



Interference Detection and Mitigation Workshop

Dr. T.D. Powell
Dr. M.A. Jeffris
Rick Hamilton
8 June 2012



Outline



- **Discussion of Proposed Spectrum Protection Efforts**
- **Case Study: Newark Airport (EWR) Event**
 - **Detection**
 - **Analysis**
 - **Testing**
 - **More Testing**
 - **Even More Testing**
 - **Findings**
- **Additional IDM and Test Events**
- **Conclusions**



U.S. SPACE-BASED POSITIONING, NAVIGATION, AND TIMING POLICY

December 15, 2004

FACT SHEET

The President authorized a new national policy on December 8, 2004 that establishes and implementation actions for space-based positioning, navigation, and timing programs, augmentations, and activities for U.S. national and homeland security, civil, scientific, and commercial purposes. This policy supersedes Presidential Decision Directive/National Science and Technology Council-6, U.S. Global Positioning System Policy, dated March 28, 1996.

I. Scope and Definitions

This policy provides guidance for: (1) development, acquisition, operation, sustainment, and modernization of the Global Positioning System and U.S.-developed, owned and/or operated systems used to augment or otherwise improve the Global Positioning System and/or other space-based positioning, navigation, and timing signals; (2) development, deployment, sustainment, and modernization of capabilities to protect U.S. and allied access to and use of the Global Positioning System for national, homeland, and economic security, and to deny adversaries access to any space-based positioning, navigation, and timing services; and (3) foreign access to the Global Positioning System and United States Government augmentations, and international cooperation with foreign space-based positioning, navigation, and timing services, including augmentations.

- “Interoperable” refers to the ability of civil U.S. and foreign space-based positioning, navigation, and timing services to be used together to provide better capabilities at the user level than would be achieved by relying solely on one service or signal;
- “Compatible” refers to the ability of U.S. and foreign space-based positioning, navigation, and timing services to be used separately or together without interfering with each individual service or signal, and without adversely affecting navigation warfare; and
- “Augmentation” refers to space and/or ground-based systems that provide users of space-based positioning, navigation, and timing signals with additional information that enables

ism has grown into a global utility whose multi-economic growth, transportation safety, and the worldwide economic infrastructure. In the

Anal

ions continues, the positioning, navigation, and timing System remains critical to U.S. and is woven into virtually every facet of U.S. military operations. The system will continue to rely on the Global Positioning System, navigation, and timing services.

Global Positioning System presents
homeland, and economic security. The
Positioning System of military, civil, and
of these systems inherently vulnerable to
or timing systems. In addition
positioning, navigation, and timing systems
capabilities that can be used in diverse
militarily, emergency, foreign intelligence
science or underpin the functioning of the

maintain the Global Positioning System, ensuring national, homeland, and economic security to meet commercial and scientific demands. In addition, it is important to deny adversary access to all space-based capabilities including services that are openly available to civilians or could be used by terrorists to threaten the security of the United States and its allies. The Department's efforts for research and development of space-based systems will include:

- Research and development of secure and resilient communications and navigation systems;
- Development of advanced positioning, navigation, and timing systems;
- Development of advanced space-based sensing and intelligence gathering systems;
- Development of advanced space-based communication and data link systems;

The Department will continue to work closely with the other agencies of the Executive Branch and the Congress to ensure that the Nation's space-based systems are secure, resilient, and capable of meeting the needs of the Nation.

tations to support their continued ability to meet
requirements.

The United States maintains space-based positioning, back-up, and service denial capabilities for positioning, navigation, and timing (PNT), economic security, and civil requirements, and maintain the pre-eminent military space-based positioning, navigation, and timing services that exceed or are beyond what other nations can provide. The U.S. provides PNT services to provide civil services that exceed or are beyond what other nations can provide. The U.S. provides PNT services and components of internationally accepted positioning, navigation, and timing services. To achieve this goal, the U.S. provides PNT services to provide civil services that exceed or are beyond what other nations can provide.

ate

se of any space-based positioning, navigation, and timing civil and commercial access to civil positioning, or for an area of military operations, or for homeland

secure, and civil, commercial, and scientific users

- Maintain the Global Positioning System as a component of multiple sectors of the U.S. Critical Infrastructure, consistent with Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection, dated December 17, 2003;
- Encourage foreign development of positioning, navigation, and timing services and systems based on the Global Positioning System. Seek to ensure that foreign space-based positioning, navigation, and timing systems are interoperable with the civil services of the Global Positioning System in order to maximize the benefit to the civil, commercial, and scientific users worldwide. Seek to ensure that foreign systems are not used to deny, degrade, or disrupt the U.S. Global Positioning System.

Investigate

- Ensure that the utility of civil services exceeds, or is at least equivalent to, those routinely provided by foreign space-based positioning, navigation, and timing services;
- Promote plans to modernize the U.S. space-based positioning, navigation, and timing infrastructure, including: (1) development, deployment, and operation of new and/or

Analyze

● Locate

Attribute

Mitigate

and its augmentations and address mutual
ent hostile use of space-based positioning.

navigation, and timing services and
and local level, to the maximum practical

Navigation, and Timing Services

-Based Positioning, Navigation, and Timing will be co-chaired by the Deputy Secretaries of Transportation or by their designated representatives at the equivalent level from the security, the Joint Chiefs of Staff, the National Weather Service, the Department of Defense, other Departments and Agencies as required. It, including the Office of Management and Enterprise Services Council staff, the Office of Economic Council staff, shall participate as members of the Federal Communications Commission Executive Committee as a Liaison. The year. The Secretaries of Defense and Energy shall also participate in the committee shall operate.

ions to its member Departments and
tatives of the Executive Office of the
II advise and coordinate with and among the
:gic decisions regarding policies,
for maintaining and improving U.S. space-
tures, including the Global Positioning
s, and relationships with foreign positioning,
xecutive Committee shall:

and civil requirements receive full and g process and facilitate the integration and used positioning, navigation, and timing



Existing and Emerging Threats



Apple Computers Cell Car Security & Electronics Surveillance Entertainment Health & Lifestyle Cameras & Photo Batteries & All Categories

Categories

- Security & Surveillance
- Jammers
- Door Phones
- Surveillance Cameras
- DVR Cards & Systems
- Cell Phone Booster
- Baby Monitors
- Baby Safety & Health

Cell Phone Signal Jammer | GPS Blocker

AMAZING DEAL!

Portable Cell Phone GPS Jammer

Block all GPS GSM CDMA
Up to 30 Feet Jamming Radius

~~US\$79.98~~

50% Off

US\$36⁹⁹

Get Your Here

WEEKLY DEAL

1600MHz GPS Signal Jammer

- Special for GPS L1
- Coverage: 3 - 6 Meter

US\$35.99

US\$25⁹⁹

SAVE \$10

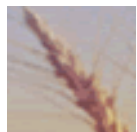
Save Now!

Buy Cell Phone Jammer Kits, take a look at Esprow's range of signal jammers & blockers.

1,978,000 hits on “GPS Jammer”



Critical Infrastructure Key Resource Sectors (CIKR)



[Agriculture and Food](#)



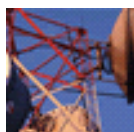
[Banking and Finance](#) *



[Chemical](#)



[Commercial Facilities](#)



[Communications](#) *



[Critical Manufacturing](#)



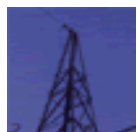
[Dams](#)



[Defense Industrial Base](#)



[Emergency Services](#)



[Energy](#) *



[Government Facilities](#)



[Healthcare and Public Health](#)



[Information Technology](#) *



[National Monuments and Icons](#)



[Nuclear Reactors, Materials and Waste](#)



[Postal and Shipping](#)



