GPS Timing in Critical Infrastructure

IEEE/NIST Timing Challenges in the Smart Grid Workshop

October 26, 2016

Sarah Mahmood
Program Manager
First Responders Group
Science and Technology Directorate

Our Economy Depends on Critical Infrastructure, & Our Infrastructure Depends on GPS

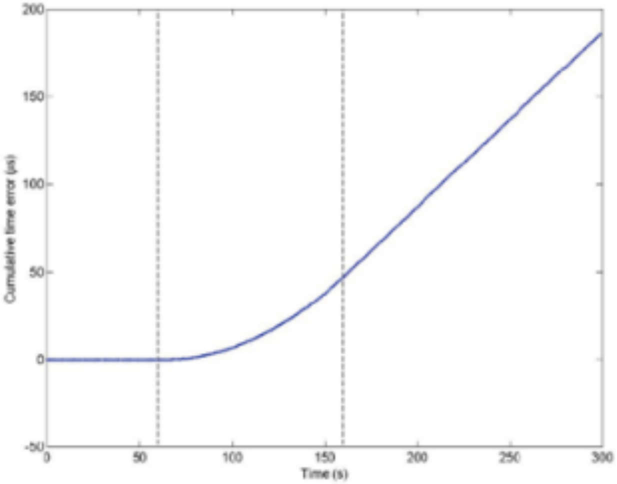
- **Usage**: Accurate position, navigation and timing (PNT) information is necessary for the functioning of many critical infrastructure sectors
  - Precision timing is particularly important
  - Primary source of distributed and accurate timing is currently through GPS
- **Problem**: GPS susceptible to disruption (both intentional and unintentional)
  - Newark/I-95 jamming incident
  - January 25, 2016 event
  - Jamming for criminal activity
  - North Korea
- **Impacts:**
  - Not well understood
  - Evolving

Homeland Security

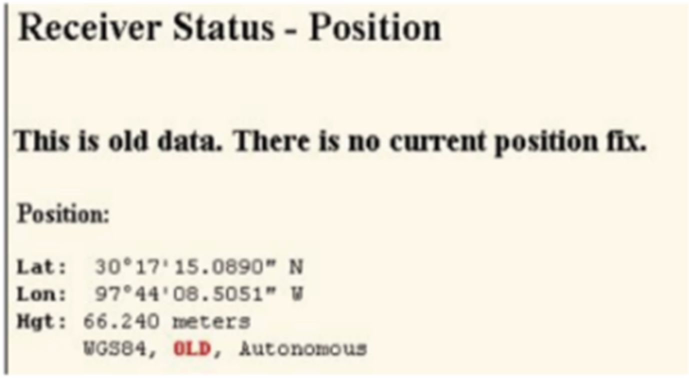
Science and Technology

Initial GPS Receiver Testing Results

- In 2014, DHS tested a small sample of GPS receivers to evaluate performance against various attacks
- All receivers tested were vulnerable with varying responses



Receiver time drifts approximately 75 microseconds in 100 seconds – orders of magnitude higher than allowed by its oscillator



Receiver Status - Position

This is old data. There is no current position fix.

