GNSS Timing: New Technical Standards and Documents

A Leading Provider of Smart, Connected and Secure Embedded Control Solutions

SMART | CONNECTED | SECURE

Lee Cosart

April 2021

Introduction

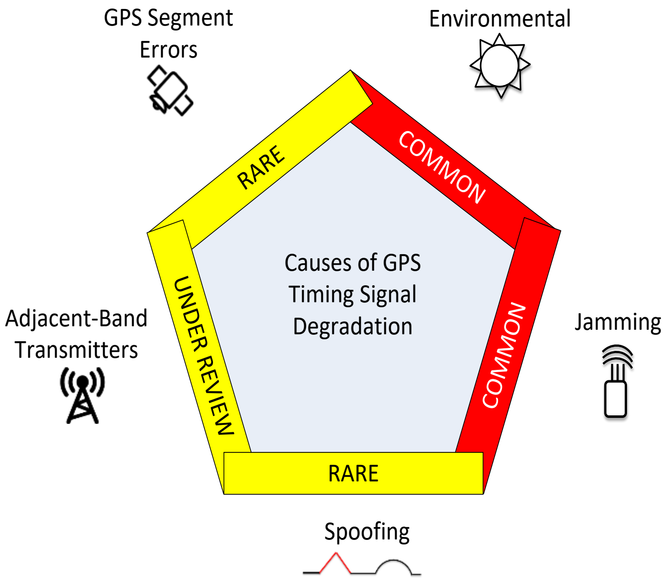
- **ITU-T Technical Report (2020)**
  - Considerations on the use of Global Navigation Satellite Systems (GNSS) as a primary time reference in telecommunications
    - ITU-T Technical Report 2020
- **U.S. Department of Homeland Security (DHS) (2020)**
  - Resilient Position, Navigation, and Timing (PNT) Conformance Framework
    - Resilient PNT Conformance Framework
- **ATIS Technical Report (2017)**
  - Global Positioning System (GPS) Vulnerability
    - GPS Vulnerability

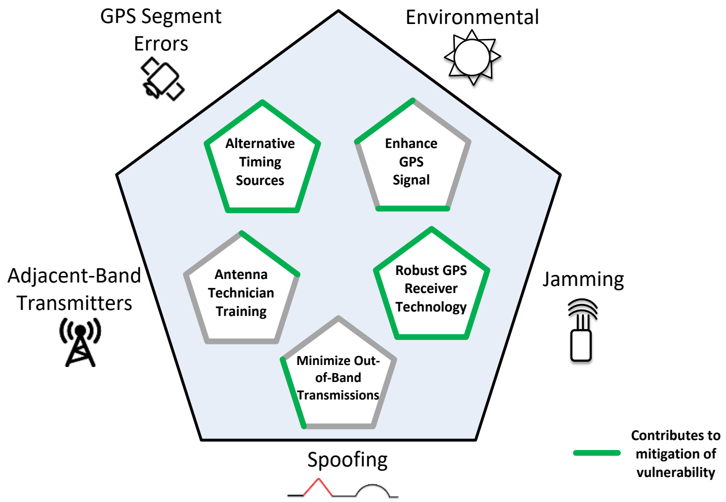
ATIS GPS Vulnerability Report

GPS Vulnerability (September 2017)

