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

Presented to the WSTS, June 20, 2018

by Marc Weiss

Consultant for Spirent

Output from Workshop on Timing Receiver Resilience

1. Emphasized output
2. Talks on threats and mitigations
3. Needs of three critical infrastructure sectors: telecom, power, finance
4. Output from Breakout Groups
5. Conclusions

Note all presentations from this workshop are available from:

http://www.atis.org/trr/agenda/

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. Talks on threats and mitigations
3. Needs of three critical infrastructure sectors: telecom, power, finance
4. Output from Breakout Groups
5. Conclusions

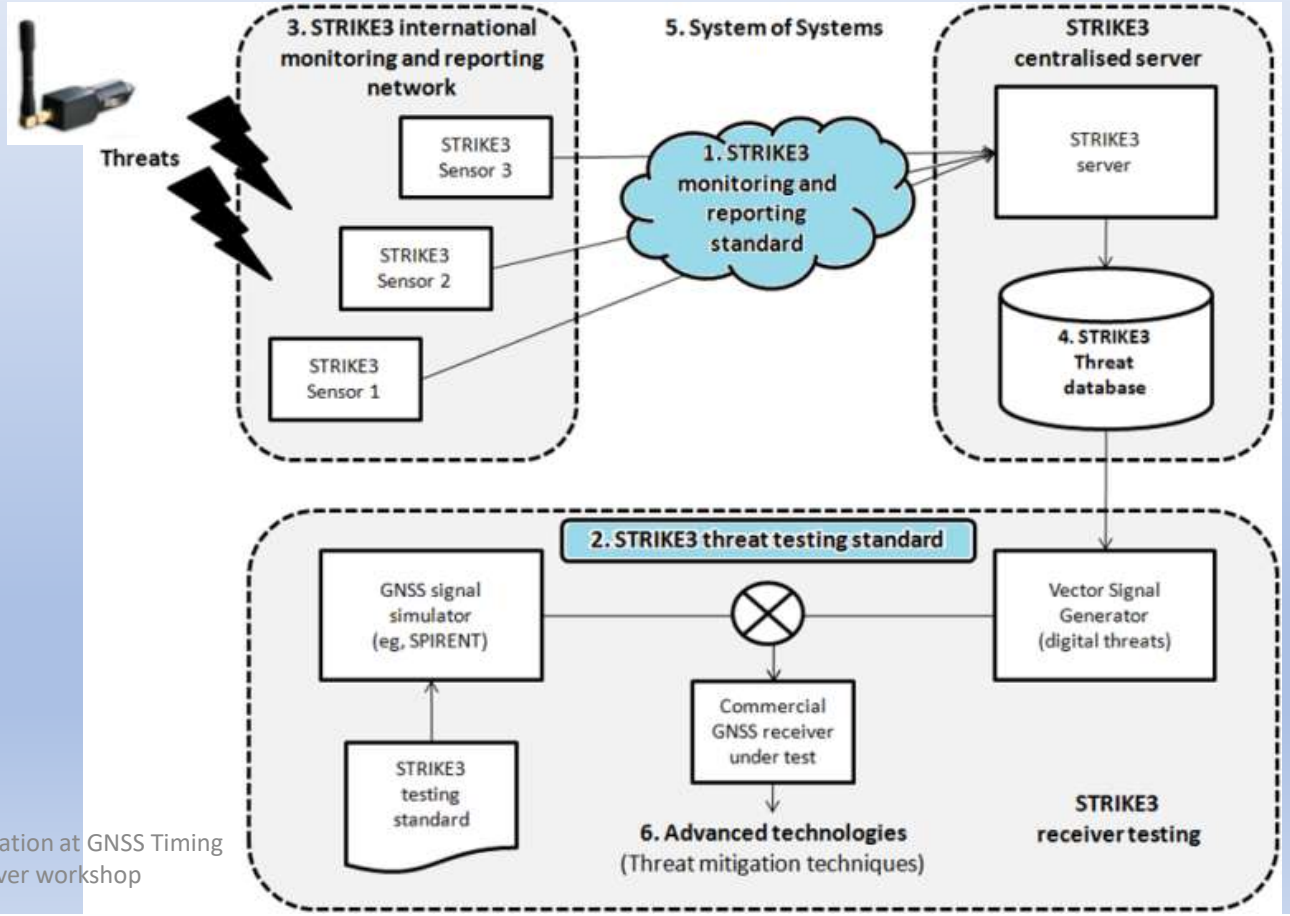
Standardisation of GNSS Threat reporting and Receiver testing through International Knowledge Exchange, Experimentation and Exploitation [STRIKE3]: Characterizing the Threats