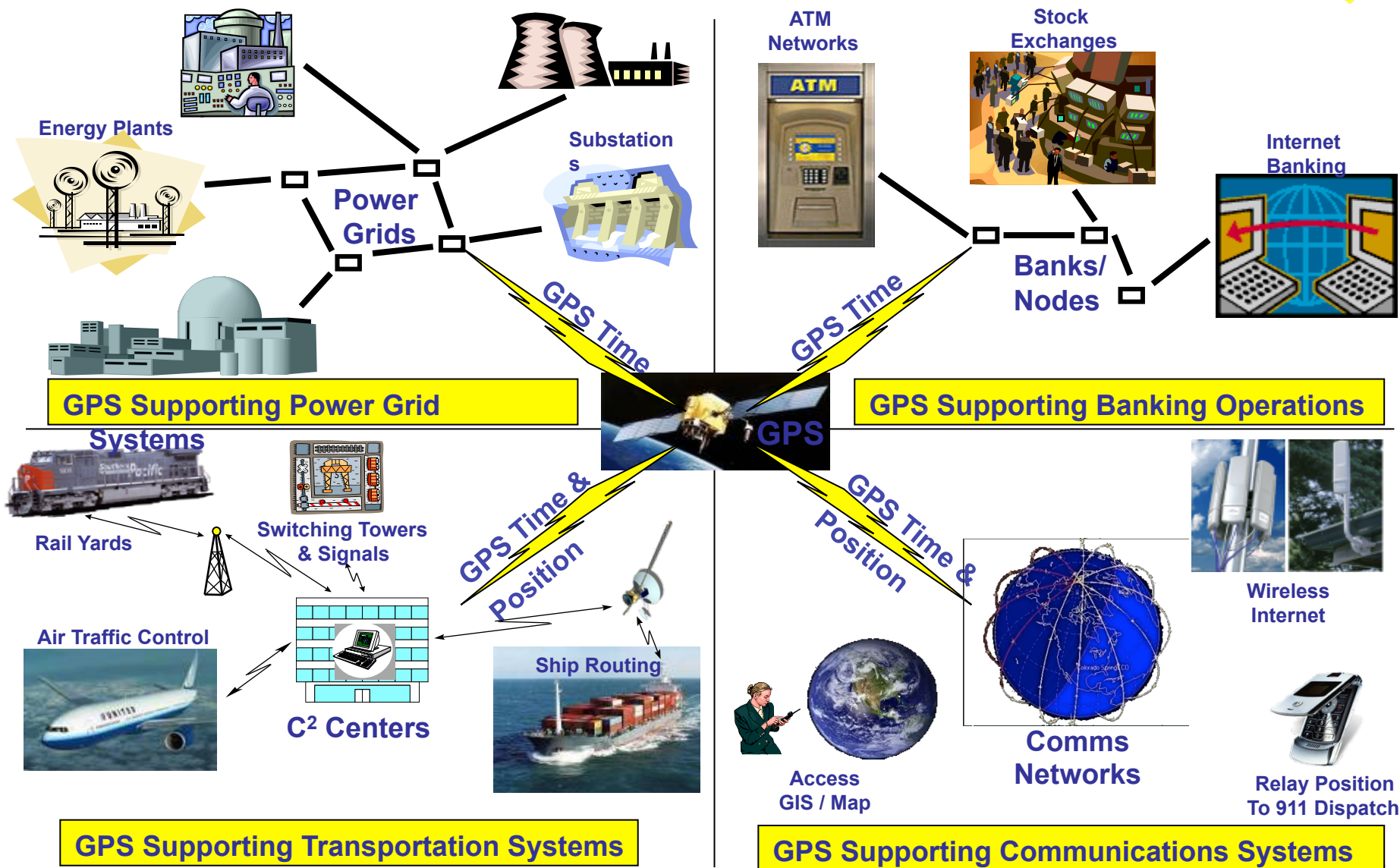
[Transportation Systems](#)



[Water](#)



Extent of GPS Dependencies





U.S. Initiative



- **Protect the Nation's 18 Critical Infrastructure & Key Resource Sectors (CIKR)**
- **System-of-Systems, Open Architecture, Multi-Phased/Multi-Layered Approach**
- **Near Real-Time Situational Awareness of Position Navigation and Timing (PNT) Interference**
 - **Leverage Existing** mature capabilities & focus on the **data**, less on system/device
 - **Common Data Structure for Information Sharing**
 - **Persistent Monitoring for Situational Awareness**

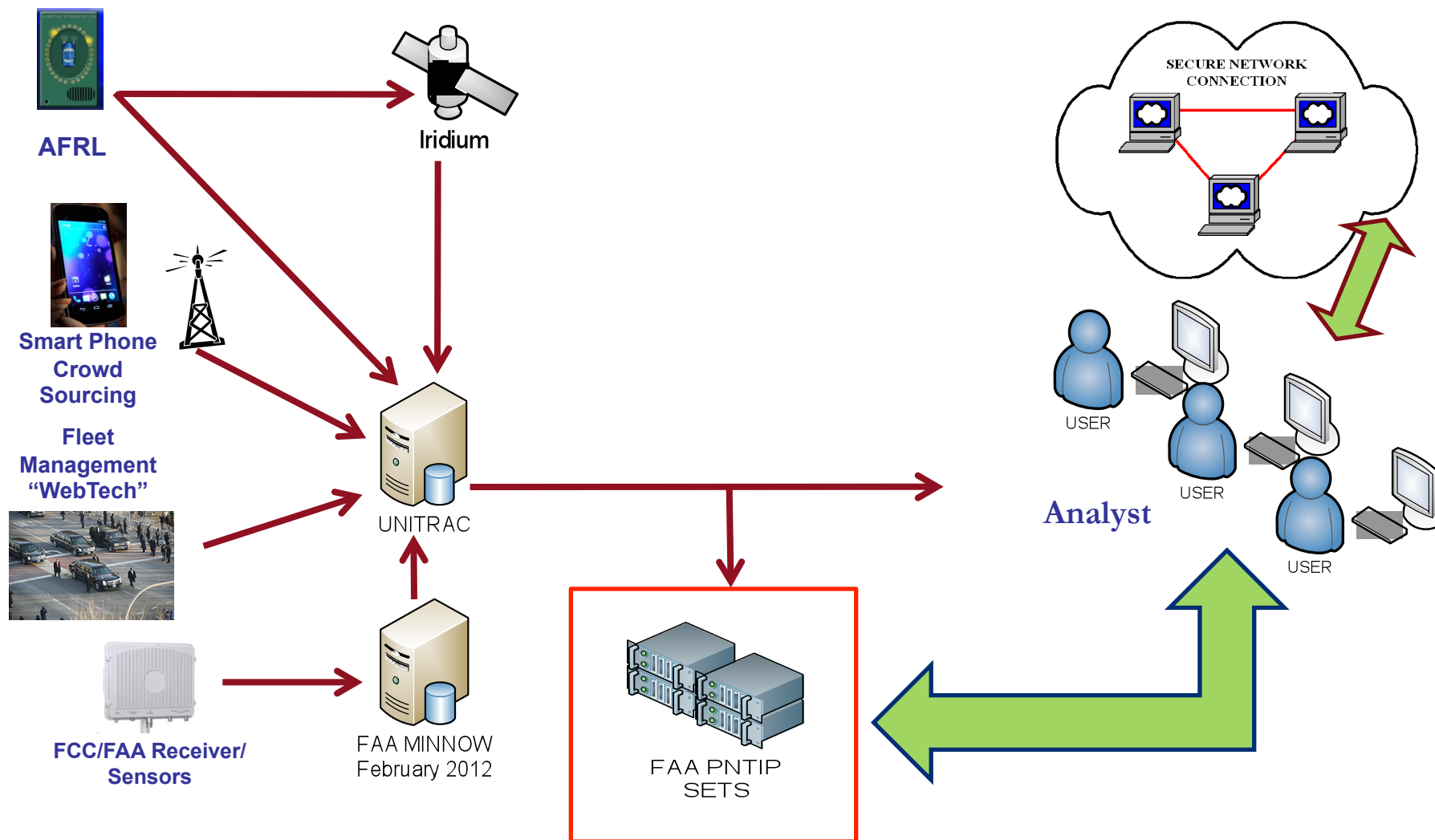


Proposed Architecture



Monitoring & Collection

Analysis & Evaluation





Outline



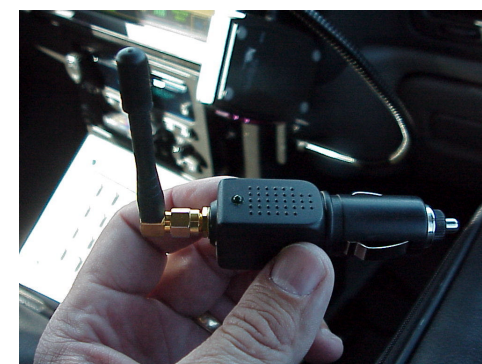
- **Discussion of Proposed Spectrum Protection Efforts**
- **Case Study: Newark Airport (EWR) Event**
 - **Detection**
 - **Analysis**
 - **Testing**
 - **More Testing**
 - **Even More Testing**
 - **Findings**
- **Additional IDM and Test Events**
- **Conclusions**



The Threat



- **GPS Privacy Jammers**
 - **Marketed to consumers**
 - Honest people who fear the loss of privacy
 - Criminals / dishonest people who want to evade law enforcement, employers, etc ...
 - **Power: milliwatts to watts**
 - Many devices are battery powered
 - **Effective Radius:**
 - Advertised: meters to tens of meters
 - Potentially 100s to 1000s of meters
 - **Cost: \$25 to \$300 USD**
- **During the week of April 26, 2010**
 - Commuter on NJ Turnpike was found by the FAA/FCC with GPS Privacy Jammer



