Does Anyone Really Know What Time It Is?

Dr. Michael L. Cohen, MITRE

October 15, 2013

MITRE

Abstract

This presentation was delivered at the North American Electric Reliability Corporation's annual security conference GridSecCon'13 on October 15, 2013.

It describes the importance of timing to North American power grid operations. It focuses specifically on timing provided by GPS, and covers four topics in relation to the power grid:

- Timing Dependency
- Threats to Timing
- Timing Threat Mitigation Measures; and
- Proposed Goals for Resilient Timing.

MITRE

The Problem: Disruption or Manipulation of Time

Source: http://www.ejumpcut.org/archive/jc52.2010/pramaggiore911/

MITRE

Topics

Recognizing the power grid is a *real-time* system, we address four topics related to time:

- **Timing Dependency**
- **Timing Threats**
- **Timing Mitigation Measures**
- **Proposed Resilient GPS Timing Goals**

Timing Dependency

Key Terms Defined

- **Time-of-Day:*** a single time of day that can referenced globally; also known as coordinated universal time (UTC).
- **Clock:*** the internal hardware and software that maintains time of day in a computer or intelligent microprocessor device.
- **Time Interval**: a unit of time duration such as one second. The constant rhythm of a clock.
- **Clock Synchronization:** Setting all clocks to the same time of day to within a specified tolerance of a reference clock time (UTC) and the same time interval (rate of advancement).
- **Time Resolution:*** The smallest increment of time to which a measurement can be distinguished.

*Adapted from NERC "Time Stamping of Operational Data Logs"