GNSS Timing Resilience Receiver Workshop

17th April, 2018

Zahidul Bhuiyan
(zahidul.Bhuiyan@nls.fi)
Research Manager
Finnish Geospatial Research Institute (FGI)

Monitor, Detect, Characterise, Mitigate, Protect



First observations on the test results

1. Both mass-market and professional grade receivers impacted significantly by the jamming tests.
2. Performance accuracy is better for professional grade RUT than mass-market RUT with the compromise in availability.
3. Availability is much better for mass-market RUT as compared to professional-grade RUT with the compromise in accuracy.
4. Galileo E1 improvements over GPS L1 can be visible while processing professional-grade RUT in all the three tested cases. The professional-grade RUT has better C/No values for Galileo than GPS when exposed to jamming: more investigation is underway with in-house multi-GNSS software receiver FGI-GSRx

EXPLOITATIONS AND MITIGATIONS

Attributes	Definition	Sample Exploitations	Sample Mitigations
Access	Ability to ensure a sufficient level of access to PNT information	Jamming Spoofing System Attack	Improved Receivers Anti-Jam Antenna System Diversity
Integrity	Ability to ensure a sufficient level of trust in PNT information	Spoofing System Attack	Improved Receivers Situational Awareness System Diversity
Affordability	Ability to afford the procurement, operations and maintenance of a capability (enabled by PNT)	Any of the above, to a point that drives the system to need an upgrade	Open-architecture System Diversity

Effective mitigation requires an understanding of the client system & how it consumes PNT information.

From K. Coggins, Booz Allen Hamilton

Implications from DoD for Critical Infrastructure

1. Adoption of GPS in Critical Infrastructure is similar to DoD in most cases
   a. Ubiquitous – GPS is universally employed
   b. Blind trust – GPS is inherently trusted
   c. Static – GPS systems are usually never patched
   d. Without resilience – GPS-only solution – single point of failure
   e. Without situational awareness – no knowledge of threats in real-time
   f. Without system understanding – limited knowledge of how the system consumes and processes PNT data
2. Threat Techniques and Systems are Readily Available
   a. Techniques are published and widely known
   b. Inexpensive and effective threat systems are available
3. Questions for U.S. Critical Infrastructure are the Same
   a. What do our systems really need?
   b. How to architect our systems and affordably enable PNT resilience?
   c. How to prioritize actions and allocate limited resources?
   d. How to update older systems?
   e. How to get organizations and people to do what we need them to?

From K. Coggins, Booz Allen Hamilton

Toward Building "Brilliant" User Equipment

Brilliant user equipment

- "Flip" to core of precision clocks & inertial sensors, disciplined by GNSS and other sensors
- Operate through spoofing
- Rigorous PVT Assurance

Smart user equipment

- Advanced antennas to block threats
- Securely upgradeable software
- Assured use of signals from foreign satnav systems
- Improved resistance to interference
- Smart signal use hierarchy
- Event data logging

Competent user equipment

- Use multiple civil GPS signals
- Handle all IS-compliant events: GPS week rollover, leap seconds, data message content
- Detect spoofing and non-IS-compliant events
  - No hazardous or misleading PVT outputs
  - Prompt recovery
- Situational awareness with reporting to user or host system

Software Assurance
- Development
- Sustainment

Supply Chain Risk Management
Cyber Security
Test & Validation

There's knowing what to do…
then there's knowing how to do it!

