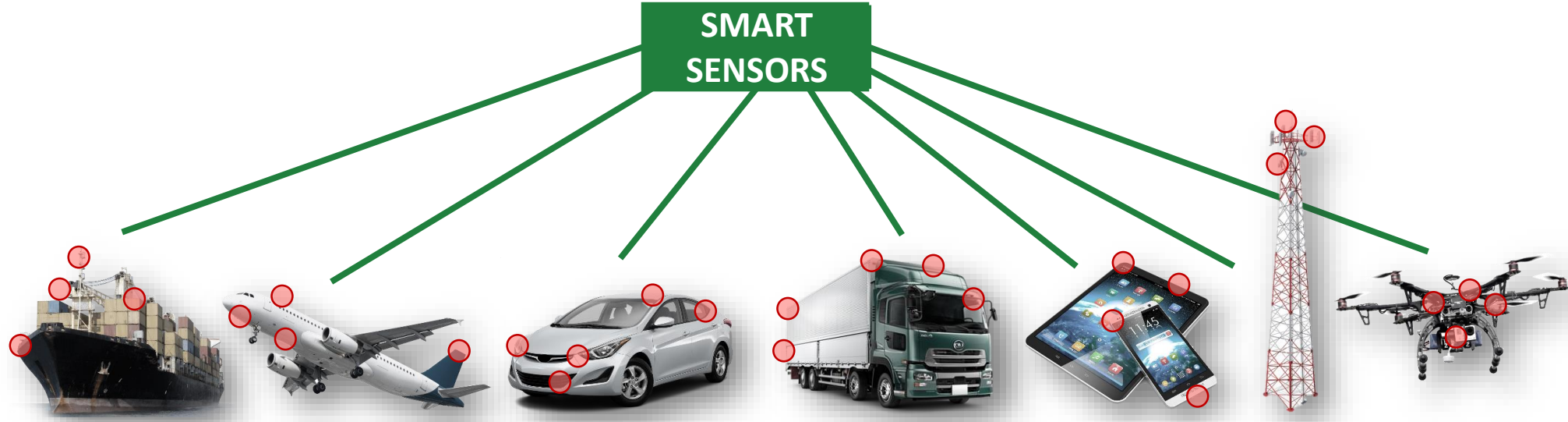


# Research on GPS Resiliency & Spoofing Mitigation Techniques Across Applications

Yoav Zangvil, CTO and Co-Founder. Regulus Cyber

# Context of our Research



## The Eyes and Ears of Modern Systems

- Our focus is on **GNSS**
  - No security
  - Easily spoofed
  - Easily jammed

# Yoav Zangvil, CTO and Co-Founder, Regulus Cyber

- B.Sc. degree in Mechanical Engineering from the Technion with major in robotics, dynamics and control systems, Cum laude.
- Military UAV Systems Engineer dealing with telecommunications protocols, encryption and resilient GNSS.
- Prior to Regulus, Elbit Systems, ADT, Rafael Advanced Defense Systems, Comverse and a Technology Division in the IDF.



# Context of our Research – GNSS Across Applications

- **LBS** – Over 90% of context-aware apps rely on GNSS.
- **Road** – The need in autonomous driving and ADAS for reliable and accurate positioning.
- **Aviation** – General positioning, ILS/GPS, approaches at airfields, ATC, ADSB.
- **Maritime** – GNSS has become the primary means of obtaining PNT information at sea.
- **Surveying** – GNSS remains the backbone technology in increasingly sophisticated applications.
- **Timing** – Keeping accurate time in sync across multiple locations is done using GNSS for critical infrastructures, including telecoms, energy, finance, sea ports and airports. Evolution of telecom networks and 5G makes GNSS increasingly essential, driving future shipments.



# Why Now?

# GNSS Spoofing – The Threat is Evolving

## Until 5 years ago

A GNSS spoofing attack would require expensive, high-end equipment in the \$50K - \$500K range



## Open Source GPS Signal Generators



## Today

Software Defined Radios and open source software allow anyone to spoof for \$100 - \$400



PlutoSDR: \$150





BladeRF: \$400



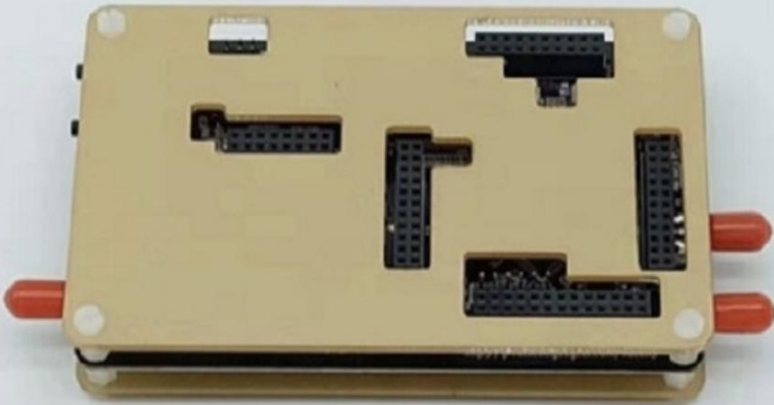
HackRF: \$100

# Software Defined Radios – Getting Cheaper and Accessible

2017 - \$193

Order ID: 501945176816259 <a href="#">View Detail</a> Order time: 07:40 Mar. 20 2017		Store name: Piswords Store <a href="#">View Store</a>   <a href="#">Contact Seller</a>		Order amount:  <b>\$ 192.85</b>
 HackRF One RTL SDR Software Defined Radio usb platform reception of signals 1MHz to 6GHz software demo board kit dongle receiver [Transaction Screenshot]		Confirmation Received <a href="#">Open Dispute</a>	Finished	<a href="#">Add to Cart</a>

