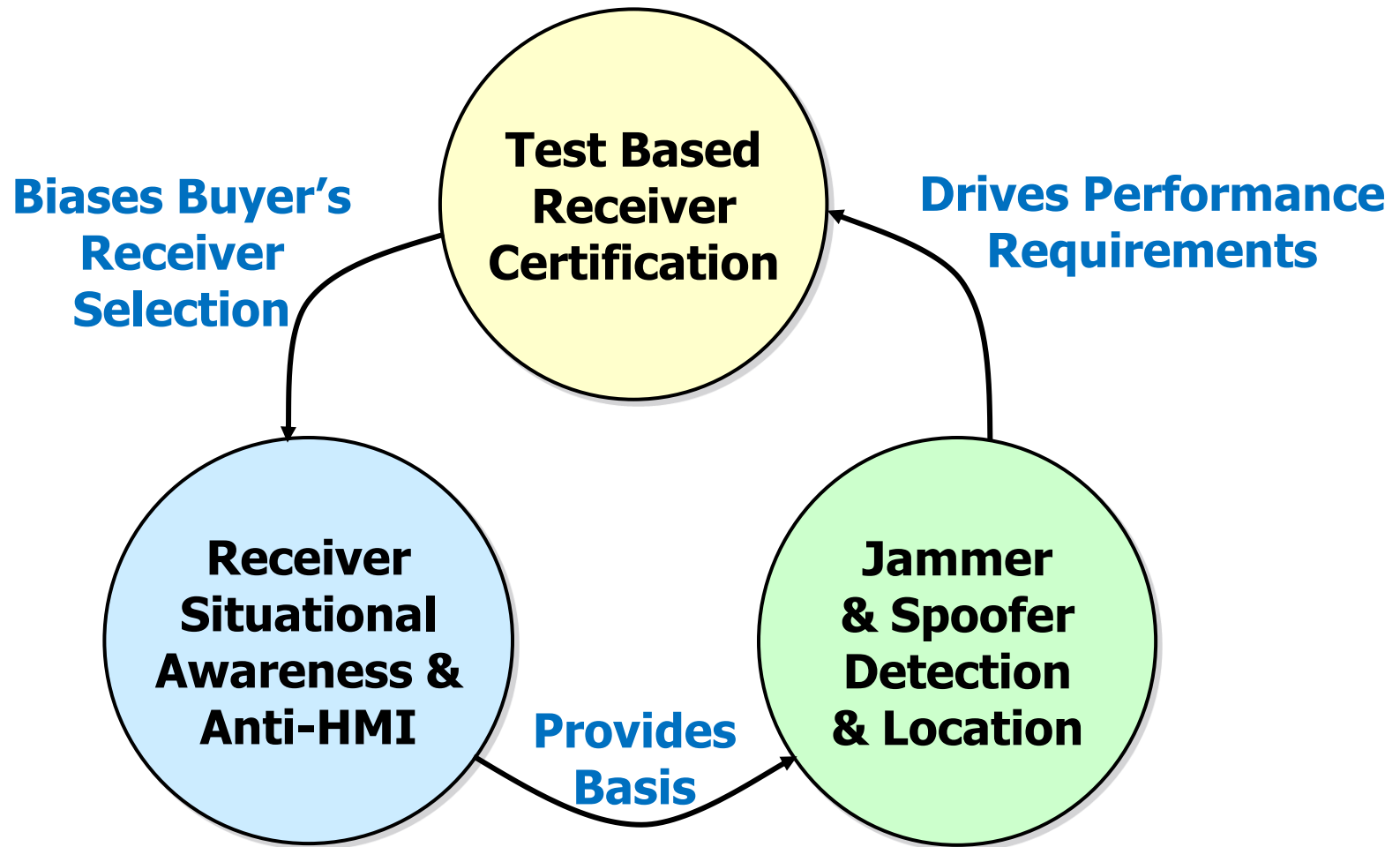


Logan Scott, LS Consulting

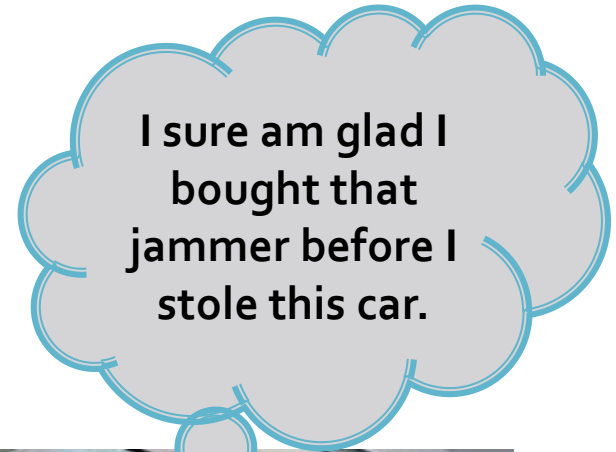
loganscott53@gmail.com

# Receiver Certification: Making the GNSS Environment Hostile to Jammers & Spoofers

# Building Situational Awareness: The Civil Protective Triad



# Low Power Jamming & Spoofing Could Is Becoming Chronic



- Newark Liberty Airport Offender Caught with A \$33 200 mW GPS Jammer
- Isoz et. al. report average of **117 events/day** at Kaohsiung International Airport - Taiwan



Isoz et al., Assessment of GPS L1/Galileo E1 Interference Monitoring System for the Airport Environment, ION GNSS 2011

# The Education Problem

- Most Civil Receiver Designers Don't Consider Jamming, Repeaters & Spoofing In Their Designs
- To Design Effective Detection Methods & Countermeasures, You Need to Understand the Threat
- Threat and Countermeasure Descriptions are Sensitive

# What If Your Receiver Is Not Educated?

Receivers Are the First Line of Defense, You Might Be Dead By the Time The Cavalry Arrives