Other Steps for Timing Applications

1. Use multiple available timing sources instead or in addition
   a. Network-based
   b. Clocks
   c. Two-way time transfer

2. Test and Validate user equipment
   a. Threat toolkits becoming available for satellite simulators

3. Design timing architectures for graceful degradation
   a. Smart Holdover
   b. Flip! – Discipline with assured sources
   c. Loss of efficiency, not loss of essential functionality

Output from Workshop on Timing Receiver Resilience

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

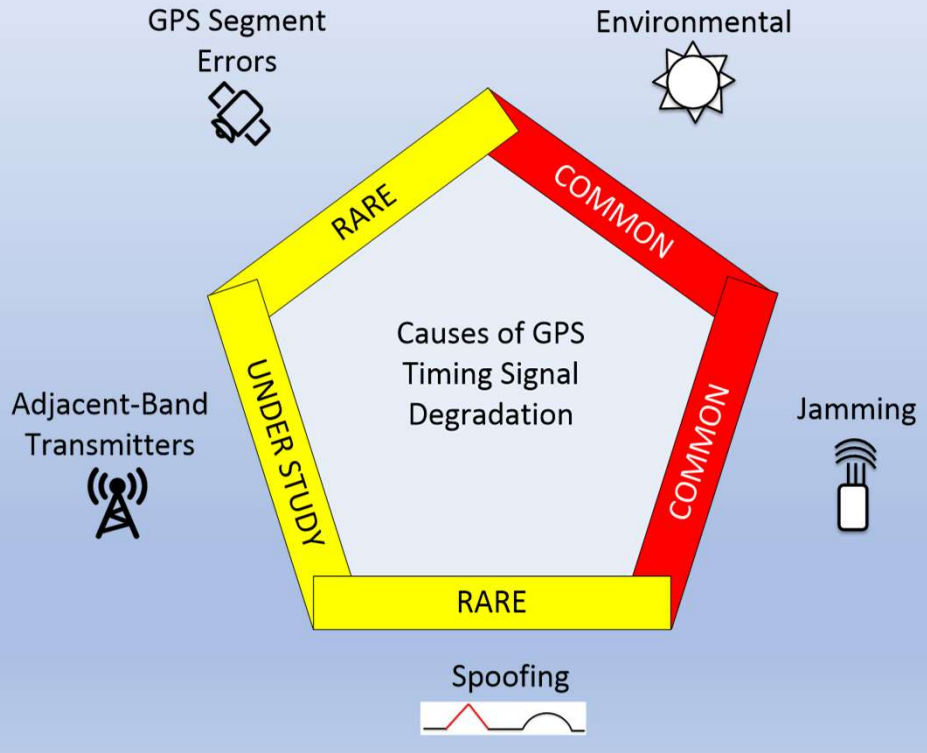
Perceived Resilience Needs from Telecom, Electric Power and Finance

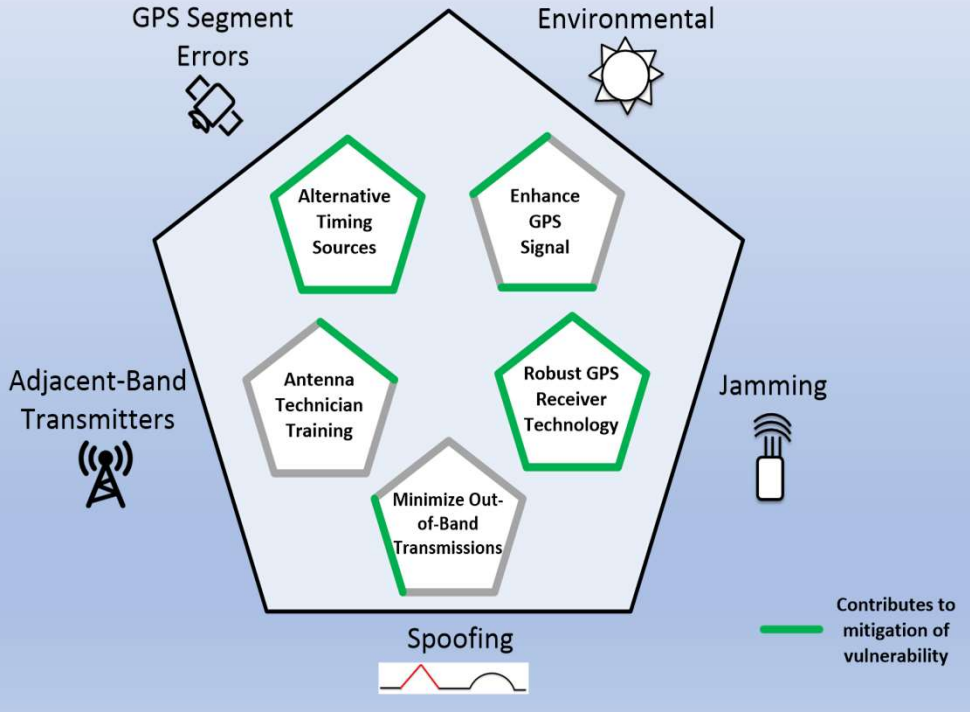
1. Individuals reached out to major players in each sector and asked for resilience concerns
2. Responses are only from those who were asked and responded: not full surveys of sectors

