

PATRIOT WATCH

INTERFERENCE DETECTION MITIGATION (IDM)

VIGILANCE

SAFEGUARDING AMERICA

**DHS Position, Navigation & Timing (PNT)
Program Management Office
John Merrill – Program Manager**

August 14, 2012



Interference Detection & Mitigation (IDM) per NSPD 39

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

December 15, 2004

FACT SHEET

The President authorized a new national policy on December 8, 2003, that sets the vision 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 Security 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 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.

For purposes of this document:

- "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

augmentations, and deny adversaries access to any space-based positioning, navigation, and timing services, particularly including services that are openly available and can be readily used by adversaries and/or terrorists to threaten the security of the United States. In addition, the diverse requirements for and multiple applications of space-based positioning, navigation, and timing services require stable yet flexible policies and management mechanisms. The existing management mechanisms for the Global Positioning System and its augmentations must be modified to accommodate multi-use applications and program planning, resource allocation, system development, and operations. Therefore, the United States Government must improve the policy and management framework governing the system worldwide;

system has grown into a global utility whose multi-sector economic growth, transportation safety, and of the worldwide economic infrastructure. In the increasing importance of the Global Positioning System, the deliberate degradation of accuracy for military, scientific, commercial, and other purposes is considered to threaten their respective national and global positioning, navigation, and timing signals in the critical infrastructure sectors of U.S. critical infrastructure.

As the system continues, the positioning, navigation, and timing services provided by the Global Positioning System remains critical to U.S. national and economic security. The system is used into virtually every facet of U.S. military operations, navigation, and timing services. The Global Positioning System presents a critical infrastructure of the United States. The system is used in many of the systems inherently vulnerable to threats, and the system is used in many of the systems inherently vulnerable to threats, and the system is used in many of the systems inherently vulnerable to threats.

The Global Positioning System presents a critical infrastructure of the United States. The system is used in many of the systems inherently vulnerable to threats, and the system is used in many of the systems inherently vulnerable to threats, and the system is used in many of the systems inherently vulnerable to threats.

maintain the Global Positioning System, and deny adversaries access to any space-based positioning, navigation, and timing services, particularly including services that are openly available and can be readily used by adversaries and/or terrorists to threaten the security of the United States. In addition, the diverse requirements for and multiple applications of space-based positioning, navigation, and timing services require stable yet flexible policies and management mechanisms. The existing management mechanisms for the Global Positioning System and its augmentations must be modified to accommodate multi-use applications and program planning, resource allocation, system development, and operations. Therefore, the United States Government must improve the policy and management framework governing the system worldwide;

- 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 and its augmentations in order to benefit civil, commercial, and scientific users worldwide.

3
stations to support their continued ability to meet their requirements.

Ensure that the United States maintains space-based positioning, navigation, and timing services, including augmentation, back-up, and service denial to ensure the availability of positioning, navigation, and timing services for national, homeland, and economic security, and to deny adversaries access to any space-based positioning, navigation, and timing services that exceed or are equal to those provided by the Global Positioning System and its augmentations, and to promote U.S. technological leadership in applications, development, and timing services. To achieve this goal, the

space-based global, precise positioning, navigation, and timing services and capabilities through the system, and to ensure that the system is dependent on foreign positioning, navigation, and timing services. To achieve this goal, the system is used in many of the systems inherently vulnerable to threats, and the system is used in many of the systems inherently vulnerable to threats, and the system is used in many of the systems inherently vulnerable to threats.

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; and to promote plans to modernize the U.S. space-based positioning, navigation, and timing infrastructure, including: (1) development, deployment, and operation of new and/or

- 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

and its augmentations and address mutual interests and deny hostile use of space-based positioning, navigation, and timing services and systems, and to ensure that the system is dependent on foreign positioning, navigation, and timing services. To achieve this goal, the system is used in many of the systems inherently vulnerable to threats, and the system is used in many of the systems inherently vulnerable to threats, and the system is used in many of the systems inherently vulnerable to threats.

Navigation, and Timing Services

Space-Based Positioning, Navigation, and Timing Services will be co-chaired by the Deputy Secretaries of the Department of Transportation or by their designated representatives at the equivalent level from the Department of Defense, the Joint Chiefs of Staff, the National Security Council, the National Security Council Staff, the Office of Management and Enterprise, the Office of Economic Security Council staff, the Office of Economic Security Council staff, shall participate as an of the Federal Communications Commission Liaison Committee as a Liaison. The Secretaries of Defense and the Committee shall operate.

