Report from the Workshop on Precision GNSS Time Resilient Receivers April 17, 2018, Tysons Corner, VA

Presented to the PNT Advisory Board, May 16, 2018

by Marc Weiss

Consultant for Spirent

Output from Workshop on Timing Receiver Resilience

1. Emphasized output
2. Needs of three critical infrastructure sectors: telecom, power, finance
3. Output from Breakout Groups
4. Conclusions

Output from Workshop on Timing Receiver Resilience: Emphasized recommendations

1. Note the role of this workshop: industry-based exploration of how to stimulate the use of more resilient GNSS receivers
    a. Resilience in receivers is a small piece of the timing security problem
    b. Even for receiver resilience: many more-complete efforts are underway
2. Establish Assured PNT Program for America's CI
3. Clarify who is responsible for which aspects of resilience in CI
    a. Without ownership of responsibilities, results will be poor
    b. Roles are required among government, manufacturers, users, and standards organizations

Output from Workshop on Timing Receiver Resilience: Emphasized recommendations

3. Shorter term actions
   a. A Procurement Language relating to resilience
   b. Testing for resilience
   c. Organizational Maturity Model – GNSS Use, Dependence, Vulnerabilities

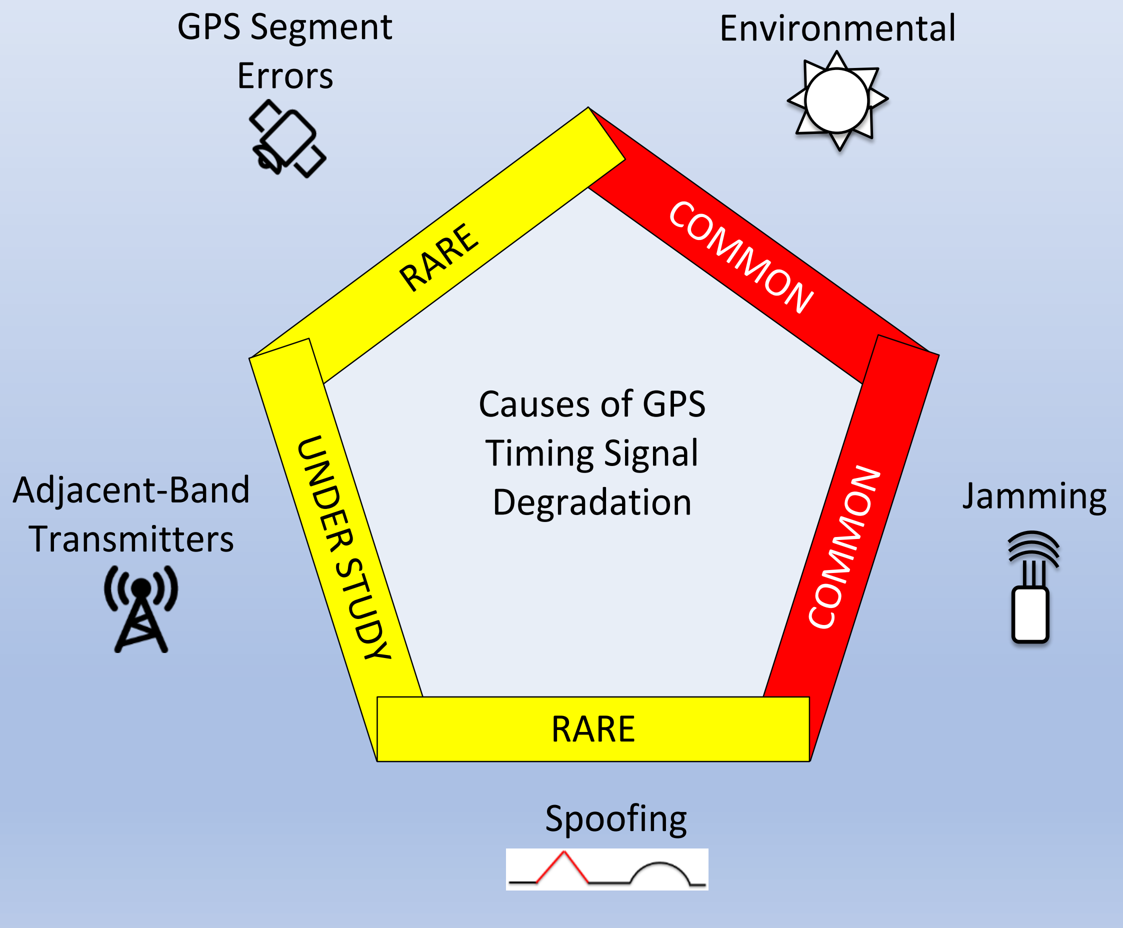
Output from Workshop on Timing Receiver Resilience