2019 - \$89



**Bundle 1**


**HackRF One + Shielding case + Acrylic case**







### HackRF One SDR Software Defined Radio 1MHz to 6GHz Mainboard Development board kit


★★★★★ 4.9 (85 votes) | 163 orders

Price: US \$102 / piece

Discount Price: **US \$88.74** / piece **-13%** **3 days left**

 [Get our app to see exclusive prices](#) | Bulk Price ▾

Bundle:      

Shipping: **US \$8.38 to Israel via ePacket** ▾  
 Estimated Delivery Time: 19-32 days 

Quantity:  piece (843 pieces available)

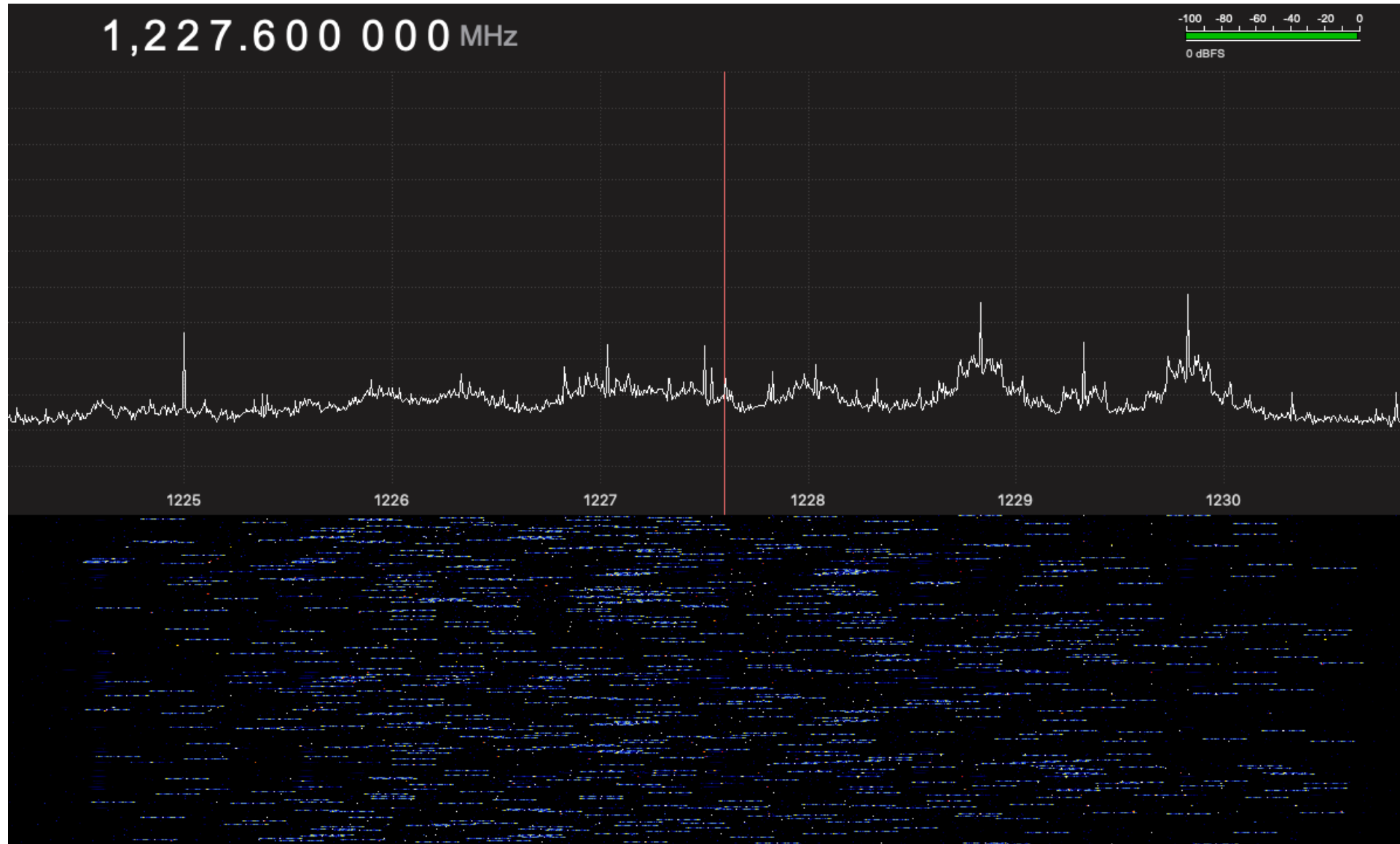
# GNSS Jamming – Smart, Portable and Undetected

- Pluto SDR
- Setup Price - \$158
  - Pluto SDR - \$149
  - Power bank - \$7
  - USB cable - \$2
- Specification:
  - Up to -15dBm channel power over 2.6M
  - Undetected by GNSS receivers as a jammer