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; and to promote plans to modernize the U.S. space-based positioning, navigation, and timing infrastructure, including: (1) development, deployment, and operation of new and/or

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; and to promote plans to modernize the U.S. space-based positioning, navigation, and timing infrastructure, including: (1) development, deployment, and operation of new and/or

- 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



Existing and Emerging Threats



Apple Accessories Computers & Peripherals Cell Car Electronics Security & Surveillance Entertainment Health & Lifestyle Cameras & Photo Batteries & Chargers 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\$73.98~~
US\$ 36⁹⁹

50% off

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 Lepo's range of signal jammers & blockers.

Four small images showing different models of signal jammers and blockers. Each image includes a 'No GPS' icon and a 'No Signal' icon.

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](#)

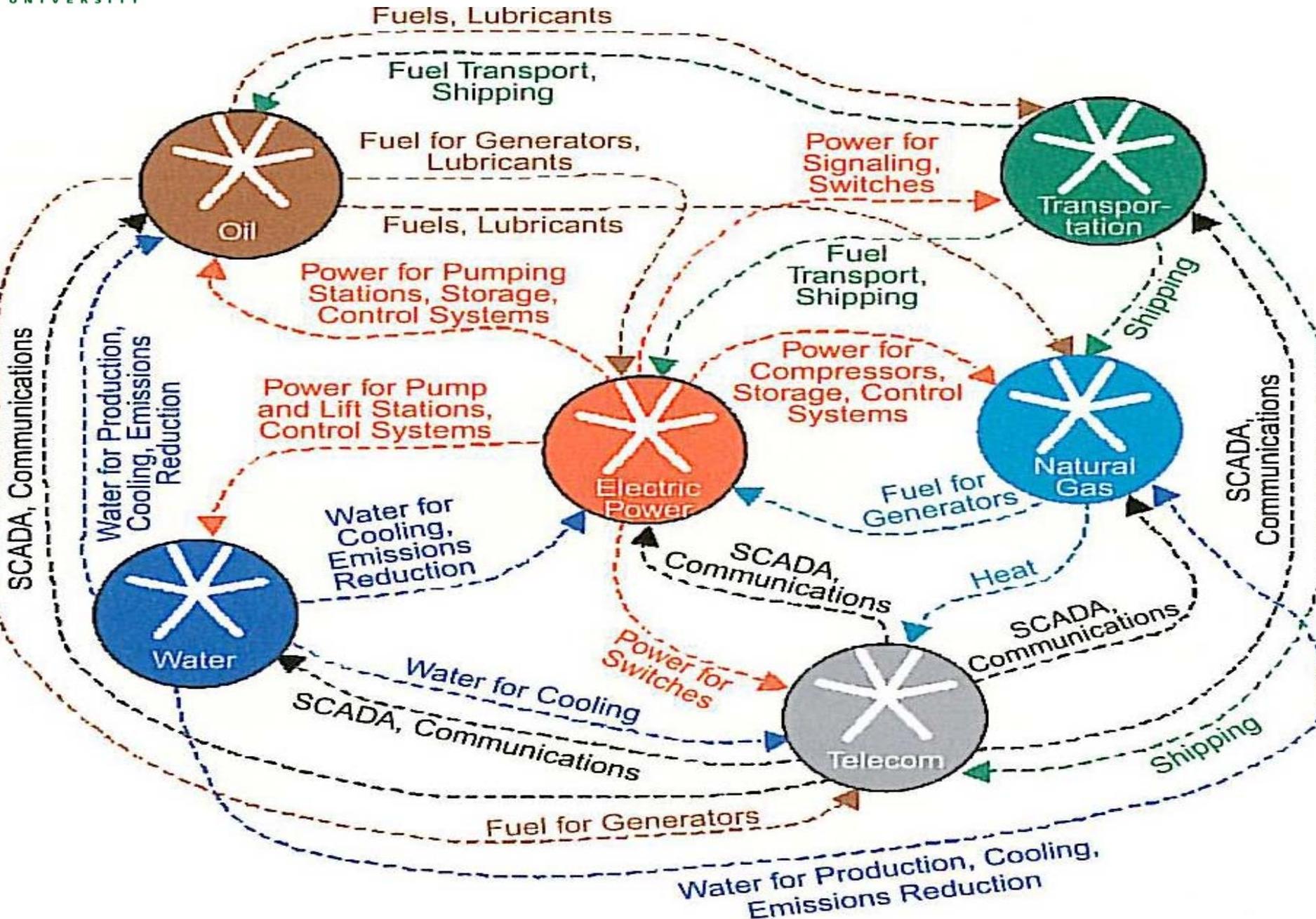


[Transportation Systems](#)



