Today's PTA Agenda

- 10:30 to 11:30 PTA Overview
- 11:30 to 12:30 Lunch
- 12:30 to 1:45 Protect, with Board Discussion
- 1:45 to 2:00 Break
- 2:00 to 3:15 Toughen, with Board Discussion
- 3:15 to 3:30 Break
- 3:30 to 4:45 Augment, with Board Discussion
- 4:45 to 5:00 PTA Summary
- 5:00 to 6:00 Board Deliberations
- 6:00 Adjourn

SPACE-BASED POSITIONING
NAVIGATION & TIMING
NATIONAL ADVISORY BOARD

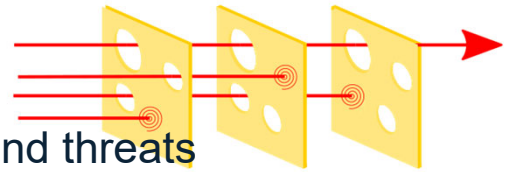
Approaches to Toughen GPS for Critical Infrastructure

12 Apr 2024 – Draft 0.7

Overview

- Introduction
- Toughening at the Source
- Toughening GNSS Receivers/User Equipment (UE)
- Toughening at the Platform/System/Use Case Level
- Recommendations
- Conclusions

Toughening GPS for Critical Infrastructure



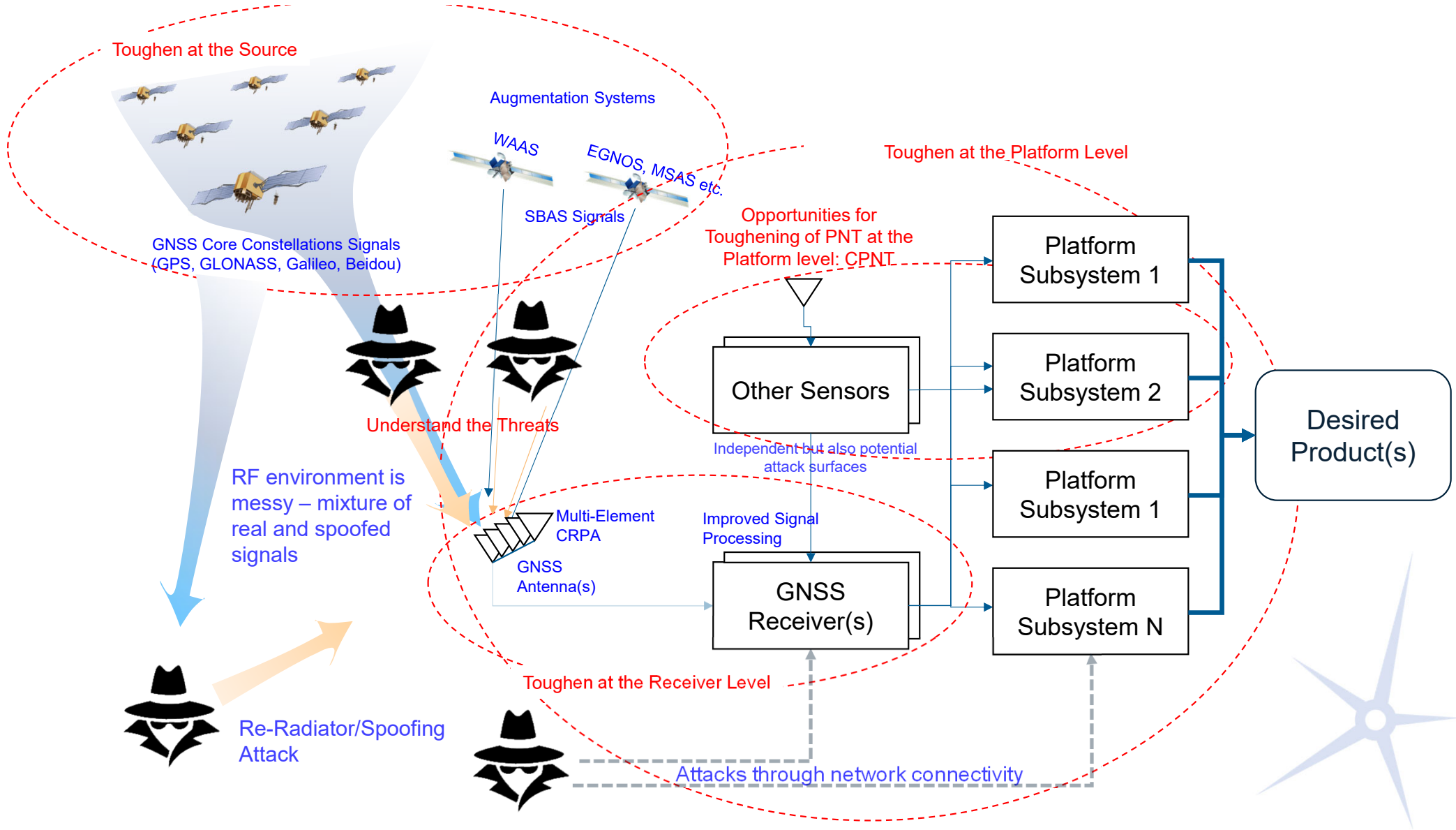
- Toughen: Measures that make GPS use better able to resist challenges and threats

- Toughening involves improving the resilience of a desired capability…
  - Making a capability less susceptible to disruption (i.e. loss of service/capability)
  - Making a capability more resistant to tampering (i.e. spoofing or cyber attacks)
  - Objective is always context dependent. (No single silver bullet to address all uses).

- GPS is widely used for positioning, navigation and timing (and others)
  - Use cases have some performance requirements at the use-case/platform level
  - Different layers of the system can be toughened to achieve desired level of resilience
  - Critical infrastructure applications are rarely based solely on the use of GPS
    - Availability and suitability of Complimentary PNT and redundant sensors must be considered

- Toughening GPS is not just toughening User Equipment (UE) – however UE is often best first line of defense
  - Many technology options for toughening UE
  - Some technology options available for toughening at the source
  - Many technology options for toughening at the use-case/platform level

PTA


Toughen at the Source
Augmentation Systems
WAAS
EGNOS, MSAS etc.
SBAS Signals
GNSS Core Constellations Signals
(GPS, GLONASS, Galileo, Beidou)
Toughen at the Platform Level
Opportunities for
Toughening of PNT at the
Platform level: CPNT
Platform
Subsystem 1
Platform
Subsystem 2
Platform
Subsystem 1
Platform
Subsystem N
Desired
Product(s)
Other Sensors
Independent but also potential
attack surfaces
Understand the Threats
RF environment is
messy – mixture of
real and spoofed
signals
Multi-Element
CRPA
GNSS
Antenna(s)
Improved Signal
Processing
GNSS
Receiver(s)
Toughen at the Receiver Level
Re-Radiator/Spoofing
Attack
Attacks through network connectivity

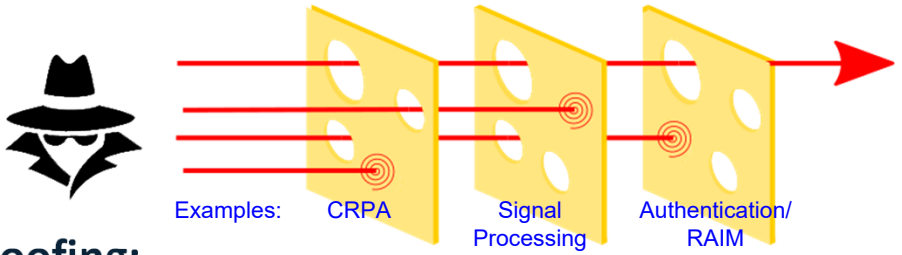
Understand the Threats

Interference

- Radio "noise" degrading use and can result in service denial
- Jamming is intentional interference

GPS/GNSS Spoofing

- Signal emissions imitating real GPS/GNSS used by GNSS receiver in combination with, or instead of, the intended signals



Two types of GPS/GNSS RF Cyber spoofing:

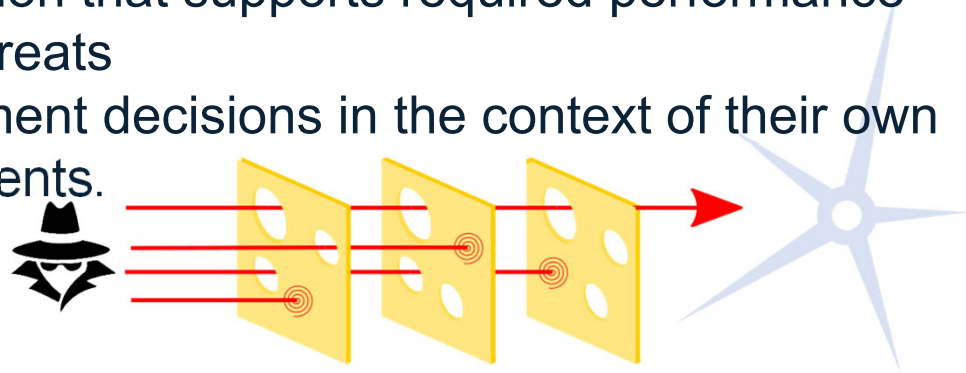
Measurement spoofing: real or simulated GPS signals manipulated to produce incorrect position, navigation or time (traditional spoofing)

Data spoofing: manipulated or simulated signals with harmful digital data used in processing and calculation of PNT

Either type has range of effects from incorrect PNT to receiver and/or application system malfunction

Systems Engineering Approach to Toughening

- Define Total System Requirements
  - Define the end capability that is to be protected
    - What are the key performance metrics?
  - Understand exactly how GPS/GNSS is used to derive/support the end capability
  - Identify the threats and all Attack Surfaces
    - What if GNSS is denied?
    - What if GNSS is compromised (i.e. incorrect data without annunciation)
    - What if an augmentation is denied/compromised
    - Are there attack surfaces associated with internal/external data connectivity
      - Particularly if it involves the GNSS receiver
  - Define architecture with layers of protection that supports required performance of end capability in the presence of all threats
- Each organization must make risk management decisions in the context of their own cyber ecosystem, architecture, and components.



