Critical Infrastructure Vulnerabilities to GPS Disruptions

DHS S&T Efforts

4 June 2014

Sarah Mahmood
Program Manager
Resilient Systems Division
Homeland Security Advanced Research Projects Agency
Science & Technology Directorate

Homeland Security
Science and Technology

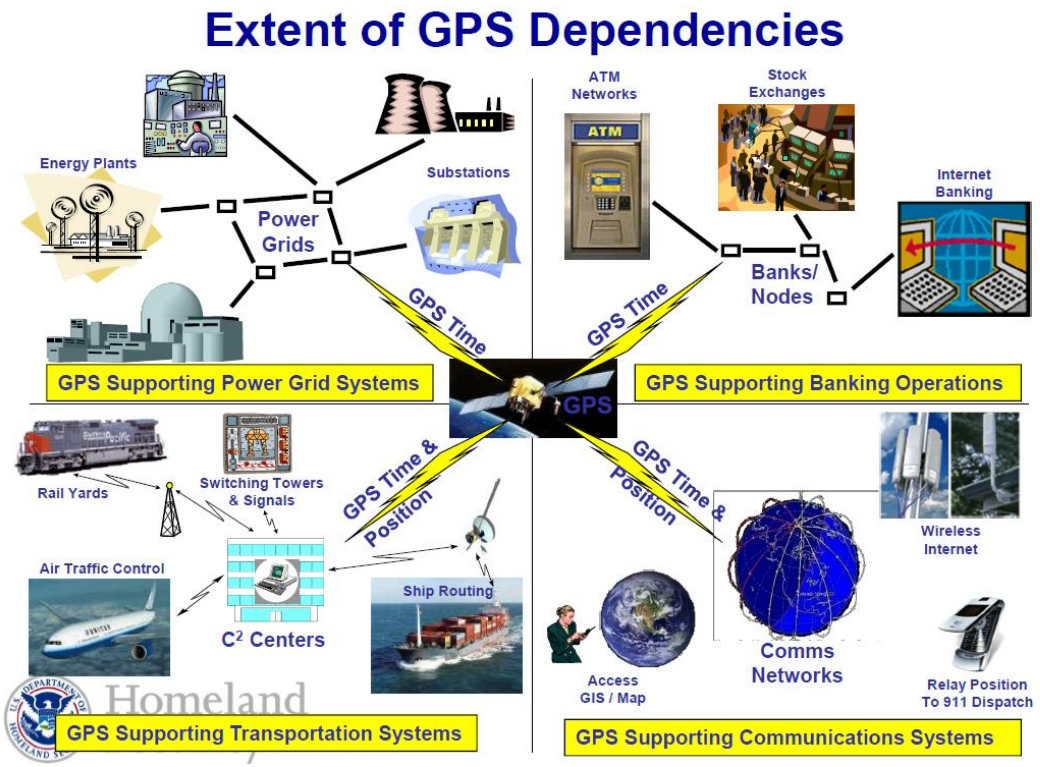
Homeland Security
Science and Technology

Operational Need

Critical Infrastructure (CI) reliance on civil GPS and impact of interference is largely unknown

- Civil GPS now plays a critical role in modern telecommunications, banking and finance transactions, and electrical power grid operations as a precise and accurate timing source.
- The majority of our 16 critical infrastructure sectors would be impacted by an extended GPS signal timing loss

- GPS jamming and/or GPS spoofing could have significant impacts on critical infrastructure operations
  - The threat continues to grow as GPS jammers, though illegal, are available for sale on the internet. GPS spoofers can be made, inexpensively, with a little know-how.
    - Recent real-world events and research initiatives have demonstrated significant CI vulnerability and potential impact from low to medium tech, low cost disruptive devices in the aviation and energy sectors.
  - Example of known impact:
    - Phasor Measurement Units (PMUs or Phasors) used for situational awareness & synchronization on the electric grid rely on GPS signals for critical timing information. Experiments show that the timing signal can be spoofed, which could have catastrophic impacts on the grid.



Homeland Security
Science and Technology

FFRDC Deep Dives (MITRE)

- Objective: To develop a detailed understanding of the current implementation of civil GPS and the level of CI sector reliance within the *electricity subsector* of the energy sector and the *communication sector*, to quantify the associated sector specific vulnerabilities, and to assess potential sector specific and cross-sector threat mitigation technologies and methodologies.