[Water](#)





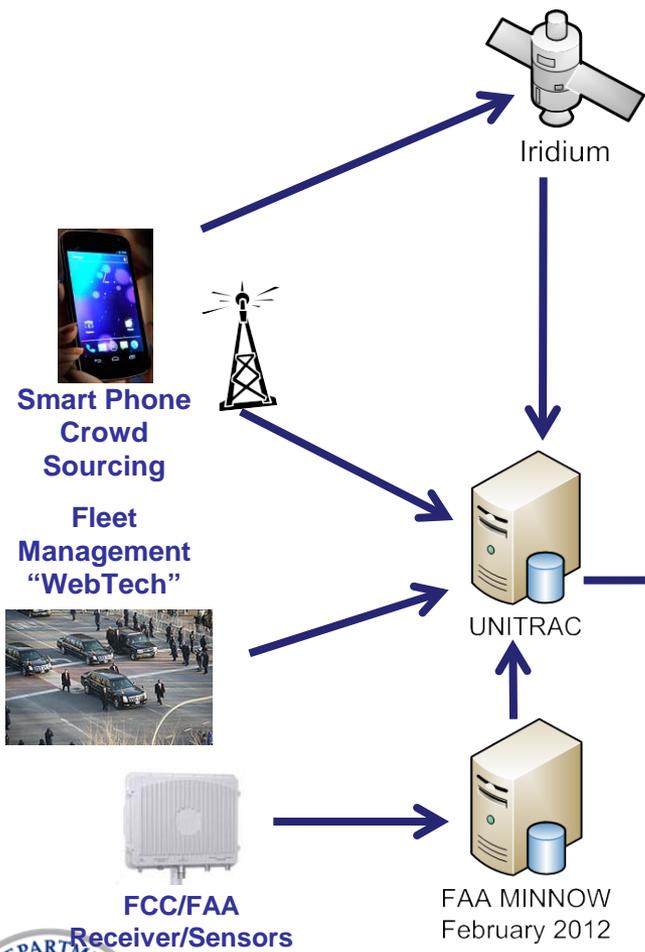
Patriot Watch Initiative

- **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



Patriot Watch Architecture

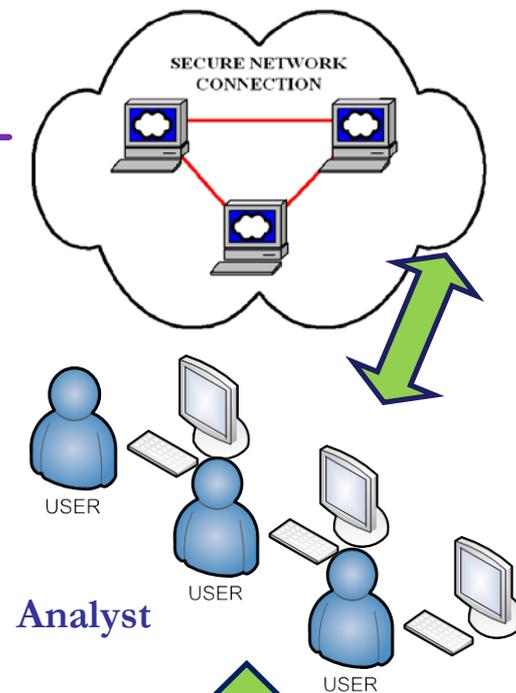
Monitoring & Collection



Processing



Analysis & Evaluation



J-Alert
CTL-3500



PNT Monitor overview

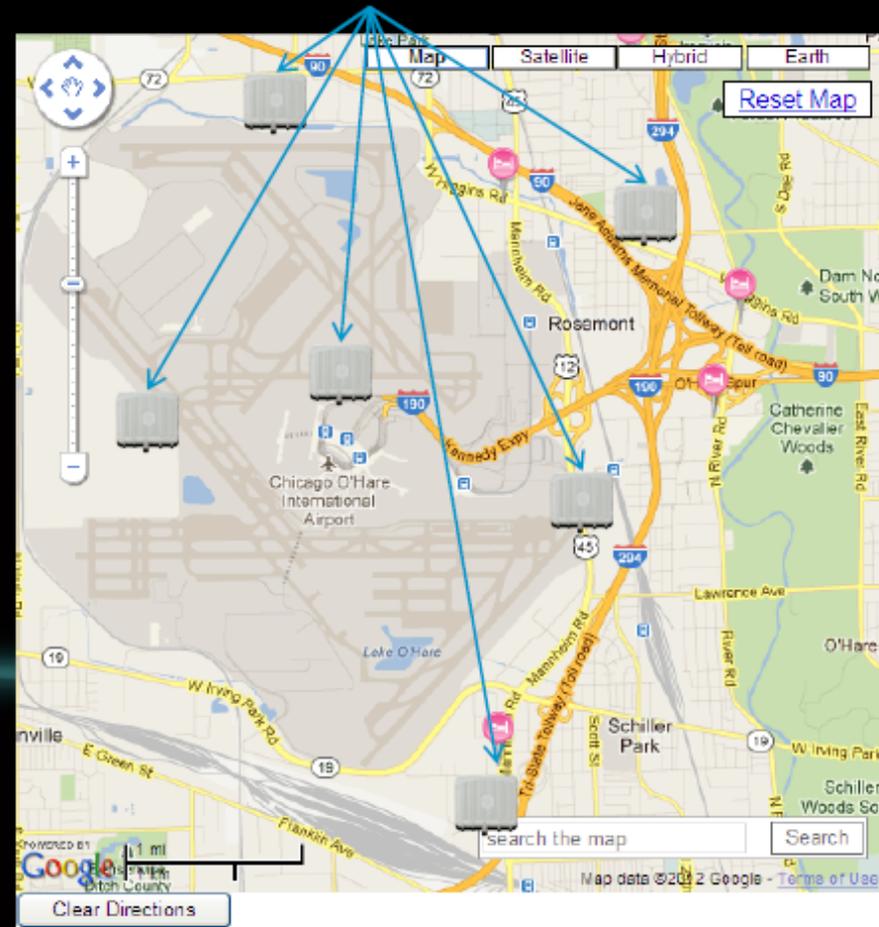
Agilent 'minnow' system: typical hardware installation

PNT monitor locations selected to detect illegal transmitters along common access routes adjacent to sensitive PNT support equipment.