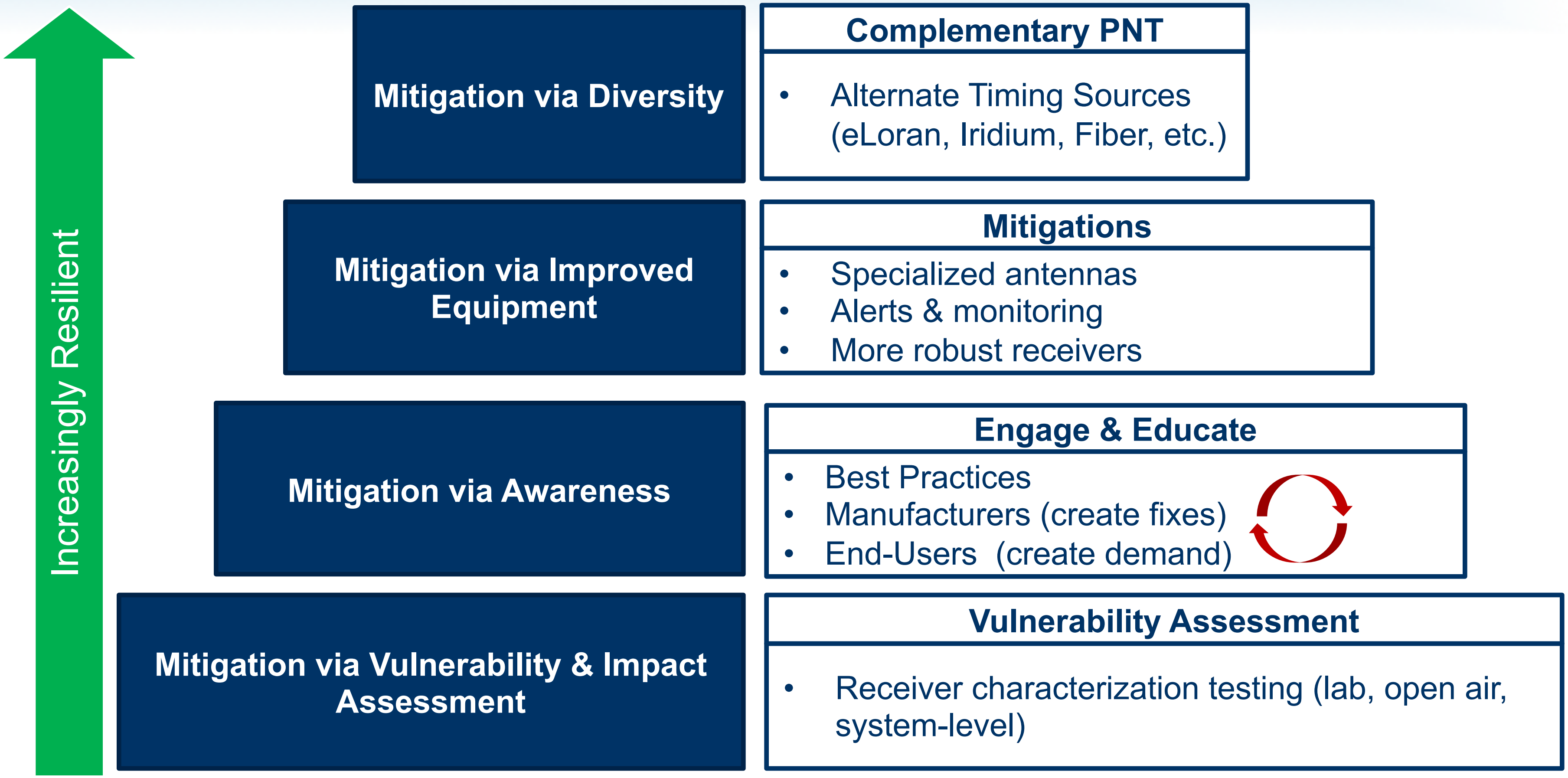
Position:

```
Lat:  30°17'15.0890" N
Lon:  97°44'08.5051" W
Hgt: 66.240 meters
     WGS84, OLD, Autonomous
```

Figure 14: Receiver fails to respond to true GPS data after receiving spoofed future data

DHS Risk Management & Program Strategy

Holistic view with a layered approach



Increasingly Resilient

Mitigation via Diversity

Complementary PNT

- Alternate Timing Sources (eLoran, Iridium, Fiber, etc.)