- Study broken down to the following elements
  1. Baseline Electrical subsector and Communication sector GPS dependencies
  2. Determine Threats and Vulnerabilities
  3. Evaluate detection and mitigation technologies
  4. Develop Deep-Dive Methodology Framework

Homeland Security
Science and Technology

Electric Sector Results

- MITRE Findings and Recommendations from Baseline Study
  - Today's grid + 5 years out
  - Timing dependent equipment includes
    - Transmission line fault detection, synchrophasors, substation control/synchronization, protective relays, frequency measurement, disturbance monitoring event recorders, bulk metering, customer premise metering, smart meters, quality of power supply measurement, EMS tools, distributed energy sources
  - Timing requirements throughout the grid vary from 1s to < 1µs
  - GPS primary reference for wide-area synchronization at 1µs level across the grid
  - Few, if any, timing backups with more than a few hours of holdover time at the 1 µs level exist

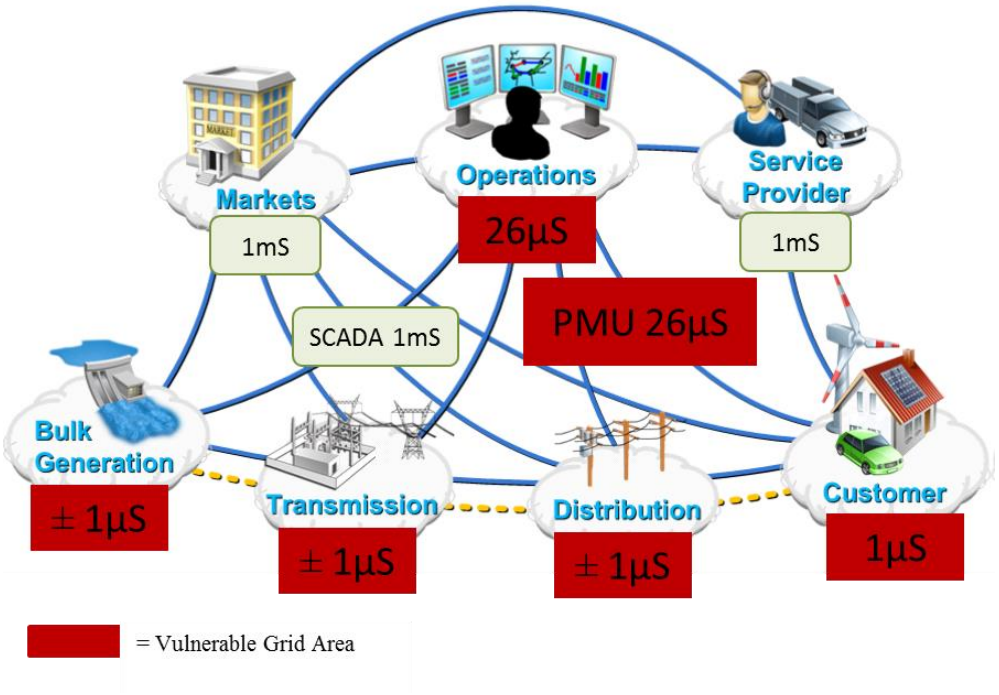
Table 8. Quantification of Timing Requirements for Power Grid/Smart Grid Domains