Information is networked back to central monitoring and alert via UNITRAC.

Information monitored and acted on by FAA agents.

PNT Monitoring points (Agilent N6841A)

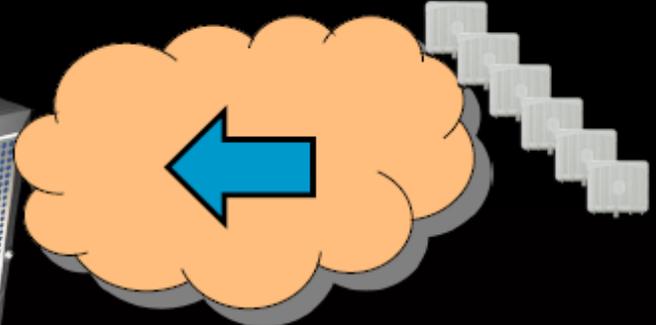
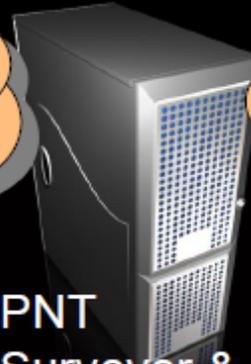
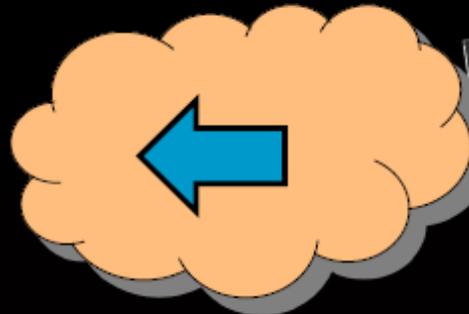
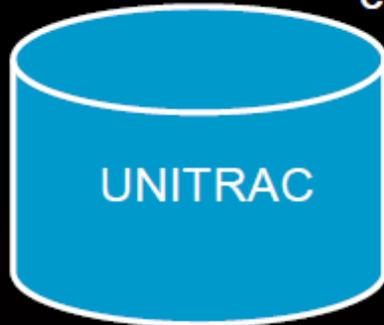


PNT Monitor overview

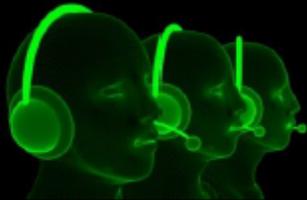
Agilent 'minnow' system: software architecture