Timing Dependency (II):
Power Grid
Time-Dependent Equipment & Networks

Phasor Measurement Unit

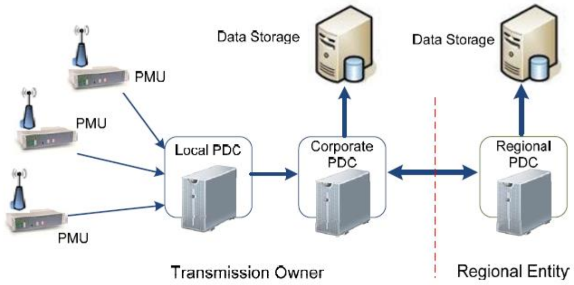
TW Fault Locator

Quality of Power Supply

Lightning Strike Measurement

Disturbance Monitoring Event Recorder

Protective Relay



Synchrophasor Network

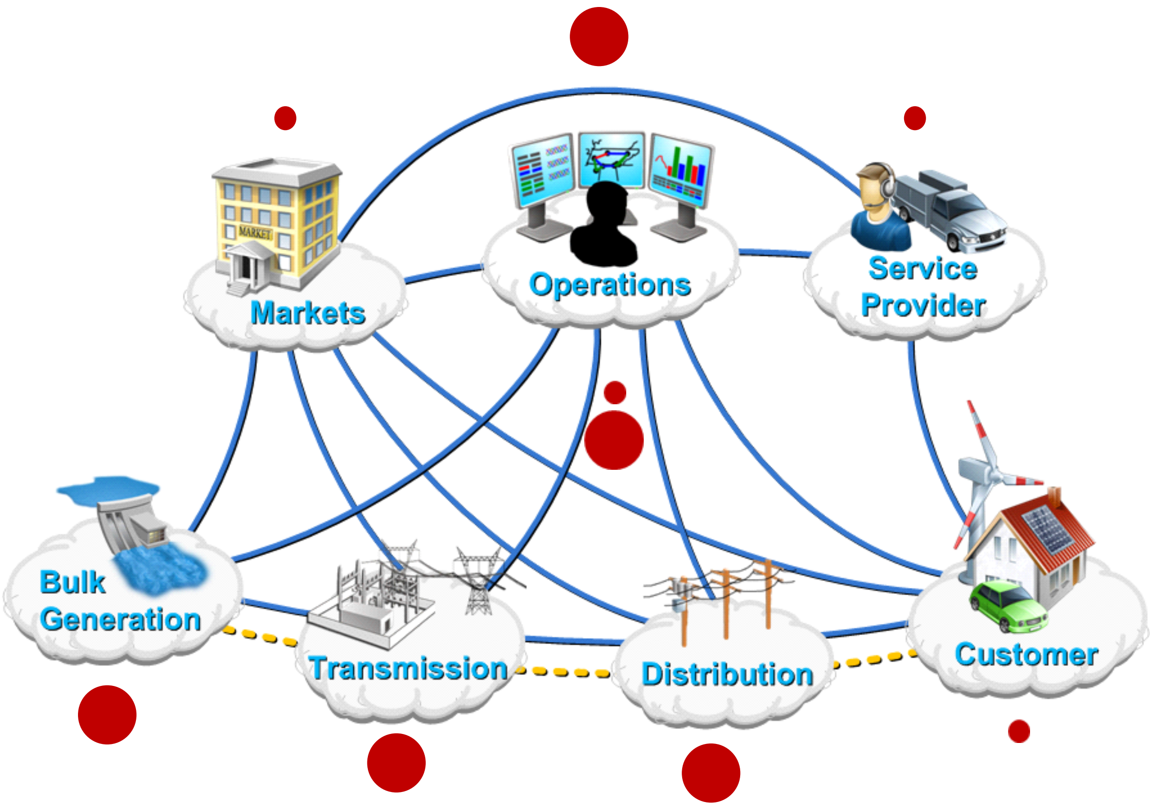
Control Center/EMS

Timing Dependency (III):
GPS: A Great Clock Setter and Synchronizer

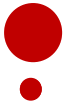
GPS Synchronizes Clocks Across the Globe

MITRE

Timing Dependency (IV):
Timing Dependencies
Across the Power Grid/Smart Grid



Key:



= Strong Timing Dependency

= Medium Timing Dependency

MITRE

Timing Dependency (V): Summary

- **All portions of the Power Grid/Smart Grid have timing dependencies**
  - Ranges over six orders of magnitude from 1 microsecond (10^{-6} s) to 1 second
- **Many, but not all, timing dependencies are met by GPS timing**
  - Other timing sources include local crystal oscillators (clocks) and time servers that obtain and distribute timing from external sources such as NIST's ACTS, WWV, or WWVB broadcasts
- **Portions of Power Grid/Smart Grid utilizing GPS timing include: Generation, Transmission, Operations, and Distribution**
  - Those portions are the portions where any disruption would be the most consequential for power grid operations
- **Based on findings from DHS GPS NRE, few timing backups exist today in the Energy Sector, including the Power Grid**
- **Both major and moderate opportunities to enhance GPS/Position, Navigation, Timing (PNT) resilience across the Power Grid/Smart Grid**

Threats & Potential Vulnerabilities

Threat Taxonomy

- **Unintentional**
  - RF Interference
  - Space Weather/ Geomagnetic Storm
- **Intentional**
  - Jamming
  - Spoofing

http://www.nyc.gov/html/oem/html/planning_response/planning_all_hazards.shtml

Threats & Potential Vulnerabilities (II)
Unintentional RF Interference

TV Pre-Amplifier GPS Interference
Moss Landing, California, JAN'03

- **Characterization:**
  - Intermittent
  - Isolated incidents

Duration of Event: Days to Months

GPS World
The Business and Technology of Global Navigation and Positioning

GNSS System | Consumer OEM | Professional OEM | Survey | Machine Control / Agriculture | Transportation | Defense | Government

Log in | Print | Email

Home > GNSS System > Signal Processing
Related topics: Emergency Response, Marine, Security & Surveillance

Home
Blogs
Inside GPS World
Opinions
Resources
How to Contact
Subscribe

RSS
Member Login
Site Feedback

CAREER LOCATOR
GPS World CAREER LOCATOR Job Tracking Made Easy
Search for the job of your choice:
Keywords:
search

INDUSTRY-SPONSORED WHITE PAPERS
Check out our white papers! Current white papers and their sponsors include:

Averna:
GPS Record and Playback System
Cast Navigation:
Guided Munitions Testing
F-16/CAST 3000
First American Spatial Solutions:
Identifying The Right Tax Jurisdiction: Data

Signal Processing

The Hunt for RFI

January 1, 2003
By: Wilbur R. Vincent, Richard W. Adler, Paul McGill, James R. Clynch, George Badger, Andrew A. Parker
GPS World

Unjamming a Coast Harbor

In April, 2001, the captain of the research vessel PT SUR, based in Moss Landing, California, made a radio telephone call from at-sea to one of the authors, stating that signal reception of GPS in the whole of Moss Landing Harbor was jammed. He was advised to contact the U.S. Coast Guard (USCG) and the Federal Communication Commission (FCC). When the problem persisted for another month, we launched an effort at the local level to determine the cause of the jamming.