Device Found at EWR

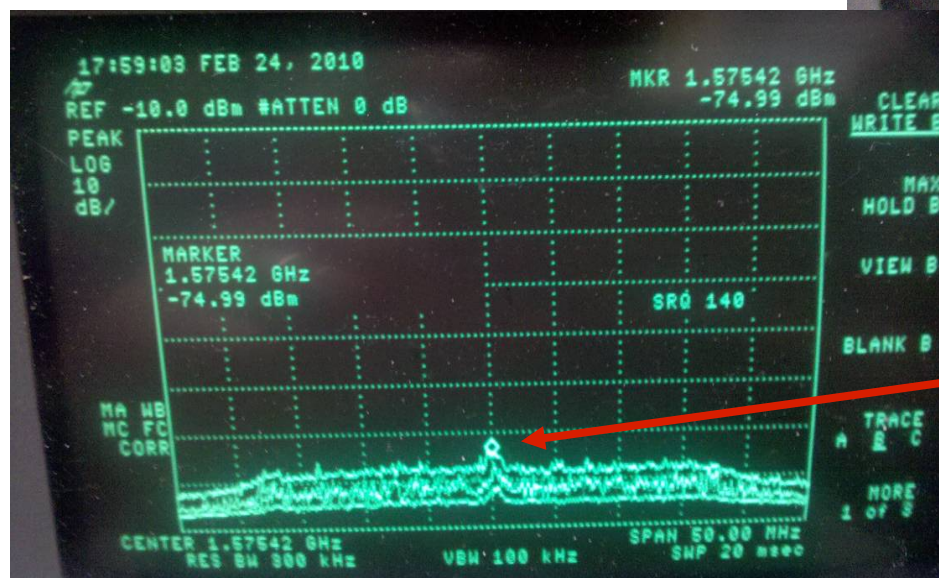
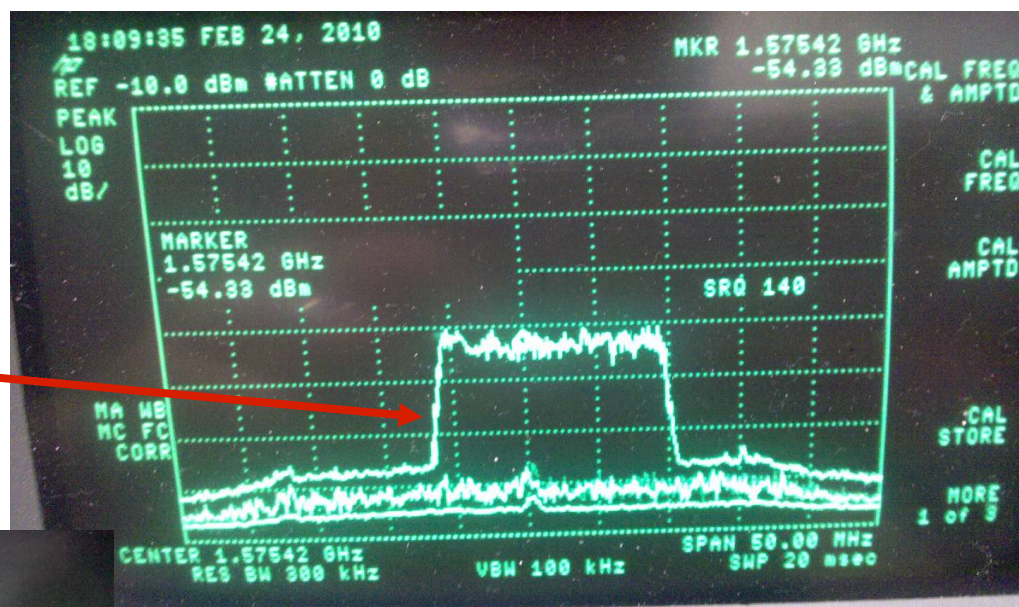


FAA Spectrum Measurements



→ **Wideband Intermittent Source** detected in December 2011 occupying approx – 20 MHz

→ **5 MHz below and 15 MHz above L1.**



→ **Normal L1 Pass Band Spectrum** when Interference Source is Not Present.



FAA Minnow System



✈ **November 23, 2009** during initial SLS-4000 stability testing the **Station Faulted and Reference Receiver Satellite Tracking was Interrupted.**

SLS-4000 Components

GPS Antenna (RRA)

- Multipath Limiting design
- Sharp cutoff/rejection at horizon

GPS Receiver (RSMU)

- 48-channel, L1 C/A GPS
- Signal Deformation Monitoring (SDM) capable



VHF Radios (VDB)

- D8PSK modulation, TDMA
- Nav band, 108-118 MHz

VHF Antenna

- Horizontal (HPOL) or Elliptical (EPOL) polarized signal



Processor HW (DCP)

- Pentium M, 1.8 GHz CPU
- Hosts integrity monitoring software

Processor SW (DCP)

- Real time monitoring for GPS failure modes, local error sources
- Differential correction determination
- User interface via Maintenance Data Terminal

DCP: Differential Correction Processor
RPDP: Robust Power Distribution Panel
VHF: Very High Frequency
VDB: VHF Data Broadcast
HW: Hardware
RRA: Reference Receiver Antenna
RSMU: Remote Satellite Measurement Unit



FAA / FCC Investigation



- **Government and Contractor Teams convened in Newark on February 24 – 26, 2010 in an attempt to locate the direction toward the source of the observed interference events.**
- **The Teams on site for the first time had a “Learning Curve” experience and effective data could not be obtained.**
 - **Three (3) Radio Frequency Interference (RFI) events were observed and measured, but not by all on-site teams.**
- **The same Teams participated again during March 22 – 25, 2010 in an attempt to draw accurate and more conclusive simultaneous lines of bearing.**
 - **Measurements and data analysis reveal interference source was MOBILE at slow and fast rates.**



Testing Summary

□ Jammer Characterization

- Attempt to build library of jammer signatures
- Testing is ongoing

□ EWR Field Test #1

□ Overview

- Single Sensor
- C/N₀ sensors placed on ground

□ Successes

- Proved sensor could detect the threat

□ Lessons Learned:

- C/N₀ sensors of limited use when placed on the ground
- Coordination among stakeholders critical

□ EWR Field Test #2

□ Overview

- Dual sensors
- Repositioned C/N₀ sensors above ground
- Utilized MITRE built data to capture interference time series
- Automated spectral recording w

□ Successes

- Sensors again successfully detected interference and data implies a moving interferer
- C/N₀ sensor data conclusively shows moving interference



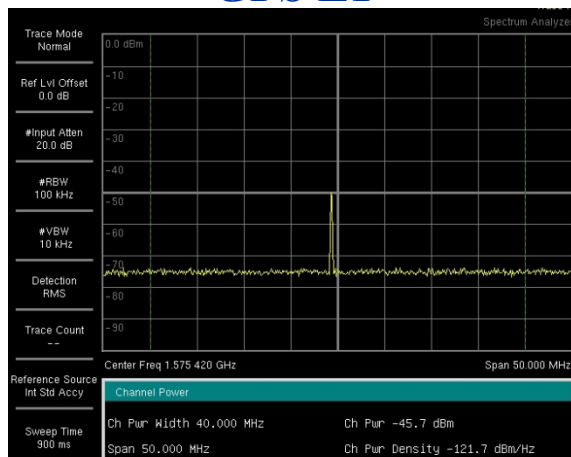
Jammer Characterization



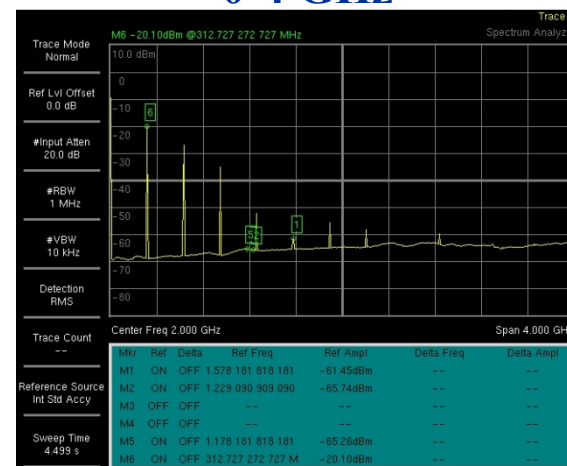
- MITRE purchased 12 GPS privacy jammers for signal characterization
- Results:
 - Very dirty outside the intended GPS bands thus capable of causing additional, collateral damage
 - Testing of EP5000 jammer similar to EWR jammer reveals an L1 tone jammer
 - Other broadband jamming waveforms observed at EWR
 - Most likely indicates there are more jammers out there

GP5000 Power Spectra

GPS L1



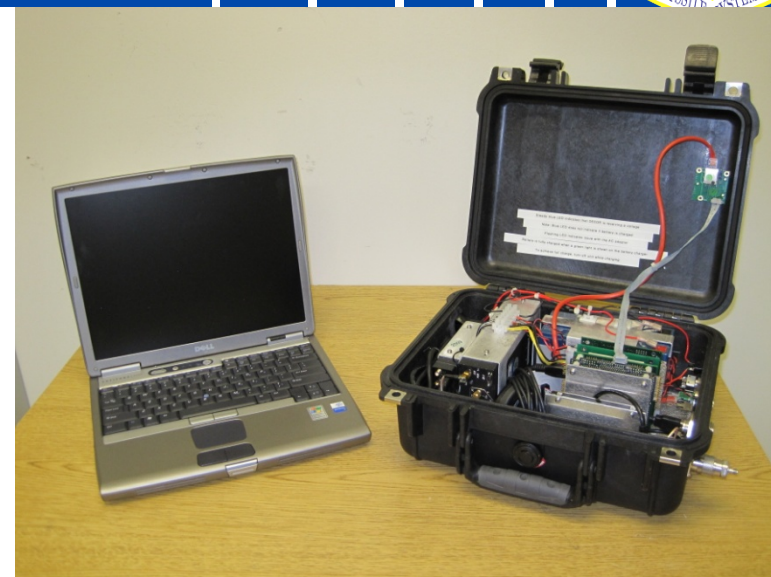
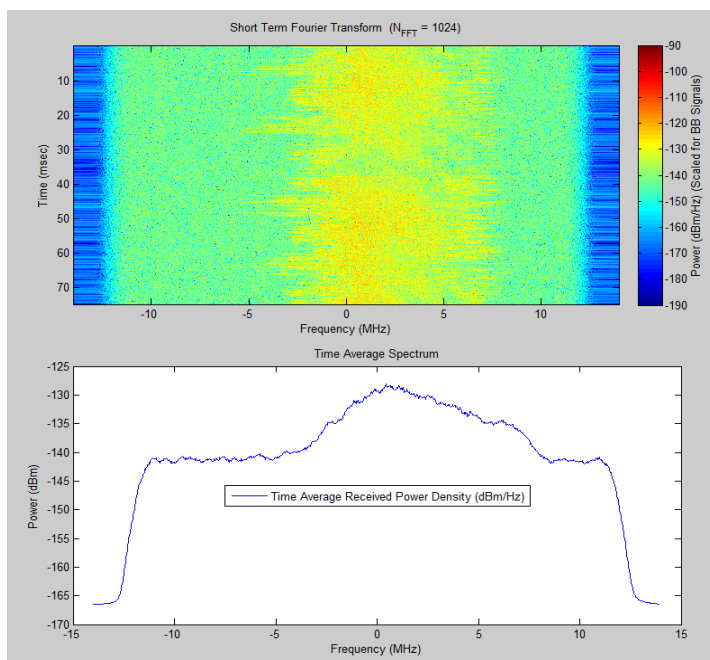
0-4 GHz