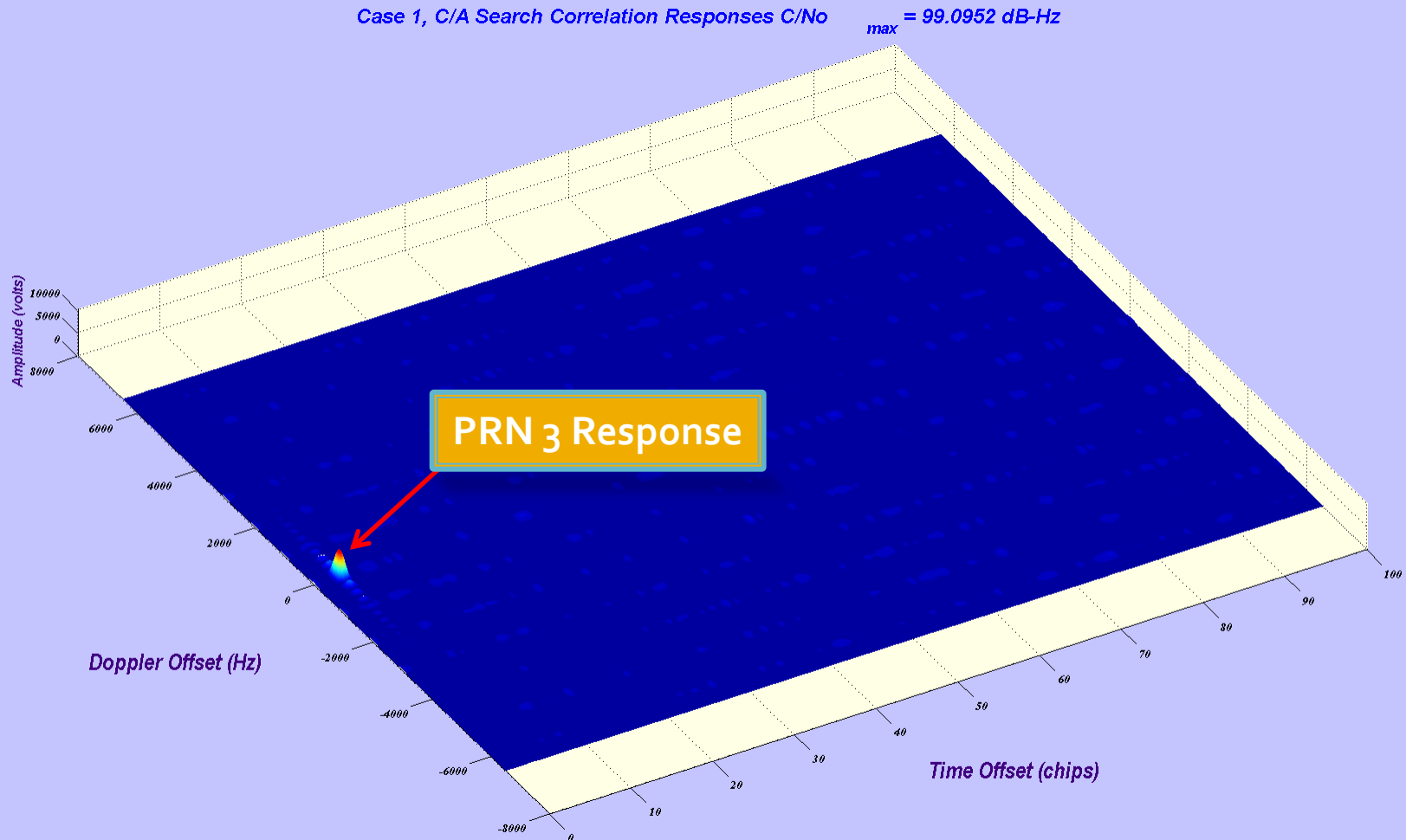
- Mesa Arizona Unintentional CW Interference (2001)
  - Day 2, 1828 MT **Gulf Stream 2** at FL120, 45nm North of PHX Lost GPS & Turned 35 Degrees Left Toward Other Traffic. ATC Vectored A/C to Ensure Safety
- *Pole Star* Maritime Jamming Experiments (2008)<sup>†</sup>
  - Shipboard GPS was “spoofed” by PRN1 jammer
    - reported speed was **greater than 100 knots**
  - **Affected, many dependent systems** that rely on GPS such as “*the AIS (Automatic Identification System) transponder, the dynamic positioning system, the ship’s gyro calibration system and the **digital selective calling system**”.*



<sup>†</sup> Grant et.al. “GPS Jamming and the Impact on Maritime Navigation”  
THE JOURNAL OF NAVIGATION (2009), 62, 173–187. The Royal Institute of Navigation