1. Emphasized output
2. Needs of three critical infrastructure sectors: telecom, power, finance: steering group members surveyed perceived requirements
3. Output from Breakout Groups
4. Conclusions

Perceived Resilience Needs from Telecom, Electric Power and Finance

1. Individuals reached out to major players in each sector and asked for resilience concerns
2. Responses are only from those who were asked and responded: not full surveys of sectors

Resilience in Telecom not considered high priority: there have been few system impairments known to be caused by jamming or spoofing



GPS Segment Errors

Environmental

Adjacent-Band Transmitters

Jamming

Spoofing

RARE

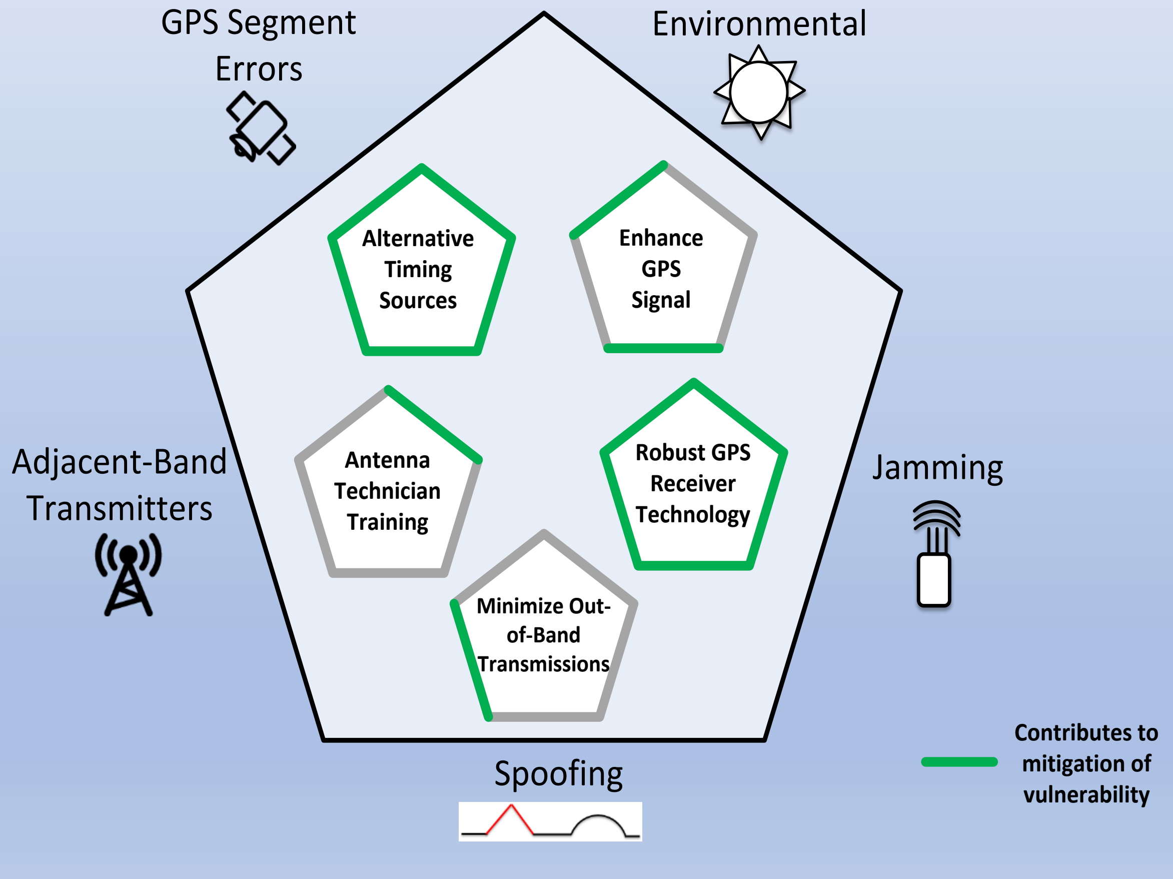
COMMON

UNDER STUDY

COMMON

RARE

Causes of GPS Timing Signal Degradation



GPS Segment Errors

Environmental

Adjacent-Band Transmitters

Jamming

Spoofing

Alternative Timing Sources

Enhance GPS Signal

Antenna Technician Training

Robust GPS Receiver Technology

Minimize Out-of-Band Transmissions

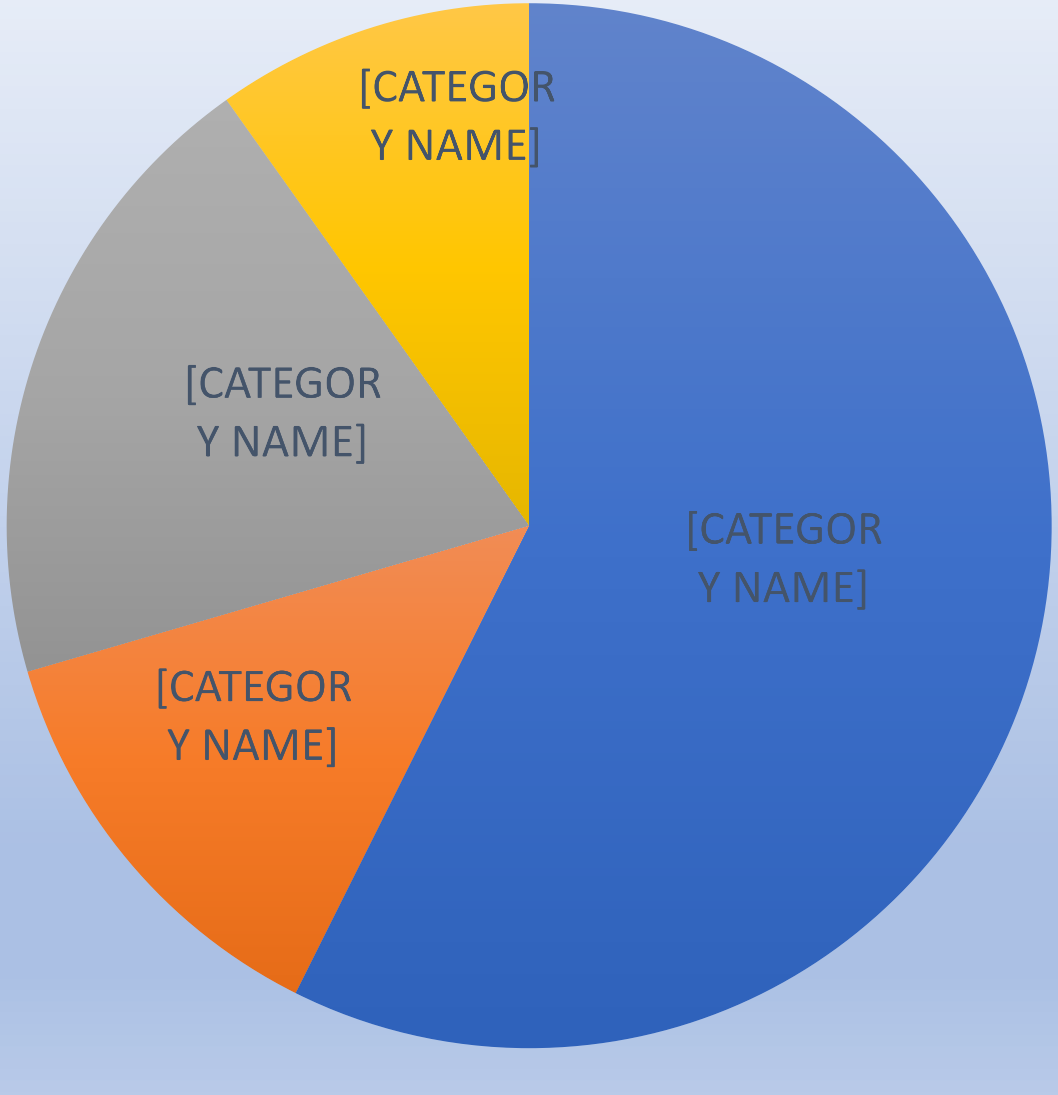
🟩 Contributes to mitigation of vulnerability

From M. Calabro, Booz Allen Hamilton, and Co-chair of ATIS SYNC

In Power, GNSS based timing is a reliability concern

All contacted operators have observed issues with deployed GNSS systems.