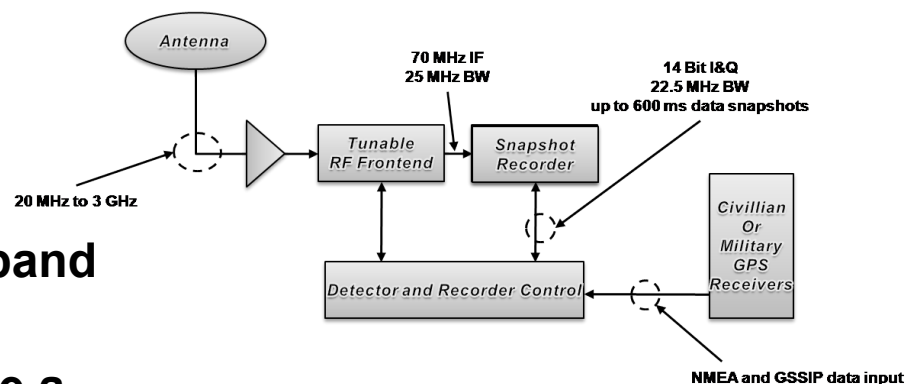


Data Recording

- Automatic detection of interference*
- MATLAB analysis toolbox



- Data from 24 Mar 2010 shows wideband modulation
- Data hopefully can be used to derive a “signature” for the jammer



Note: automatic detection mode not used at EWR



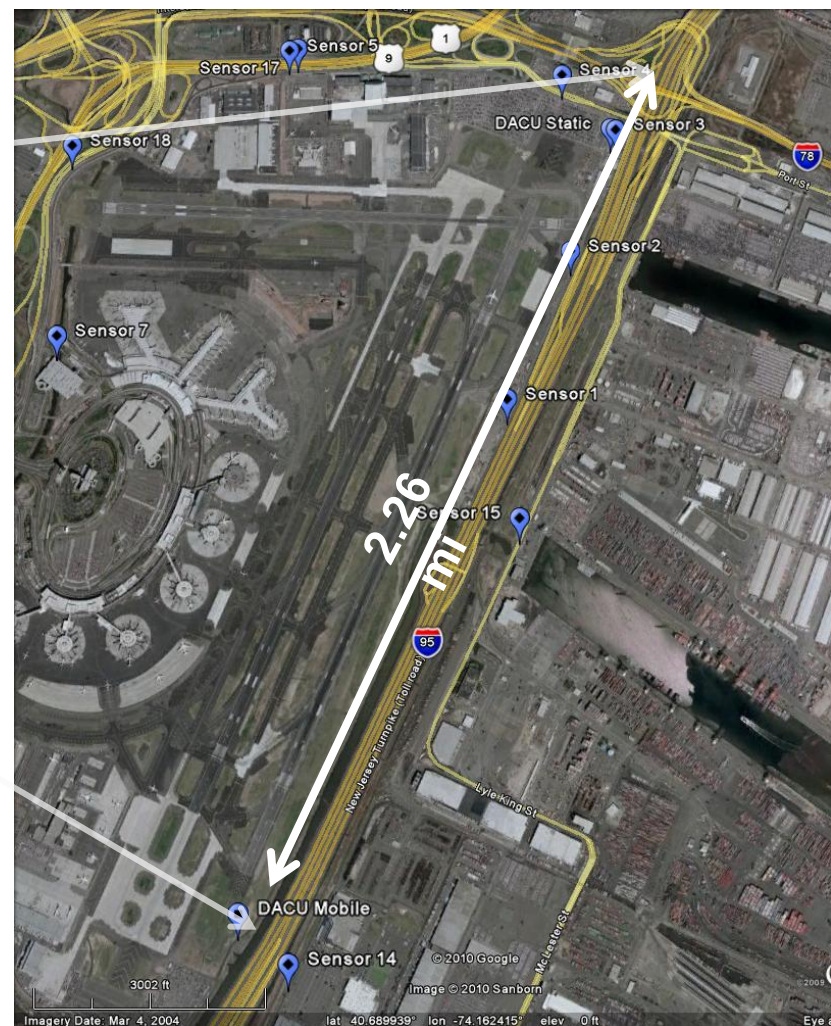
Dual Sensor Laydown



Static Sensor



Mobile Sensor





Testing Results

Static DACU

Hit Times

Duration (sec)

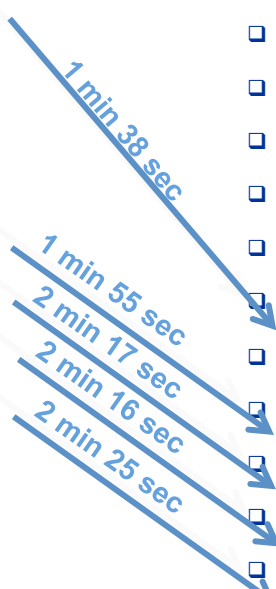
❑ 25-Mar-2010 11:55:34	4
❑ 25-Mar-2010 18:53:42	4
❑ <u>25-Mar-2010 18:59:51</u>	7
❑ 25-Mar-2010 19:05:47	7
❑ 25-Mar-2010 19:13:28	5
❑ 25-Mar-2010 19:21:44	7
❑ <u>25-Mar-2010 20:10:48</u>	4
❑ <u>25-Mar-2010 20:30:07</u>	7
❑ <u>25-Mar-2010 21:16:08</u>	22
❑ <u>25-Mar-2010 21:24:07</u>	8
❑ 25-Mar-2010 21:37:03	4
❑ 25-Mar-2010 21:43:23	10

Mobile DACU

Hit Times

Duration (sec)

❑ 25-Mar-2010 11:47:51	7
❑ 25-Mar-2010 12:08:46	6
❑ 25-Mar-2010 13:21:09	4
❑ 25-Mar-2010 14:46:47	3
❑ 25-Mar-2010 14:47:52	3
❑ 25-Mar-2010 15:16:22	10
❑ 25-Mar-2010 15:21:39	3
❑ 25-Mar-2010 18:30:24	3
❑ <u>25-Mar-2010 19:01:29</u>	9
❑ 25-Mar-2010 19:03:05	6
❑ <u>25-Mar-2010 20:12:43</u>	3
❑ <u>25-Mar-2010 20:32:24</u>	3
❑ <u>25-Mar-2010 21:18:23</u>	3
❑ <u>25-Mar-2010 21:26:32</u>	10