# Pole Star Receiver Expected to See Something Like This on PRN<sub>3</sub>

PRN<sub>3</sub> Reception, 3chip Offset, 0 Hz Doppler, 5 msec PIT

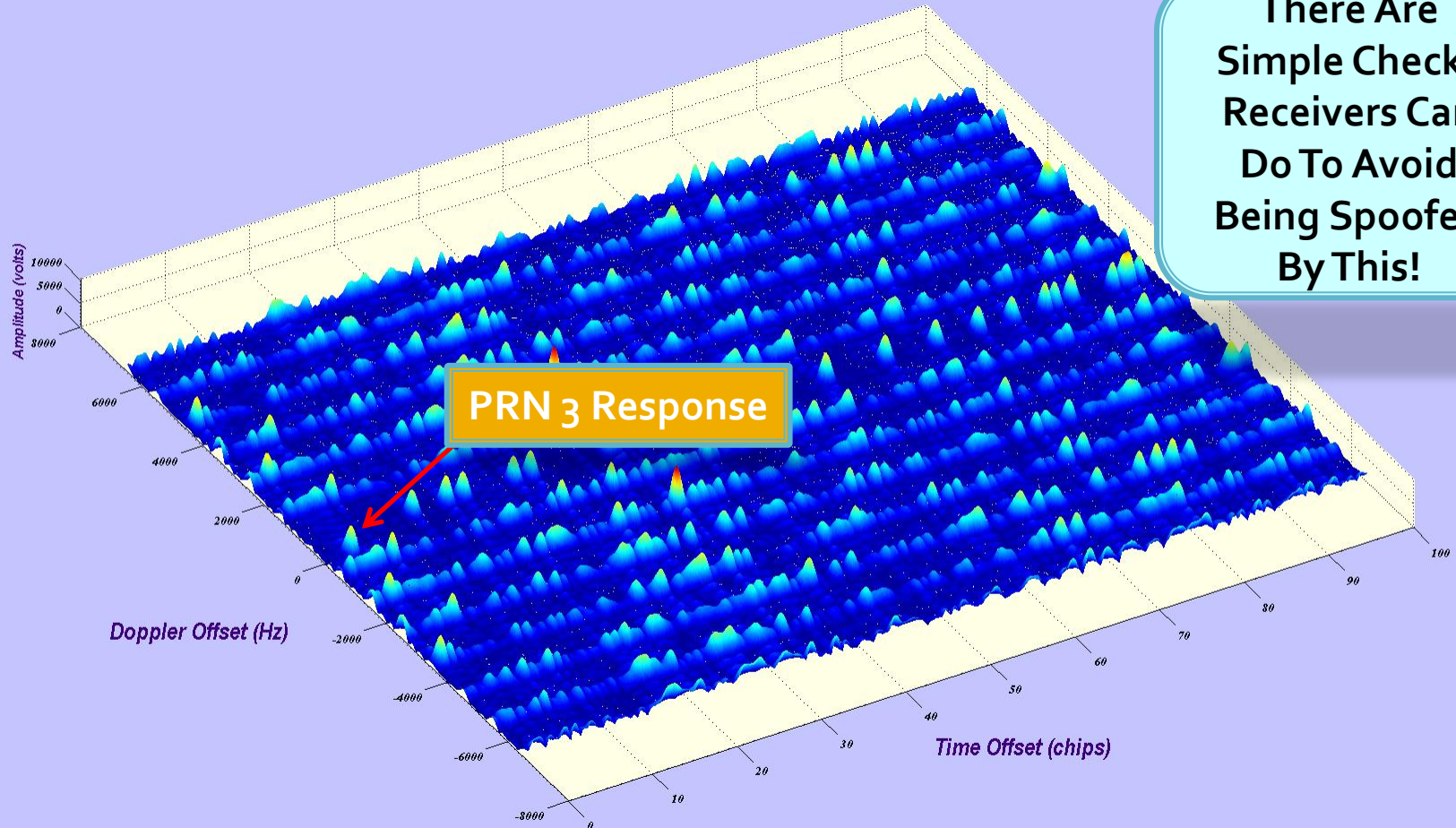


acq/stage1i.m

# Instead, Pole Star Receiver Saw Something Like This on PRN<sub>3</sub> & Got Confused (Jamming as Spoofing)

PRN<sub>1</sub> Jammer at J/S = 24 dB, 500 Hz Offset, 5 msec PIT

Case 1, C/A Search Correlation Responses C/No<sub>max</sub> = 103.0165 dB-Hz



There Are Simple Checks Receivers Can Do To Avoid Being Spoofed By This!

acq/stage1i.m

# Intelligent Receivers Continuously Assess The Environment

## Like Trained Witnesses

- Using Simple Algorithms, Receivers Can Measure Numerous Jammer Parameters
  - Apparent C/No
  - Received Jammer Power (J/N)
  - Jammer Type
    - Gaussian
    - CW
    - Swept FM
    - Gold
  - Pulse Characteristics
    - PRF, Sweep Rate and Duty Factor
- Most Measurements Can Be Accomplished in Less than 1 msec



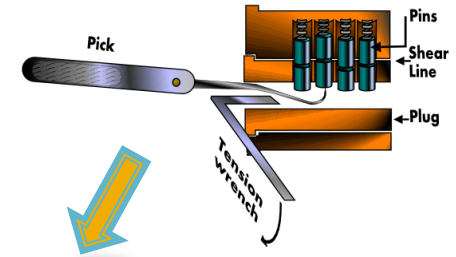
# Intelligent Receivers Harden Infrastructure

- **Reports Interference to User**
  - Less Time Debugging Dependent Systems
- **Protects Against Generating Hazardously Misleading Information (HMI)**
  - Spoof Resistant
- **Signature Information Improves Interference Monitoring**
  - Can Sort Jammer Reports Into Track Files
  - Can Associate Reports from Different Sites
  - Can Do Time of Day vs. Location Analysis

# Signals Based Antispoofing / Anti HMI Measures

## Easy Moderate Hard

- Use Y/M-code
  - Must Obtain & Key Receiver



- Signal Checks

Can Detect Many Spoofers

- Use J/N meter (AGC) to check for above normal energy levels
- Monitor C/No meter for Consistency / Unexpected C/No
- Deep Acquisition to Look for Weak, Real Signals
- Tracking Loop Capture Detection
- Time of Day C/No Expectations (Stationary Receiver)
- Vector Tracking to Harden Against Walkoff
- Agreement between L1/L2/L5 Signals
- Monitor Phase Difference Between Antenna Elements
- Add GPS Civil Signal Cryptographic Authentication Features
  - Use Galileo Commercial Services Signals

# Navigation Based Antispoofing / Anti HMI Measures

Easy Moderate Hard

- Compare “Internal Watch Time” with “External Signals Time”
- Continuity Checks in Time and Position
- Movement Checks for Stationary Receivers
- RAIM/FDE Type Functions
- Anomalous Time Bias & Time Bias Rate States
- Large Residuals, Particularly in Differential Correction Channel(s)
- Consistency with other Navigation Sensors

# How Do I Know My Receiver Does These Checks?


Receiver Certification: A Simple Receiver Selection Criteria for the Non Expert User Community

**Certified**

**NOT STUPID**

# User Community Needs Voluntary Test Based Receiver Certification to Aid Selection Process

- Start With Basic Situational Awareness Standard
  - RTCM Standard?
  - DHS Sponsor?
- Level 1 Certification Tests For:
  - J/N Measurement
  - High C/No Measurement
  - Jammer Type Identification/Signature Analysis
  - Basic Spoofing Detection
  - PVT Discontinuity Detection
- Up to Manufacturer On How to Pass the Tests
- Level 1 Draft Posted At:  
<http://logan.scott.home.comcast.net/~logan.scott/>