Some Relevant Guidance Already Exists

- DHS - Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework - Version 2.0
- DHS – Receiver Allow List Development Guide, July 12, 2021
- DHS – Receiver Whitelist Development Guide, July 12, 2021
- NIST - Framework for Improving Critical Infrastructure Cybersecurity (V 1.1)
- NIST - IR 8323r1 - Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services
- Cybersecurity and Infrastructure Security Agency (CISA) - Federal PNT Services Acquisitions Guidance
- GAO – CRITICAL INFRASTRUCTURE PROTECTION National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods
- IEEE P1952 Standard – (Under development)
- SAE – ARP 4754A – Certification Considerations for Highly-Integrated or Complex Aircraft Systems

Need for Additional Guidance to System Integrators of Critical Infrastructure

- Some important guidance for system developers/architects
  - GPS SPS Positioning Service – Performance Standard 5th Edition
    - Has basic information about predicted satellite reliability and constellation maintenance
  - Similar documents for L5 and WAAS (and other constellations)
- Additional information and assumptions needed by the system designer/integrator
  - Probability of long-term outages
  - Probability of experiencing interference
  - Probability of tampering
- Previous recommendation from advisory board:

National PNT Advisory Board Protect, Toughen, Augment Subcommitee Recommendation 19 May 2022

- **Title of Recommendation:** Establishing the Extent That We Should We Rely on the GPS Infrastructure
- **Finding:**
  - There are no authoritative assessments of the likelihood and extent (temporal, geographic) that the GPS Infrastructure (monitoring and control, constellation and satellites, signals) could fail in different time frames, due to any cause.
- **Recommendation:**
  - The U.S. Government establish, publish, and maintain estimates of the likelihood that GPS would not provide sufficient useful civil signals, due to failures of the GPS Infrastructure (Ground Segment, GPS Space Segment, and GPS signals) from any cause. These estimates would describe the likelihood of GPS Infrastructure failure for different durations in different time frames.
- **Reasons for Recommendation:**
  - There currently are wildly diverse opinions concerning the likelihood and extent that the GPS Infrastructure could fail in different time frames. Those making risk management decisions, and those investing in Protecting, Toughening, and Augmenting GPS lack the information needed to select the right approaches and how urgent it is to implement them. Only a team with the right expertise and information can assess the aggregate likelihood of such failures due to various causes—benign, natural, and malicious.
- **Consequences of No Action on the Recommendation:**
  - Currently, the U.S. risks inconsistent development and fielding of Protecting, Toughening, and Augmenting GPS. Some may be investing in Protect and Toughen when Augment is more appropriate, or vice versa. Some may be undertaking greater expense and disruption than is needed, while others may risk experiencing a problem before they are ready for it.

Toughening GNSS at the Source

- Cyber resilience through signal authentication
  - In band solutions (like Chimera)
  - Out of band solutions (like HARS)

- Better interference rejection through signal design
  - Modernized Signals
  - Higher chipping rates perform better against RFI
  - Higher power or flex power signals offer some advantages
  - Benefits are marginal compared to costs and timeframe for implementation

- Implementing these things takes a long time and benefits are small compared to costs
- Requires changes to UE in addition to Constellation and ground segment

Chimera: a Backwards Compatible Security Overlay for the L1C Civil Signal IS-AGT-100 Defines an Experimental NTS-3 KISS Signal

Data Authentication

- Message Signing
- KISS & TESLA Options

Ranging Authentication

Fast & Slow Watermark Channels

- 6 or 1.5 second epoch (Fast)
- 3 or 1.5 minute epoch (Slow)

OSNMA on E1

Galileo Counterparts

ACAS on E6

SPD-7: "develop and validate requirements and a funding strategy to implement data and signal authentication of civil GPS and wide area augmentations for homeland security and public safety purposes"

IS-AGT-100
17-APR-2019

AIR FORCE RESEARCH LABORATORY
SPACE VEHICLES DIRECTORATE
ADVANCED GPS TECHNOLOGY

INTERFACE SPECIFICATION
IS-AGT-100

Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User Segment Interface

APPROVED BY:
Digitally signed by CHAPMAN.DAVID.C.1392891761 Date: 2019.04.17 16:49:32 -06'00'
David C. Chapman, DR-03, DAF
Program Manager
Advanced GPS Technologies Program
Date

DISTRIBUTION STATEMENT A. Approved for Public Release; Distribution is Unlimited

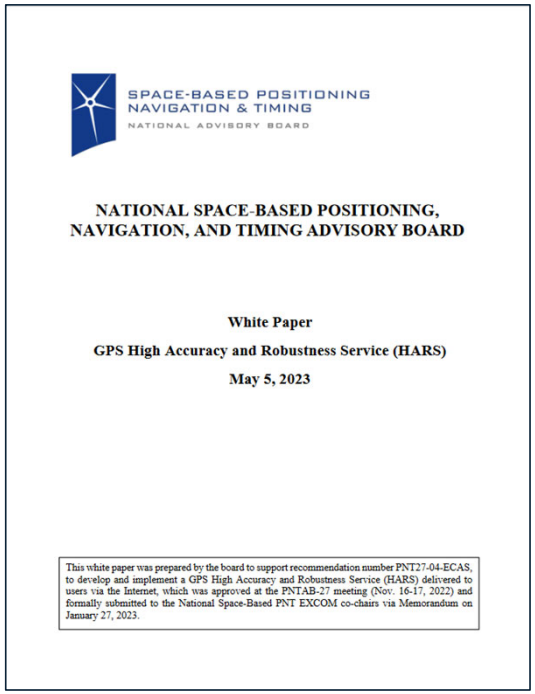
Had Its Origins In the Film Industry ca. 2002

Formally Proposed for L1C in 2005

Signal Specification and Select Papers are at
http://www.gpsexpert.net/chimera-specification

High Accuracy and Resiliency Service (HARS)

- Could be the fastest to implement – no change to program of record
- Multiple Layered Services to provide protection from data spoofing and enhance A/J



SPACE-BASED POSITIONING NAVIGATION & TIMING
NATIONAL ADVISORY BOARD

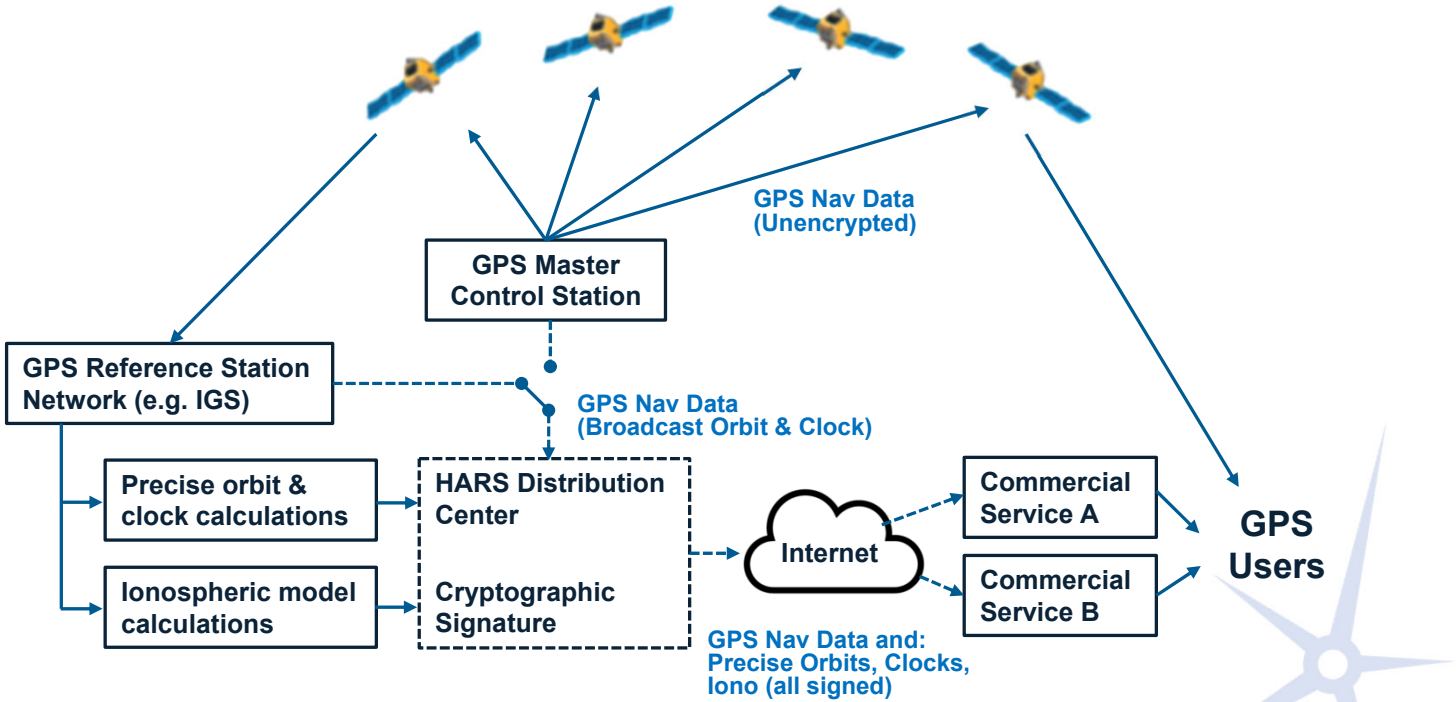
NATIONAL SPACE-BASED POSITIONING, NAVIGATION, AND TIMING ADVISORY BOARD

White Paper

GPS High Accuracy and Robustness Service (HARS)

May 5, 2023

This white paper was prepared by the board to support recommendation number PNT27-04-ECAS, to develop and implement a GPS High Accuracy and Robustness Service (HARS) delivered to users via the Internet, which was approved at the PNTAB-27 meeting (Nov. 16-17, 2022) and formally submitted to the National Space-Based PNT EXCOM co-chairs via Memorandum on January 27, 2023.



National Space-based Positioning, Navigation, and Timing Advisory Board, White Paper, *GPS High Accuracy and Robustness Service (HARS),* May 5, 2023.
www.gps.gov/governance/advisory/recommendations/2023-05-white-paper-GPS-HARS.pdf

High Accuracy Services.