Correlated but non-coincident times imply a moving interferer



C/N₀ Sensor

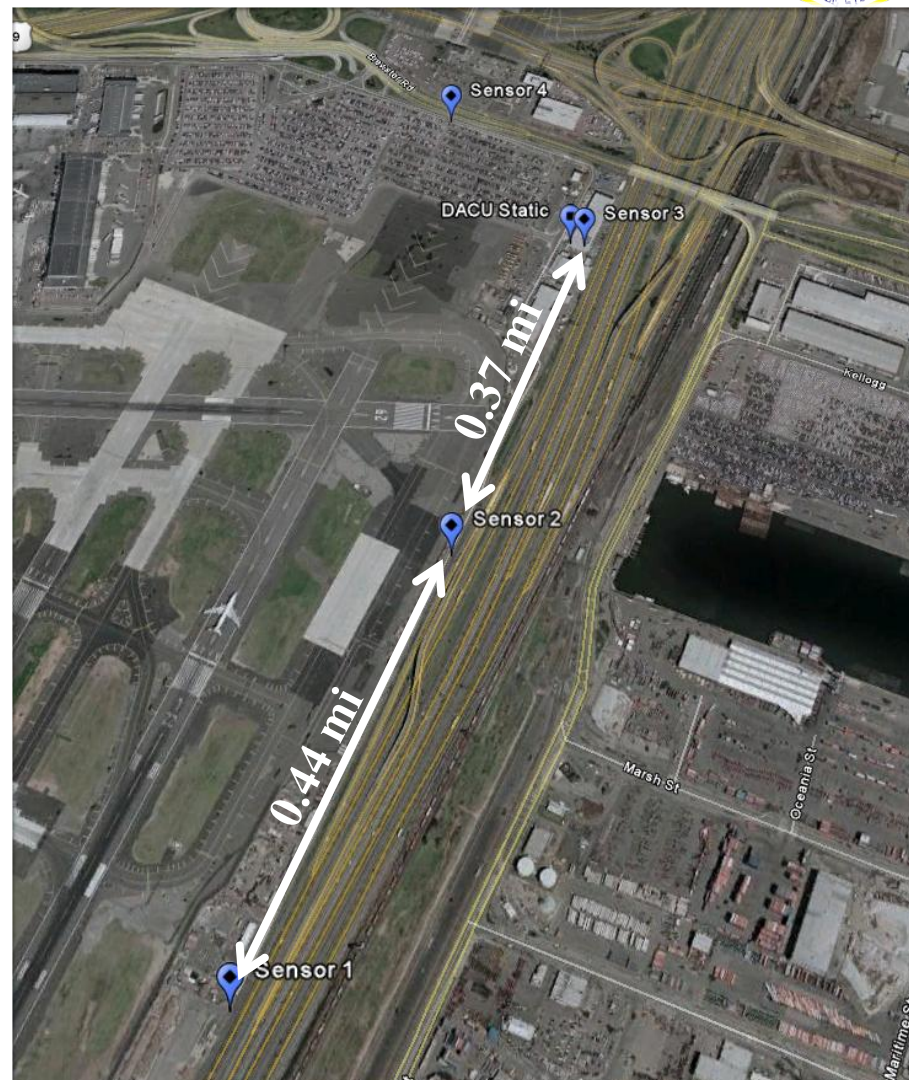
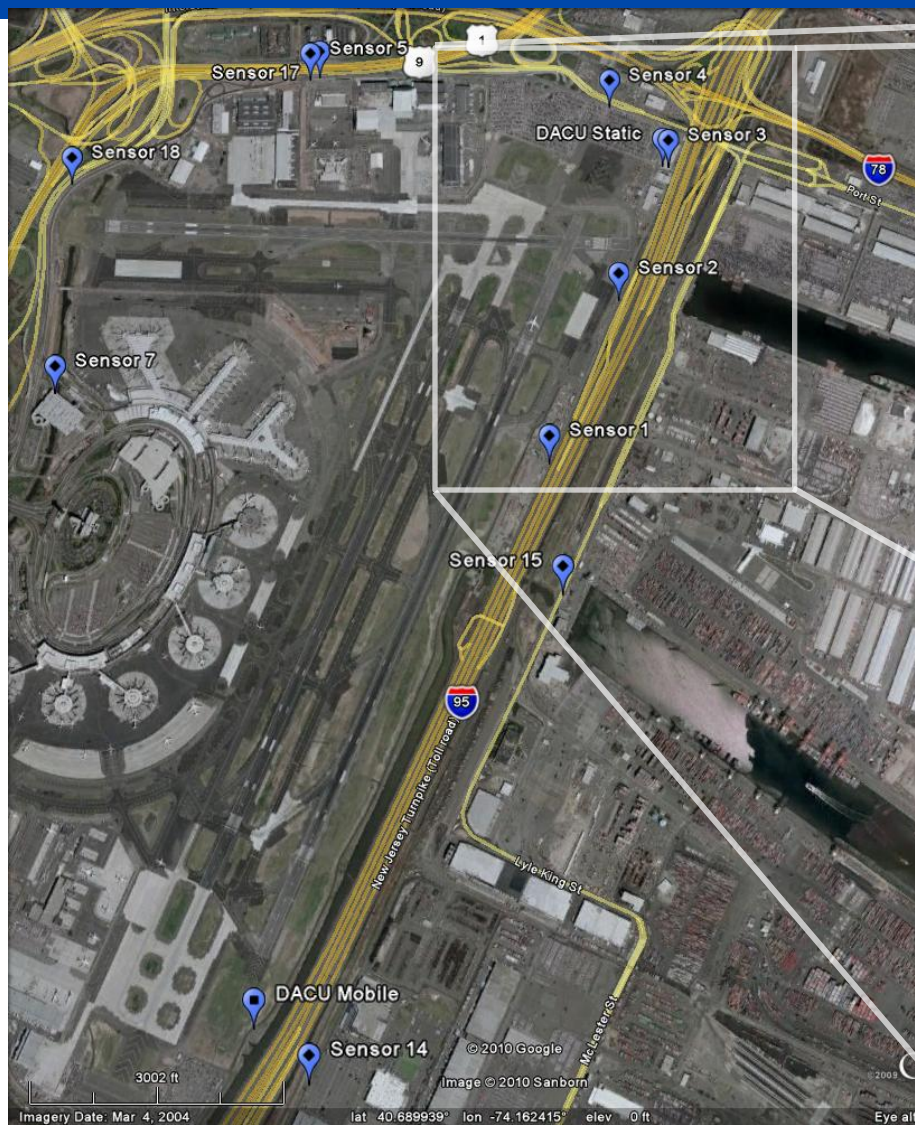


- **Qstarz Q-1000X**
 - Affordable, high performance & low SWaP integrated GPS receiver plus data logger
 - **GPS Receiver**
 - 66 Channel, high sensitivity, AGPS
 - **Data Logger**
 - Records PVT, C/N₀ and more
 - Export to NMEA, CSV, Google Earth
 - 7 hour capacity at 1 Hz
 - **Low SWaP**
 - 72 x45 x 20 mm
 - 0.3 Ounces
 - Rechargeable battery rated for up to 42 hrs
 - **Cost : \$100 (amazon.com)**