Mitigation via Improved Equipment

Mitigations

- Specialized antennas
- Alerts & monitoring
- More robust receivers

Mitigation via Awareness

Engage & Educate

- Best Practices
- Manufacturers (create fixes)
- End-Users (create demand)

Mitigation via Vulnerability & Impact Assessment

Vulnerability Assessment

- Receiver characterization testing (lab, open air, system-level)

Homeland Security

Science and Technology

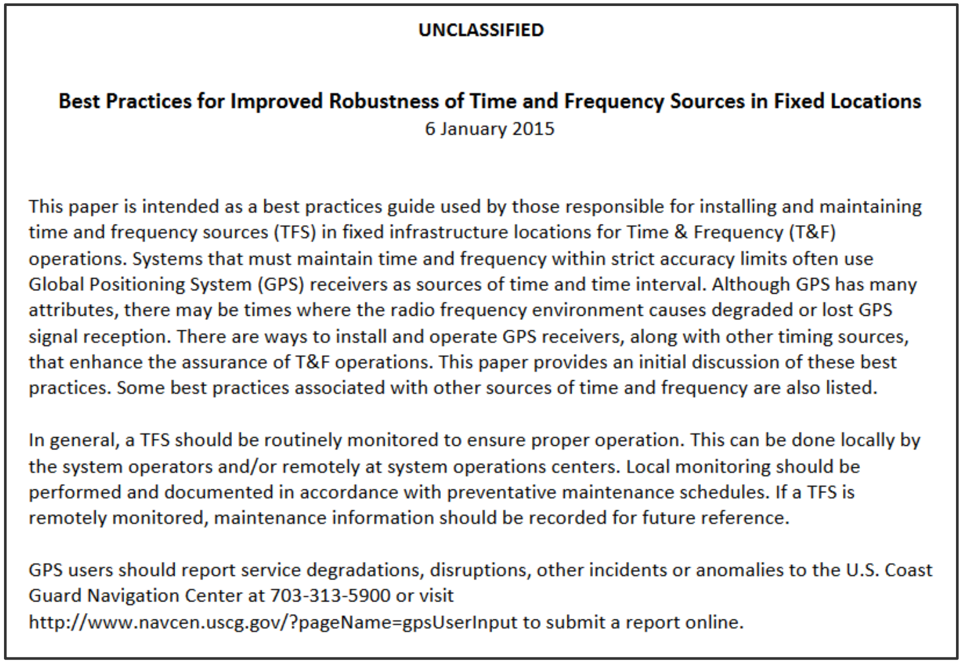
Vulnerability Assessment & Awareness: WSMR Exercise Overview

- **Purpose**: Conducted live testing and demonstrations of first responder communications in electronic jamming threat environment provided by White Sands Missile Range, including:
  - First responder communications systems against commercial jamming
  - Anti-jamming technologies against commercial jamming
  - Satellite communications against commercial jamming
  - Unmanned Aircraft Systems (UAS) against DoD complex GPS and commercial jamming
  - Fixed timing receivers (used in critical infrastructure) against DoD complex GPS and commercial jamming
- **Outcomes**: Understand impact of electronic threats on first responder communications and mission operations; identify training gaps and mitigation strategies; and share lessons learned and best practices with first responders nationwide

WHITE SANDS MISSILE RANGE
BIRTHPLACE OF AMERICA'S MISSILE & SPACE ACTIVITY
Homeland Security

Awareness:
Best Practices "Time & Freq Sources"

- "Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations"
  - Issued January 6, 2015 via US-CERT
  - https://ics-cert.us-cert.gov/sites/default/files/documents/Best%20Practices%20-%20Time%20and%20Frequency%20Sources%20in%20Fixed%20Locations_S508C.pdf



UNCLASSIFIED

Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations
6 January 2015

This paper is intended as a best practices guide used by those responsible for installing and maintaining time and frequency sources (TFS) in fixed infrastructure locations for Time & Frequency (T&F) operations. Systems that must maintain time and frequency within strict accuracy limits often use Global Positioning System (GPS) receivers as sources of time and time interval. Although GPS has many attributes, there may be times where the radio frequency environment causes degraded or lost GPS signal reception. There are ways to install and operate GPS receivers, along with other timing sources, that enhance the assurance of T&F operations. This paper provides an initial discussion of these best practices. Some best practices associated with other sources of time and frequency are also listed.