# Jamming GPS L2 with the Pluto SDR



# GNSS Spoofing – Simple Setup, Pluto SDR

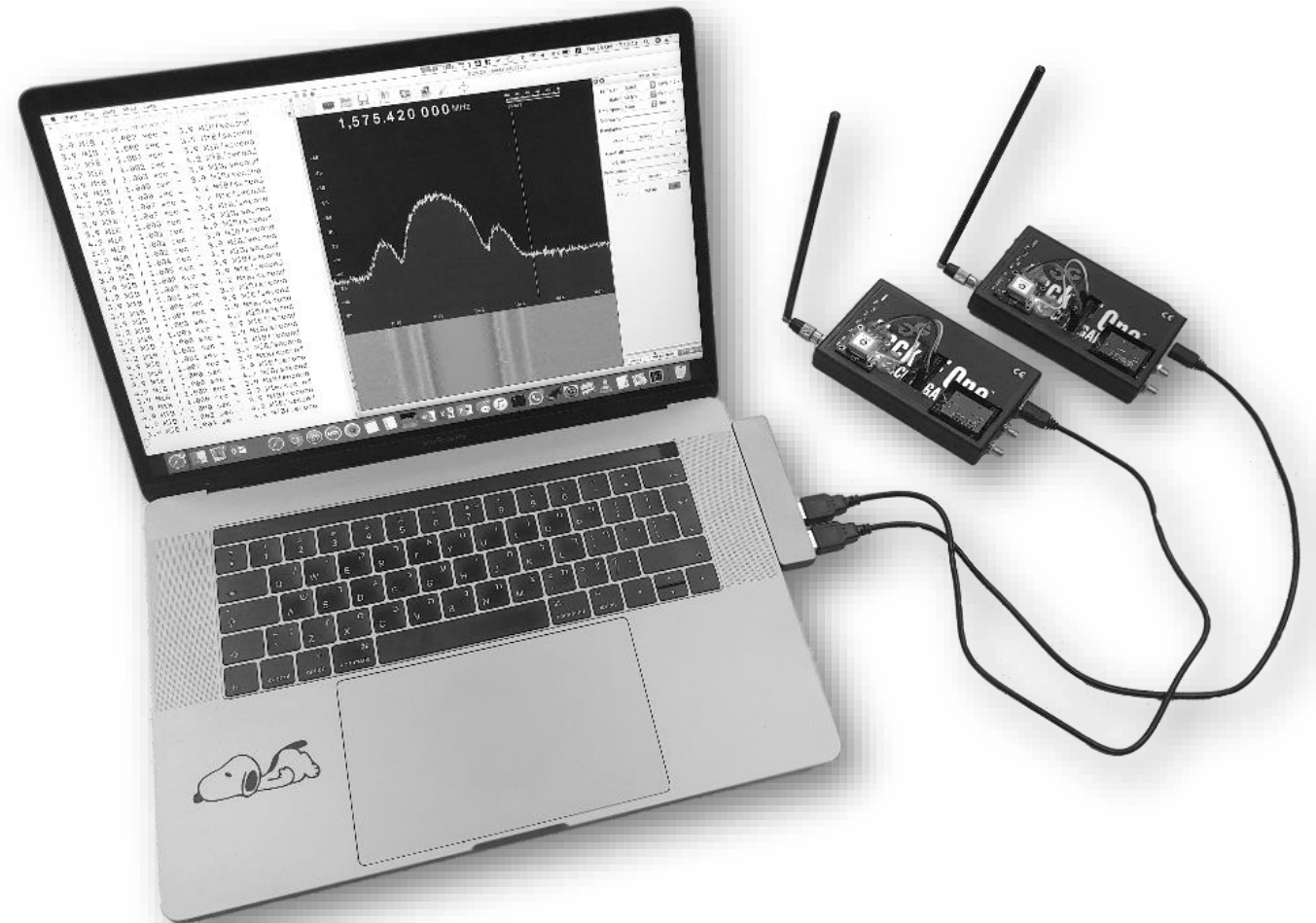
- Setup Price - \$165
  - Pluto SDR - \$149
  - Power bank - \$7
  - 16GB Flash drive - \$5
  - OTG USB Cable - \$2
  - USB cable - \$2
- Capabilities:
  - Reply recorded files
  - Reply generated scenarios
  - Smart jamming
- How to spoof:
  1. Generate or record an I/Q data file with 2.6M sample rate.
  2. Copy to a flash drive
  3. Create a file called runme0.sh with 3 lines:
 

```
iio_attr -a -c ad9361-phy TX_LO frequency 1575420000
iio_attr -a -c -o ad9361-phy voltage0 sampling_frequency 2600000
cat /media/sda1/spoof.bin | iio_writedev -a -b 50000 cf-ad9361-dds-core-lpc
```



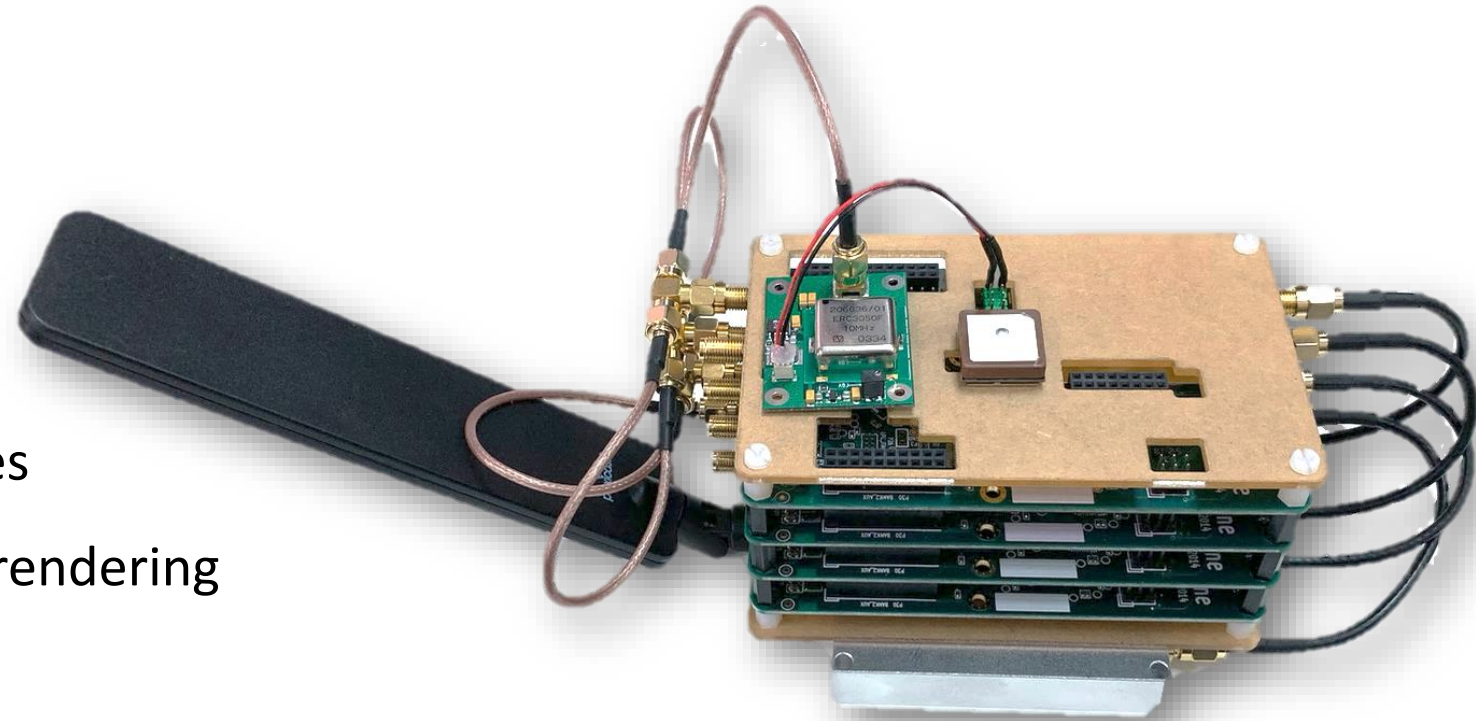
# GNSS Spoofing – Intermediate Setup, HackRF