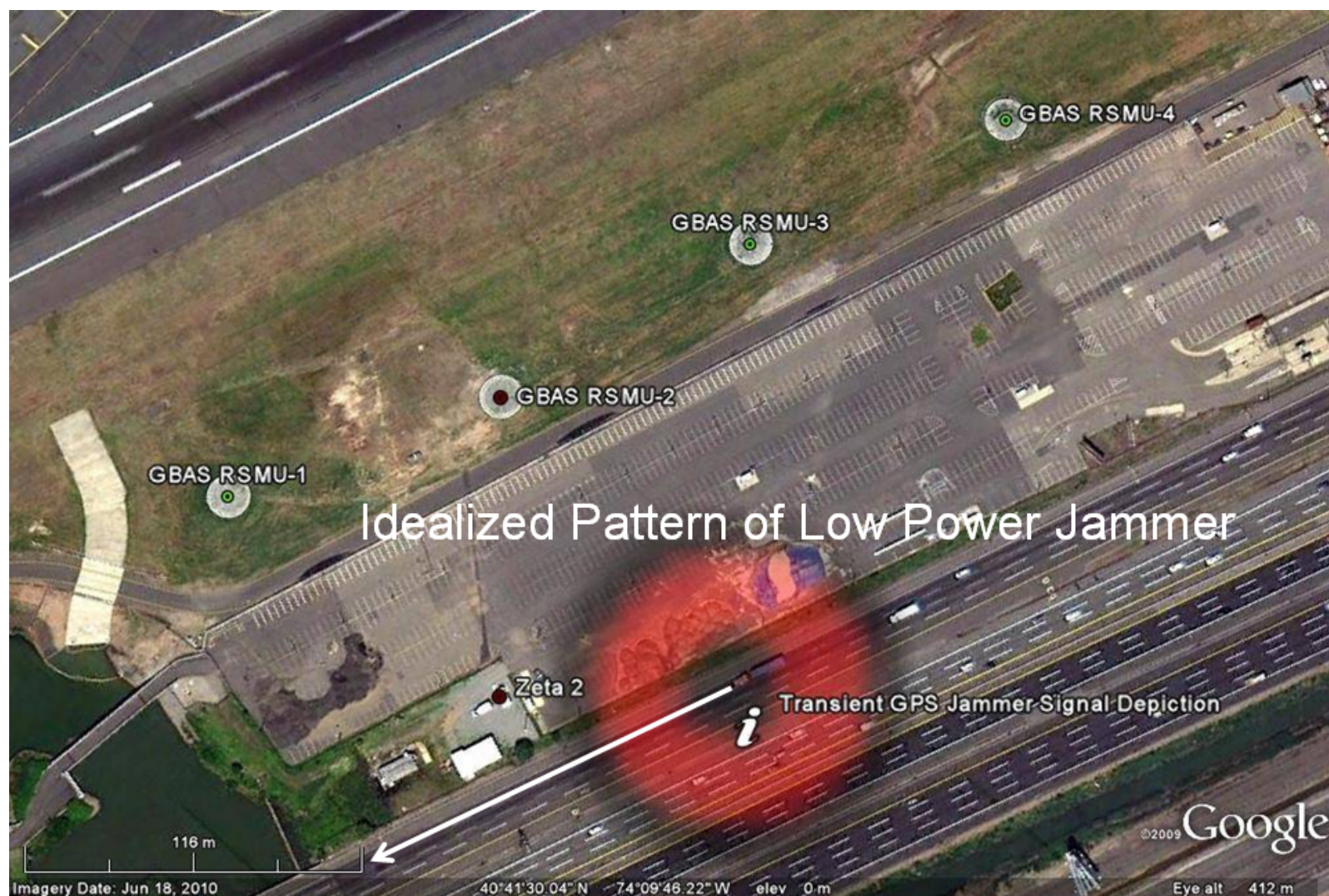


C/N₀ Sensor: Laydown





Analytical Pattern

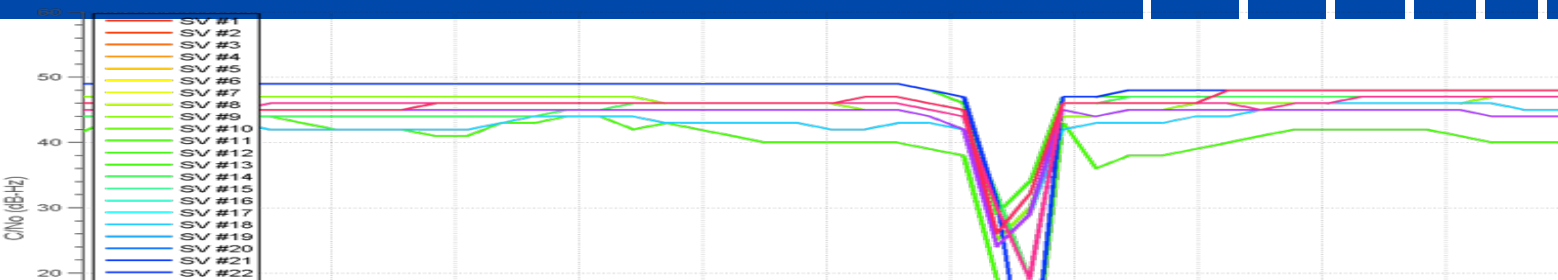




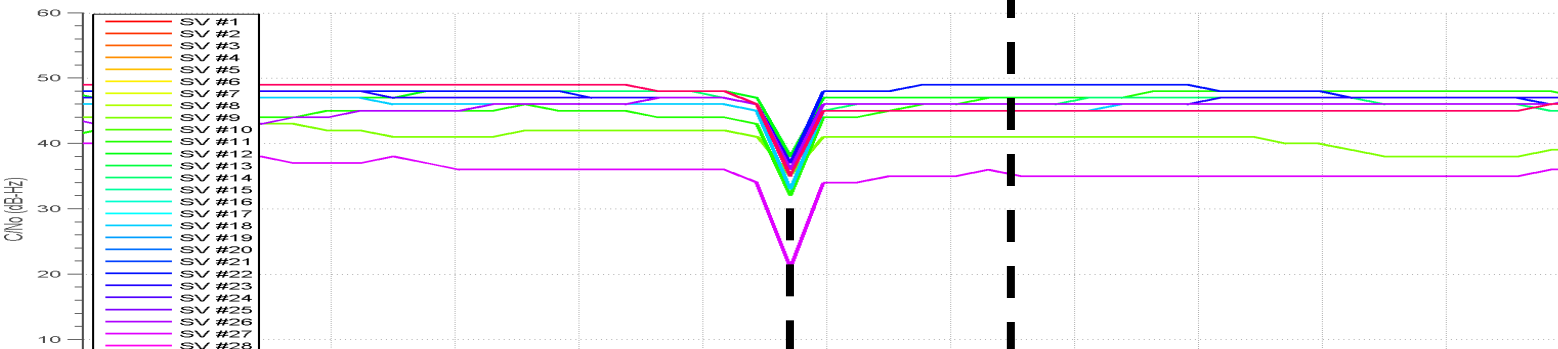
C/N₀ Sensor: Results: Wednesday 23 Mar 2010 20:51:00 GMT



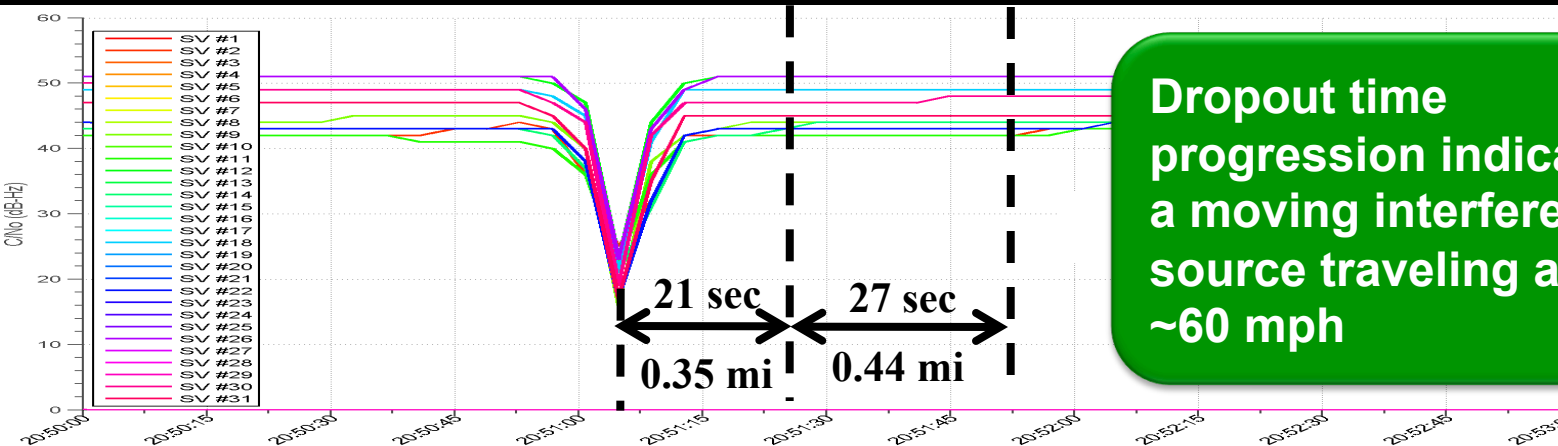
Sensor 1



Sensor 2



Sensor 3



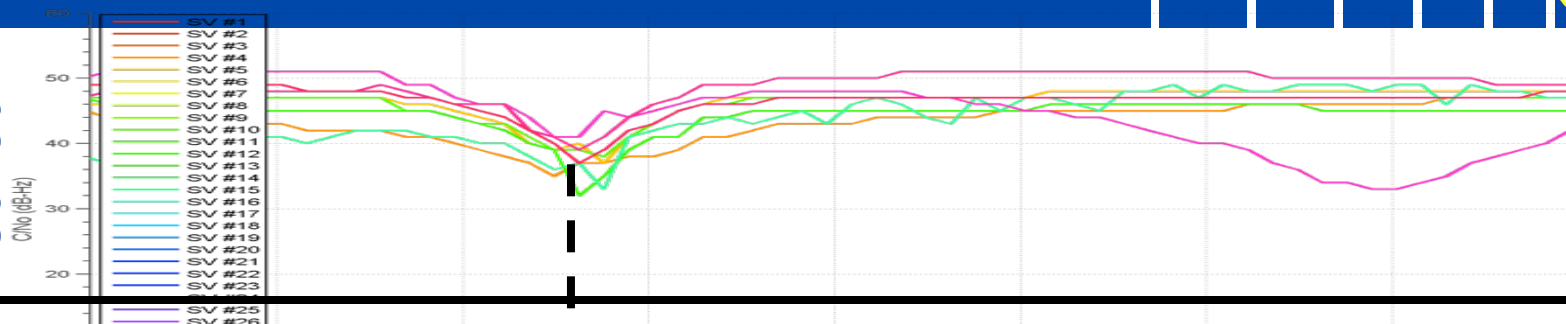
Dropout time progression indicates a moving interference source traveling at ~60 mph



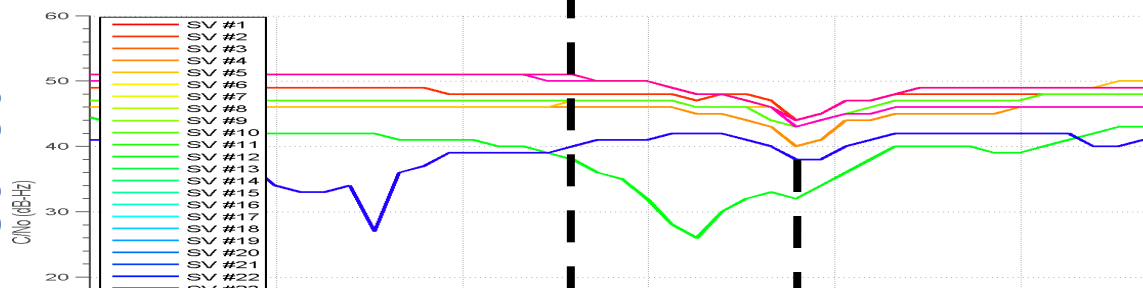
C/N₀ Sensor: Results: Wednesday 23 Mar 2010 13:28:00 GMT