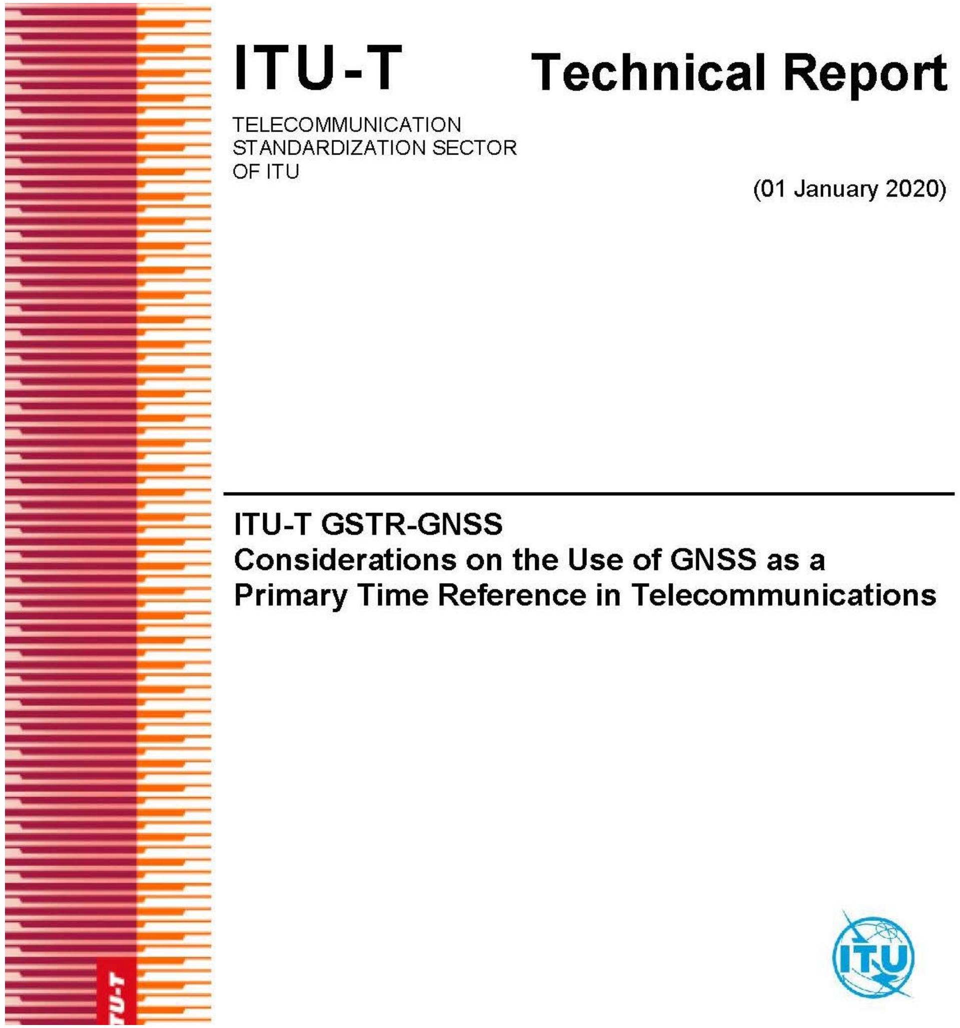
Organization of GPS Vulnerability Report

- Known GPS vulnerabilities
- GPS performance and synchronization requirements
- GPS vulnerability mitigation and alternatives to GPS timing
- Recommendations to assure time for telecom




GPS Segment Errors
Environmental
Alternative Timing Sources
Enhance GPS Signal
Antenna Technician Training
Robust GPS Receiver Technology
Minimize Out-of-Band Transmissions
Adjacent-Band Transmitters
Jamming
Spoofing
Contributes to mitigation of vulnerability

ITU-T GNSS Timing Technical Report



ITU-T **Technical Report**

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(01 January 2020)

ITU-T GSTR-GNSS
Considerations on the Use of GNSS as a
Primary Time Reference in Telecommunications

- Published January 2020
- Focused on GNSS timing
- Companion document to:
  - G.8272 (PRTC)
  - G.8272.1 (ePRTC)
- G.8272 and G.8272.1 address PRTC (Primary Reference Time Clock) and ePRTC (enhanced Primary Reference Time Clock) performance requirements
- This document aims at an in-depth understanding of GNSS systems from the standpoint of timing and synchronization