- Other constellation already have high accuracy services
  - **Galileo** – High Accuracy Service – HAS
    - Designed for Global validity
    - Disseminated via E6-B signal (1278.75 MHz) on all MEO satellites & Internet
    - Provides corrections for Galileo E1/E5a/E5b/E6; E5 AltBOC ***and*** *GPS L1*; and L2C.
  - **Beidou** – PPP-B2b – From GEOs
    - Regional System
    - Corrections for Beidou CNAV1 or BDS B1C ***and*** for GPS L1C/A
  - **QZSS** – Centimeter-Level Augmentation Service (CLAS)
    - Regional System
    - Corrections for QZSS ***and*** GPS (PPP-RTK)

Table 6-2 The PPP Service Performance Standard

Constellation	Performance Characteristics	Performance Standard	Constraints
BDS	HorizontalPositioning Accuracy (95%)	≤0.3m	The correction targets: PPP-B2b information is used to correct the CNAV1 NAV message of the BDS B1C signal and the LNAV NAV message of the GPS L1C/A signal; Requirements for the correction targets: the BDS RNSS service performance meets the requirements of this specification; GPS service performance meets the requirements of "GPS Standard Positioning Service Performance Standard (Version 5.0)". Elevation mask is 10 degrees; Dual-frequency positioning; The statistical time interval is 7 days, and all points in the service area are averaged.
	Vertical Positioning Accuracy (95%)	≤0.6m	
	Convergence Time	≤30min	
BDS+GPS	Horizontal Positioning Accuracy (95%)	≤0.2m	
	Vertical Positioning Accuracy (95%)	≤0.4m	
	Convergence Time	≤20min	

Zero Trust and Verify…

- Opportunity for HARS to be an extensible architecture
  - Add capabilities over time
- Opportunity: Monitor **all** GNSS core constellations
    - Provide warnings if **any** system element is not performing nominally
    - Can mitigate some concerns with using foreign satellite systems
  - Provide corrections for all GNSS core constellations
    - Provide the most robust and accurate high accuracy service
    - Treat all other GNSS constellations as augmentations to GPS
  - Provide signed, authenticated navigation messages (with some delay)
    - Mitigate potential data spoofing attacks
- HARS users could have powerful tools to aid in detection and mitigation of spoofing in addition to a high accuracy service

Recommendation

- Previous Recommendation:
  - The GPS system should add a corrections service and digitally signed Nav Data, available over the internet.
  - The HARS system must be funded and have an operator, such as the US Space Force, the Department of Transportation, or similar.
- New Additional Recommendations:
  - HARS should provide corrections/status/health data for other core constellations
    - Rationale:
      - Galileo HAS provides high accuracy corrections for Galileo E1/E5a/E5b/E6; E5 AltBOC and *GPS L1*; and L2C.
      - Beidou HAS provides corrections for Beidou and GPS
      - Monitoring and timely alerting of anomalies mitigates some concerns with use of foreign satellite signals

Toughening User Equipment

Logan Scott

Pragmatic Steps Towards Toughening

Logan Scott has over 45 years of military and civil GPS systems engineering experience. He is a consultant specializing in radio frequency signal processing and waveform design.

At Texas Instruments, he pioneered approaches for building high-performance, jamming-resistant digital receivers and adaptive arrays. In 1985 his team developed the world's first all-digital GPS receiver. At Omnipoint (now T-Mobile), he developed spectrum sharing techniques that led to a Pioneer's preference award from the FCC. He is a cofounder of Lonestar Aerospace, an advanced decision analytics company located in Texas.

Logan has been an active advocate for improved civil GPS location assurance for over 20 years and was the first to describe how civil navigation signals could be authenticated using delayed key concepts central to the Chimera signal. For the past 8 years he has been developing advanced signal concepts, including Chimera, for NTS-3, AFRL, and the University of Colorado.

Logan is a Fellow of the Institute of Navigation and a Senior Member of IEEE. In 2018 he received the GPS World Signals award. He received the ION PVH Weems award for 2022 and is a member of the President's National PNT Advisory Board. He is the author of Interference: Origins, Effects, and Mitigation in PNT21 and holds 46 US patents.

BLUF

- **Situational Awareness Is Foundational**
  - And Not That Hard
- **Diverse Sensing Methods Improve Resilience**
  - Doesn't Always Have to Cost a Lot
- **Adaptive Arrays Require Caution**
  - Large Measurement Errors are Possible
- **Exposure Testing is Crucial**
  - Surprises in the Wild are Confusing and Sometimes Dangerous
- **User Community Needs Clear Signals On What to Buy**

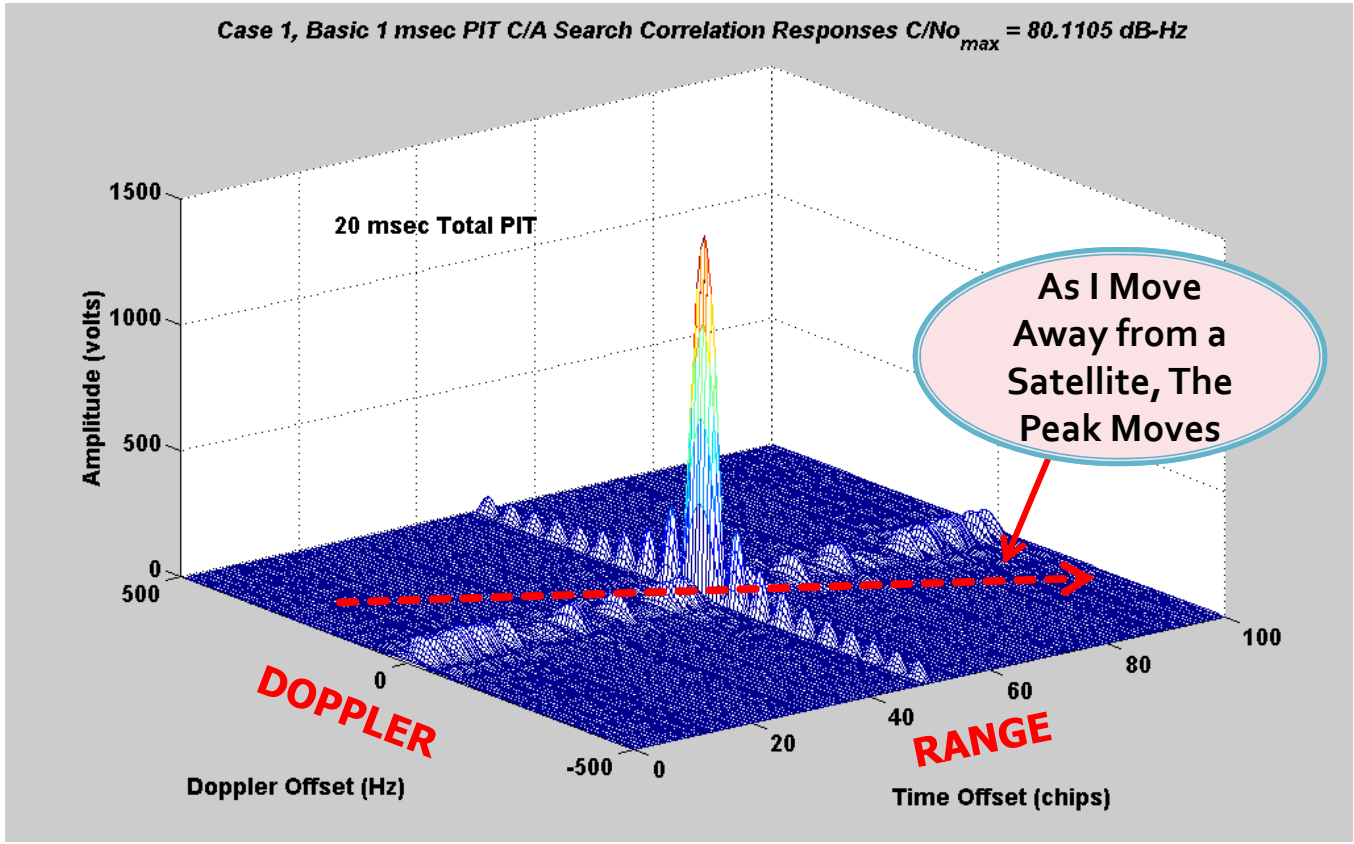
Autonomy Raises the Stakes

Jamming vs. Spoofing

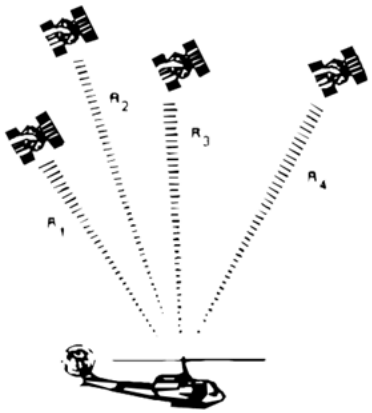
- Jamming's Objective
  - Denial of Navigation Service by Masking Signals with Interference
  - Tends Towards Area Denial
- Spoofing's Objective
  - Convince You That You Are Somewhere or Sometime You Are Not
    - Overlaying Real Signals With False Signals
    - Cyber Attack (Lying) is often easier and more effective
  - Often, But Not Always, Targets A Specific Victim
- Structure Jamming (aka Smart Jamming) Can Act Like Uncontrolled Spoofing

A GNSS Receiver Tracks the Correlation Peak to Measure PseudoRange to a Satellite

Each Point is the Output of a Narrow Band Filter Matched to a Particular Doppler and Code Phase