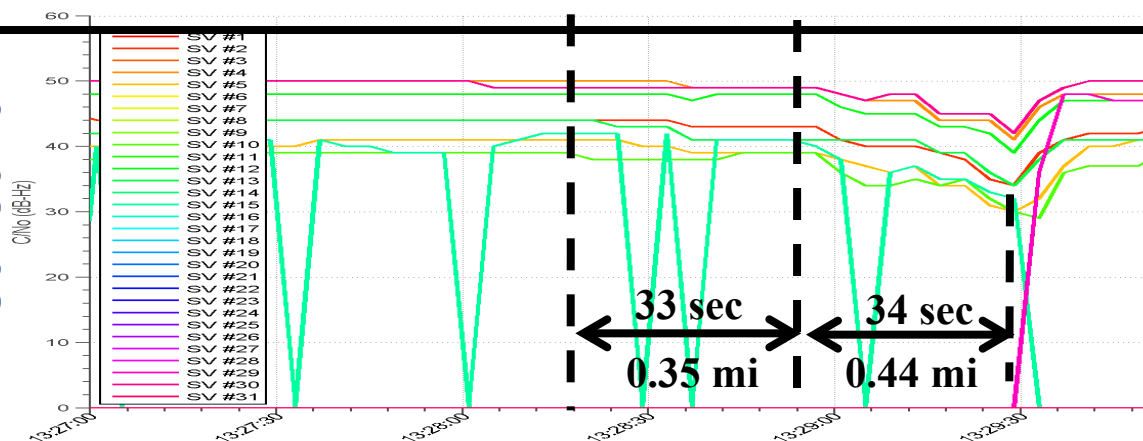
Sensor 1



Sensor 2



Sensor 3

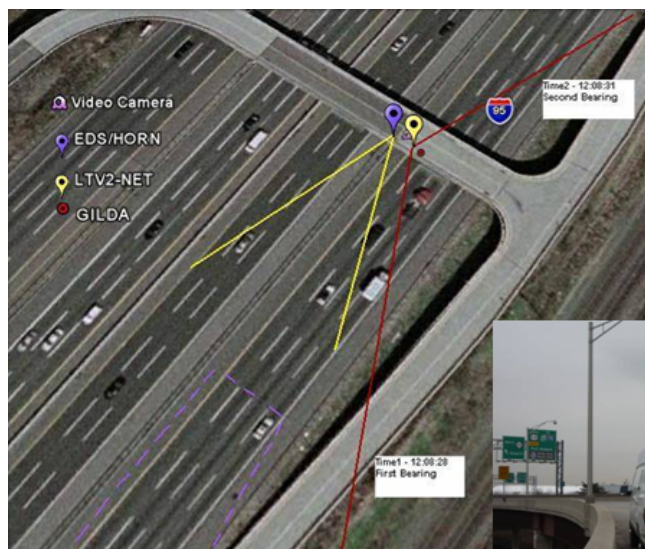
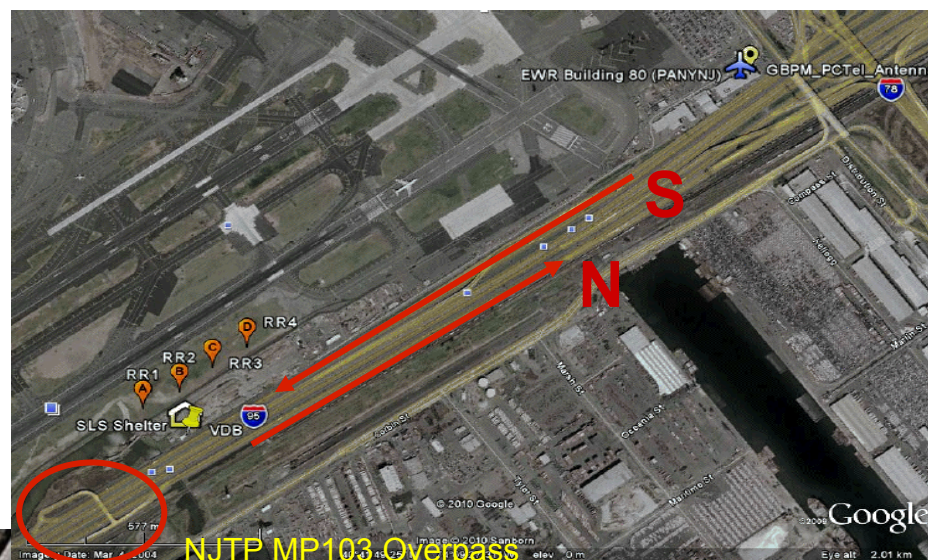


Dropout time progression indicates a moving interference source traveling at ~40-45 mph

Weaker response and lower velocity may imply vehicle on surface road, not NJ Turnpike