A view from the location of an unintentional GPS jammer across Moss Landing Harbor to the Monterey Bay Aquarium Research Institute. A GPS receiver with its antenna on the other side of the roof was continuously jammed for months.

Moss Landing is a moderate-sized harbor about 100 kilometers south of San Francisco, in the middle of Monterey Bay. It has a mixed fleet of working fishing boats, pleasure craft, and three large research vessels used by the local scientific community.

The Naval Postgraduate School (NPS), with a large program in science and engineering, is located at the south end of Monterey Bay. The Monterey Bay Aquarium Research Institute (MBARI) has its headquarters in Moss Landing and two major research vessels berthed there. This organization supports the Monterey Bay Aquarium and also has a large engineering program, especially in underwater remotely operated vehicles.

MBARI has used GPS for precision location of their vessels since the early 1990's, before the U.S. Coast Guard set up their system of DGPS stations along the coast. MBARI, with assistance from NPS, set up a differential station at their location at Moss Landing, using a UHF data link to send the corrections to their vessels.

Locations of the RFI emitter and MBARI; power plant upper right

After the April jamming report, NPS set up a monitor of the MBARI DGPS corrections to log the number of satellites being tracked. This clearly showed that the station was being heavily jammed. Reports of other GPS users in Moss Landing confirmed that it was a jamming issue and not a faulty receiver.

FIGURE 2 search bearing for Source-1
Click to enlarge image.

The jamming had impacted MBARI in several ways, including causing it to loose its GPS-based high-accuracy time reference. It would have caused difficulty at the narrow harbor entrance in fog. In at least two cases it caused small-boat owners to buy new GPS receivers, only to find they still could not get GPS in and around Moss Landing. One of the major ships in the harbor paid for a technician and new equipment to fix the problem, but finally had to turn off GPS in the harbor area, give the alarm that GPS was off line, and use radar only for harbor entrances in bad weather.

The GPS signal that feeds the MBARI reference station was also distributed to several laboratories and offices in the MBARI headquarters building, through a series of splitters and inline amplifiers. In an office with one of these drops, we set up a high-quality spectrum analyzer to examine the energy in a wide band about the GPS L1 frequency. Because there were several long cables and amplifiers between the antenna and the spectrum analyzer, the signals were not calibrated at the time they were taken. Later the system was calibrated. Figure 1 shows an example of the data recorded with a clear peak from the radio frequency

MITRE

Threats & Potential Vulnerabilities (III): Space Weather/Geomagnetic Storm

- **Characterization:**
  - Correlated to 11-year solar cycle
  - Bombards satellites with relativistic particles in near-earth environment
    - May cause premature satellite failure (rare)
  - Radio scintillation causes GPS signal degradation on all satellite signals
    - May cause degradation or complete PNT failure for hours, with some events lasting for days

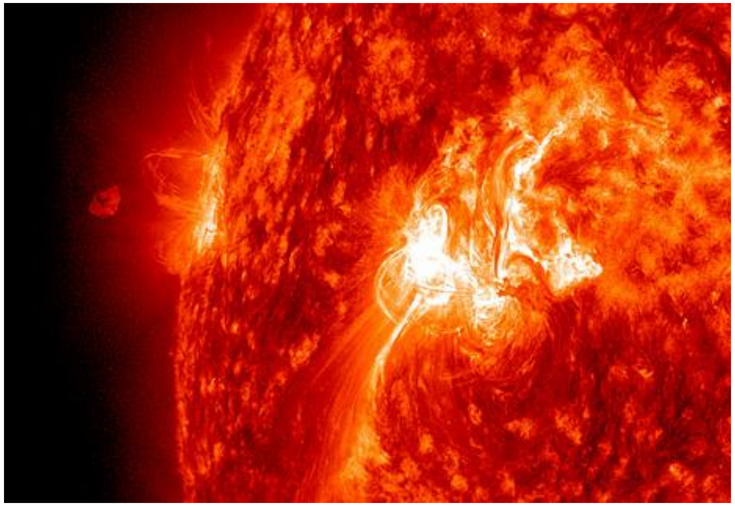


Photo: Solar Dynamics Observatory/NASA

Duration of Event: Several days

Threats & Potential Vulnerabilities (IV): Intentional Threats

2001 DOT Volpe Report

"[a]s GPS further penetrates into the civil infrastructure, it becomes a tempting target that could be exploited by individuals, groups, or countries hostile to the U.S."