Alarms formatted into
common UNITRAC messages

PNT Monitor Points



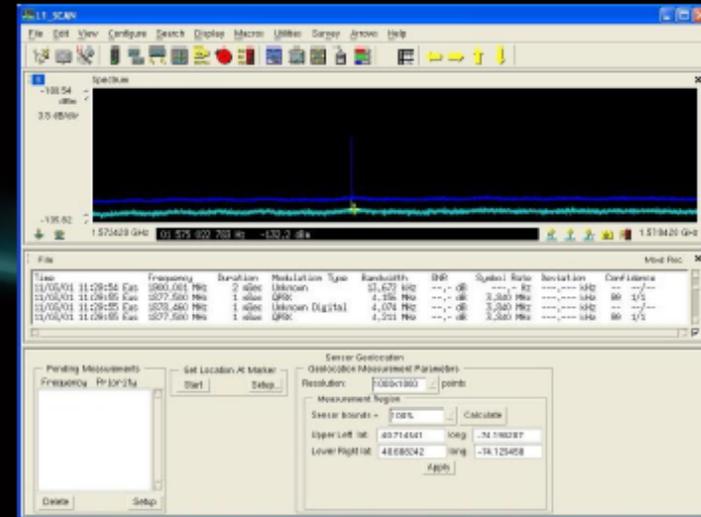
UNITRAC Analysts



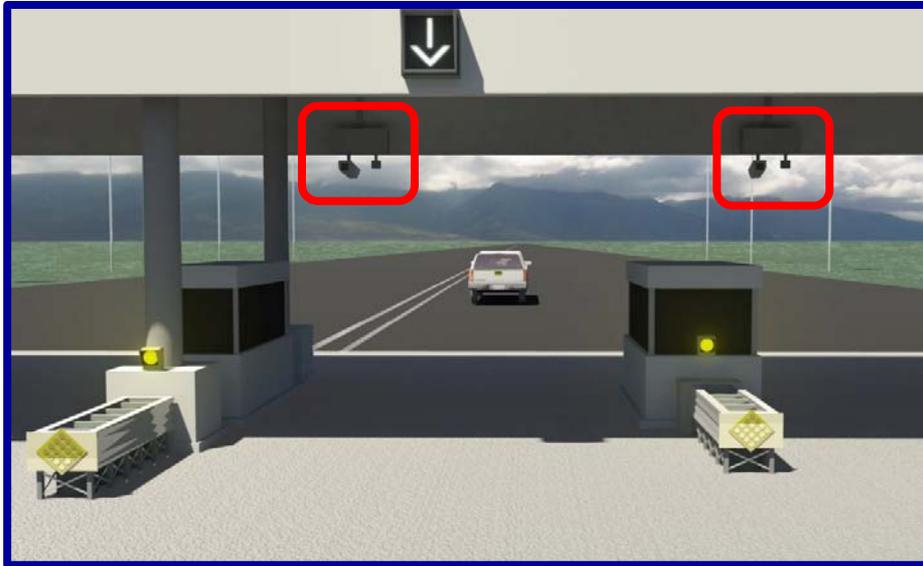
PNT
Surveyor &
Location
Server

Agilent Signal Surveyor SW

Agilent GEO Server SW



Jammer Geo-Location Port Of Entry Concept



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



chronos

TECHNOLOGY



J-ALERT

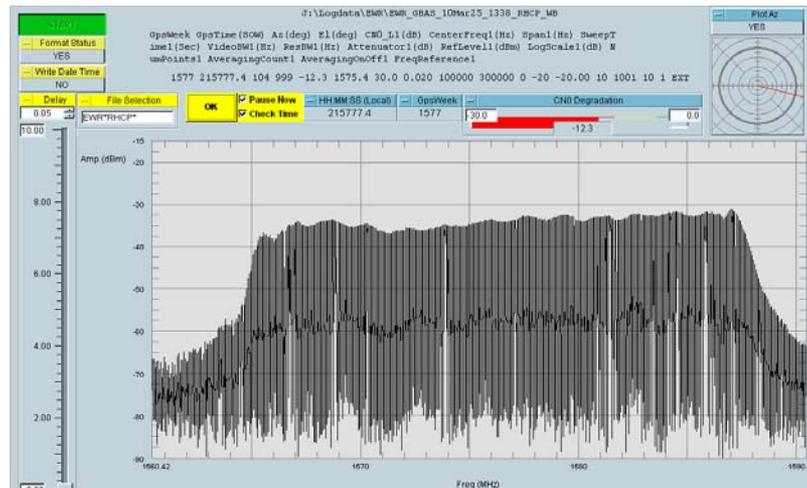
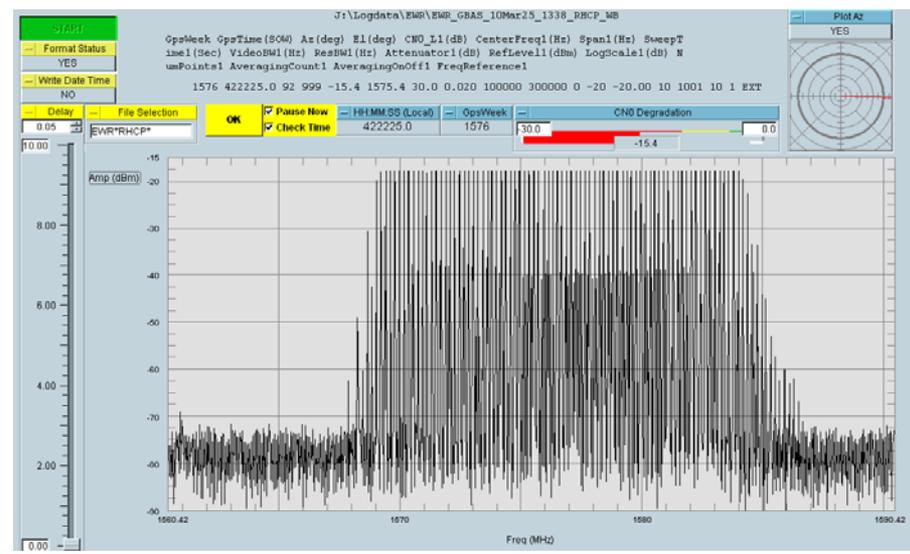
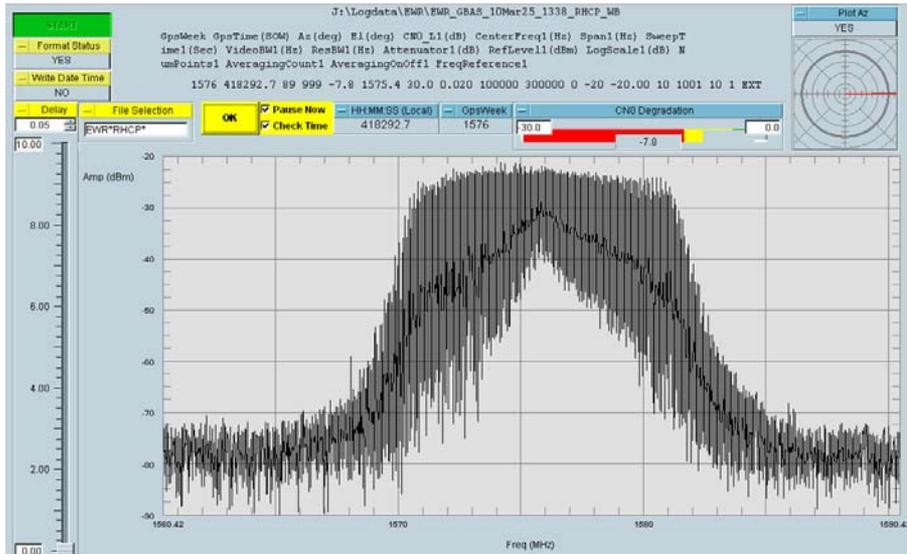
Radio Frequency Jammer Detector

DYPLEX
COMMUNICATIONS LTD

brimtek

A black rectangular device with three antennas on top, labeled "J-ALERT" and "DYPLEX". It has several indicator lights and buttons on the front panel.A black and white police car with a J-ALERT device mounted on its roof. The car has "POLICE" written on the side and a license plate. In the background, there is a road with other vehicles and hills.Two red prohibition signs (a circle with a diagonal line) over a drone and a mobile phone, indicating jamming or detection of these devices.

GPS Jammer Source Signal Characteristics – Digital Library



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.

Conclusion

- **FAA, FCC, DHS and other Government agencies working closely to address PNT IDM**
- **Collaboration and teamwork is key to successful PNT IDM**
- **Leverage existing mature technologies and collaborate to obtain interference data**
- **Collecting data to support formal analysis; trends on jammers**
- **Research is underway for alternative sources of time**



QUESTIONS?

John.Merrill@dhs.gov

(202) 447-3731 PNT PMO

(202) 731-9628 Mobile