Telecom Requirements: Microsecond or Tighter

Application/ Technology	Accuracy
W-CDMA (Home NodeB)	µs level accuracy
LTE-A	µs level accuracy
WCDMA MBSFN	12.8 µs
LTE-TDD (wide-area)	10 µs
LTE-TDD to CDMA	10 µs
CDMA2000	3 µs
TD-SCDMA	3 µs
LTE-TDD (home-area)	3 µs
WCDMA-TDD	2.5 µs
WiMAX (downlink)	1.428 µs
WiMAX (base station)	1 µs
LTE MBSFN	1 µs
PRTC	100 ns
ePRTC	30 ns

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





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

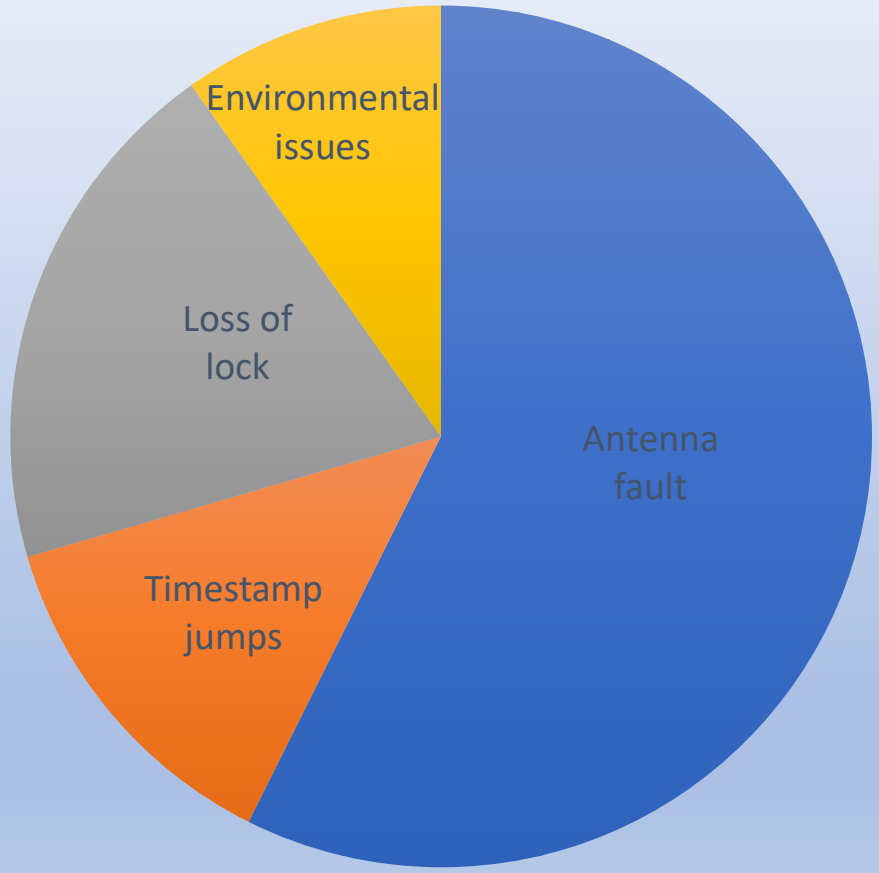
Synchrophasors are a Critical Time Consumer in the Electric Power Grid