Threats & Potential Vulnerabilities (V): Jamming: Types

Definition: Deliberate drowning out of legitimate PNT signals using higher power signals to cause loss of satellite lock and to prevent reacquisition.

Source: GPS NOTAMS (Notice to Airmen) from http://silvereage.blogspot.com/2011_02_01_archive.html

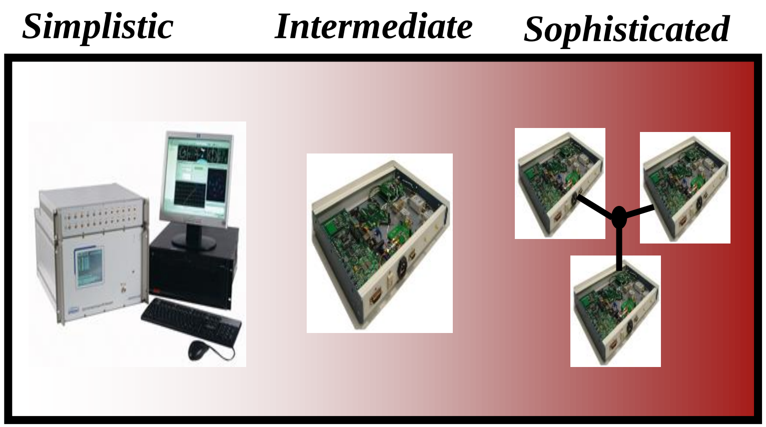
Types:

- **Tone – Single frequency broadcast within a GPS band**
- **Swept tone – A tone whose frequency is swept over a range of frequencies in a GPS band**
- **Matched spectrum – A interference signal with the same modulation characteristics as the signal being targeted**
- **Filtered noise – Amplified noise that is filtered to a bandwidth commensurate with the signal being targeted**

Duration of Event: Days to Weeks

Threats & Potential Vulnerabilities (VI): Spoofing: Types

- Spoofing (I): the deliberate emitting of legitimate-appearing false signals to shift arbitrarily the computed position or time of a victim's receiver
- Spoofing (II): a type of spoofing in which GPS signals are precisely controlled and transmitted so as to produce a predetermined false navigation and/or false timing solution in the victim's receiver.



Commercial Signal Simulator | Portable Software Radio | Multiple Phase-locked Spoofers

Source: Humphreys, *Assessing the Civil GPS Spoofing Threat,* 2008

Duration of Event: Days to Weeks

MITRE

Threats & Potential Vulnerabilities (VII): Threats Reveal Need for Holdover/Backups

Durations of threat events indicate need for Holdover Times/Backups within critical infrastructure lasting at least several days (e.g., 72 hours)

- RF Interference
- Space Weather/Geomagnetic Storm
- Jamming
- Spoofing

Threats & Potential Vulnerabilities (VIII): Potential Vulnerabilities

Potential Vulnerabilities Include:

– Lack of threat detection/alarming for users
– Lack of long holdover timing backups
– Lack of resilience to threats

MITRE

Timing Mitigation Measures

Perfect Time versus Good Enough Time:
The Trade Space

- In theory, there are two ways to always have perfect time:
  - 1. Obtain *perfect* clocks
  - 2. Continuously *set* clocks
  - Neither are possible
  - Engineers must balance "clock quality" and "clock setting"
- Example Cesium versus "GPS disciplined" inexpensive clock…

Outstanding Clock
Time reset every 10 years
Cost: $50,000

Low-Cost Alternative

Mediocre Clock + GPS
Time reset every 10 seconds
Cost: Less than $1,000

GPS Synchronized Clocks are Ubiquitous

Timing Mitigation Measures (II): Low Cost/Best Practices for Anti-Jamming

Anti-Jamming Measures

- First:
  - Identify mission-critical systems dependent on GPS timing
  - Assess *jamming* risks to and from those GPS-dependent systems
- Then implement measures such as:
  - Hiding the antenna from direct view
  - Orienting antenna to favor high elevation angles
  - Using choke ring/CRPA antennas
  - Adding jamming alarms and failover to holdover timing sources
  - Acquiring dual-frequency GPS receivers (2016)/ multi-frequency, multi-platform GNSS receivers

Sample of Commercial Technology Based on Advertisements (Unverified Claims)