Equipment / Function	Power Grid/Smart Grid Domains						
	Gen.	Trans.	Dist.	Ops.	Market	Serv. Prov.	Cust.
Transmission Line Fault Location		1 µs					
Synchrophasors/Phasor Measurement Units	< ±1 – 46.3 µs	< ±1 – 46.3 µs	< ±1 – 46.3 µs				
Substation Control/ Re-Synchronization		1 µs – 1 ms	1 µs – 1 ms				
Protective Relays		1 ms	1 ms				
Lightning Strike Measurement		1 ms	1 ms				
Quality of Power Supply Measurement			1 ms			1 ms	1 ms
Control Center/ EMS/SCADA/RTU	1 ms	1 ms	1 ms	1 ms			
Frequency Measurement		1 ms		1 ms			
Internet-based Market Transactions (NTP)				1 ms	1 ms		1 ms
Disturbance Monitoring Event Recorders		2 ms	2 ms				
Bulk Metering	0.5 sec	0.5 sec	0.5 sec				
Customer Premise Metering						1 sec	1 sec
Smart Meters/Home Area Network						0.5 sec	0.32 ms
Distributed Energy Resources			< ±1 – 46.3 µs				< ±1 – 46.3 µs
SCADA Networks	1 ms	1 ms	1 ms	1 ms			
Synchrophasor Networks	<26 µs	<26 µs	<26 µs	<26 µs			
Most Stringent Timing:	**< ±1 µs**	**< ±1 µs**	**< ±1 µs**	**26 µs**	**1 ms**	**1 ms**	**< ±1 µs**

Homeland Security
Science and Technology

Electric Sector Results

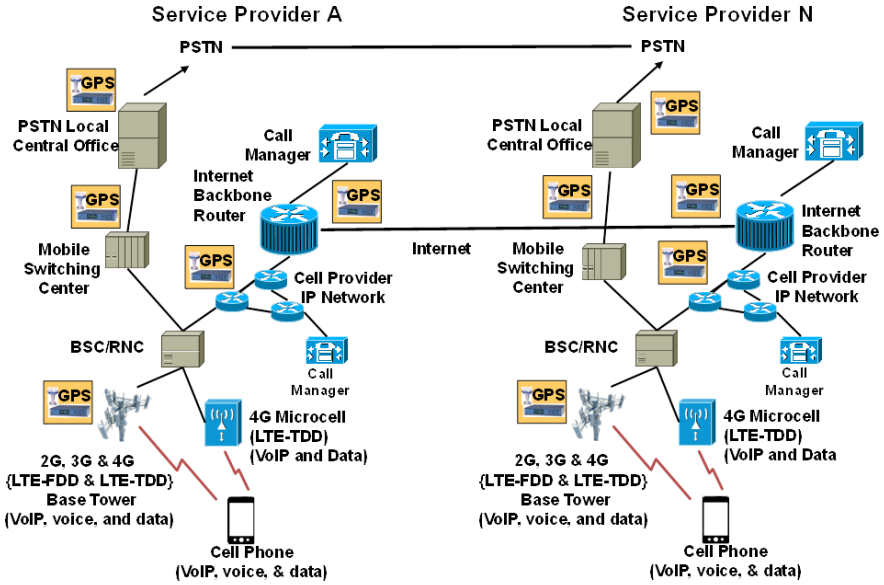
- MITRE Findings from Threat & Vulnerability Analysis
  - Threats
    - Unintentional
      - RF Interference
      - Space Weather
      - Unintentional Jamming
    - Intentional
      - Intentional Jamming
      - Spoofing
      - Cyber attack
  - Equipment/networks most effected
    - Transmission fault location
    - Synchrophasor measurement units
    - Substation control/re-synchronization
    - Distributed energy resources
    - Synchrophasor networks
  - Impacts vary based on threat

