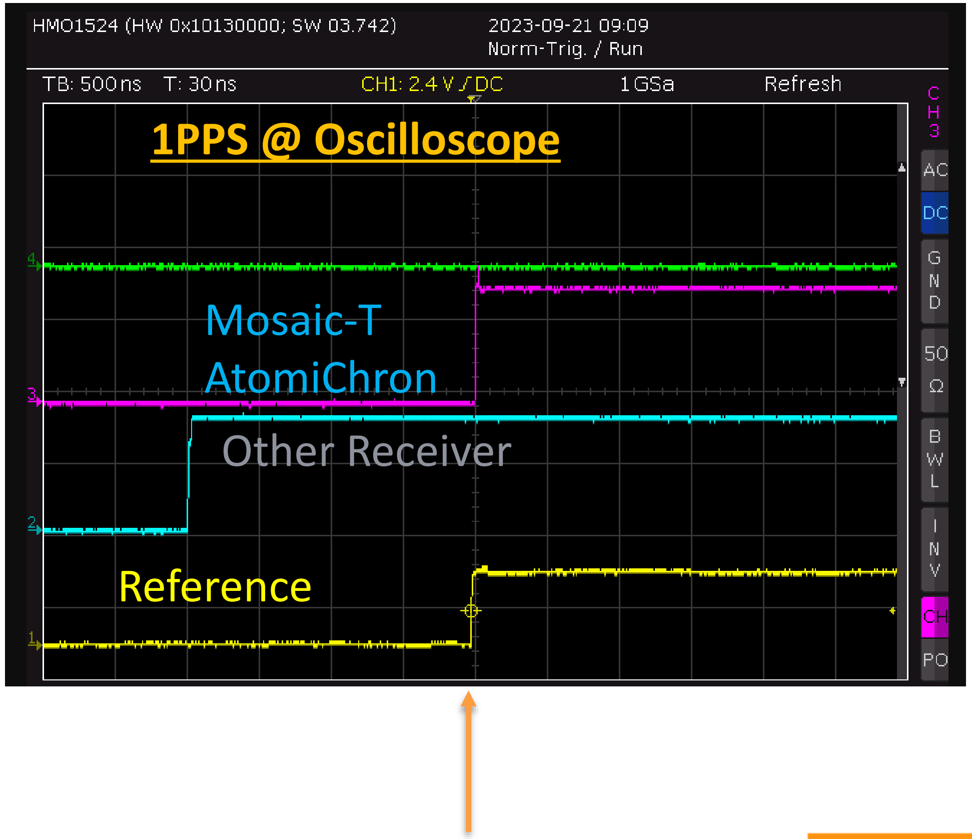
1PPS Output

Reference 1PPS
Organizers

Closing up: Spoofing Mitigation by Mosaic-T with AtomiChron







HMO1524 (HW 0x10130000; SW 03.742) 2023-09-21 09:09

Norm-Trig. / Run

TB: 500 ns T: 30 ns CH1: 2.4 V ⟋DC 1 GSa Refresh

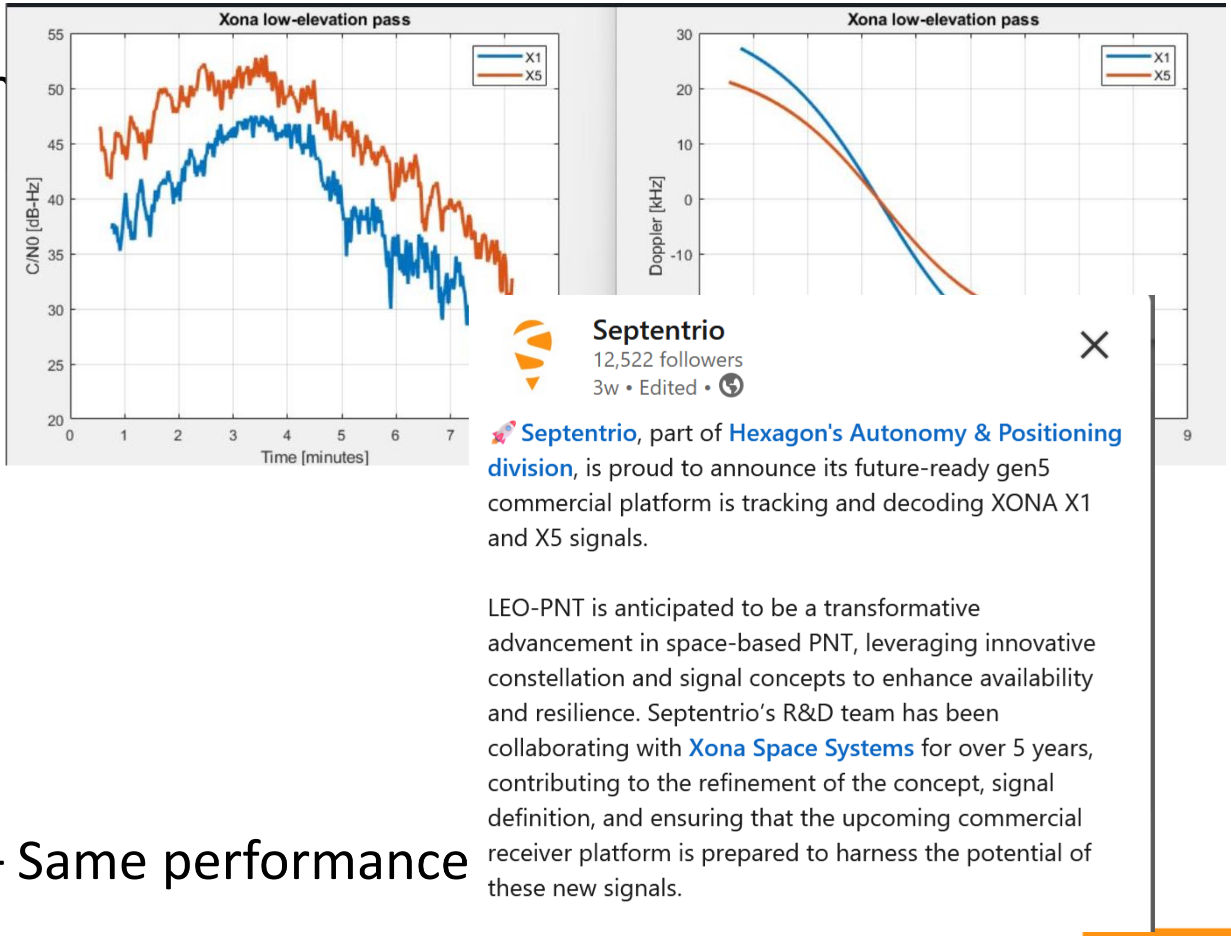
Why LEO PNT?

- **Potential Game Changer for Precise Positioning**
  - Very Fast PPP convergence
  - Improved Correction Data Dissemination

- **Resilience**
  - High Power → More Margin
  - Frequency Diversity
  - Encryption & Watermarks

- **C-band: Compact Systems**
  - Maxwell Equations are Linear
  - → 4x smaller systems
  - → Compact Heading
    - 25 cm baseline instead of 1 meter – Same performance

- **Major Differentiator**



Septentrio
12,522 followers
3w • Edited •

🚀 Septentrio, part of Hexagon's Autonomy & Positioning division, is proud to announce its future-ready gen5 commercial platform is tracking and decoding XONA X1 and X5 signals.

LEO-PNT is anticipated to be a transformative advancement in space-based PNT, leveraging innovative constellation and signal concepts to enhance availability and resilience. Septentrio's R&D team has been