In general, a TFS should be routinely monitored to ensure proper operation. This can be done locally by the system operators and/or remotely at system operations centers. Local monitoring should be performed and documented in accordance with preventative maintenance schedules. If a TFS is remotely monitored, maintenance information should be recorded for future reference.

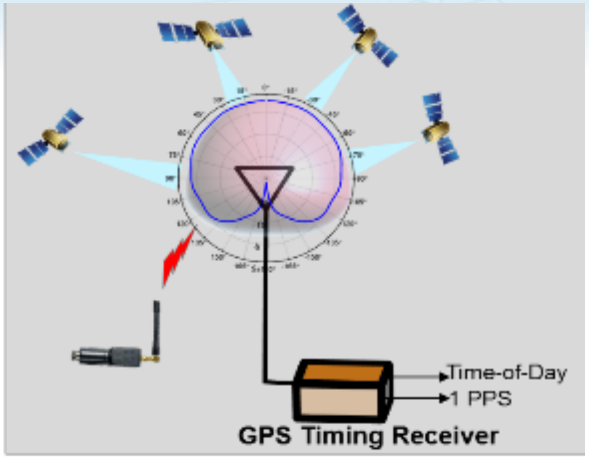
GPS users should report service degradations, disruptions, other incidents or anomalies to the U.S. Coast Guard Navigation Center at 703-313-5900 or visit http://www.navcen.uscg.gov/?pageName=gpsUserInput to submit a report online.

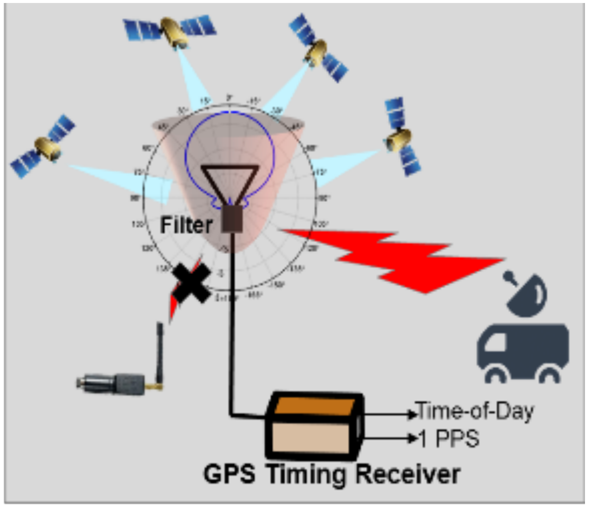
Awareness:
Best Practices “Time & Freq Sources”

- Receiver Guidance:
  - “If the receiver has the capability, record average signal strength/Automatic Gain Control level once the stabilization is complete as a benchmark to be checked during routine maintenance.”

- Antenna Guidance:
  - “Place the antenna where it cannot be seen from publically accessible locations, or deny view of the antenna from public locations using an RF-transparent material… place the antenna where a roof line or structure blocks direct line of sight to the antenna from publically accessible locations.”