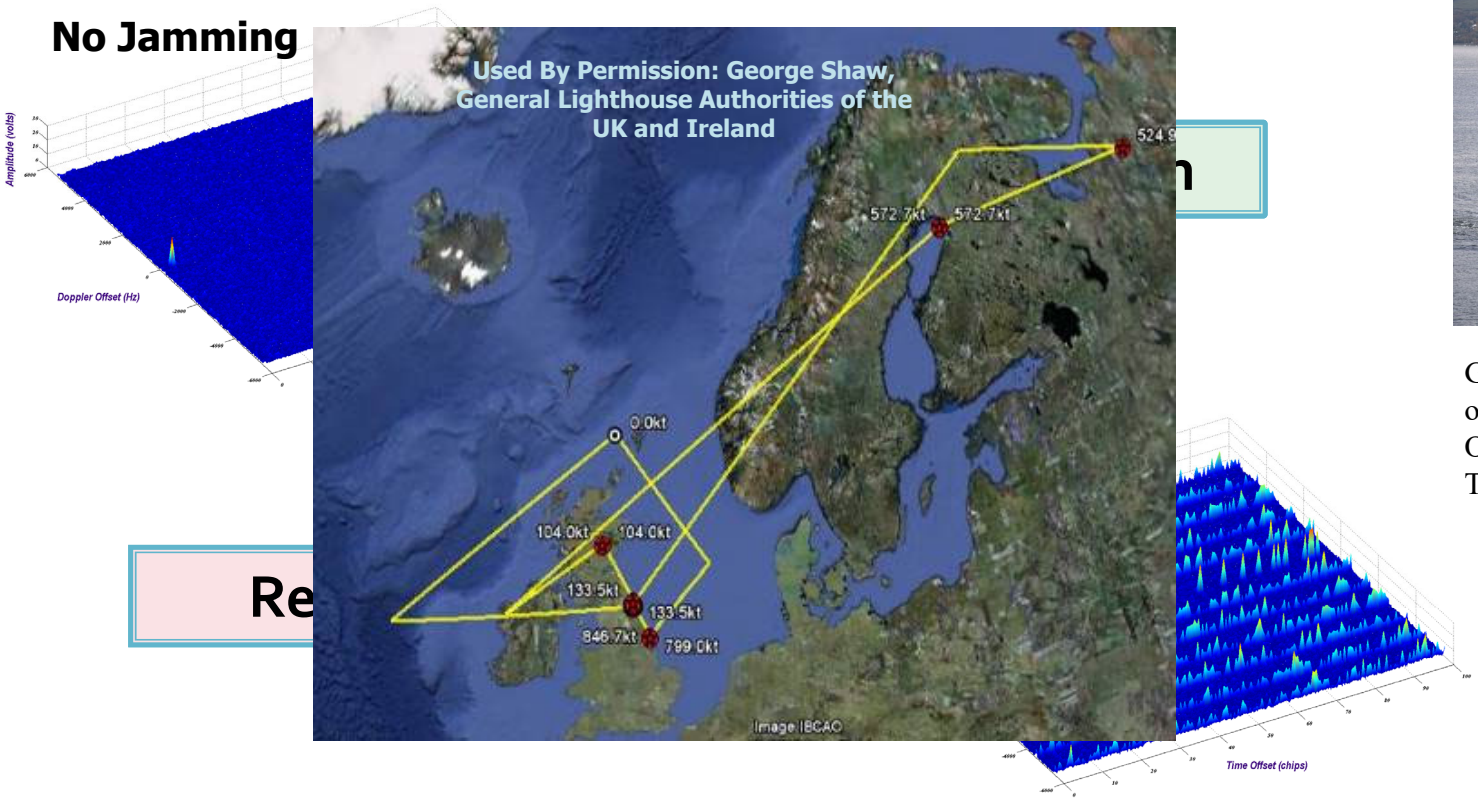


Track Four Satellites and You Can Figure Out Your Position & Time



What if Expectation Doesn't Match Reality

Simple Checks Would Have Kept Receiver From Reporting False Position

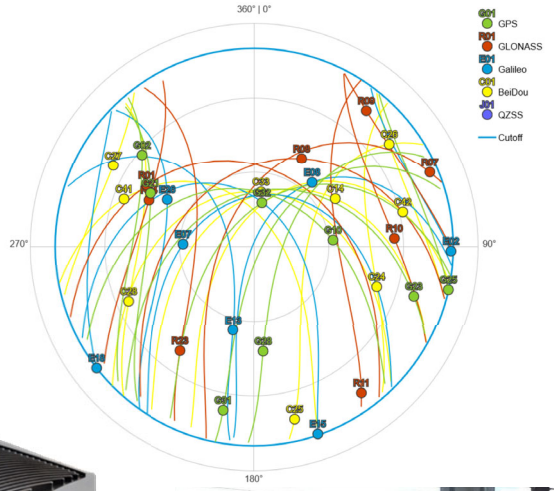


Grant et.al. "GPS Jamming and the Impact on Maritime Navigation" THE JOURNAL OF NAVIGATION (2009), 62, 173–187. The Royal Institute of Navigation

"This trial also raised awareness of the number of alarms that can sound on the bridge and how the sheer quantity can be distracting."

Situational Awareness (SA) is the Key First Step to Success!

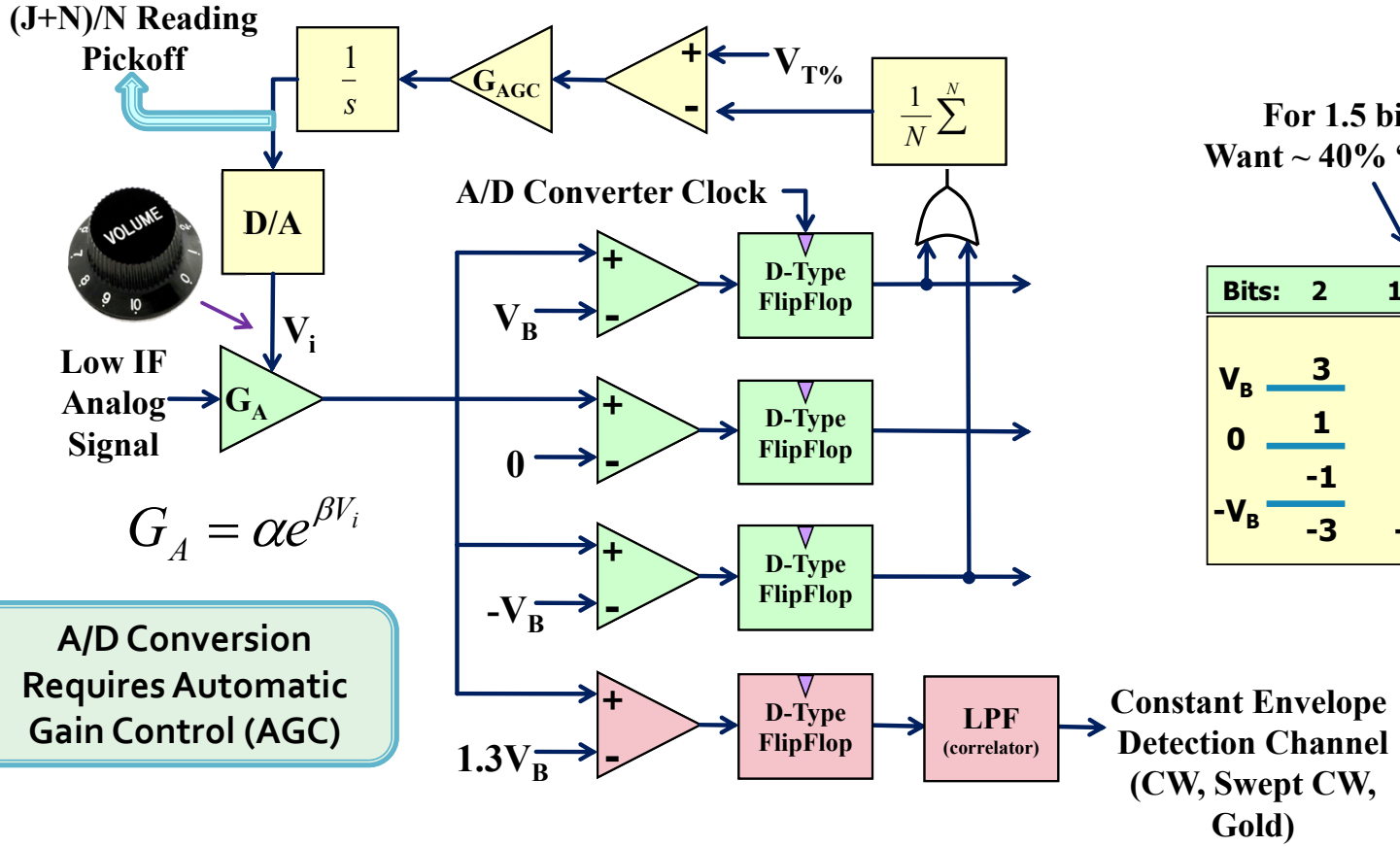
- **What are My Tools?**
  - Signals Environment
    - What Signals Are Available?
  - Available Data Sources
    - Connectivity, Utility & Reliability
- **What are My Obstacles?**
  - Multipath Environment
  - Interference Environment
  - Cyber Environment
    - Navigation Devices are Computers!
- **What am I Trying to Do?**
  - Intended Use of Position Data
  - Accuracy, Integrity, Continuity (AIC) Requirements