New Jersey Turnpike Overpass Point





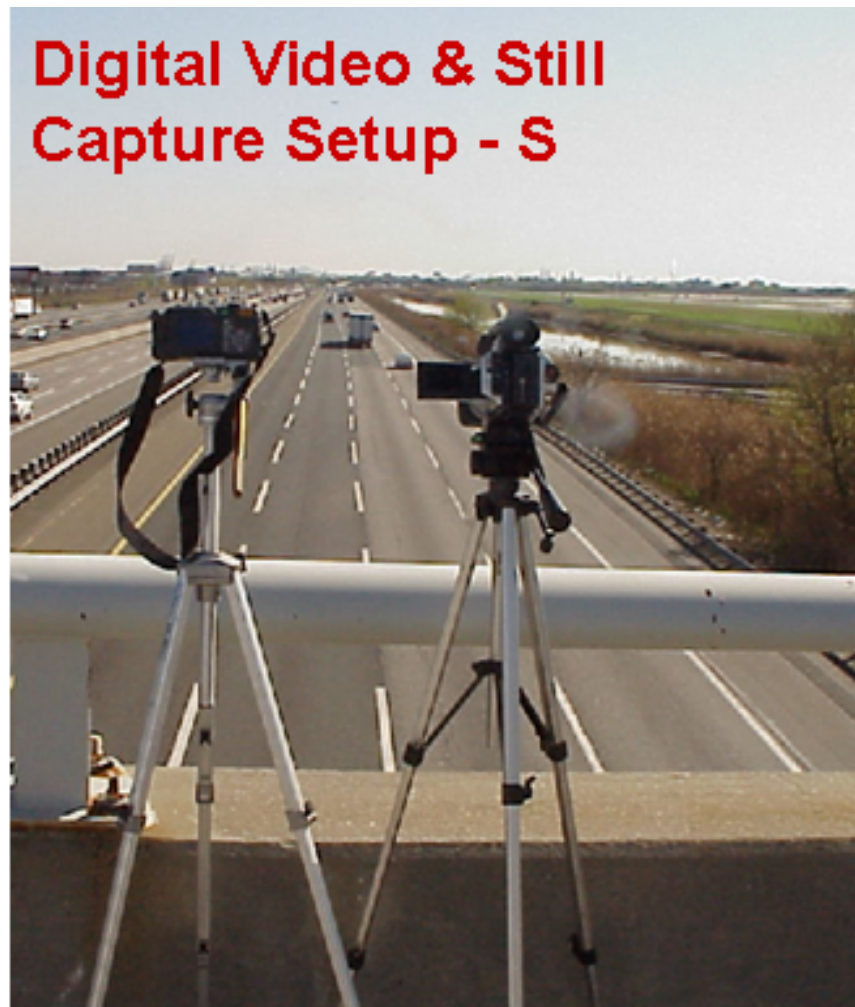
Equipment Capture Setup



Directional SA Measurement Setup - S

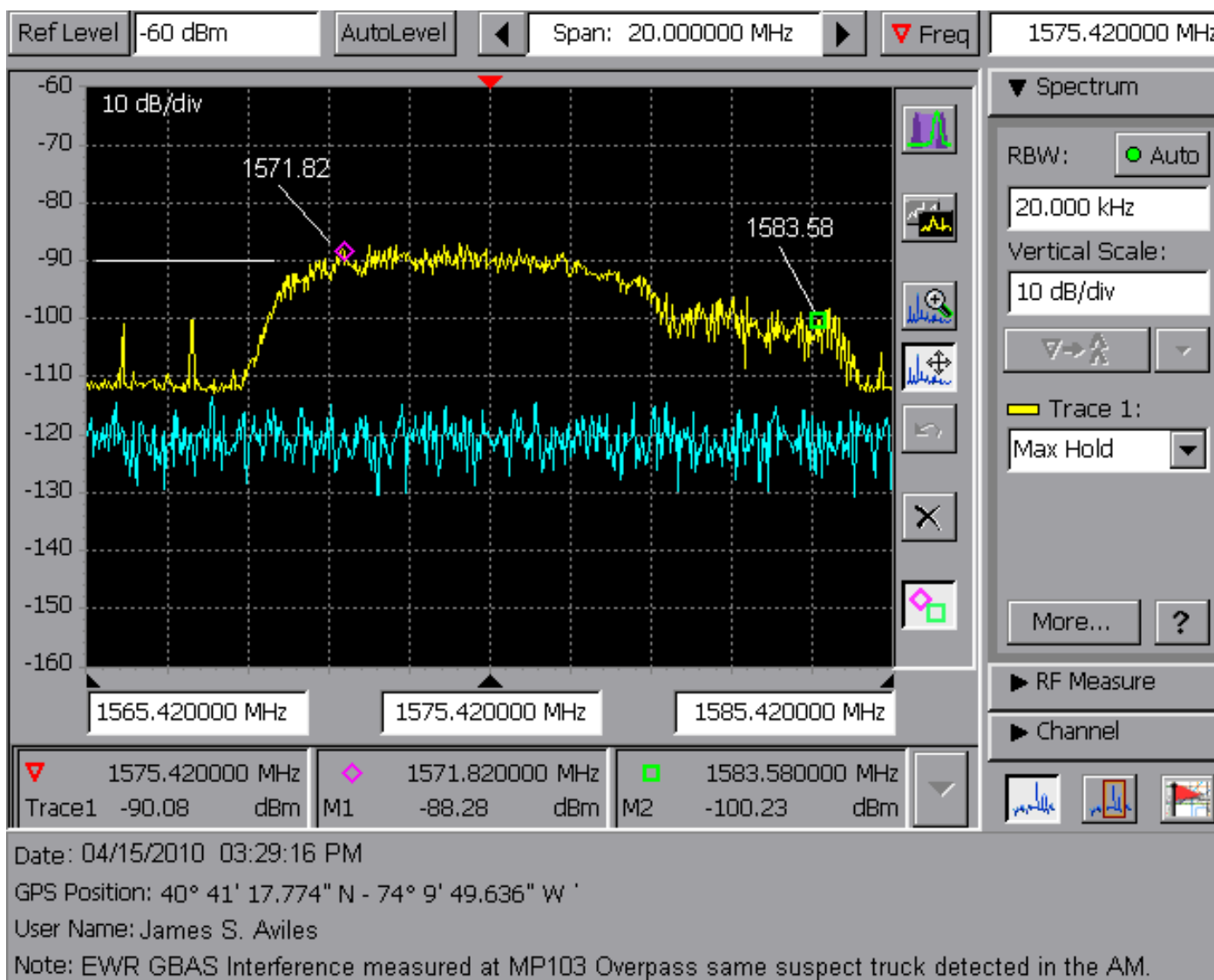


Digital Video & Still Capture Setup - S



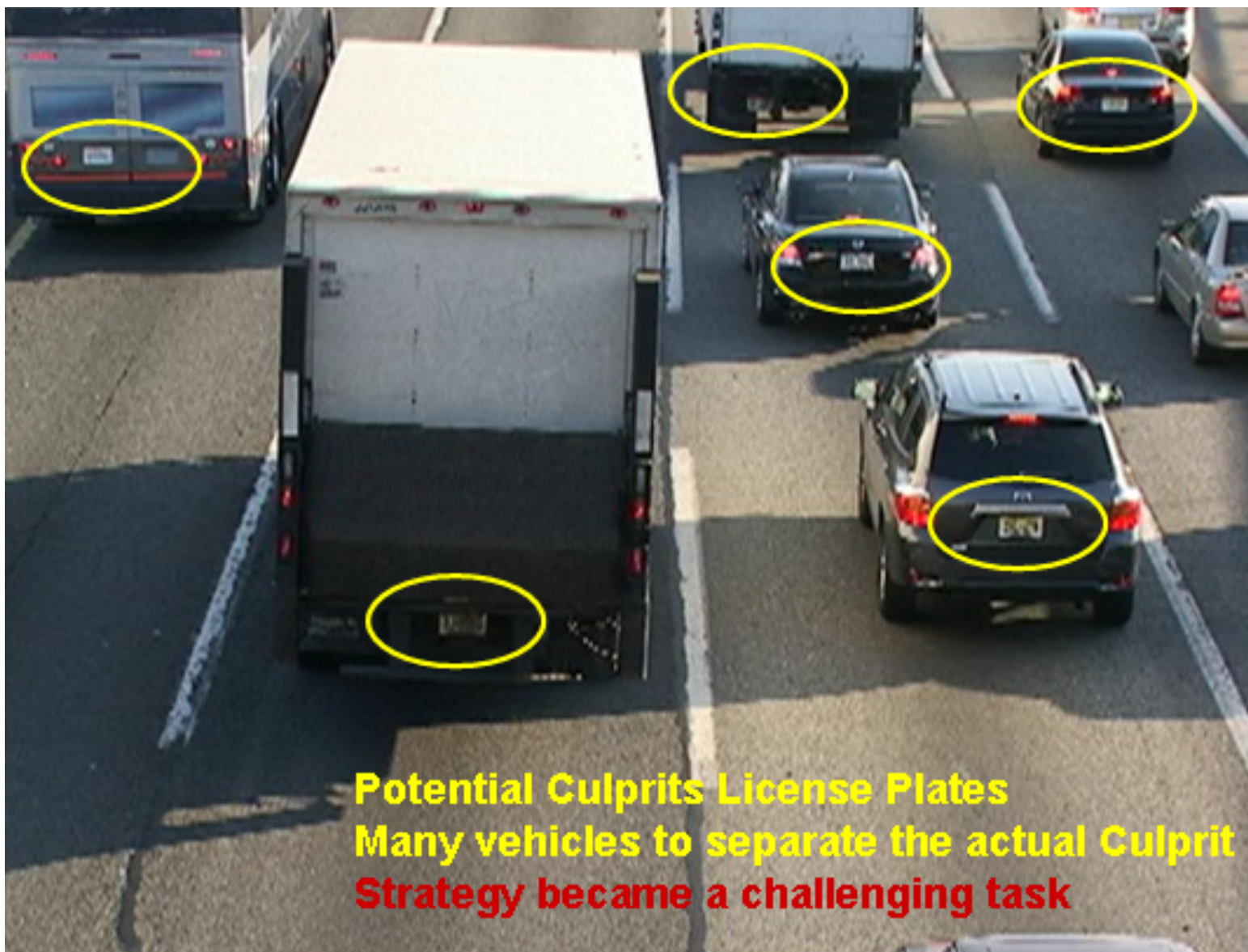


Sample Measured Data





Difficulties



Potential Culprits License Plates
Many vehicles to separate the actual Culprit
Strategy became a challenging task



Another Strategy: Closer Observation





Implementation Reality: Traffic



**Traffic Buildup
Challenge the
Strategy**





Interference: Hot Pursuit



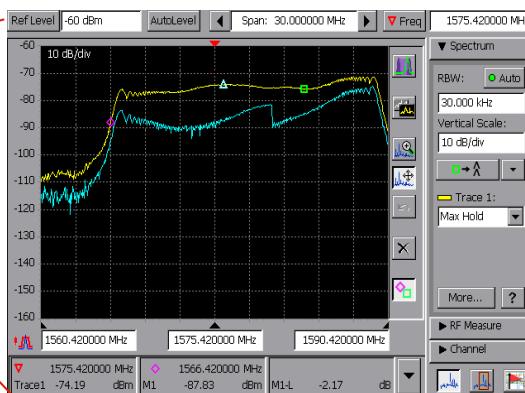
FCC Equipment



FAA Equipment



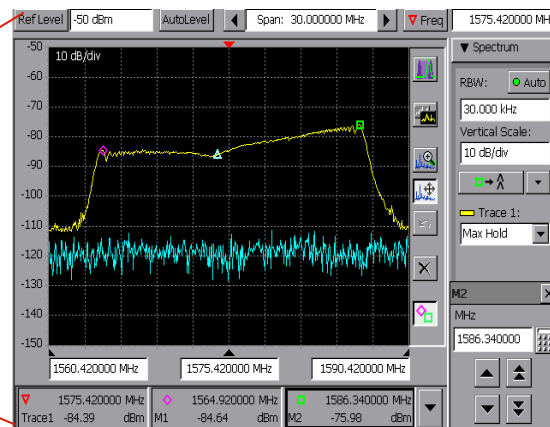
FAA "Tip Off"



**RFI source "Locked-on"
and pursued until
vehicle stop at traffic
light further south**



Interference Source Revealed

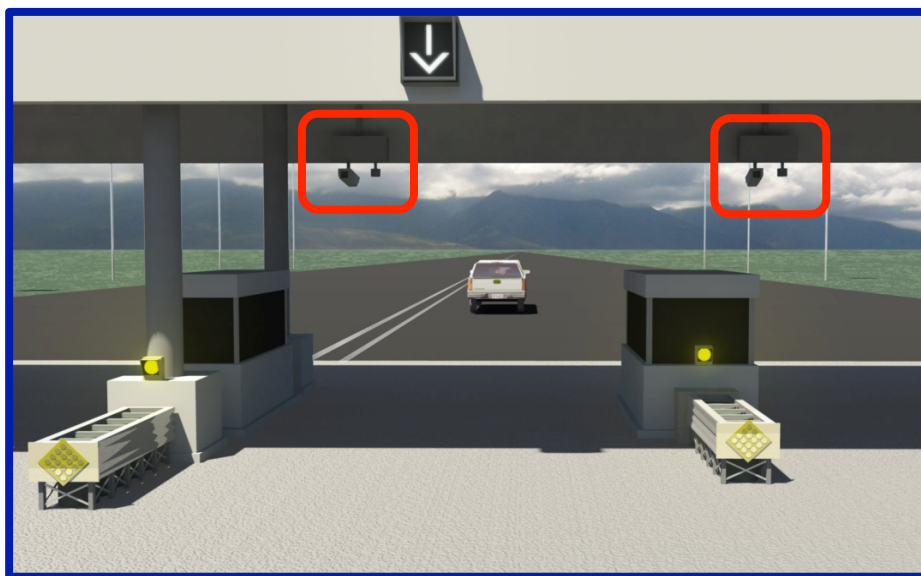


On Site ON-OFF tests confirm surrendered GPS RFI source on April 29, 2010

**Period of several months to locate
1 GPS jammer!**



Additional IDM Concepts



- **Integrated with Camera System**
- **Alert Enforcement Personnel to Jammer Presence**
- **Detect & Track Jammers Approaching Entry Point**
- **Multi-Lane Distinction**
- **UNITRAC Database Connection**



Outline



- **Discussion of Proposed Spectrum Protection Efforts**
- **Case Study: Newark Airport (EWR) Event**
 - **Detection**
 - **Analysis**
 - **Testing**
 - **More Testing**
 - **Even More Testing**
 - **Findings**
- **Additional IDM and Test Events**
- **Conclusions**



Additional Test Events



- **Civil Focus, Test/Training; June 18 – 22, 2012**
- **746th Test Squadron Support**
- **1st open air transmission using Commercial Jammers**
- **Training Opportunity**
- **Capability Testing**
- **Encourage participant collaboration**
- **Multiple scenarios, moving targets**
- **Jammer Characterizations**



PNT Collaboration Sites



Homeland Security Information Network

Welcome to HSIN


User Name:
Password:

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use or access of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following: You have no reasonable expectation of privacy when you use this information system; this includes any communications or data transiting or stored on this information system. At any time, and for any lawful government purpose, the government may, without notice, monitor, intercept, search and seize any communication or data transiting or stored on this information system. The government may disclose or use any communications or data transiting or stored on this information system for any lawful government purpose, including but not limited to law enforcement purposes. You are NOT authorized to process classified information on this system.

DO NOT PROCESS CLASSIFIED INFORMATION ON THIS SYSTEM

U.S. Department of Homeland Security

PNTIP Application Login Page



Login Email:
Password:

[Change password?](#) [Lost password?](#)

Warning: This is a Federal Aviation Administration (FAA) computer system. [1370.79a](#)

This computer system, including all the related equipment, networks and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. FAA computer systems may be monitored for all lawful purposes, to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify the security of this system.

During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this FAA computer, authorized or unauthorized, constitutes consent to monitoring of this system.

Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.



Conclusions



- **US is actively pursuing threat monitoring**
 - **Open Architecture**
 - **Scalable**
 - **Crosses Organizational Boundaries**
- **Recent real-world case study**
 - **Highlight difficulties in observation and attribution**
 - **Demonstrates success**
- **This is just the beginning**