- Setup Price - \$252 + laptop
  - 2 x HackRF - \$200
  - 2 x USB Cable - \$4
  - 2 x TCXO - \$28
  - 2 x GPS Receiver (for 1PPS) - \$20
- Specification:
  - Dual frequency
  - 1PPS Sync from GPS
  - Accurate TCXO
- Capabilities:
  - Real time spoofing static/dynamic scenarios
  - Reply recorded and generated files
  - Smart jamming



# GNSS Spoofing – Sophisticated Setup

- Four different constellation
- Four different frequencies
- Accurate OCXO
- 1PPS Sync from a GNSS Receiver
- Multi frequency antenna
- Start with valid navigation messages
- Transition to corrupted messages, rendering NMA useless





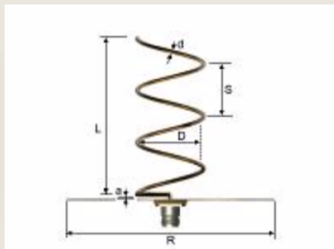
# GNSS Spoofing – Long Range 3D Printed Antenna

## Helix antenna design and construction details

### Input data (design requirements)

Design frequency	1575.42 MHz
Number of turns	13
Turn spacing	0.23 wavelengths
	<button>Calculate</button>

### The results



Legend. The letters in the image are used in the table below.

To get a large version, click on the image.

Wavelength		190.4 mm
Ideal diameter (internal)	<b>D=</b>	66 mm
Gain		14.46 dBi
Conductor diameter	<b>d=</b>	3.8 mm
Winding step (between centers)	<b>S=</b>	43.7 mm
Separation of the adapter section	<b>a=</b>	1.8 mm
Total conductor length		2757.7 mm
Minimum reflector diameter	<b>R=</b>	118 mm
Total antenna length	<b>L=</b>	569.3 mm

## Design performance

Bandwidth (@ -1dB)	Fmax/Fmin:	1.06
	Fmax:	1622.82 MHz
	Fmin:	1529.4 MHz
Bandwidth (@ -3dB)	Fmax/Fmin:	1.12
	Fmax:	1671.65 MHz
	Fmin:	1484.72 MHz
Beam width (@ -3dB)		30 degrees



Calculator: <http://jcoppens.com/ant/helix/calc.en.php>

# GNSS Spoofing and Jamming – Proposed Categories for Civil Aviation

Jamming	Spoofing
<b>J1</b> - Collateral Jammers	<b>S1</b> – Repeaters
<b>J2</b> - High Power Interferers	<b>S2</b> – Errant signals
<b>J3</b> - Targeted Jammers	<b>S3</b> - Collateral Spoofers – Simulators
<b>J4</b> - Targeted Sophisticated Jammers	<b>S4</b> - Collateral Spoofers – Re-radiators
	<b>S5</b> - Targeted Spoofers – Simulators
	<b>S6</b> - Targeted Spoofers – Re-radiators
	<b>S7</b> - Targeted Sophisticated Spoofers

**Table 1 – New Interference Types (Jamming, Spoofing) and Categories (J1-J4, S1-S7)**

*“INCREASING INTERNATIONAL CIVIL AVIATION RESILIENCE: A PROPOSAL FOR NOMENCLATURE, CATEGORIZATION AND TREATMENT OF NEW INTERFERENCE THREATS”, January 28 - 31, 2019*