The Receiver is The First Line of Defense

Knowing You Are Jammed (or Spoofed) Is the First Step

Look for Excess Energy Coming In



$$G_A = \alpha e^{\beta V_i}$$

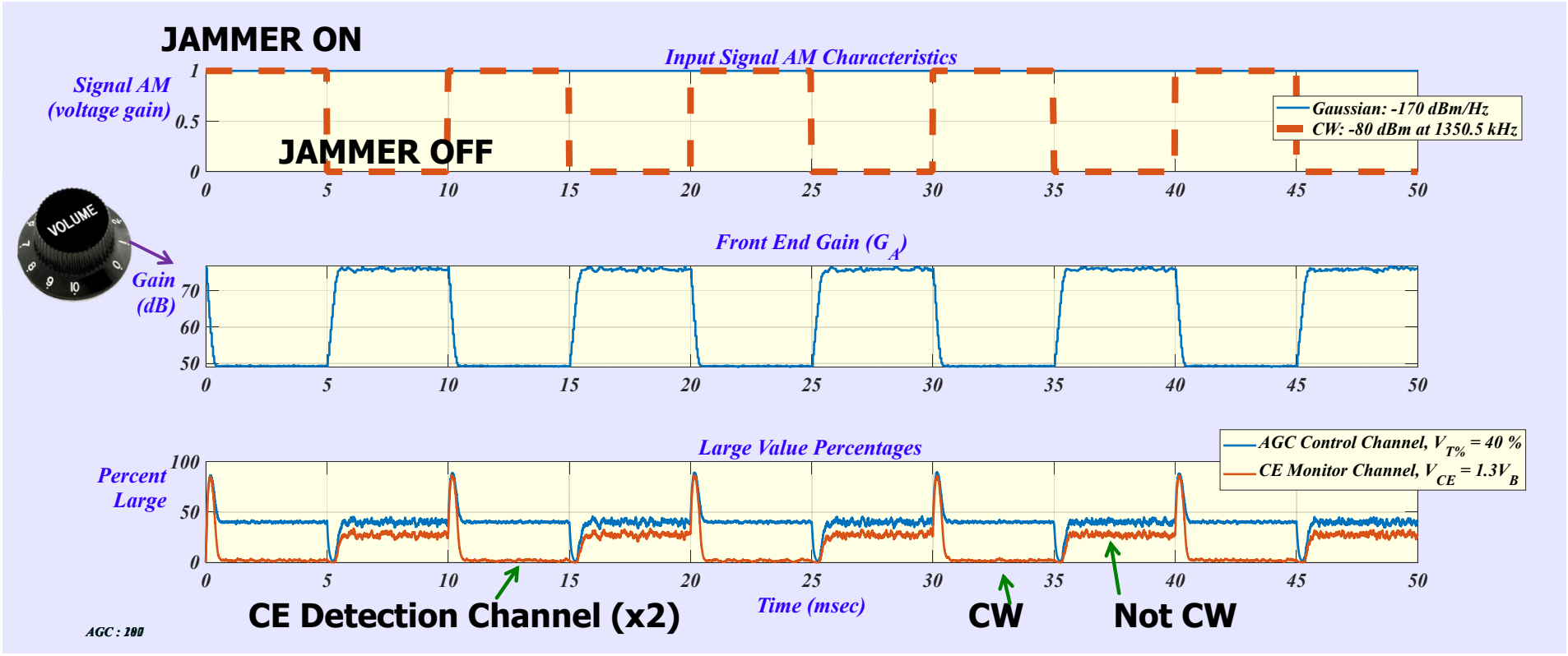
A/D Conversion Requires Automatic Gain Control (AGC)

For 1.5 bit ADC
Want ~ 40% "1" & "-1"

Bits:	2	1.5	1
V_B	3	1	1
0	1	0	1
	-1	0	-1
$-V_B$	-3	-1	-1

AGC Can Measure J/N, Pulse Rate & Jammer Type

Pulsed CW at 30 dB J/N (50 dB J/S), 100 Hz PRF



Combining Total Input Power with Signal to Noise Ratio Enhances Situational Awareness

Report

Signal to Noise Ratio Measured By C/No Meter

High

Nominal

Low

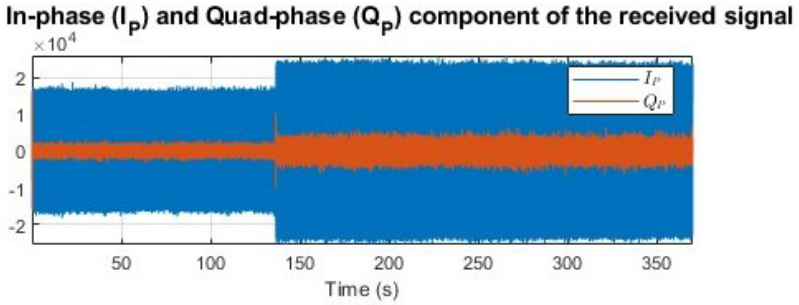
It Is Probably OK	It Is Probably a Spoofer or Structured Jammer DON'T USE
You Probably Walked Inside or Under a Tree	It Is Probably a Jammer BE CAREFUL

Nominal High

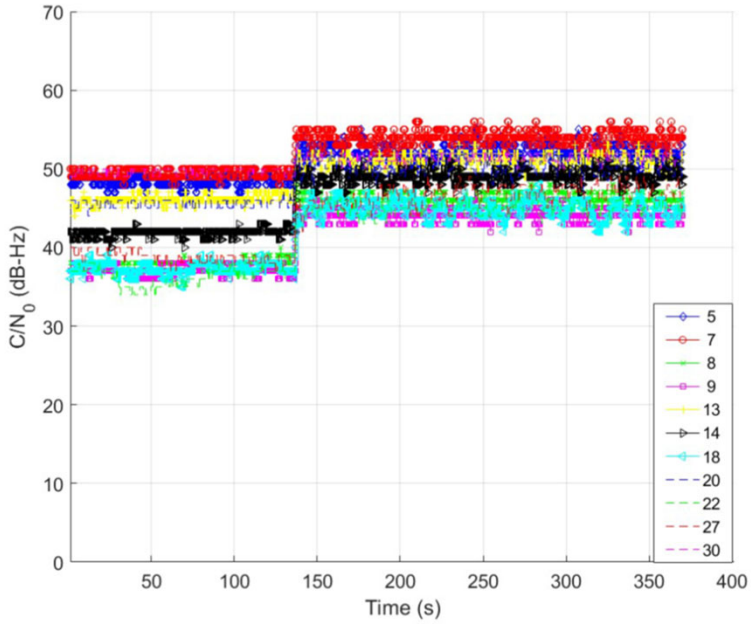
Total Input Power Measured By J/N Meter (AGC)

An Example Synchronous Spoofing Attack

Power Goes UP



SNR (C/No) Goes UP



Figures from: "An Open GNSS Spoofing Data Repository: Characterization and Impact Analysis with FGI-GSRx Open-Source Software-Defined Receiver" Saiful Islam et.al, 2024 https://doi.org/10.21203/rs.3.rs-4021306/v1

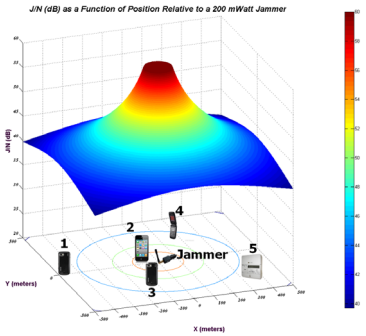
Intelligent Receivers Continuously Assess The Environment

Like Trained Witnesses (or Smoke Alarms)

- Using Simple Algorithms, Receivers Can Measure Numerous Jammer Parameters
  - Time and Observer Location
  - Apparent C/No(s) (Signal to Noise Ratio)
  - Received Jammer Power (J/N) is Measurable By AGC
  - Jammer Type
    - Gaussian
    - CW
    - Swept FM
    - Gold
  - Pulse Characteristics
    - PRF, Sweep Rate and Duty Factor

This Is the Jammer's Signature

Aggregate Measurements Can Determine Location of Jammers and Perform Pattern of Life Analysis



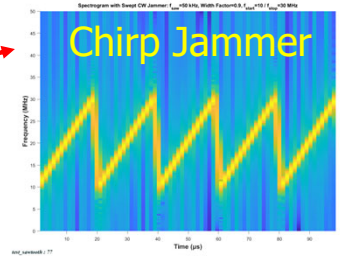
- Most Measurements Can Be Accomplished in Less than 1 msec
  - Not a big power impact

from Logan Scott: J911: *The Case for Fast Jammer Detection and Location Using Crowdsourcing Approaches*, ION-GNSS-2011, September 20-23, 2011

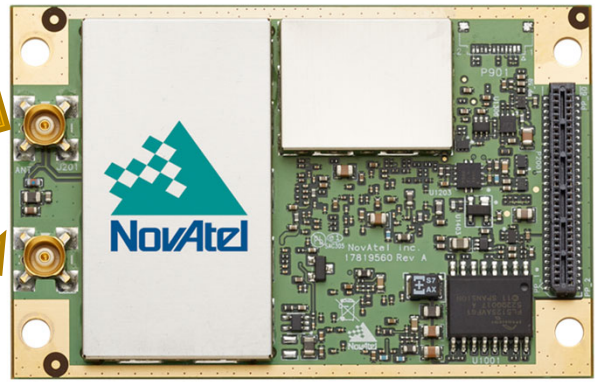
Many Receiver Capability Enhancements Can Also Provide Basis for Detecting & Analyzing Interference

- Two Antennas for Bearing Estimation
  - Could also Detect Spoofing
  - Basic CRPA for Anti Jamming
- MultiGNSS and MultiFrequency Options
  - Adds Complexity to Jammers and Spoofers if they Have to Cover All Signals
- RF Memory
  - Jamming Analysis / ML Classifiers
  - Delayed Key Ranging

    Authentication (Chimera, ACAS)
- IMU/Clock
  - IMU Motion Should Correlate with Receiver Motion
  - Time from Signals Should Match Golden Time



NovAtel OEM7720



LGA-14L
Typ: 2.5 x 3.0 x 0.83 mm³

from: Logan Scott,
23 June 2021 InsideGNSS Webinar

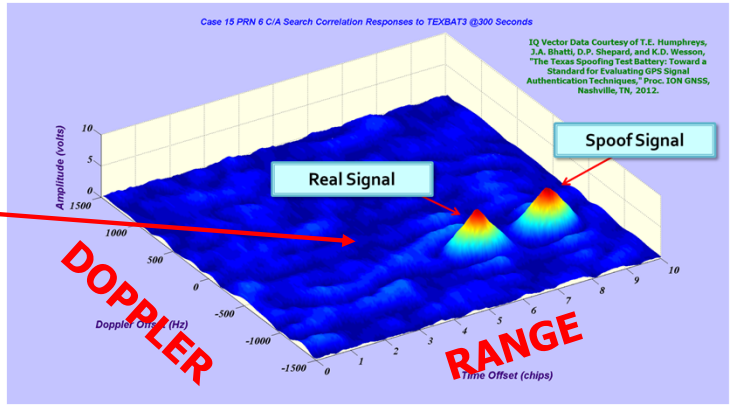
Signals Based Antispoofing Measures

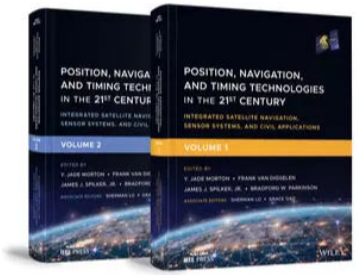
Easy Moderate Hard

- Signal Checks Look For Suspicious Characteristics

Can Detect Most RF Spoofers

  - Use J/N meter to check for above normal energy levels
  - Monitor C/No meter for Consistency / Unexpected C/No
  - Periodic Range/Doppler Map Examination to Look for Weak, Real Signals
  - Tracking Loop Capture Detection / Phase Glitches / Amplitude Fluctuation
  - Correlated Channel Response Between Signals (Common Fading)
  - Vector Tracking to Harden Against Walkoff
  - Agreement between L1/L2/L5 , Galileo, Glonass etc. Signals
  - Monitor Phase Difference Between Antenna Elements
  - Provision for Cryptographic Location Authentication
    - (Galileo OSNMA & ACAS, GPS CHIMERA)