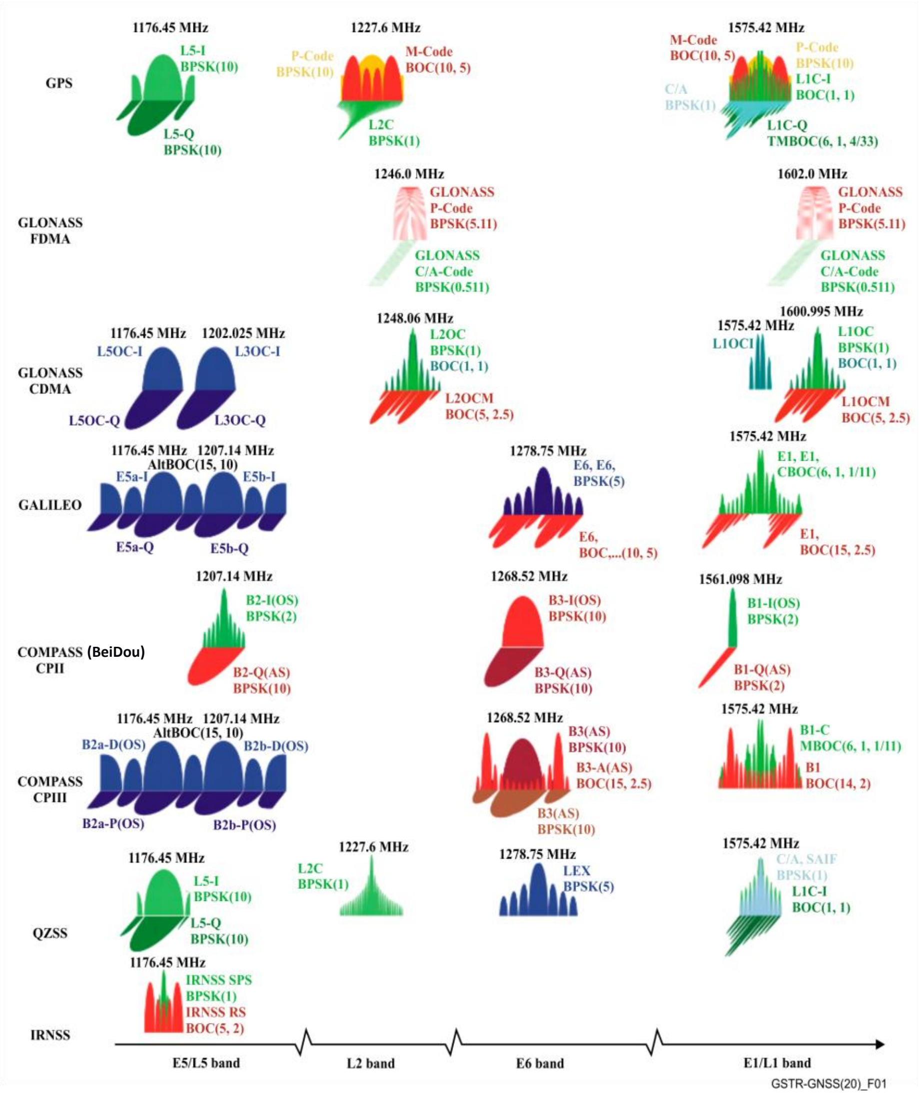
ITU-T GNSS Timing Technical Report

- **Focus on delivery of accurate time**
  - This technical report provides information relevant to optimal GNSS reception in telecommunication applications where highly accurate time recovery is critical.

- **Stationary receivers rather than navigation receivers**
  - Unlike commonly used GNSS navigation applications where position is the goal, the focus in telecommunications is on accurate time recovery with stationary receivers, which provide accurate time to such equipment as Primary Reference Time Clocks (PRTCs) and base stations in mobile networks.

- **For operators, manufacturers, silicon vendors, test equipment vendors**
  - This technical report is addressed to telecommunication operators, manufacturers, silicon vendors and test equipment vendors who are interested in a high-level view of the information and issues associated with GNSS reception. This includes general information; basic variables, parameters and equations; modes of operation; and the nature of the challenges and methodology to mitigate them.