# GNSS Spoofing - Common Assumptions and Rebuttals

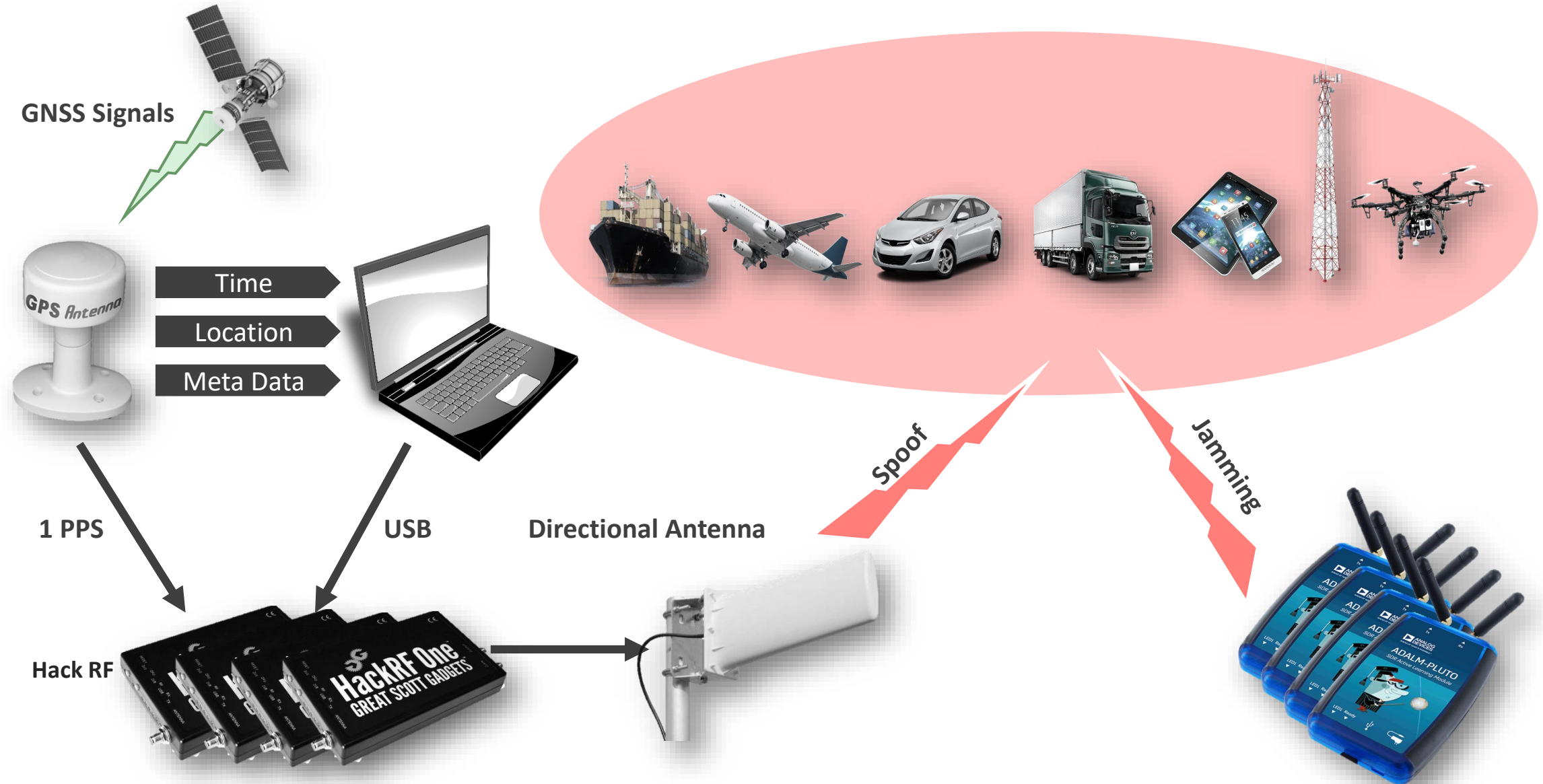
Countermeasures	Spoofers
Check Time Shift	Hacker can be perfectly aligned with real-time signals, achieving a seamless takeover and making it very hard to detect
Check Position Shift	Hacker can start spoofing to the current position and after a while, add drift to the position
Multi Constellation Receiver	Hacker can spoof other constellations or jam them
Multi Frequency Receiver	Hacker can jam other frequencies
Accurate Receiver Clock	Hacker can use a TCXO or a OCXO
Navigation Message Authentication (NMA)	Replay attacks with a time shift Corrupted CRC – receiver can still track the signal
Sensor Fusion (IMU, odometer, WiFi, Cellular)	Commercial grade IMU drift very fast Sensor fusion aimed to improve accuracy not security

# Spoofing Techniques – From Simple to Complex

- Meaconing – replay recorded sky
- Spoof using a generated scenario on L1
- Add 1PPS sync to allow real-time spoofing
- Add TCXO and OCXO
- Since L1 and E1 are the same frequency, we developed a selective jammer that allows us to jam E1 (BOC) but allows us to spoof L1 (BPSK)
- Spoof GPS L1 and jam everything else
- Multi constellation and multi frequency spoofing



# Advanced Spoofing Setup



# Research: GNSS Resiliency Report



- Developing Pyramid GNSS technology – spoofing detection for commercial GNSS receivers.
- Lab and field tests to verify reliability of detection technology.
- Advanced GNSS spoofing capabilities, using open source hardware and modified software
- Reveal vulnerabilities of commercial GNSS receivers.
- Aid development of mitigation techniques.

## What is the status of commercial GNSS security?

# GNSS Resiliency Report – Scenarios

Manufacturer	Model	Successfully Spoofed
GlobalTop	PA6C/GTPA010	Yes
u-Blox	NEO-6M	Yes
u-Blox	NEO-7M	Yes
GlobalSat	G-Star IV	Yes
STM	Teseo-LIV3F	Yes
u-Blox	NEO, CAM, SAM M8	Yes
Furuno	GN-87	Yes
Javad	TRH-G2	Yes
u-Blox	ZED-F9	Yes
Manufacturer	Model	Successfully Spoofed
Apple	iPhone XS	Yes
Samsung	Galaxy Prime Pro	Yes
Huawei	Mate 10 Pro	Yes
Xiaomi	Mi8	Yes
Manufacturer	Model	Successfully Spoofed
Mercedes	CLS 400D	Yes
BMW	BM 318A	Yes
Cadillac	CT6	Yes
Tesla	S	Yes
Toyota	RAV4	Yes

Table 4: Indoor Test Results

## Indoor Tests: **Standalone Receivers and Mobile Phones**

- Inside a lab, where no external GNSS signals are available

## Indoor Tests: **Cars**

- Inside underground parking garage, where no external GNSS signals are available.