**Must Report  
Disturbances  
with Maximal  
Effort**  
•Display/Alarm

# Standard Is Not Hard to Meet; With a Few Software Tweaks u-blox 6 Might Meet Level 1

I don't work for u-blox



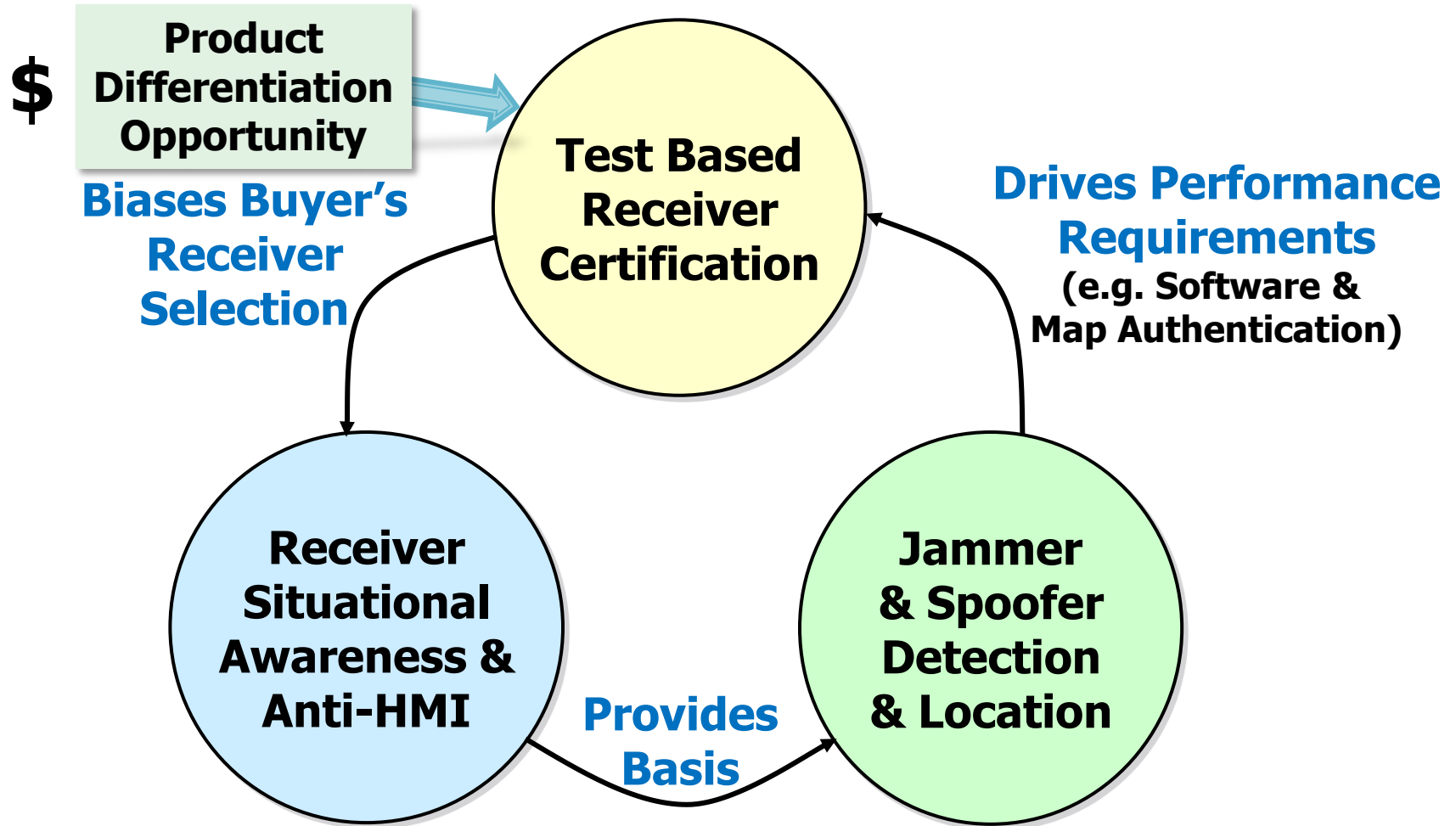
## Jamming/Interference monitor reported states

<i>Value</i>	<i>Reported state</i>	<i>Description</i>
0	Unknown	jammer monitor not enabled, uninitialized or antenna disconnected
1	OK	no interference detected
2	Warning	position ok but interference is visible (above the thresholds)
3	Critical	no reliable position fix with interference visible (above the thresholds); interference is probable reason why there is no fix

- Reports J/N Level
- Reports Jamming Type (CW detection)
- Needs Spoof Detection Algorithms

**Table from:** u-blox 6 Receiver Description Including Protocol Specification, GPS.G6-SW-10018, 9 December 2010

# What's In It for The Civil Manufacturer?



**Backup**

---



# Some of My Papers on the Topic

## ■ Cryptographic Signal Authentication

1. *Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems* ION GNSS 2003
2. *L1C Should Incorporate Cryptographic Authentication Features* May 2006 Comments on ICD-GPS-800
3. *Expert Advice - Location Assurance* GPS World 2007
4. *Civilian GPS Signal in Space Enhancements for AntiSpoofing and Location Authentication*, presented at JNC 2011, 28 June, 2011

## ■ J911

1. *J911: The Case for Fast Jammer Detection and Location Using Crowdsourcing Approaches*, paper presented at ION-GNSS-2011, September 20-23, 2011
2. *J911: Fast Jammer Detection and Location Using Cell-Phone Crowd-Sourcing* in November 2010 issue of GPS World

## ■ Receiver Certification

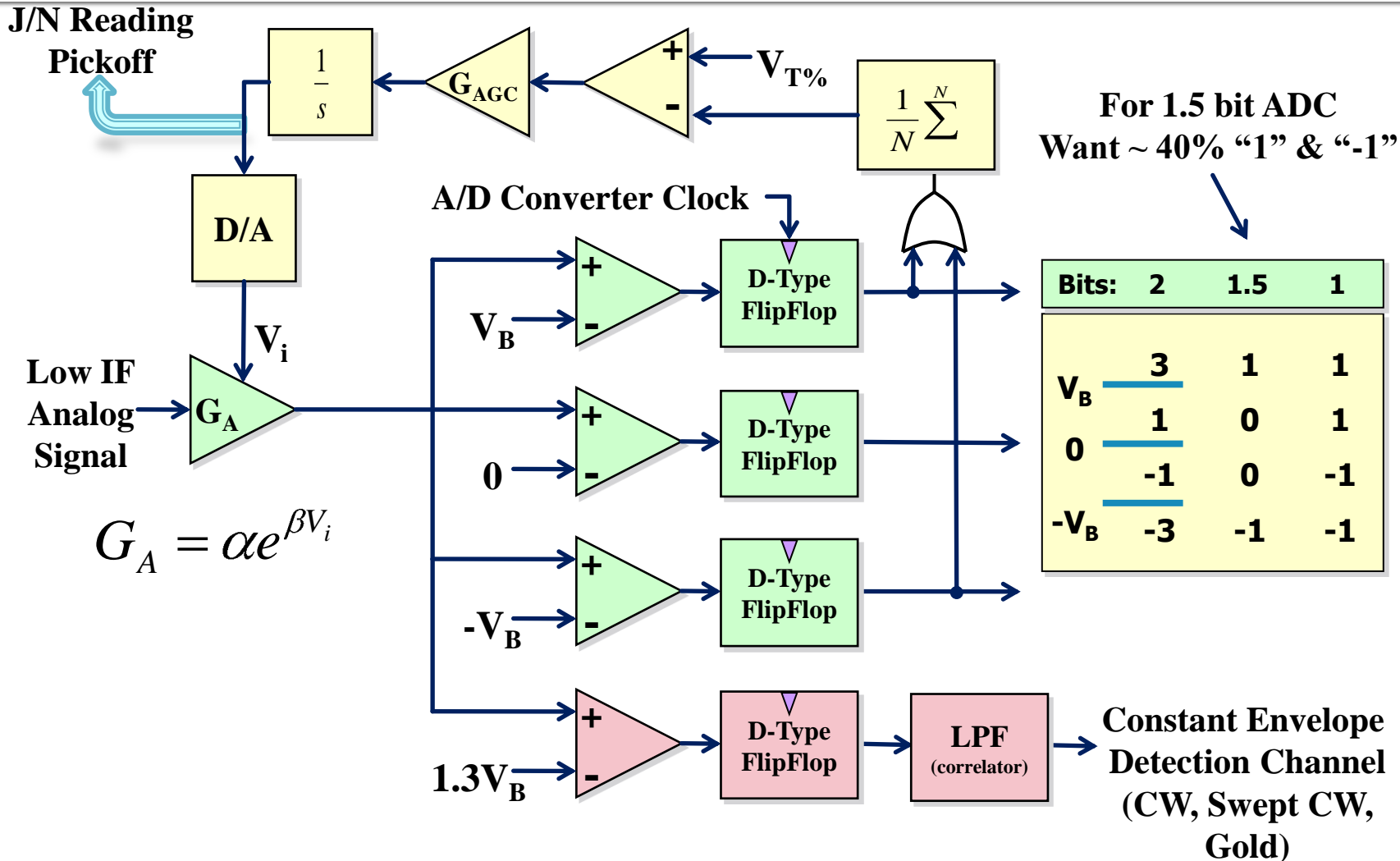
1. Level 1 Draft Specification attached to pdf version of this presentation and posted at: <http://logan.scott.home.comcast.net/~logan.scott/>