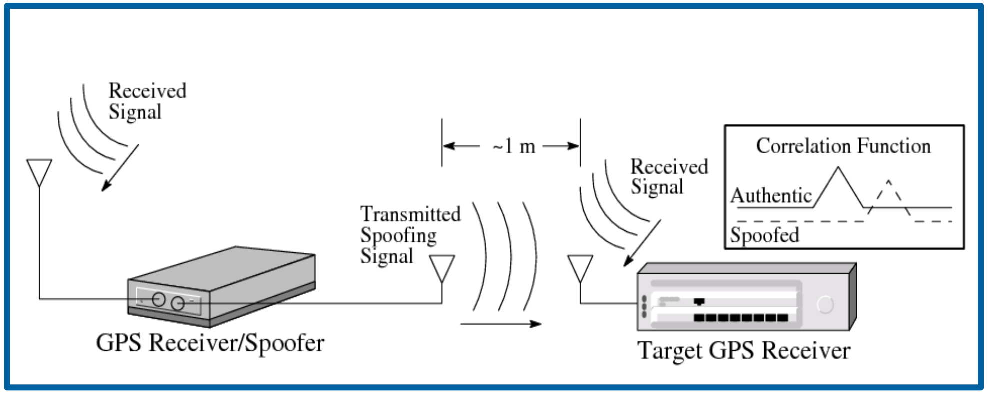
Manufacturer/Product	Description in Manufacturer Advertisement
C-Nav 3050	Patented interference rejection
Geodetics Inc. Geo-DL	Extreme noise and interference rejection
GlobalTop Tech AntiJACK™	GPS jammer detection and notification
Inventek models	Built-in jamming detection and mitigation
Javad models	In-Band interference rejection
Leica Viva SmartTrak	Jamming resistant
Navcom models	Superior interference suppression both in-band and out-of-band
Navis Core GNSS	Uses sharp channel separation of GPS NAVSTAR and SNS GLONASS to secure advanced jam-protection
Navman units	Jupiter modules outperform competitors in close proximity to RF noise sources
Septentrio models	Advanced interference monitoring and mitigation successfully protects receivers against in-band continuous wave and pulsed interference signals
SiRFstarIV GSD4t	Reliable choice for difficult environments; active jammer remover, tracks up to 8 continuous wave jammers
Spirit DSP	Excellent resistance to interference," "EMI suppression"
u-blox	An advanced, proprietary adaptive digital filtering technology which actively suppresses interference

Source: MITRE

Timing Mitigation Measures (III): Low Cost/Best Practices for Anti-Spoofing

Anti-Spoofing Measures

- First:
  - Identify mission-critical systems dependent on GPS timing
  - Assess *spoofing* risks to and from those GPS-dependent systems
- Then implement measures such as:
  - Hiding the antenna from direct view
  - Monitoring received signal strength and constancy; spoofed signals are constant and relatively strong
  - Monitor acquisition times of all received signals (they should be different)
  - If a *fixed* receiver shows it has *moved* it indicates re-radiator/ repeater spoofing