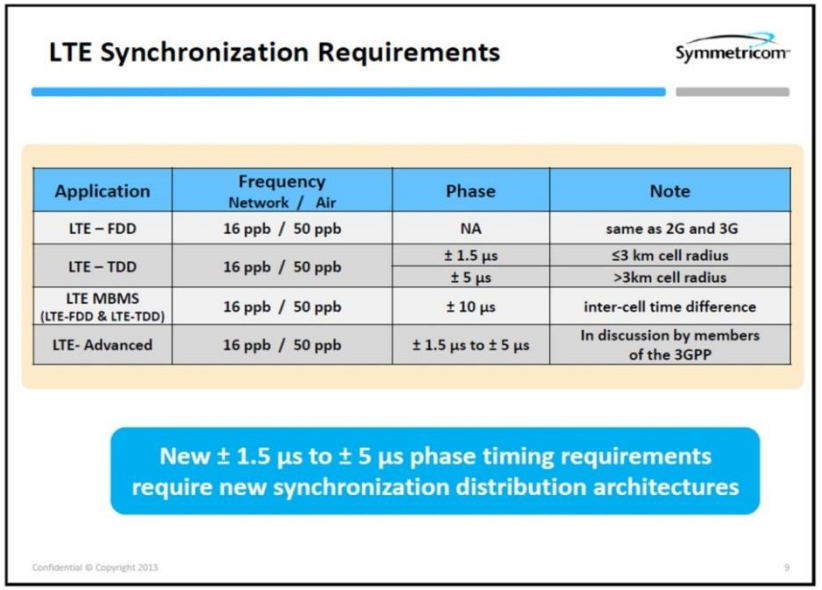


Homeland Security
Science and Technology

Communication Sector Results

- MITRE Findings and Recommendations from Baseline Study
  - Today's network + 3 years out
  - Timing dependent equipment includes
    - SONET/SDH nodes, SynchE nodes, Clock nodes, Switching offices, mobile switching centers, cellular base tower transceivers, micro-cell transceivers
  - Timing requirements vary from 1.5 µs for Cellular Networks to 62.5 µs for the PSTN and Internet Backbone
  - Irrespective of the timing distribution mechanisms deployed, GPS remains the primary reference source and primary mechanism to achieve synchronization
    - Micro-cells will require 1µs timing, unclear how it will be implemented
    - FirstNet deployment should ensure that the precise timing required by LTE and normally derived from GPS can be maintained during incidents.





Homeland Security
Science and Technology

Communication Sector Results

- MITRE Findings and Recommendations from Threat & Vulnerability Analysis
  - Threats
    - Unintentional
      - RF Interference
      - Space Weather
      - Unintentional Jamming
    - Intentional
      - Intentional Jamming
      - Spoofing
      - Cyber attack
- Each threat affects the same set of timing dependent equipment but in different ways;
- Due to the three clock sources (GPS receiver, local holdover oscillator, and landline), and monitoring by network operators, jamming and spoofing attacks will have limited impact on the PSTN and Internet backbone segments of the Communications Sector.
- The cellular network is more vulnerable to jamming and spoofing attacks than the PSTN or Internet backbone. However, jamming and spoofing also have limited impact on the cellular network since these attacks would be directed at the edge of the network (cell towers) where the effects are localized.

Homeland Security
Science and Technology

Mitigations Report

- MITRE Findings and Recommendations from Mitigations Report
  - Antennas
    - Quick fixes: Proper antenna placement & orientation
      - Hidden from view, unobstructed sky view, minimize multi-path
    - Types of antennas
      - High gain directional, multi-band, fixed reception pattern
  - Multi-GNSS receivers
    - May not improve jamming resistance if same center frequency, spectral shape, received power
  - Training
    - Equipment problem vs jamming/spoofing, increase awareness
  - Integrated back-up timing
    - Extended holdovers
    - Precision Time Protocol (CRADA) / or other local network timing
    - Example products
      - Symmetricom SyncServer SGC-1500 synchronizes via GPS to within 50nsec of UTC and provides 1 microsecond timing distribution for substations with two backups: extended holdover Rb oscillator, PTP (if available)
      - Schweitzer Engineering Laboratories (SEL) Integrated Carrier Optical Network (ICON) for inter and intra-substation timing distribution applications “distributed time over a wide-area network with better than 1 microsecond accuracy so that very accurate relative time is maintained in the event of a GPS failure.”

Homeland Security
Science and Technology

Mitigations Report (con't)

- MITRE Findings and Recommendations from Mitigations Report
  - Commercially available stand-alone anti-jamming products
    - Provides detection, notification, in some cases suppression/rejection of jamming signal
      - Detection & Localization Technologies / Systems
        - Hammerhead
        - J-ALERT
        - Signal Sentry 1000
  - Reduce number of GPS receivers needed
    - SONET/SDH with PTP over GigE
    - SynchE with PTP
  - Nationwide Timing Backup Alternatives
    - e-LORAN
    - PNT Cloud concept

DHS S&T SBIR – Phase 1

- SBIR (Small Business Innovation Research)
  - Phase 1 effort -- GPS Disruption, Detection, and Localization (completed October 2013)
    - Objective: Conduct deep-dive survey into at least 2 critical infrastructures to determine their vulnerability to GPS disruptions. Develop a low-cost suite of sensing and reporting technologies to detect and localize fixed and mobile sources (intentional and unintentional) of GPS receiver disruption for critical infrastructures.
    - 6 months, $100k, proof-of-concept
    - 4 awardees with various approaches.
      - Scientific Systems Company
      - Coherent Navigation
      - NAVSYS Corporation
      - Toyon Research Corporation