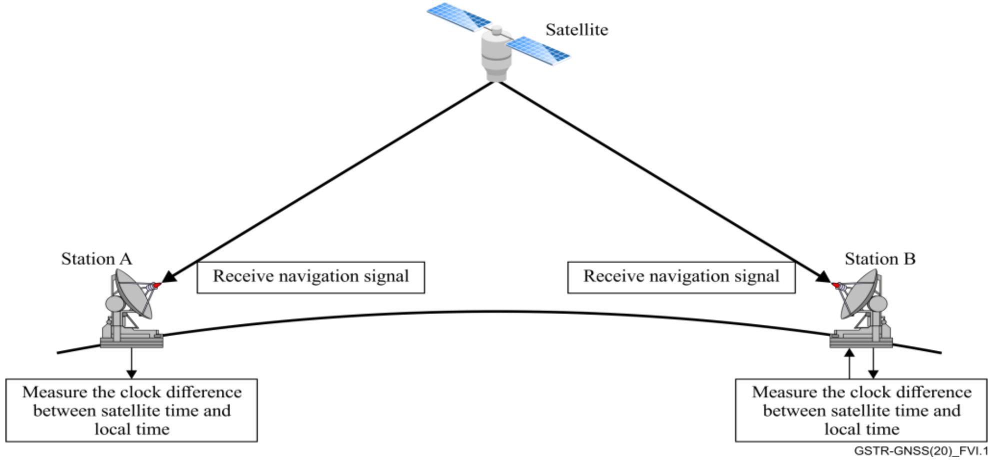
ITU-T GNSS Timing Technical Report



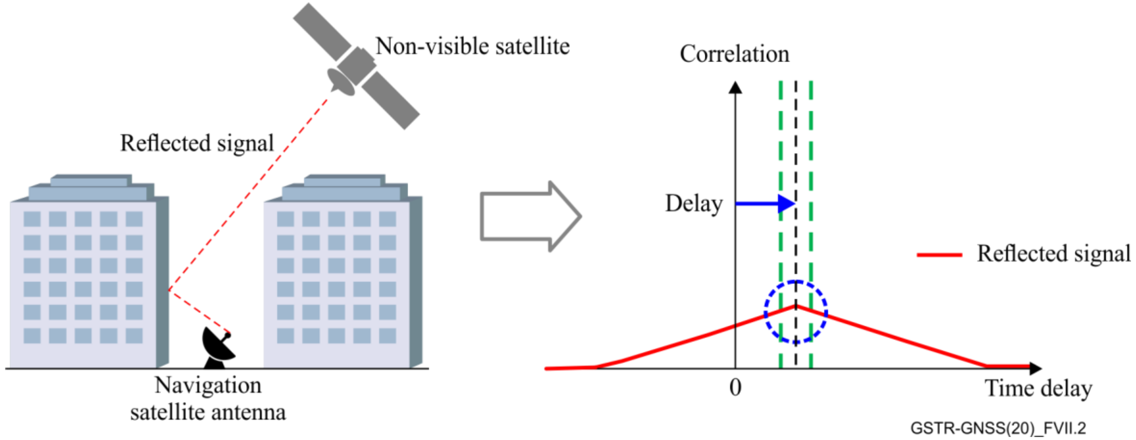
Chapters

1. **Introduction** (including high-level description of various GNSS systems worldwide)
2. **Factors influencing the performance of a GNSS-based PRTC**
3. **Sources of time error in GNSS time distribution**
4. **Mitigation of time error in a GNSS-based PRTC**
5. **Operational schemes for mitigation of time error in GNSS time distribution**

ITU-T GNSS Timing Technical Report


Satellite
Station A
Receive navigation signal
Receive navigation signal
Station B
Measure the clock difference between satellite time and local time
Measure the clock difference between satellite time and local time