collaborating with Xona Space Systems for over 5 years, contributing to the refinement of the concept, signal definition, and ensuring that the upcoming commercial receiver platform is prepared to harness the potential of these new signals.

septentrio part of HEXAGON

Take Away

Jamming

- Receiver must have:
  - High-dynamic range **RF Demodulators** and **Wide-range ADCs**
  - **Notch filters** (the more the better) and **Wide Band Mitigation capability**
- Up to **10 dB** Inherent Rejection from Signal Design
  - Larger Signal Bandwidth Limits Impact Zone Interference
- Up to **48 dB** Rejection from Receiver Interference Mitigation (AIM+)

Spoofing

- Difficult on the chip level
- Needs a more heuristic approach => Not easy
- Signal authentication is **key** => OSNMA, Commercial Services, LEO-PNT

CELEBRATING 25 YEARS
OF SECURE & ROBUST
GNSS POSITIONING

septentrio
part of HEXAGON

EMEA (HQ)

Greenhill Campus
Interleuvenlaan 15i,
3001 Leuven, **Belgium**

Espoo, **Finland**

Americas

2601 Airport Drive, Suite 360
Los Angeles (Torrance),
CA 90505, **USA**

septentrio.com/contact

Asia-Pacific

Shanghai, **China**
Yokohama, **Japan**
Seoul, **Korea**

septentrio.com