Improved Equipment: Horizon Ring Nulling Timing Antenna



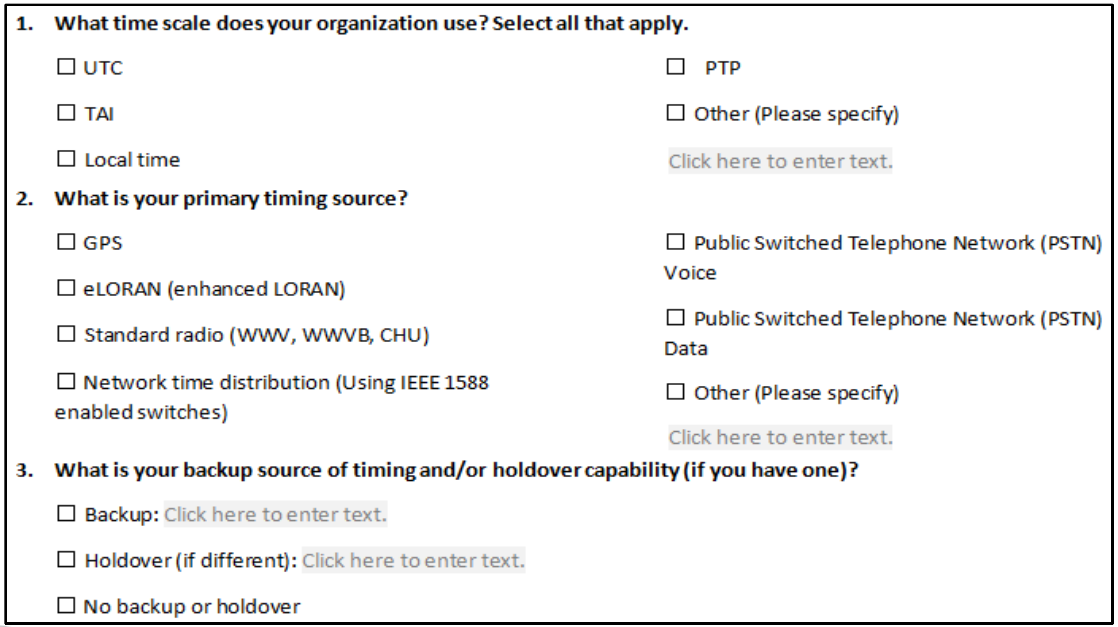


- Wide variety of threats to fixed site GPS timing receivers
  - Unintentional interference: e.g., spectrum encroachment and out-of-band RF interference
  - Intentional interference
  - Interference sources tend to be below antenna mounting
- MITRE’s *low cost* horizon ring nulling (HRN) helix timing antenna
  - Reduces impact of interference and multipath slightly above to below the horizon
  - Antenna design available for commercial transition via *no cost* license agreement

Diversity: CPNT Requirements

- **Purpose**
  - Define and validate PNT requirements with end-users in critical infrastructure sectors

- **Approach**
  - Engage directly with CI end-users for input
  - Initial focus on electricity and wireless communications



1. **What time scale does your organization use? Select all that apply.**

☐ UTC

☐ TAI

☐ Local time

☐ PTP

☐ Other (Please specify)

Click here to enter text.

2. **What is your primary timing source?**

☐ GPS

☐ eLORAN (enhanced LORAN)

☐ Standard radio (WWV, WWVB, CHU)

☐ Network time distribution (Using IEEE 1588 enabled switches)

☐ Public Switched Telephone Network (PSTN) Voice

☐ Public Switched Telephone Network (PSTN) Data

☐ Other (Please specify)

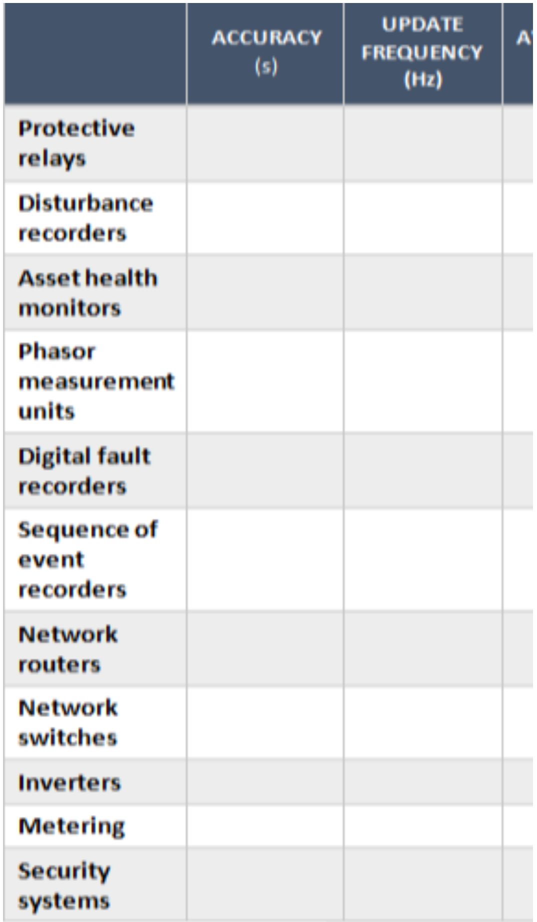
Click here to enter text.