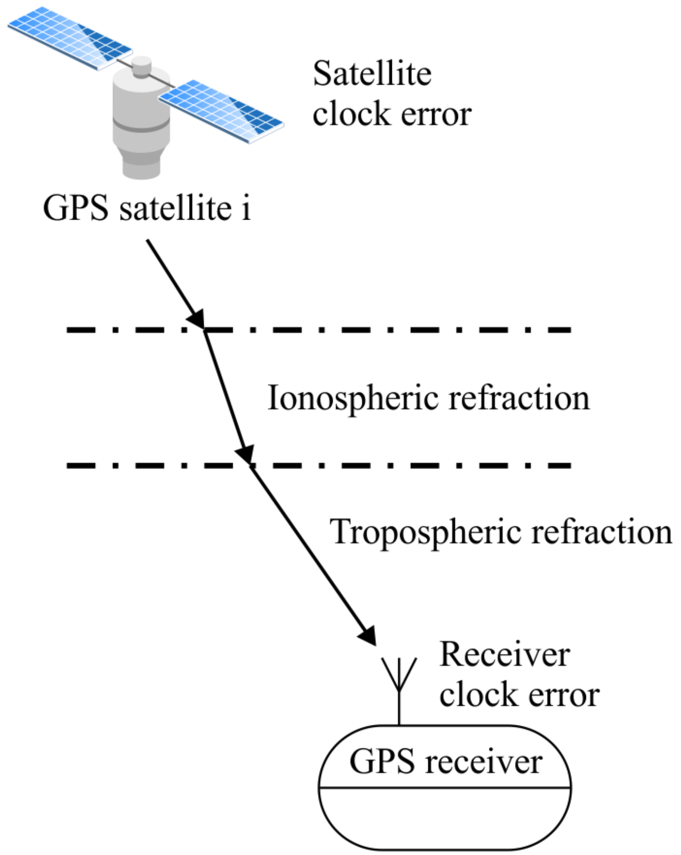
GSTR-GNSS(20)_FVI.1



GSTR-GNSS(20)_FVII.2

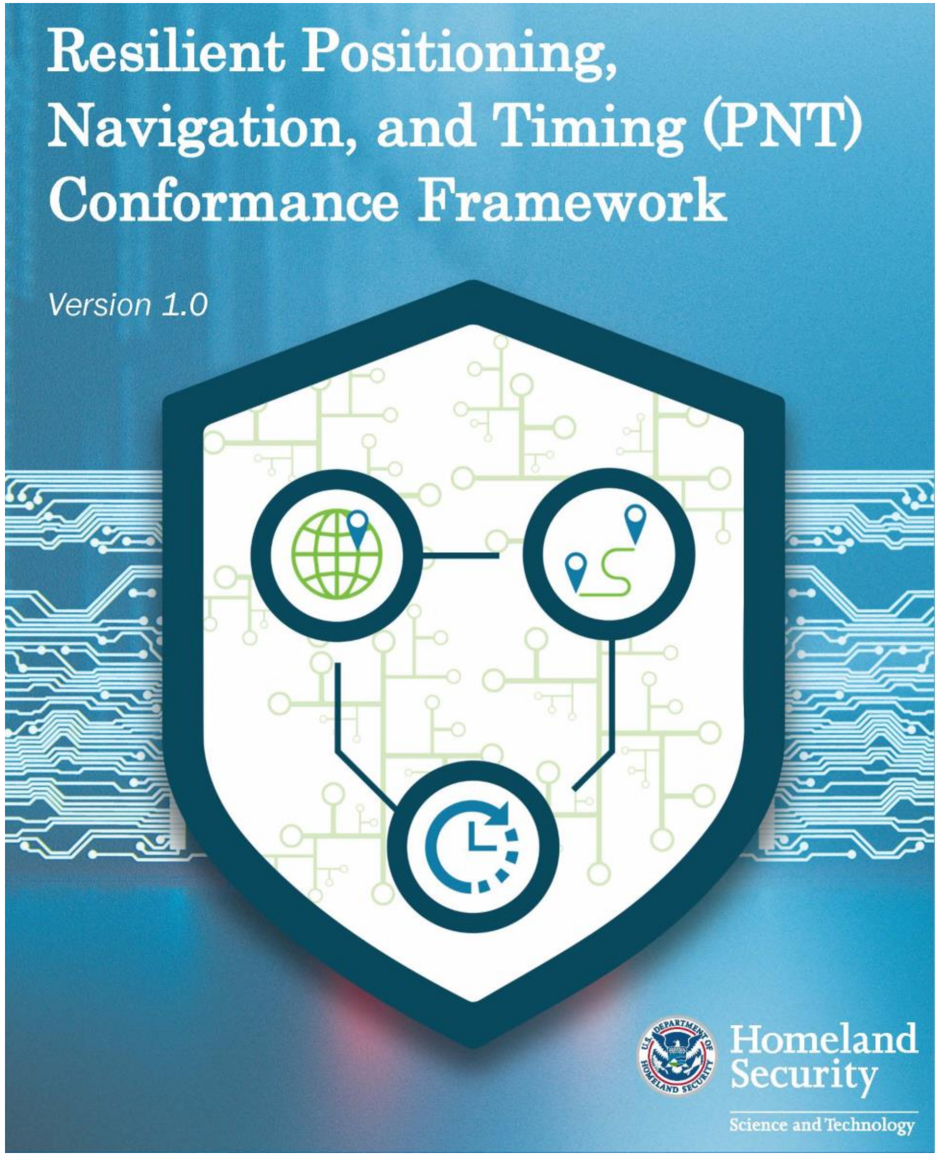
- Appendices
  I. Cable delay effects and correction in a GNSS receiver
  II. Ionospheric delay, its effect on GNSS receivers and mitigation of these effects
  III. Time receiver autonomous integrity monitoring
  IV. Solving GNSS equations to establish position and time
  V. The effect of multiple reflections within the antenna cable
  VI. Satellite common-view
  VII. The effect of multipath within the receiver signal processing