# GNSS Resiliency Report – Scenarios

Manufacturer	Model	Successfully Spoofed
GlobalTop	PA6C/GTPA010	Yes
u-Blox	NEO-6M	Yes
u-Blox	NEO-7M	Yes
GlobalSat	G-Star IV	Yes
STM	Teseo-LIV3F	Yes
u-Blox	NEO, CAM, SAM M8	Yes
Furuno	GN-87	Yes
Javad	TRH-G2	Yes
u-Blox	ZED-F9	Yes
Manufacturer	Model	Successfully Spoofed
Apple	iPhone XS	Yes
Samsung	Galaxy Prime Pro	Yes
Huawei	Mate 10 Pro	Yes
Xiaomi	Mi8	Yes

*Table 5: Results of Outdoor Spoofing, Scenario A*

Outdoor Test, **Scenario A:**

Spoofing attack is initiated after the target has locked on a real GNSS signal



# GNSS Resiliency Report – Scenarios

Manufacturer	Model	Successfully Spoofed
GlobalTop	PA6C/GTPA010	Yes
u-Blox	NEO-6M	Yes
u-Blox	NEO-7M	Yes
GlobalSat	G-Star IV	Yes
STM	Teseo-LIV3F	Yes
u-Blox	NEO-M8	Yes
Furuno	GN-87	Yes
Javad	TRH-G2	Yes
Manufacturer	Model	Successfully Spoofed
Mercedes	CLS 400D	Yes
BMW	BM 318A	Yes
Cadillac	CT6	Yes
Tesla	S	Yes
Toyota	RAV4	Yes

*Table 6: Results of Outdoor Spoofing, Scenario B*

Outdoor Test, **Scenario B:**

Spoofing attack is initiated before the target is powered on.

Since a mobile phone is always on, it was not a part of this scenario.

# GNSS Resiliency Report – Findings

## Standalone Receivers

- Reports wrong position and/or time
- No spoofing alarm is activated
- No jamming alarm is activated
- Additional effects are system dependent

**100% vulnerable**

## Mobile Phones

- All LBS are not useable
- Find My iPhone
- Photo geo-tagging
- Unable to plan or follow a route
- Unable to use navigation apps
- Unable to use ride hailing apps like Uber, DiDi and Lyft.

**Major privacy implications where a user can be “placed” in a location that he is not.**

# GNSS Resiliency Report – Findings in Cars

## Safety:

- Exit at the wrong interchange.
- Aggressive braking and steering.
- Accelerate to 100 km/h in a 30 km/h zone.
- Slowed down to 50 km/h on a 100 km/h road.
- Failed to slow down before intersections.
- Braked on main road thinking an intersection is close.
- Height of the car's suspension changed while driving.
- SOS feature reports wrong position to dispatch.
- Confusing and distracting navigation cues while trying to follow a planned route.

## Non-safety:

- The car's built-in navigation system displays wrong position on the map.
- Car's clock displays wrong time.
- Unable to plan or follow a route.
- Unable to activate adaptive cruise control.
- GPS-based alarm services do not work.

100% vulnerable

**Our employee was genuinely frightened while holding the wheel, and despite the fact he could manually control the car and regain control, the split second of speeding, turning, and other aggressive maneuvers resulted in panic on a highway. This proves that regulation has to be actively involved in ensuring PNT resiliency for public safety.**

# GNSS Resiliency Report – Responsible Disclosure

Mixed reactions from major corporations across industries:

## Negative:

- More often than not, companies did not take visible responsibility for vulnerability of their product
- Referred to it as a ‘Global problem across industries’
- Impression that Spoofing threat is beyond their reach and realm of responsibility

## Positive:

- Number of companies asked for extension
- Some indicated interest in cooperating towards testing their technology and finding a solution



**Responsibility for GPS vulnerabilities and their effects on platforms and users need to be defined. Government needs to take lead in this matter. Still early – Now is the time to act.**



# GNSS Resiliency Report – Responsible Disclosure

Mixed reactions from major corporations across industries:

## Negative:

- More often than not, companies did not take visible responsibility for vulnerability of their product
- Referred to it as a ‘Global problem across industries’
- Impression that Spoofing threat is beyond their reach and realm of responsibility

## Positive:

- Number of companies asked for extension
- Some indicated interest in cooperating towards testing their technology and finding a solution



**Responsibility for GPS vulnerabilities and their effects on platforms and users need to be defined. Government needs to take lead in this matter. Still early – Now is the time to act.**

# Responsible Disclosure – Tesla

## Main Points From Quote From Tesla Motors:

- It doesn't demonstrate any issues specific to Tesla
- Any product or service that uses the public GPS broadcast system can be affected by GPS spoofing
- That hasn't stopped us from taking steps to introduce safeguards in the future
- Drivers using those features must still be responsible for the car at all time

# Responsible Disclosure – Mobile Manufacturer

## Quote:

“As we mentioned earlier, the scenario you are describing is not a vulnerability affecting specific devices but a challenge to current smartphone devices in general with little immediate threat.

While we are working with our partners to enhance the functions of our smartphone devices, **we do not acknowledge that this is a specific vulnerability.**

This is a known scenario that is already covered by the multiple media outlets, but if there is anything that we missed please feel free to let us know.”