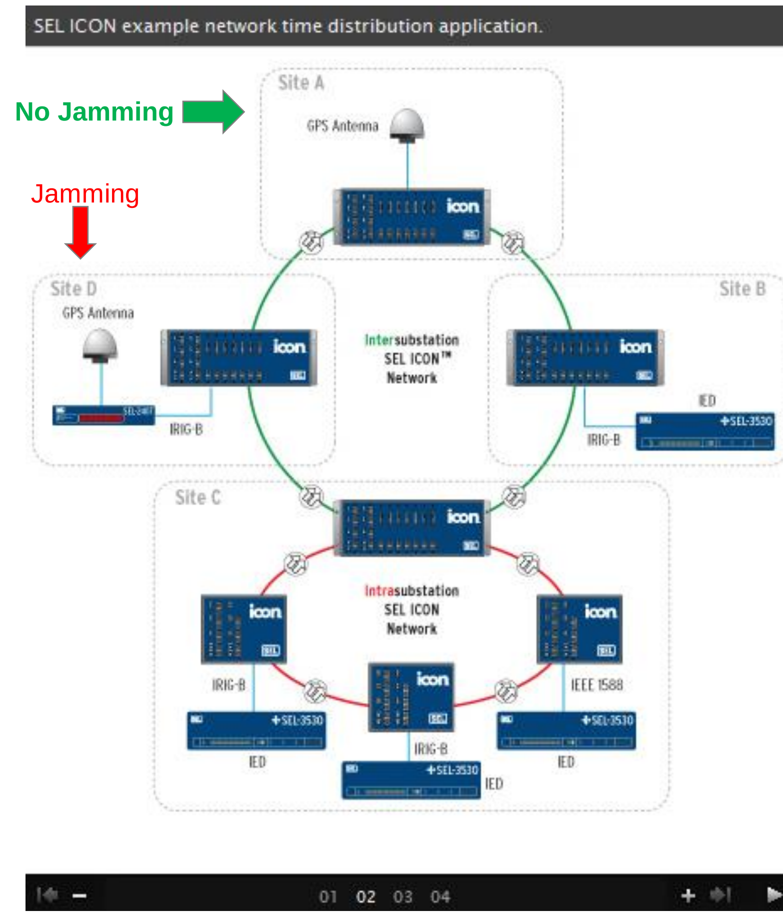


Source: Humphreys, "Assessing the Civil GPS Spoofing Threat," 2008

MITRE

Timing Mitigation Measures (IV): Emerging Anti-Loss/Anti-Jamming Technology

- **SEL ICON System**
  - Referenced in NERC *Extended Loss of GPS Impact on Reliability* White Paper
  - Terrestrial distribution of precise time via multiplexed fiber-optic communications systems
  - “Distribute time over a wide-area network (WAN) with better than 1 microsecond accuracy so that very accurate relative time is maintained in the event of a GPS failure.”
  - May be able to circumvent localized jamming

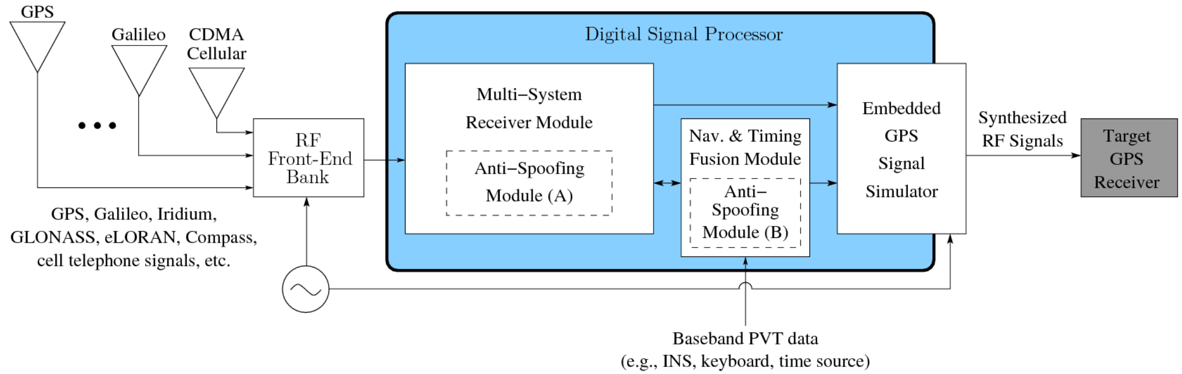


[Source: https://www.selinc.com/ICON/](https://www.selinc.com/ICON/)

MITRE

Timing Mitigation Measures (V):
Emerging Anti-Jamming/Anti-Spoofing Technology

- **University of Texas/Coherent Navigation – GPS Assimilator/In-Line Anti-Spoofing Device**



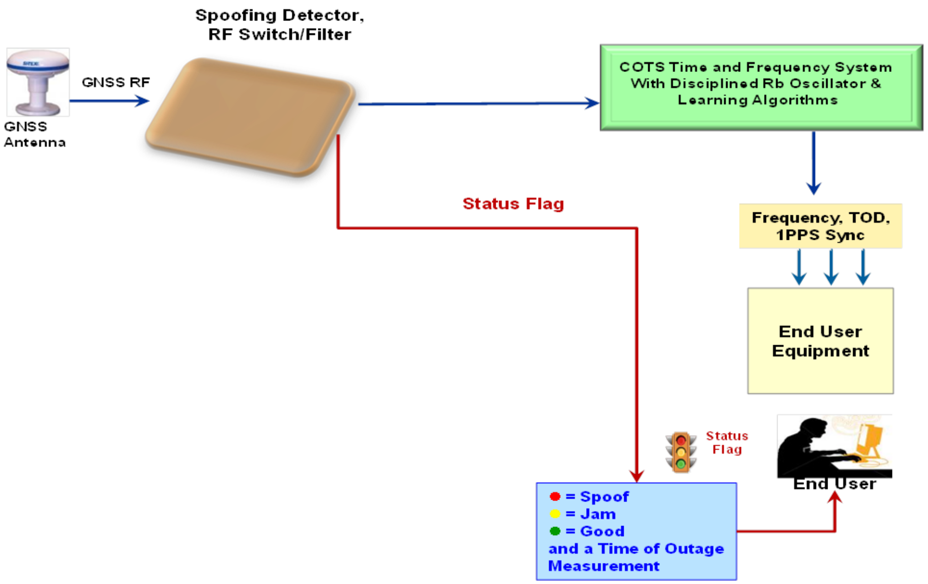
  - Weak-signal tracking
  - RF Interference robustness
  - Spoofing resistance
  - No hardware or software modifications to GPS receiver required