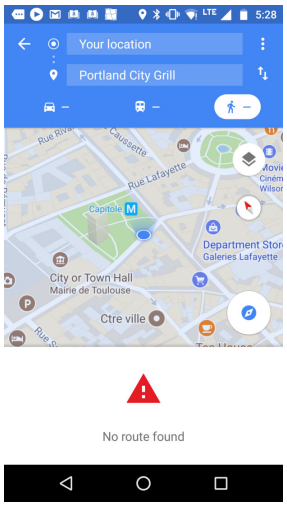
More Info in Chapter 24

Navigation Based Antispoofing Measures

Easy Moderate Hard

- Continuity Checks / Unexplained State Changes
  - Continuity Checks in Time and Position
  - Anomalous Time Bias & Time Bias Rate States
- Movement Checks for Stationary Receivers
- RAIM/FDE Type Functions
- Consistency with other Navigation Sensors

How Did I Teleport to Toulouse?



Major Cautions on AntiSpoof Measures

1. Makes Testing Receivers Harder
2. May Be Exploited In Denial-of-Service Attacks

Civil Defenses Emphasize Situational Awareness, Uncorrelated Vulnerabilities, and Agility to Operate in Impaired Environments

The Whack a Mole Defense

Common Smart Phone Capabilities

- Sanity Checks and Signal Authentication to **Identify & Discard Suspect Signals**
- Global SatNav Systems
  - GPS L1/L2/L5 (30 SV)
  - GLONASS (24 SV)
  - BEIDOU (Compass) (46 SV)
  - GALILEO (25 SV)
- Regional SatNav Systems
  - QZSS (4 SV)
  - SBAS
  - IRNSS

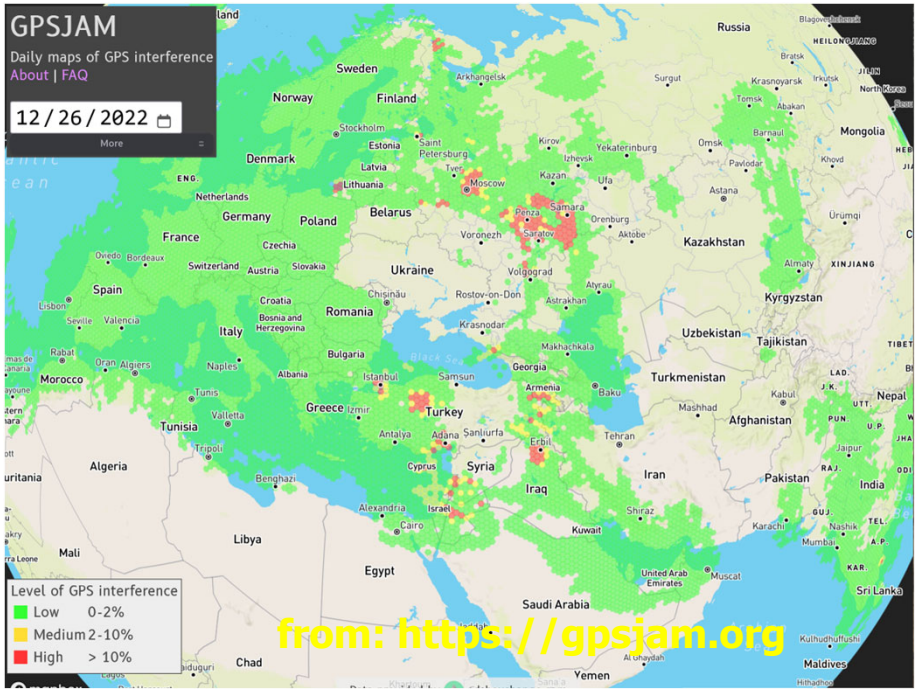
Uncorrelated Vulnerabilities?

- Some Other Navigation Sensors
  - WiFi
  - Cellular TOA/TDOA
  - Bluetooth
  - IMU
  - Magnetic Field Sensor
  - Point Space Database
  - Atomic Clock or Equivalent
  - Locatalites
  - Barometric Altimeter
  - eLORAN
  - Authenticatable Certified Systems
- Size, Weight, Power, Cost & Export (ITAR) Considerations are Paramount

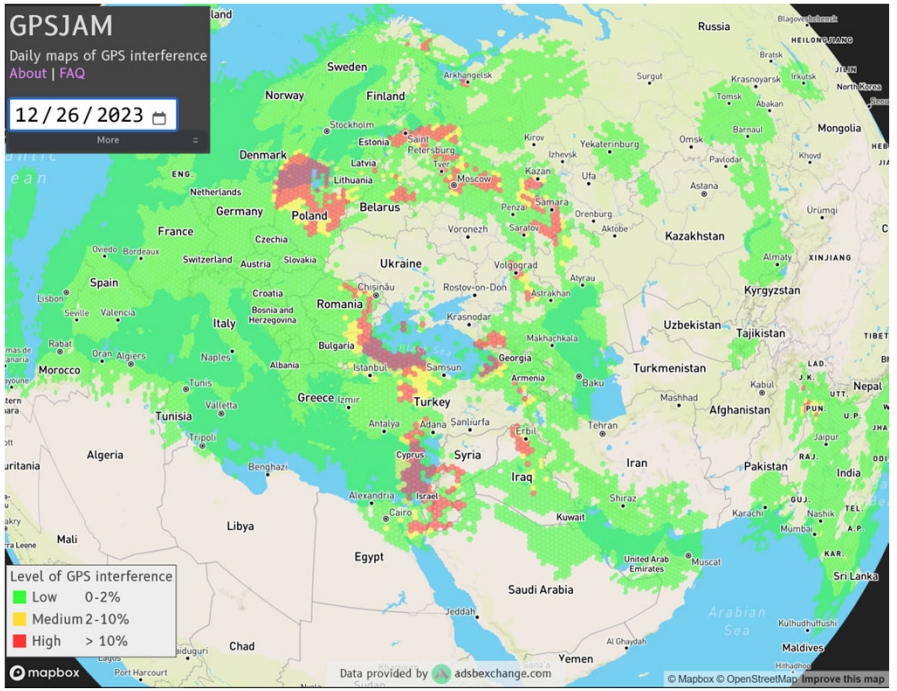
Look for Consistency Between Observables!

Military Jamming and Spoofing Is Increasingly Affecting Civil Operations

26 December 2022

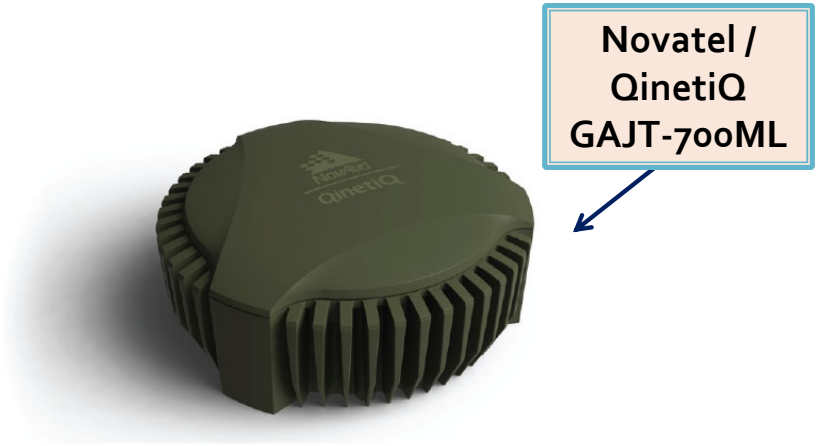


26 December 2023



Military Defenses Emphasize Signal Protection
The Bunker Defense

- Electronic Counter Counter Measures (ECCM)
  - Strong Out of Band Signal Rejection
  - Avoid Relying on "As Is" Civil Signals
  - **Maintain Situational Awareness**
  - Tightly Coupled IMU Aiding
  - **Adaptive Arrays**
    - **These are the Big Guns of Antijam**
    - **1,000x to 10,000,000x Improvements in Jamming Resistance (30 to 70 dB)**



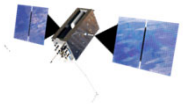
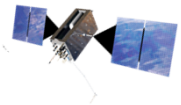
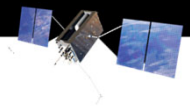
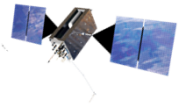
- **Most ECCM Techniques Degrade Accuracy**

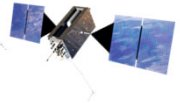
A Deeper Dive into Their Applicability in Civil Applications

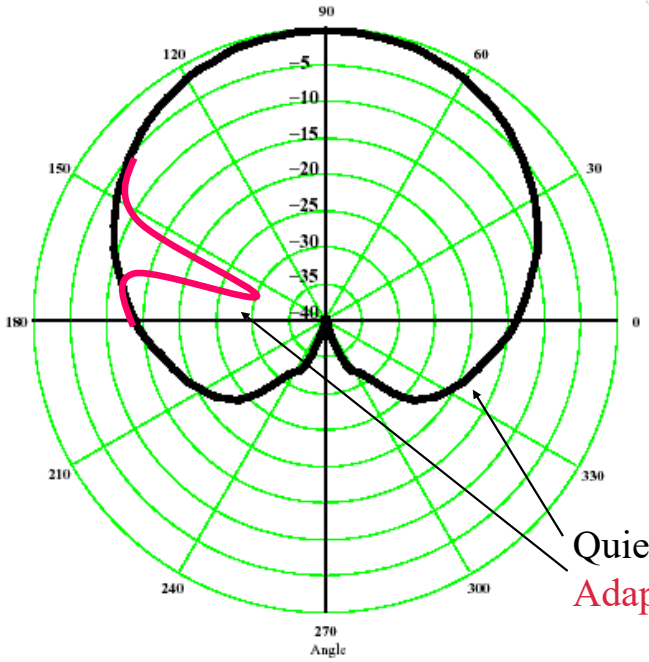
Adaptive Arrays

More on this on 3 June 2024 at JNC2024

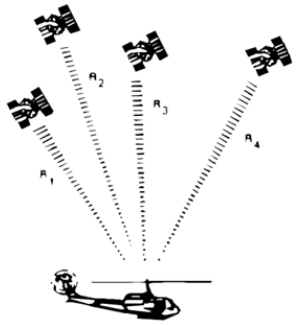
Adaptive Arrays are Multiple Element Antennas That Actively Steer Nulls In the Direction of Jammers (and Sometimes Signals)