Homeland Security
Science and Technology

SBIR Findings (Phase 1)

- GPS receiver testing & performance
  - Receiver testing performed against various NRE Scenarios
    - Receivers tested
      - High quality reference station receiver, popular network time server (Quartz oscillator & Rubidium oscillator), time & frequency receiver common to cell towers (Quartz oscillator), others
    - Results
      - Receiver logic does not always handle the various non-physical conditions that can be introduced by spoofing

Homeland Security
Science and Technology

SBIR Findings (Phase 1)

- Types of attacks
  - Potential for multi-pronged attacks
    - An RF-based spoofing attack could create an entry point for a follow on cyber attack
- Engagement with equipment vendors
  - For minimal cost impact to the end user, address vulnerabilities via enhancements or mitigations to existing product lines
    - E.g. detection & alerting of time degradation, “voting” scheme for networked time control, tracking of unexpected antenna movement
- Overall
  - Multi-Emitter Geolocation techniques and mitigation methods are fairly mature: TDOA, FDOA, and AOA
    - Mission Planning Software (how to optimize implementation) is not mature
  - Industry perceptions of the problem vary
    - Need to have a convincing case before CI owners & operators will be willing to invest in a given solution

Homeland Security
Science and Technology

SBIR Findings (Phase 1) con't

- Recommendations from SBIR performers
  - Need better user education -- issue bulletins to appropriate users to advise them of the need to be aware that GPS measurements can be faulty.
  - Additional work needs to be done to better understand the threat level for multi-pronged attacks
  - Use networked timing with redundancy to handle GPS service disruptions
  - Embed detection of GPS interference or spoofing at Critical Infrastructure target receivers
  - Use built-in sensor interfaces for wide-area GPS threat alerting and geolocation
- Key Findings
  - → Need to have a convincing case before CI owners & operators will be willing to invest in a given solution
  - → Additional receiver testing/characterization/certification especially for receivers used within critical infrastructure
  - → For minimal cost impact to the end user, address vulnerabilities via enhancements or mitigations to existing product lines

Homeland Security
Science and Technology

SBIR Phase 2

- Phase II – Down-select
  - Objective: Develop a scalable, working prototype that can be field tested and assessed for reliability and effectiveness at detecting, reporting and providing the timely localization of GPS disruptive events.
  - 24 months, $750k
  - Awarded to Coherent Navigation
    - Multi-tiered effort
    - Primary focus on 1st tier
      - Crowd sourcing approach based on (anonymized) smartphone location data
        - Via existing location-based apps – no new app needed
        - Partner with app developers, deploy algorithms to their servers, no user data transmitted back, only maps of GPS disruption areas
      - Approximately 1 trillion measurements / day
        - Determine if location is provided by GPS satellites, wi-fi, or cellular
        - GPS satellites in view, C/N
      - Initial performance metrics
        - Event reporting w/i 1 hour
        - Location accuracy w/i 500 m
      - Advantages
        - Low-cost (subscription-based service)
        - No additional infrastructure needed
    - Additional testing of GPS receivers used within Energy sector
    - → Will be looking for partners to help field test this technology

Homeland Security
Science and Technology

Areas to consider for future work

1. **CI GPS receiver characterization & testing**
2. **Industry outreach/education**
3. **Development of spoofing mitigations**
   - Add-on solutions are going to be difficult to sell/transition to CI sectors
   - Focus on integrated HW solutions
     - Work with equipment vendors
4. **Localization Capability (specific to spoofing)**
   - Pursue other end users // are they seeing enough incidents to warrant investment?
5. **Back-up timing capability for key critical infrastructure nodes**

Homeland Security
Science and Technology

Contact Info

Thank you!

Questions?

Sarah Mahmood
Program Manager
HSARPA/RSD
DHS Science & Technology

sarah.mahmood@dhs.gov
Tel: 202.254.6721
Mobile: 202.360.2360

Homeland Security

Science and Technology