# Need to Detect Gold Code Jamming to Avoid Jamming as Spoofer Effect

- Simple Tests to Detect Gold Code Jamming
  1. Code and Carrier Doppler's Match?
  2. 50 bps data present and valid?
  3. What does Range/Doppler map look like?
  4. Large residuals in navigation solution?
  5. Large time bias, time bias rate variance?
  6. Can you acquire satellites that are on the other side of the earth?
  7. And many more...

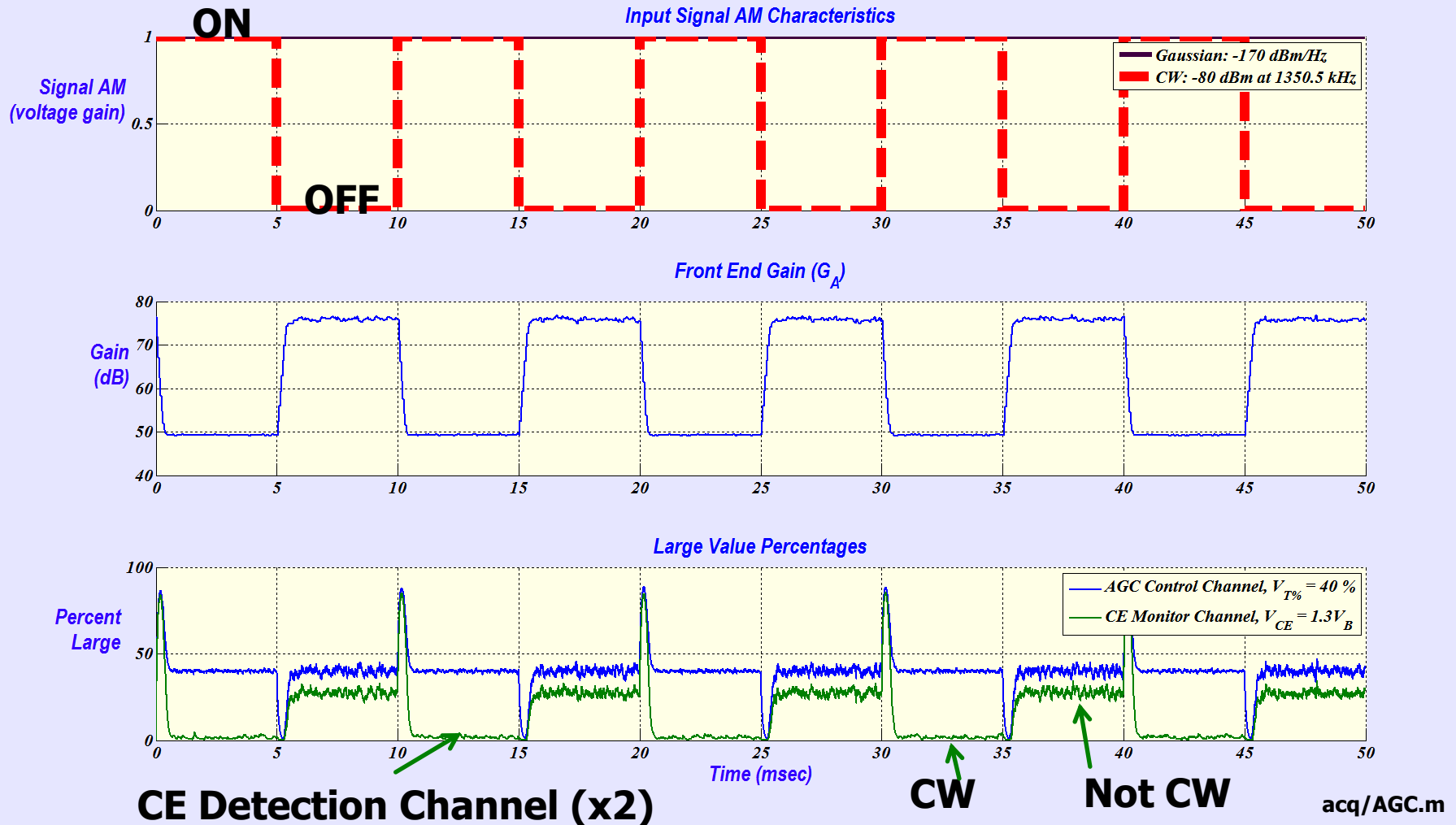
# Adaptive A/D Converter with J/N Meter Output