ITU-T GNSS Timing Technical Report



- **Example topic: Ionospheric Delay**
  - When the GNSS electromagnetic wave signal traverses the ionosphere, the plasma will cause reflection, refraction and scattering of this electromagnetic wave signal, which affects the propagation speed. In quiet ionospheric conditions, the resulting additional delay ranges from a few nanoseconds to 20 to 25 ns for GNSS signals.
- **Mitigating ionospheric delay**
- **Model ionosphere and correct (for single-band receiver)**
- **Use regional correction service (SBAS – satellite-based augmentation system)**
- **Mitigate with primary atomic clocks (diurnal filtering and space weather detection - ePRTC)**
- **Utilize multiband GNSS receiver (actively compensates for ionospheric time delay)**

DHS Resilient PNT Conformance Framework


Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework

Version 1.0

Homeland Security

Science and Technology

- Released December 2020
- Concerned with Position, Navigation and Timing (PNT)
- Committee of contributors included government and industry participants
- Government participants from various agencies such as DHS, FAA, DOE, DOT, NIST
- Industry participants included carriers, vendors, government contractors, consultants
- Addressing critical infrastructure such as power sector, financial sector, communication, transportation, emergency services

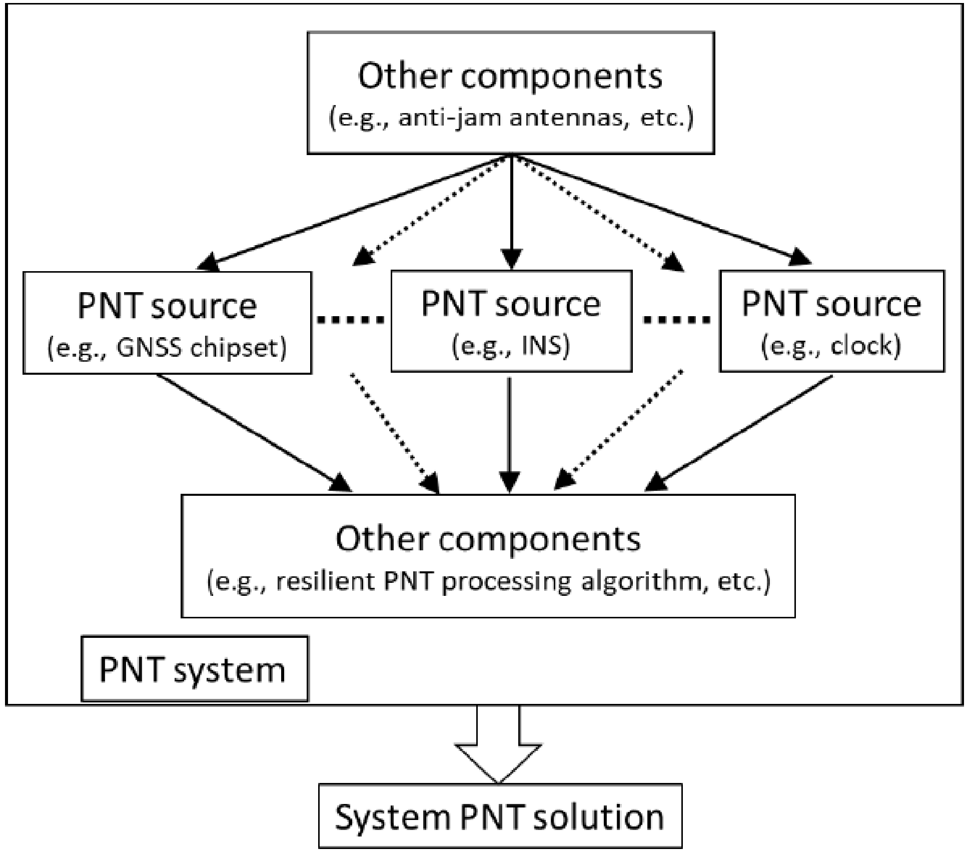
DHS Resilient PNT Conformance Framework

- **GNSS systems have enabled widespread adoption of PNT**
  - Therefore, disruption of or interference with PNT systems (whether GNSS-dependent or otherwise) has the potential to have adverse impacts on individuals, businesses, and the nation’s economic and national security.

- **Work sponsored by U.S. DHS Science and Technology Directorate**
  - The Resilient PNG Conformance Framework document provides guidance for defining expected behaviors in resilient PNT user equipment (UE), with the goal of facilitating development and adoption of those behaviors through a common framework that enables improved risk management, determination of appropriate mitigations, and decision making by PNT end-users. To encourage industry innovation, this framework is PNT source agnostic and outcome based.

- **Four levels of resilience defined**
  - It also contains four levels of resilience so end-users can select a level that is appropriate based on their risk tolerance, budget and application criticality. Therefore, a lower-level receiver is not necessarily better or worse; instead, it simply reflects a level that meets the user’s particular needs.