3. **What is your backup source of timing and/or holdover capability (if you have one)?**

☐ Backup: Click here to enter text.

☐ Holdover (if different): Click here to enter text.

☐ No backup or holdover



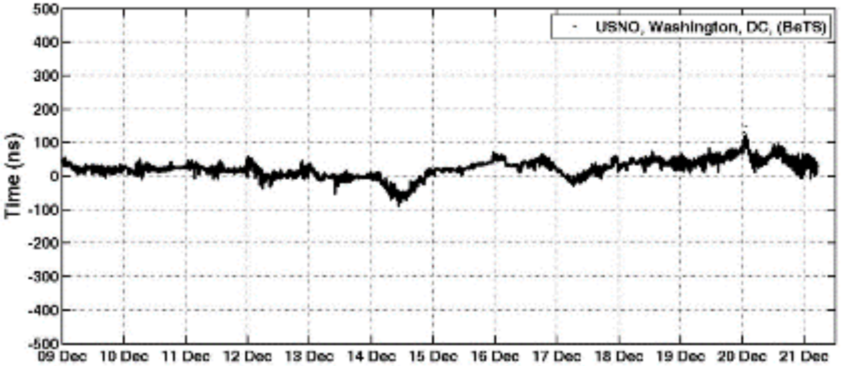
	ACCURACY (s)	UPDATE FREQUENCY (Hz)	A
Protective relays			
Disturbance recorders			
Asset health monitors			
Phasor measurement units			
Digital fault recorders			
Sequence of event recorders			
Network routers			
Network switches			
Inverters			
Metering			
Security systems			

Homeland Security

Science and Technology

Diversity: Explore Technologies

- Study and test potential other technologies to provide PNT solutions for critical infrastructure applications
  - eLoran
    - NYSE Demonstration (April 19, 2016)
      - eLoran signal successfully received inside building to within 30 nanoseconds of UTC reference where GPS signals were not receivable



  - Iridium
    - Testing conducted October 17-20 at Savannah River National Lab
  - BAA call for additional technologies (closed August 12)
    - Under review

Supporting R&D Opportunities

- S&T Assured Timing BAA (closed August 12, 2016)
  - "Assured Timing for Critical Infrastructure" (BAA Call HSHQDC-15-R-B0008)
    - https://www.fbo.gov/index?id=c5f6e8a9ab7242b322d2ed8879241e26
- Technical Topic Areas
  - TTA #1: Development of Assured Timing Technologies
    - Develop assured timing technologies for critical infrastructure, including prototype development and testing that can provide robust timing inputs to critical infrastructure
  - TTA #2: System-Level Testing & Analysis to Understand Impacts
    - Provide a fundamental baseline understanding of risk profile of timing disruptions to critical infrastructure through system-level testing and analysis to understand both short- and long-term (30+ days) impacts of undetected manipulation or denial of timing service disruptions to key critical infrastructures
  - TTA #3: Development of Timing Manipulation Detection Capabilities
    - Develop detection capabilities for timing issues specific to critical infrastructure, including prototype testing and results, which can be easily integrated into existing operations

Homeland Security

Science and Technology