## Knowing You Are Jammed Is the First Step



# A/D Process Can Measure J/N, Pulse Rate & Jammer Type

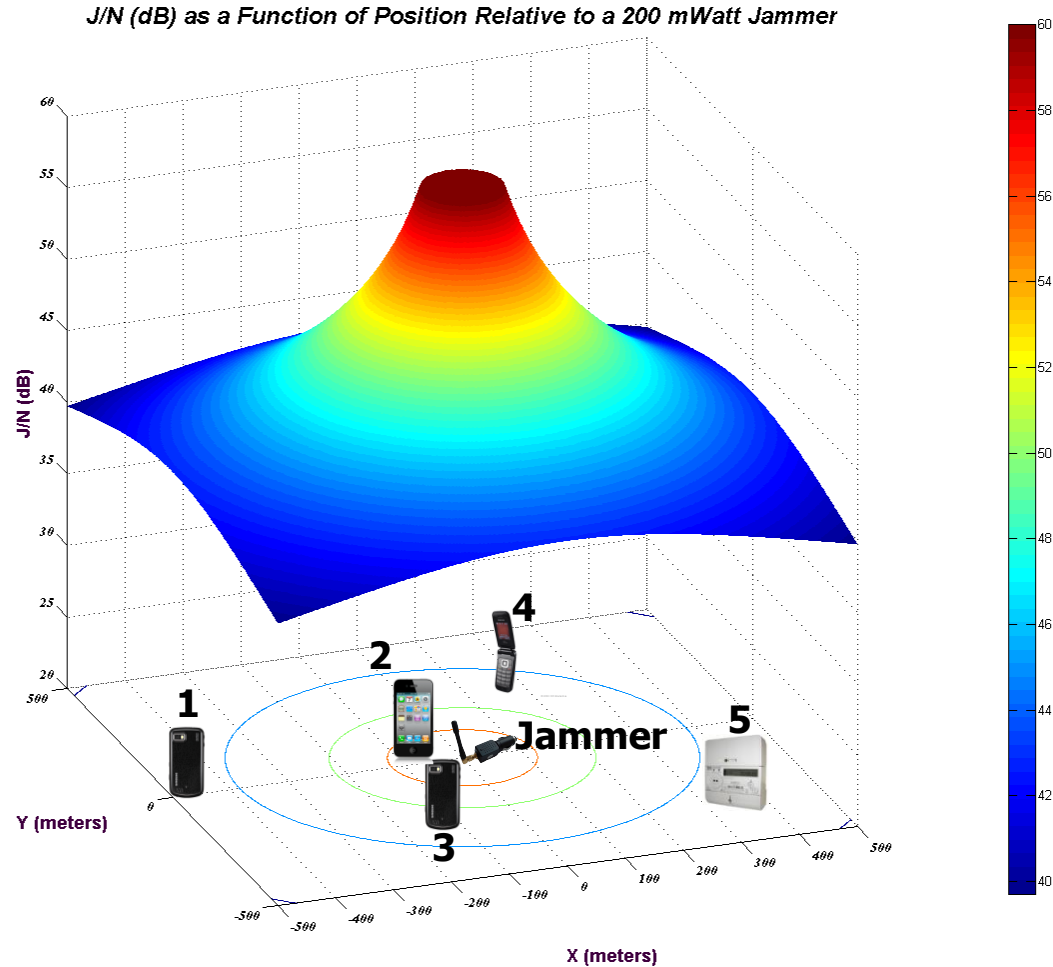
## Pulsed CW at 30 dB J/N (50 dB J/S), 100 Hz PRF



# Crowdsourcing for Jammer Detection & Location (10 seconds / 40 meter goal)

There are 5 billion cellphones worldwide

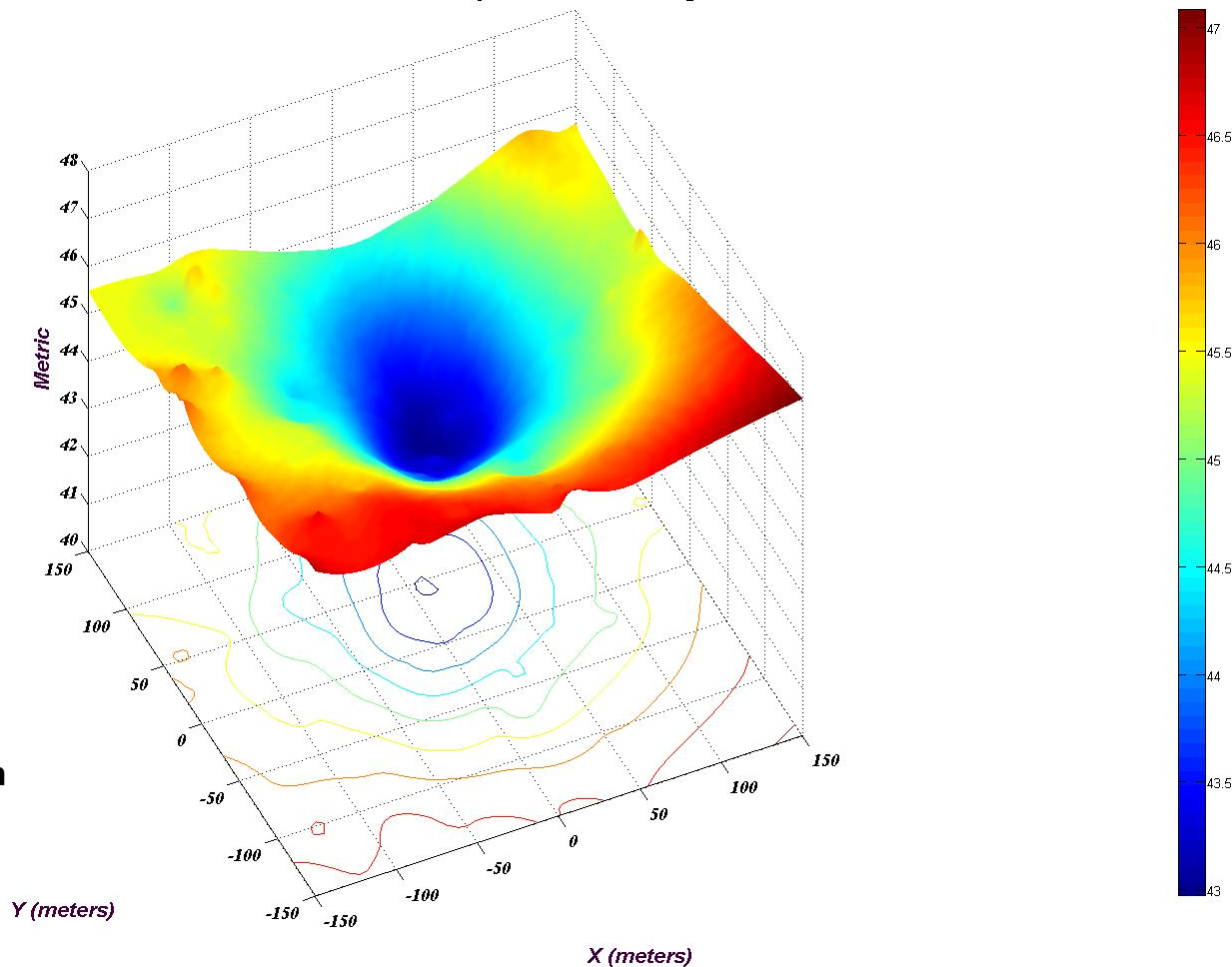
- CTIA Semi-Annual Wireless Industry Survey (<http://www.ctia.org/advocacy/research/index.cfm/AID/10316>)
  - 302 million wireless subscriber connections in the US
  - 253,086 cell sites
  - \$310 billion cumulative capitol investment