DHS Resilient PNT Conformance Framework

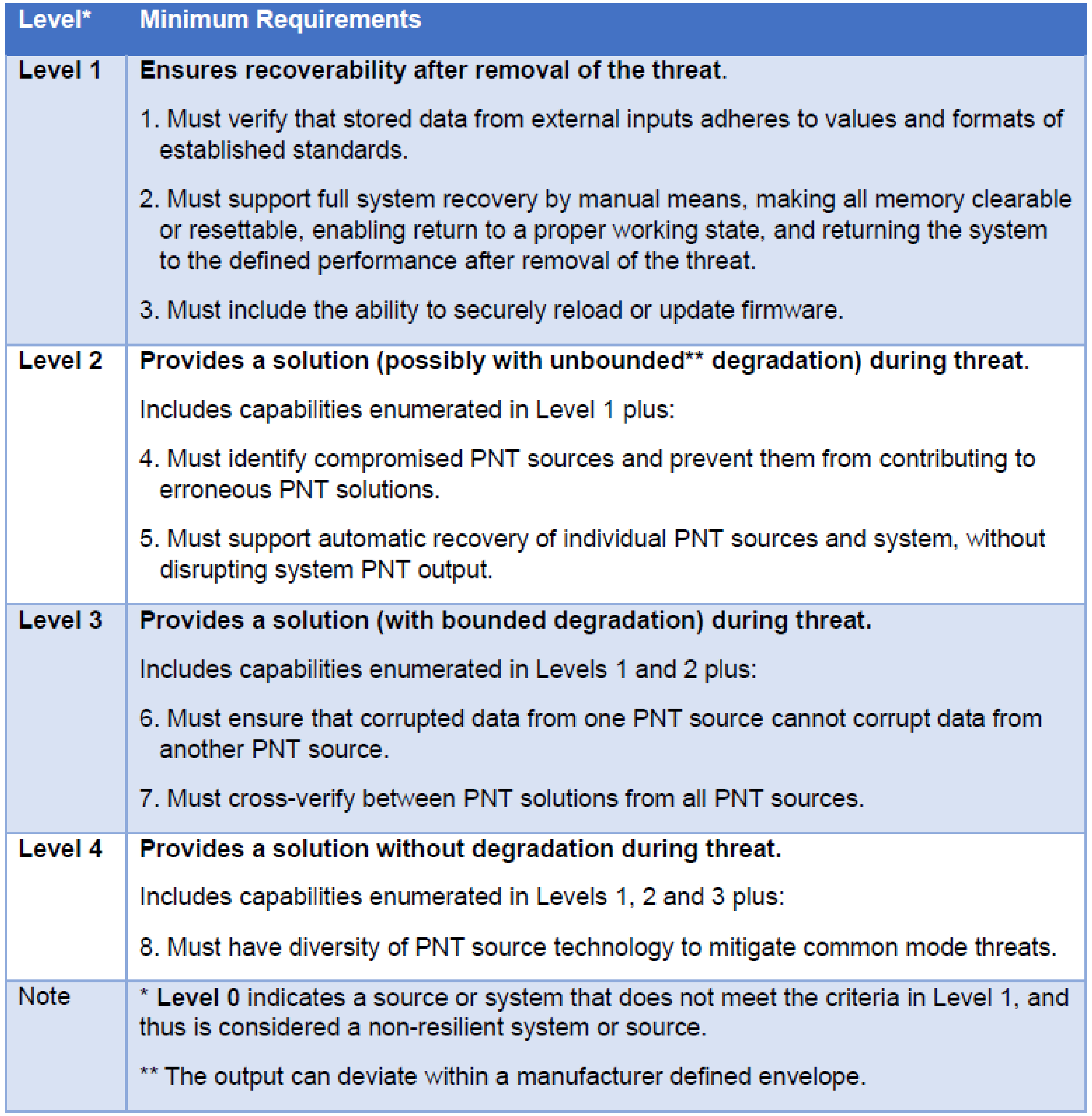


- **PNT System:** The components, processes and parameters that collectively produce the final PNT solution for the consumer.

- **PNT Source:** A PNT system component that is used to produce a PNT solution. Examples include GNSS receivers, networked and local clocks, inertial navigation systems (INS), and/or timing services provided over a wired or wireless connection.

- **PNT System:** The full solution provided by a PNT system or source, including time, position and velocity. A PNT system or source may provide a full PNT solution or a part of it. For example, a GNSS receiver provides a full PNT solution, while a local clock provides only a timing/frequency solution.

DHS Resilient PNT Conformance Framework



Level*	Minimum Requirements
Level 1	**Ensures recoverability after removal of the threat.** 1. Must verify that stored data from external inputs adheres to values and formats of established standards. 2. Must support full system recovery by manual means, making all memory clearable or resettable, enabling return to a proper working state, and returning the system to the defined performance after removal of the threat. 3. Must include the ability to securely reload or update firmware.
Level 2	**Provides a solution (possibly with unbounded** degradation) during threat.** Includes capabilities enumerated in Level 1 plus: 4. Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions. 5. Must support automatic recovery of individual PNT sources and system, without disrupting system PNT output.
Level 3	**Provides a solution (with bounded degradation) during threat.** Includes capabilities enumerated in Levels 1 and 2 plus: 6. Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source. 7. Must cross-verify between PNT solutions from all PNT sources.