- Precise timing is widely used to support synchrophasor applications in the electric power sector
- Synchrophasors have long been used for important applications, such as validating power system dynamic models
- There are emerging applications being deployed that utilize synchrophasors for operational applications
- Increased robustness of wide-area time synchronization is required to support these emerging applications

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

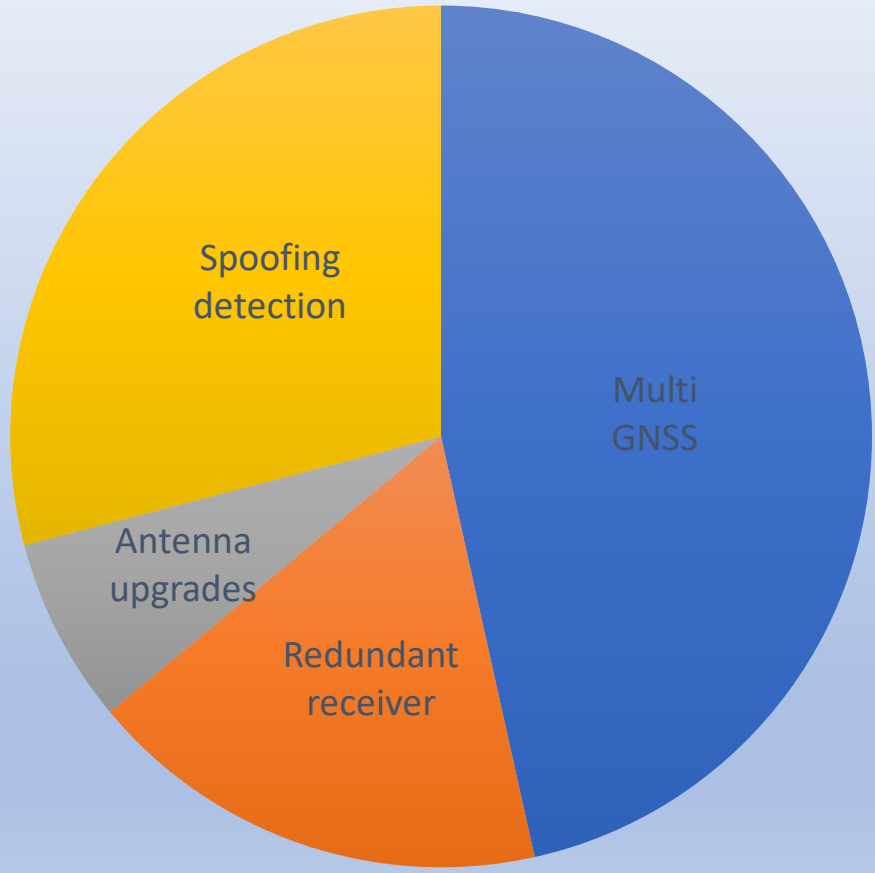
In Power, GNSS based timing is a reliability concern

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. Talks on threats and mitigations
3. Needs of three critical infrastructure sectors: telecom, power, finance
4. Output from Breakout Groups: workshop had two breakout groups to explore what can be done to stimulate more resilience in GNSS
5. 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
   a. Designate and task responsible person
   b. Leader must have enough authority to get this done
2. Make disruption reports public
   a. 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
   a. Define metrics and language
   b. Help organize testing—not specifically testing by standards organizations
2. Propose a way to evolve testing for threats
   a. Can there be standard ways of detecting threats?
   b. 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. Talks on threats and mitigations
3. Needs of three critical infrastructure sectors: telecom, power, finance
4. Output from Breakout Groups
5. Conclusions

Note all presentations from this workshop are available from:
http://www.atis.org/trr/agenda/

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