# Location Metric As A Function Of Position Relative to True Jammer Position

## (Observer Errors: 30 meter $1\sigma$ / 6 dB $1\sigma$ J/N)

Goodness of Fit Metric as a Function of Position Relative to True Jammer Position, min at  $[x,y]=[10,45]$   
Observer Position Accuracies  $\sigma_x = \sigma_y = 30$  meters,  $\sigma_{\log \text{ normal}} = 6$  dB

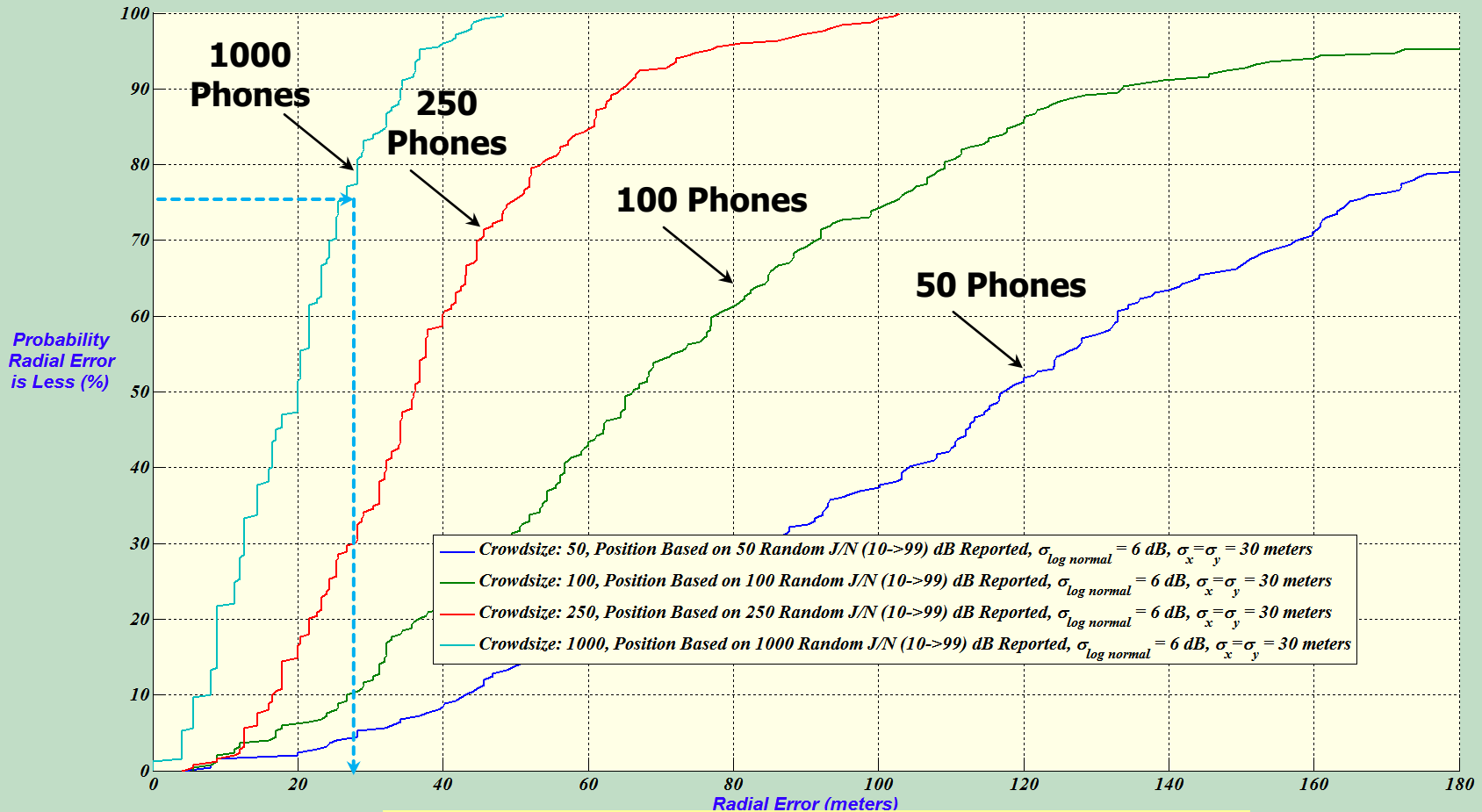


normr using 250 highest non saturating J/N of crowd of 1000/km<sup>2</sup>, J/N Sat=60 dB