Level 4	**Provides a solution without degradation during threat.** Includes capabilities enumerated in Levels 1, 2 and 3 plus: 8. Must have diversity of PNT source technology to mitigate common mode threats.
Note	* **Level 0** indicates a source or system that does not meet the criteria in Level 1, and thus is considered a non-resilient system or source. ** The output can deviate within a manufacturer defined envelope.

- This table captures the minimum requirements for each resilience level. The descriptions represent minimum behaviors (either allowable or resulting) that must occur to achieve that resilience level. Note that the resilience levels build upon each other, that is, Level 2 includes all enumerated behaviors in Level 1, and so forth. The final PNT output solution behavior for each level is specified as well.

- The descriptions cover key features of the resilience levels. The capabilities associated with each of the resilience levels are generally increasingly sophisticated and leverage deeper architectural access. The benefits are cumulative with increasing resilience levels; that is, Level 2 is more resilient than Level 1, etc. Finally, descriptions also indicate the depth of architecture access necessary to achieve the resilience levels.

Summary

- Three reports discussed: ATIS, ITU-T, DHS
- Wide GNSS adoption throughout numerous industries
- Thus, GNSS has become an essential component for a wide range of critical infrastructure
- Consequently, increased attention is being paid towards GNSS vulnerability and PNT security and resilience
- Time and frequency is a central component for the consideration of PNT resilience
- Efforts on resilience are underway with the participation of industry and government

Thank you

Lee Cosart

Research Engineer

lee.cosart@microchip.com

Phone: +1-408-428-7833