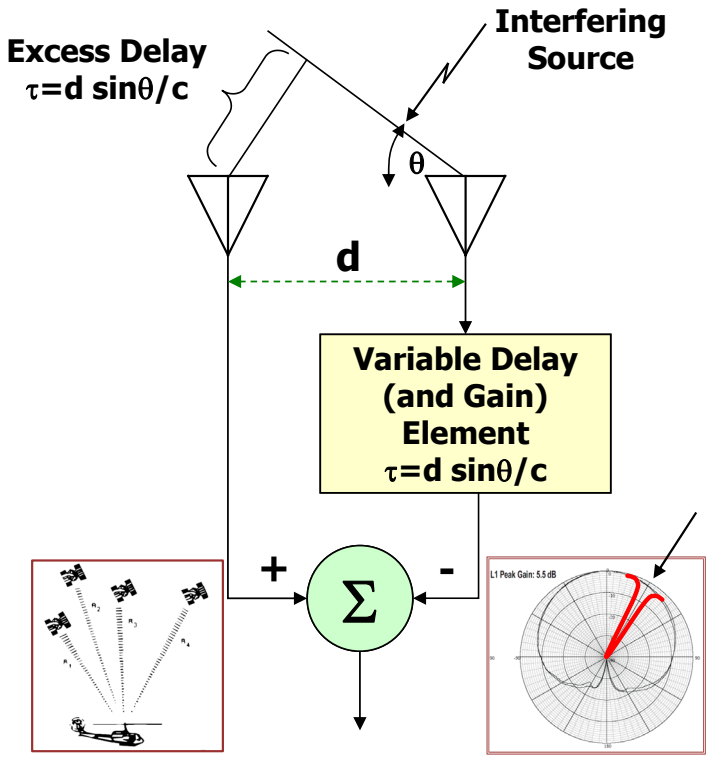


Track Four Satellites and You Can Figure Out Your Position & Time



Question: where do you put the null?

Adaptive Nullers & Beamformers Try to Create Nulls In the Direction of Interferers

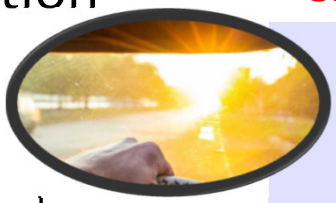


- N-1 Independently Steerable Spatial Nulls with N element array

- Wide Variety of Control Algorithms
- 2-element Horizon Nullers Can Be Very Effective in Stationary Timing Applications
- ITAR Controlled in US

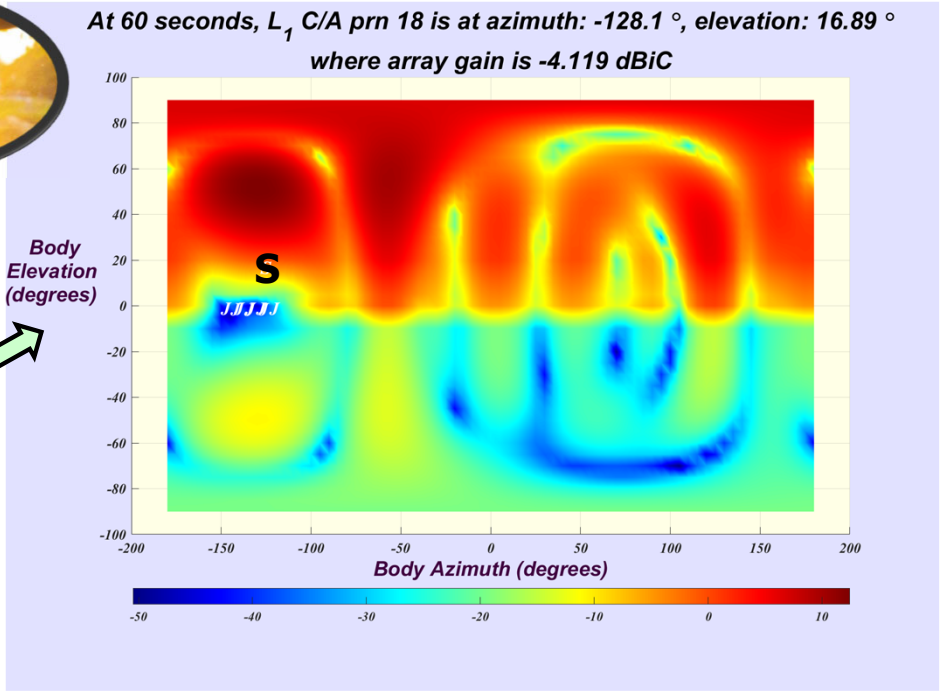
Large Measurement Errors Can Occur When The Antenna Squints
It's Sort of Like Driving Into The Sun

- An Adaptive Array Is a Direction Dependent Filter
  - Objective is to Maximize SNR
    - Maximize Gain In Direction of Signal
    - Minimize Gain In Direction of Jammer(s)



- Elements and Channels Are Not Exactly Matched
  - Errors with C/A Code Can Be Large
  - L5 Errors Usually Under 1-meter

8.6 Meter Pseudorange Bias with C/A Code



CRPA ITAR Rules are Not Just About the Number of Elements

Code of Federal Regulations, Title 22, Part 121-The United States Munitions List
https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-121

- (10) Antenna, and specially designed parts and components therefor, that:

3-element ITAR

☑
- (i) Employ **four or more elements**, electronically steer angular beams, independently steer angular nulls, create angular nulls with a **null depth greater than 20 dB**, and achieve a beam switching speed **faster than 50 milliseconds**;

☒
- (ii) Form adaptive null attenuation greater than **35 dB with convergence time less than one second**;

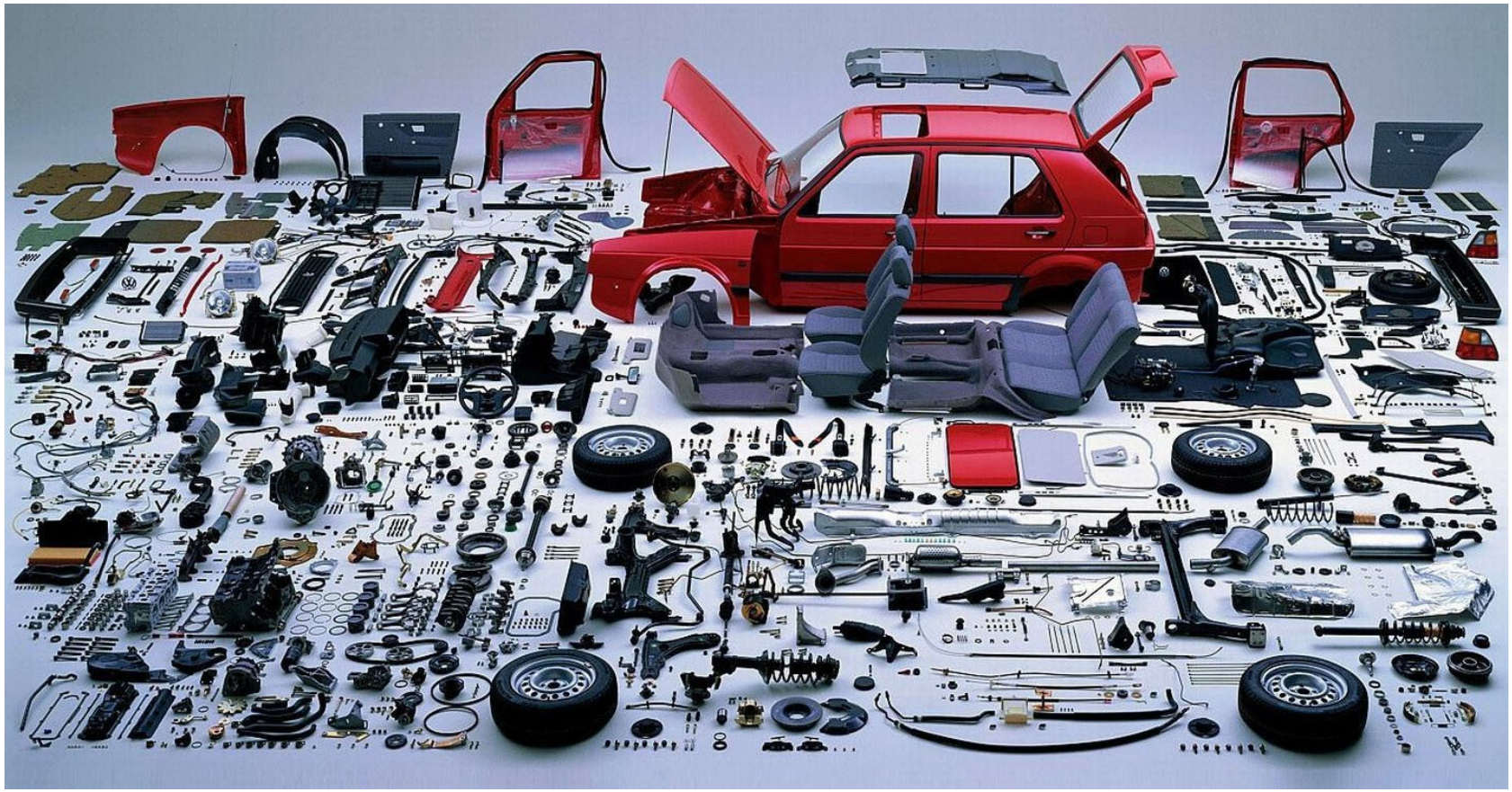
- (iii) Detect signals across multiple RF bands with matched left hand and right hand spiral antenna elements for determination of signal polarization; or