About 20% would say that GNSS timing issues affected operations (mostly offline analysis and commissioning delays).



From D. Anand, NIST smart grid program

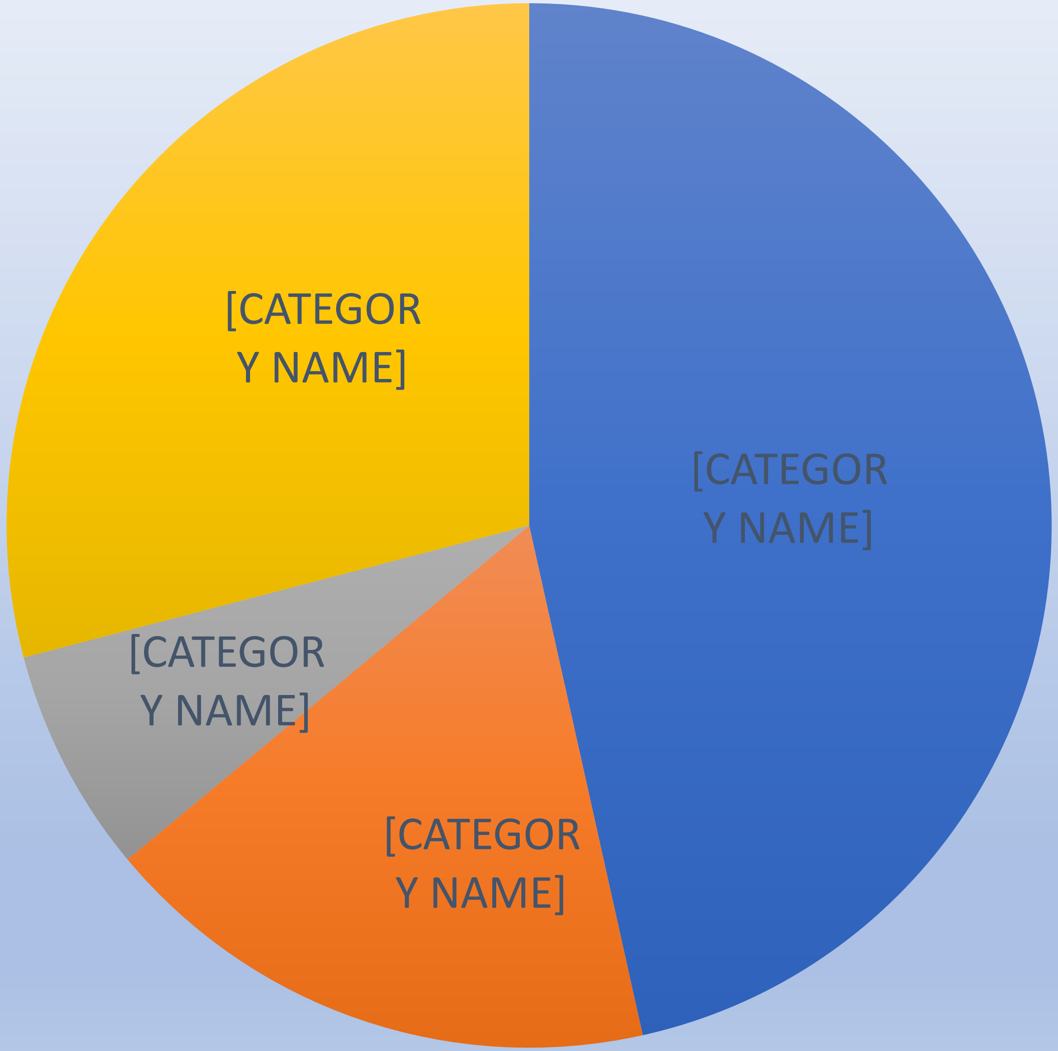
In Power, GNSS based timing is a reliability concern

All contacted operators have observed issues with deployed GNSS systems.

About 20% would say that GNSS timing issues affected operations (mostly offline analysis and commissioning delays).