# Easy To Execute Spoofing Scenarios

- At the base of operations
- Inside an office building or a mall
- Disrupt ride-sharing and mobility services (potential theft)
- Inside an airport/maritime port
- Target single car by tailing (Cargo theft)
- Initiate spoof in parking lot
- Unintentional (taxi drivers, Pokémon Go)

# So What Can We Do?

Short-term Solution

Long-term Solution



- **Detection and Prevention**

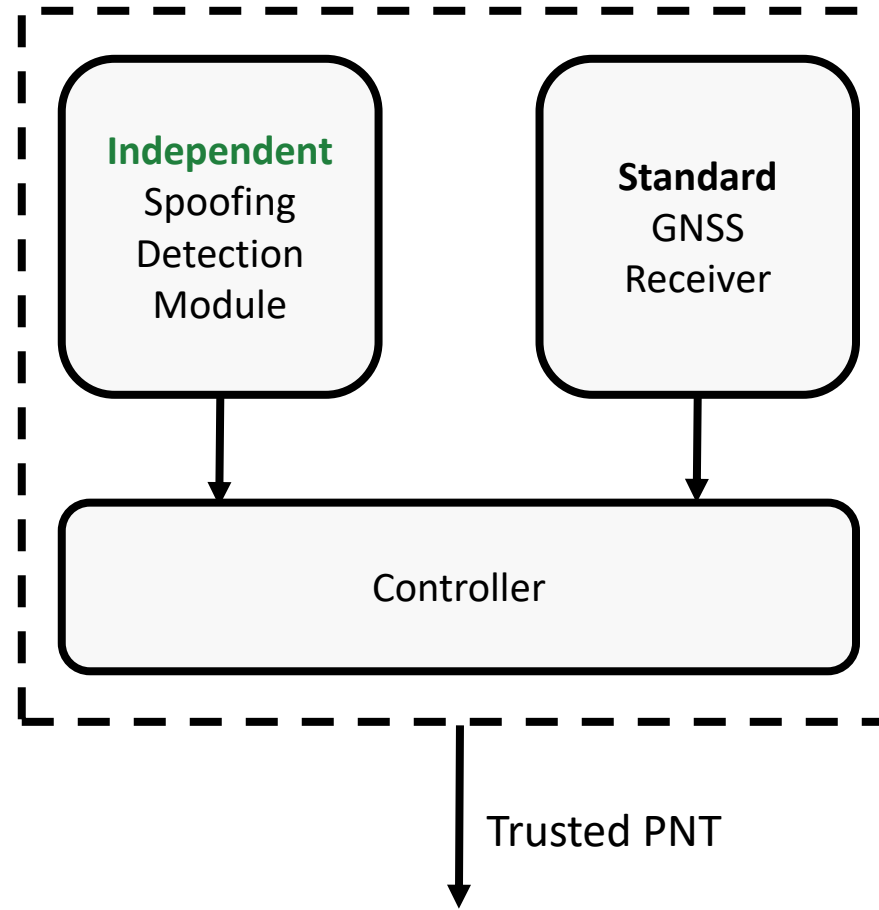
- Prevent false PNT effects
- Fortify existing receivers
- Solution at the board level
- Use today's GNSS chips

- **Mitigation**

- Provide valid PNT under spoofing
- For new receivers
- Solution at the chip level
- Re-design GNSS chips