crowdsourcing\_simulation\_multicase.m

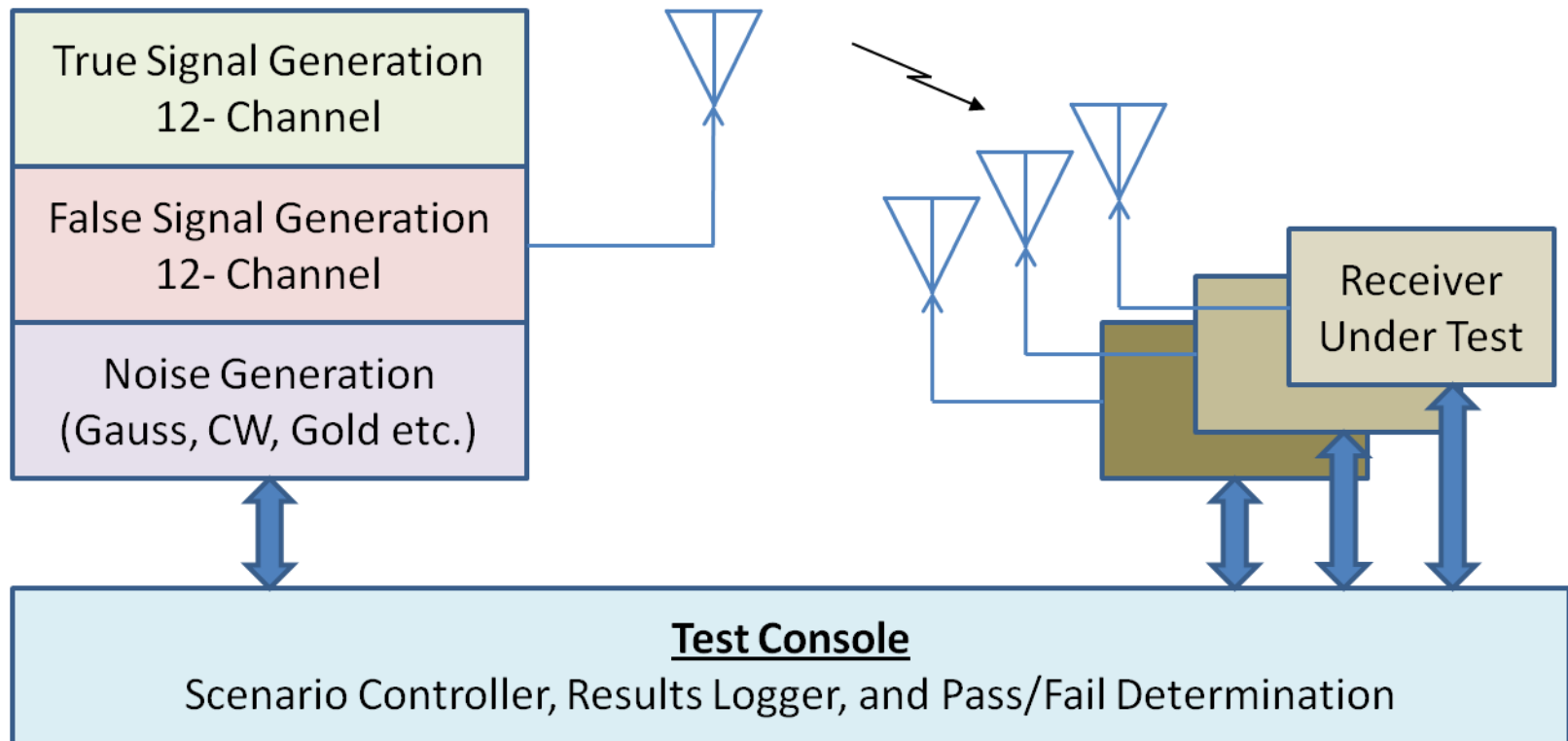
# Radial Error Statistics with Random Selection of [50,100,250,1000] Phones, 200 mW Jammer

Radial Error Statistics, Phones Uniformly Distributed over 4 km<sup>2</sup>  
0.200 Watt Jammer,  $J/N_{sat} = 60$  dB



$$Radial\ Error = \sqrt{\left( \left( j_{jammer\ estimated} - x_{jammer\ true} \right)^2 + \left( j_{jammer\ estimated} - y_{jammer\ true} \right)^2 \right)}$$

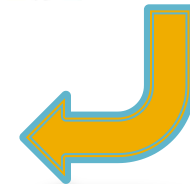
# Automated Test Setup Supports Simultaneous Testing of Multiple Receivers



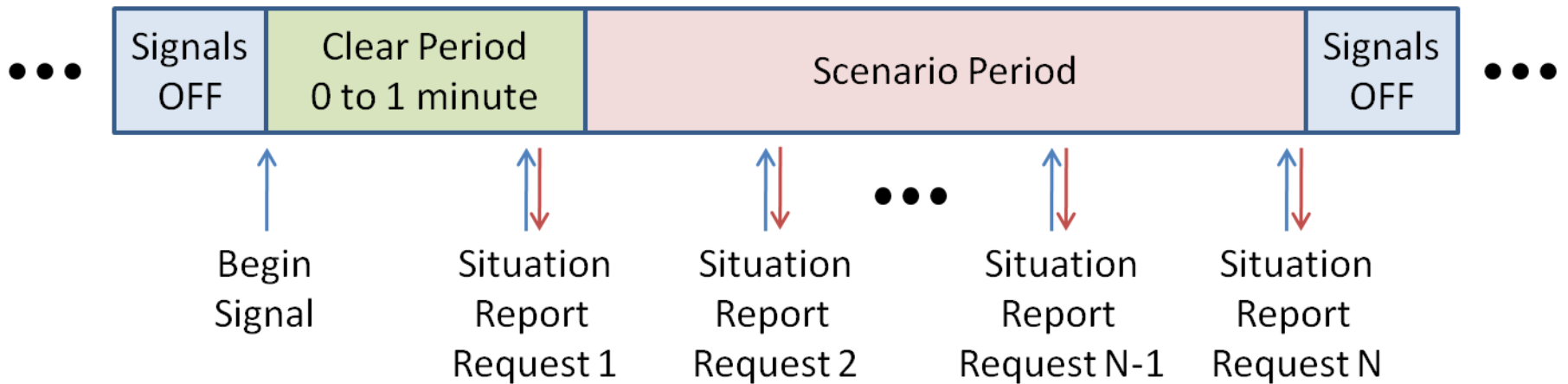


# Stored Scenarios Avoids Major Test Equipment Investment & Release of Scenario Details

- **National Instruments PXIe-5672 2.7 GHz Vector Signal Generator**
  - 250 kHz to 2.7 GHz
  - 32, 256, or 512 MB memory
  - 20 MHz real-time bandwidth
  - Full bandwidth stream-from-disk capability
  - -145 to +10 dBm output power



# Scenario Segment



- To Prevent Test Gaming
  - Scenarios Are Equal Length
  - Scenarios Are Presented In Random Order
  - In Some Scenarios, Nothing Happens

# Higher Level Certifications Provide Additional Protections

- Level 2 (Crypto & Out of Band Rejection)
  - Level 1 +
  - Software/Map Authentication
  - Attestation & Provenance (Proof of Origin)
  - Cryptographic Signal Authentication
    - Data Message Signing
    - Spread Spectrum Security Code Bursts
  - Out of Band Interference Rejection
- Level 3 (Physical Security)
  - Level 2 +
  - Physical Security (FIPS-140?)

Trusted  
Platform  
Module  
Role?



RQ-11 Auto  
Pilot Uses Civil  
Receiver?

# TPM (Trusted Platform Module) Is Sort of Like a Smart Card for the Machine

Included in over 300 million computers

- Securely stores digital keys, certificates and passwords.
- Used to authenticate the machine & its operating system & applications software
- Is not a bulk encryption/decryption device
- Available as IP