All of them have approached vendors for ‘resilience’ features.

All of them think an industry wide harmonization of reliability requirements would improve interoperability, firmware updates and facilitate benchmarks for anomaly detection.



From D. Anand, NIST smart grid program

What challenges does the Finance Service Sector (FSS) care about?

1. Reliability
   a. Detection of a time shift (remember the 13 µS oops, Leap second, or DST)
   b. Correction of a time shift
   c. Extended hold over on signal loss for any reason
2. Traceability
   a. Detect and advise on constellation change
   b. Correct for constellation time delta
3. Precision & Accuracy
   a. Continuously validate precision and alignment against internal ST1 source and space references

From A. Bach, Consultant to FSS

FSS Enhanced requirements

1. Better urban penetration
2. Better resistance to both space and terrestrial weather
3. Access to terrestrial based timing source (E-LORAN or Land Lines)
4. Cyber protection
5. FSS is not cost sensitive for improved overall performance

From A. Bach, Consultant to FSS

Output from Workshop on Timing Receiver Resilience

1. Emphasized output
2. Needs of three critical infrastructure sectors: telecom, power, finance
3. Output from Breakout Groups: workshop had two breakout groups to explore what can be done to stimulate more resilience in GNSS
4. Conclusions

Output from Breakout Groups

1. Material is organized as recommendations to different groups
2. Suggests who is responsible for which aspects of resilience in CI

TRR Recommendations to Government

1. Establish Assured PNT Program for America’s CI
    1. Designate and task responsible person
    2. Leader must have enough authority to get this done
2. Make disruption reports public
    1. Publish government’s analysis of reports and recommendations
3. Promote development & use of PNT maturity model by industries/sectors
4. Monitor for disruptions/interference and impacts (like EU’s Strike3)
5. Enforce against violations of the spectrum: jamming and spoofing

TRR Recommendations for Standards Organizations

1. Define resilience and how to test for it
   1. Define metrics and language
   2. Help organize testing—not specifically testing by standards organizations
2. Propose a way to evolve testing for threats
   1. Can there be standard ways of detecting threats?
   2. Can there be standard or uniform ways of validating receiver resilience?
3. Promote the development of a procurement language relating to resilience

TRR Recommendations to Users/Industries

1. Organizational Maturity Model – GNSS Use, Dependence, Vulnerabilities
2. Case studies by industry
3. Industry common procurement language
4. Monitor for problems and impacts
   a. Use results to improve system resilience
      i. GNSS systems can have improved resilience to many effects
      ii. Use of alternative timing signals is essential for timing security
   b. Leverage base of users’ receivers to detect and report events to authorities
      i. Support protection of the spectrum
      ii. Collaborate with government to enforce protection

Output from Workshop on Timing Receiver Resilience

1. Emphasized output
2. Needs of three critical infrastructure sectors: telecom, power, finance
3. Output from Breakout Groups
4. Conclusions

Next Steps

1. Explore timing Security issues at the Workshop on Sync and Timing Systems (WSTS) June 18-21, 2018, San Jose, CA: https://www.atis.org/wsts/
2. Following WSTS and collocated: a NIST/DHS workshop on Timing Security on June 22, http://www.atis.org/assured-access/
3. This group will explore further options for stimulating resilient receivers
   a. Working with user demand and manufacturer options
   b. Options for testing receivers
4. Timing Security is a much bigger issue than just GNSS resilience. Ongoing research will be reported at various forums.
   a. A local timing system generally has multiple timing inputs and outputs
   b. Resilience can be understood as what happens in between

Conclusions: Emphasized recommendations

1. Note the role of this workshop: industry-based exploration of how to stimulate the use of more resilient GNSS receivers
   a. Resilience in receivers is a small piece of the timing security problem
   b. Even for receiver resilience: many more-complete efforts are underway
2. Establish Assured PNT Program for America's CI
3. Clarify who is responsible for which aspects of resilience in CI
   a. Without ownership of responsibilities, results will be poor
   b. Roles are required among government, manufacturers, users, and standards organizations

Conclusions: Emphasized recommendations

3. Shorter term actions
    a. A Procurement Language relating to resilience
    b. Testing for resilience
    c. Organizational Maturity Model – GNSS Use, Dependence, Vulnerabilities