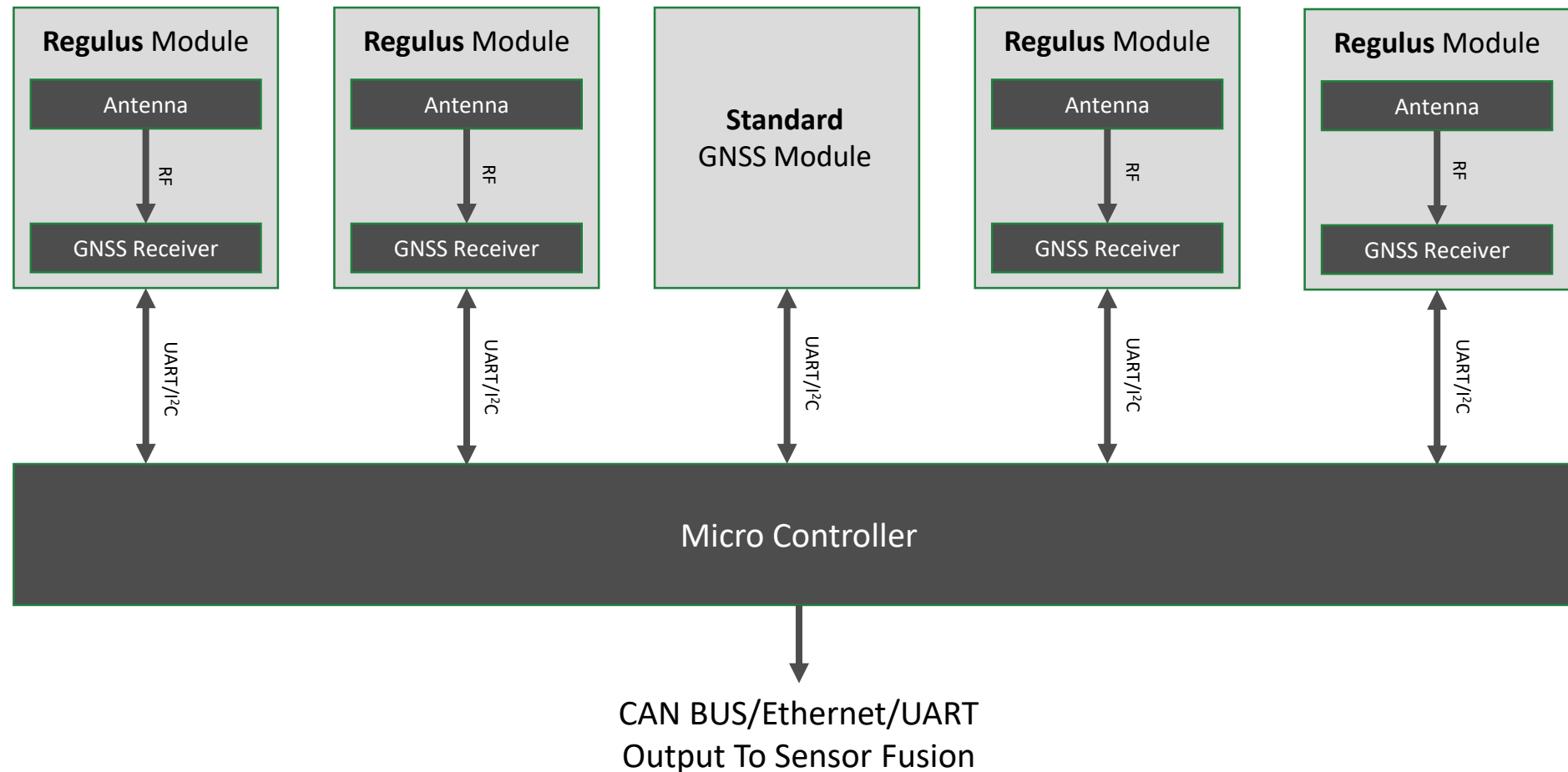


## Short Term Solution – Board Level



# Short Term Solution – Pyramid GNSS Receiver

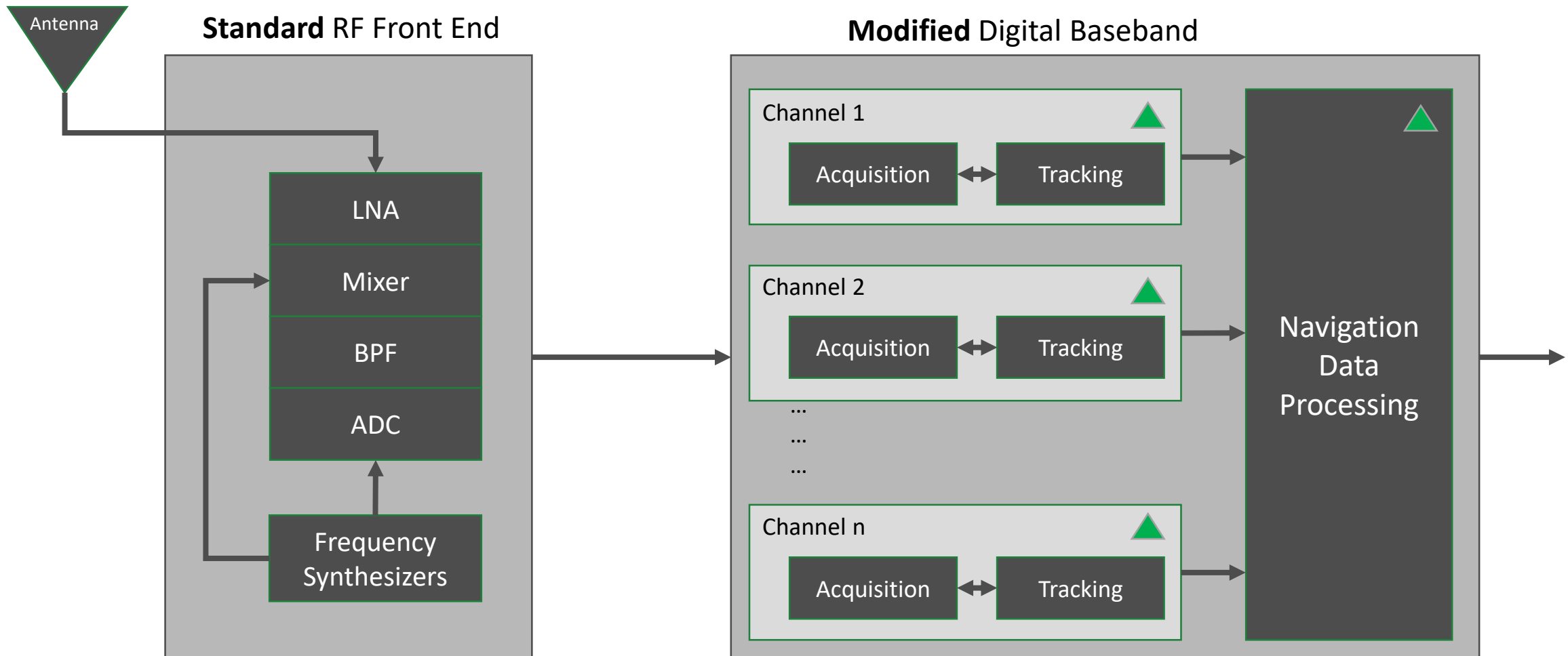
Based on DOA, yet not a CRPA!



## Long Term Solution – Chip Level

- Multi constellation should not be mandatory
- Multiple correlation peaks tracking – clear sign of spoofing
- Instead of throwing away these PRNs, use them!
- Need a smart way to group those peak
- Once grouped, two converging PNT solutions can be found

# Long Term – Pyramid IP Core



# Summary

- The new goals of the industry – **security and reliability**
- Sensor fusion helps but is not the holy grail – the receiver must deal with spoofing
- The threat evolves – we must solve the **future** threat today
- Providing a PNT with a confidence level does not tell if you are spoofed – a fully deterministic solution must be used
- Deploy a Red Team capable of testing the effects of interference, jamming, and spoofing
- **Define and enforce GNSS security standards**



[www.regulus.com](http://www.regulus.com)  
[yoav@regulus.com](mailto:yoav@regulus.com)