Source: “The GPS Assimilator: A Method for Upgrading Existing GPS User Equipment to Improve Accuracy, Robustness, and Resistance to Spoofing”, ION, 2010; Also: http://coherentnavigation.com/an-in-line-anti-spoofing-device-for-legacy-civil-gps-receivers/

| 21 |

Timing Mitigation Measures (VI): Emerging Anti-Jamming/Anti-Spoofing Technology

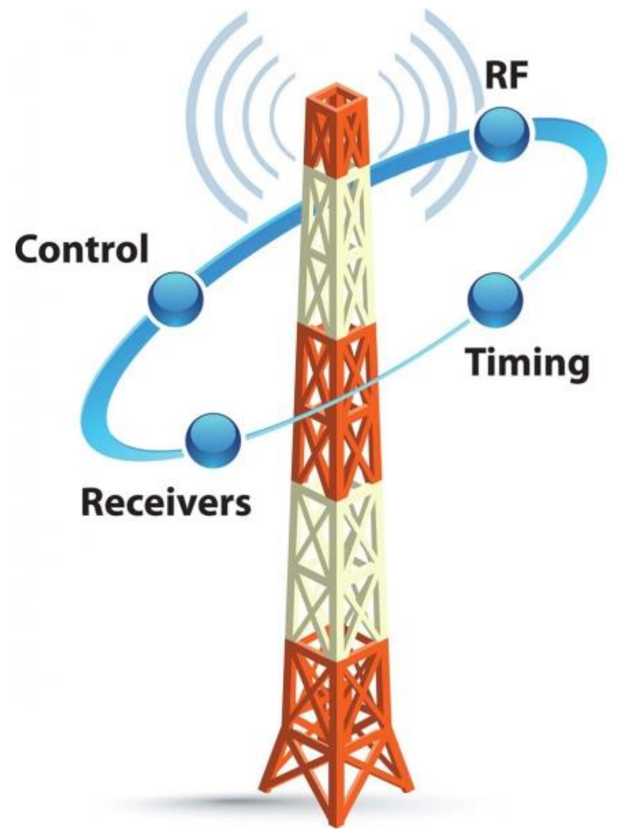
- **MITRE/SEDI prototype under development:**
  - Detects jamming and spoofing
  - Alarms user
  - Potentially reports to NERC, DOE and/or DHS for threat geolocation
  - Mitigates via failover to high-stability atomic clock
- **After Lab testing, prototype will be pilot tested in the field and transitioned to commercial vendors**



Source: MITRE/SEDI

Timing Mitigation Measures (VII): Longer-Term Timing Alternatives

- **Leveraging emerging Communications Sector carrier synchronous Ethernet (SyncE) – Timing is pulled from comms**
- **Implementing a commercial Low Frequency Terrestrial Wide-Area Timing System (aka eLORAN)**



Source: http://www.ursanav.com/

MITRE

Proposed Resilient GPS Timing Goals

- **Develop GPS time and frequency systems (TFS) that detect, warn of, and resist both unintentional and intentional GPS threats. Upon threat detection, GPS TFS should failover to internal or known valid external timing sources.**

- **Employ multiple layers of backup capabilities, mitigation strategies, and contingency plans to provide protection against GPS timing loss, manipulation, and its critical infrastructure impacts.**

Questions or Comments?

Dr. Michael L. Cohen
Principle CI Systems Engineer
(703) 983-7372
mlc@mitre.org

MITRE