- (iv) Determine signal angle of arrival less than two degrees (e.g., interferometer antenna);

Matching the CRPA to the Application Is Essential!
Adaptive Arrays are Not a Panacea PlugnPlay Solution

- Adaptive Arrays are Direction Dependent Filters and **Can Cause Operational Failures** Even Though Signals Are Tracked
  - **May Not Meet Required Accuracy in Precision Applications**
  - **RTK and PPP are Particularly Susceptible, May Not Converge with Some CRPAs**
  - **Curation Can Remove High Bias Signals** From Navigation Set
    - Using More SV's Helps (Galileo etc.)
- **L5 Errors ~10x Smaller than L1 C/A**
  - Wider Bandwidth Signals Yield Lower Inherent Distortion / Bias
- ITAR Regulations Limit Even 3-element Adaptive Antennas

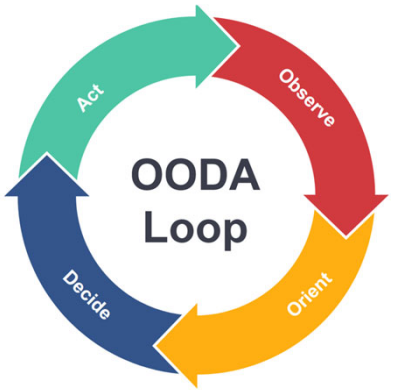
Some Assembly Required



Until You Test It You Don't Know If You Got it Right

And Even Then, You Will Still Have Vulnerabilities

- Initial Results are Often Dismal BUT Informative
  - 100% Failure Rate In Portland Spoofing Incident



- The Testing Conundrum for Jamming & Spoofing
  - Knowing What Electronic Attacks (EA) Look Like Is Very Helpful In Designing SA / Countermeasures
    - EA Techniques are Not Something You Want to Propagate
  - Testing is Fundamentally an Electronic Attack (EA)
    - Testing Will Improve Receiver Competence
    - Testing Will also Reveal Ways to Improve EA

The User Community Needs Clear Signals

- **Hire a Firm to Do Bespoke Assembly**
  - Very Expensive But Viable in Offshore Drilling, Cable Laying, Port Facilities, Mines etc.
  - Problem Diagnosis & Service Contracts are also Included in Many Cases
- **Receiver/System Standards ala. FAA**
  - Rigid, Slow to Adapt to Emerging Threats

Structured Interference Will Evolve FAST!

- **Government Signaling**
  - Test Thoroughly and then Make Purchase Decision
  - Implicit Endorsement
- **Self Certification**
  - Perhaps Using Standard Set of Scenarios
- **Exposure Based Certifications By 3rd Party Labs**
  - Can Slow Development Cycles

Mostly a Question of Whom

Toughening At the Platform/Use Case Level

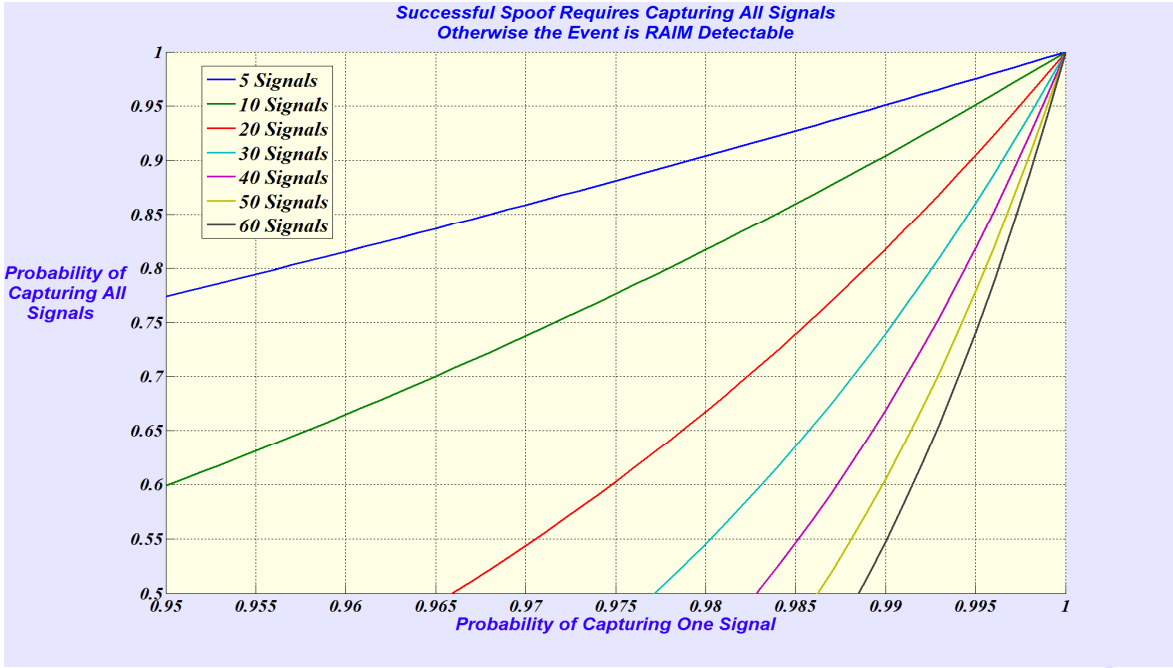
Toughening at the Platform/Use Case Level

- Toughening by Augmentation
  - Use of complementary systems/sensors to enhance detection and mitigation of jamming and spoofing
    - Independent source of time (e.g. chip scale atomic clock)
    - Independent source of motion sensing (e.g. Inertial system)
    - Independent source of position (e.g. eLORAN, DME/DME, other signals of opportunity)
    - Independent source of satellite orbit and clock information (e.g. SBAS, GDGPS, etc.)
    - Independent source of ***trusted*** satellite data (e.g. Authenticated SBAS, OSNMA, HARS)
- Role of augmentation in Toughening
  - Appropriate combinations of augmentation elements is use-case dependent
    - Example: Timing receiver with fixed antenna has inherent independent source of position/motion
  - Some augmentations require calibration when GPS is available and performance will degrade with time after GPS is lost.
    - Inertial Systems
    - Independent clock (e.g. atomic clock).
    - Must protect against calibration corruption prior to protection.
  - Complementary PNT (CPNT) systems
    - Requirements for backup capabilities may be different than normal operations
  - “All source PNT” multi-sensor navigation systems – optimal combination of all sensor/system data for accuracy and integrity – cross check for detection

Multi-Constellation Multi-Frequency GNSS for Resilience

- Use of MCMF GNSS can significantly improve resilience
  - Multiple frequencies less likely to experience unintentional interference simultaneously
  - If user is using multiple systems and frequencies, then a spoofer needs to successfully spoof multiple systems and frequencies to be effective.

- Prohibiting use of foreign satellite systems without a license is counter productive
  - Denies US users a useful tool in combating spoofing and improving resilience
  - Puts US industry at a disadvantage globally.
    - There is global demand for chips and receivers that can support all GNSS systems
    - Prohibition will limit the ability to develop and test some capabilities in the US



COURTESY LOGAN SCOTT / LS CONSULTING

Even One Inconsistent Signal Should Raise Suspicions

What are the Gaps that the USG can Address?

- Recommendations….
  - Accelerate implementation of out of band resilience augmentation (i.e. HARS)
    - Develop a roadmap for system implementation
    - Provide accuracy and resilience services for all GNSS core constellations
  - Address GAPs in service definitions that make assessment of requirements at the use-case level difficult
    - Previous Recommendation on probabilities of outages
    - Identify GAPs in current standards development work
      - E.g. IEEE P1952: Standard for Resilient Positioning, Navigation and Timing (PNT) User Equipment -
      - RTCA/EUROCAE standards for aviation UE
  - Remove/mitigate prohibitions on use of foreign navigation satellite systems
    - Either blanket license core constellations **or** change the law so that a license is not required
    - Provide strong guidance on zero-trust use of foreign signals and Signals of Opportunity (SOOP)
  - Relaxation of export restrictions
    - **Remove export barriers for Controlled Reception Pattern Antennas (CRPAs) (previous recommendation)**
    - Example: CPNT based on SOOP could potentially benefit from bearing measurements with interferometric antennas of better than 2 degrees - currently controlled by ITAR.

Recommendations for Industry

- Recommendations
  - Development of a standard taxonomy for jamming and spoofing attacks
    - Something is already under development by RTCA and ICAO for aviation.
    - Can this be extended to other critical infrastructure applications?
  - Develop standard testing for GPS/GNSS receivers and systems incorporating GPS/GNSS receivers
    - Show resilience to threats in the standard taxonomy
    - Manufacturers to indicate levels of resilience that equipment has been tested to
    - System integrators to verify resilience of systems and services that use GPS/GNSS
  - Users should update to MCMF receivers wherever practical
    - Implement cross checking, ARAIM, augmentation as needed to verify all GNSS signals
  - Users to adopt augmentations for resilience whenever possible/practical

Conclusions

- Toughening GNSS
  - Many options for toughening applications at different layers
  - CRPAs are a powerful tool – deployment should be supported/enabled
  - MFMC GNSS is a powerful tool which should be supported/enabled
  - CPNT is an important tool
- USG should eliminate barriers to use
  - Facilitate timely adoption by users
- Additional Guidance and Standards needed for
  - Jamming/Spoofing scenarios
  - Testing standards for demonstration of resilience against standard scenarios

Today's PTA Agenda

- 10:30 to 11:30 PTA Overview
- 11:30 to 12:30 Lunch
- 12:30 to 1:45 Protect, with Board Discussion
- 1:45 to 2:00 Break
- 2:00 to 3:15 Toughen, with Board Discussion
- 3:15 to 3:30 Break
- 3:30 to 4:45 Augment, with Board Discussion
- 4:45 to 5:00 PTA Summary
- 5:00 to 6:00 Board Deliberations
- 6:00 Adjourn