Positioning Infrastructure – A case study on Resilient PNT

Ruban Jacob

Jointly Organized by

GEOSPATIAL WORLD
ADVANCING KNOWLEDGE FOR SUSTAINABILITY

United Nations Statistics Division

Partners

esri
GEONOVUM
HEXAGON
ORACLE
Trimble
USGS science for a changing world
Spatial Vision
aws
Open Geospatial Consortium
Ordnance Survey
NIAS
JRC EUROPEAN COMMISSION
Blue Sky Analytics

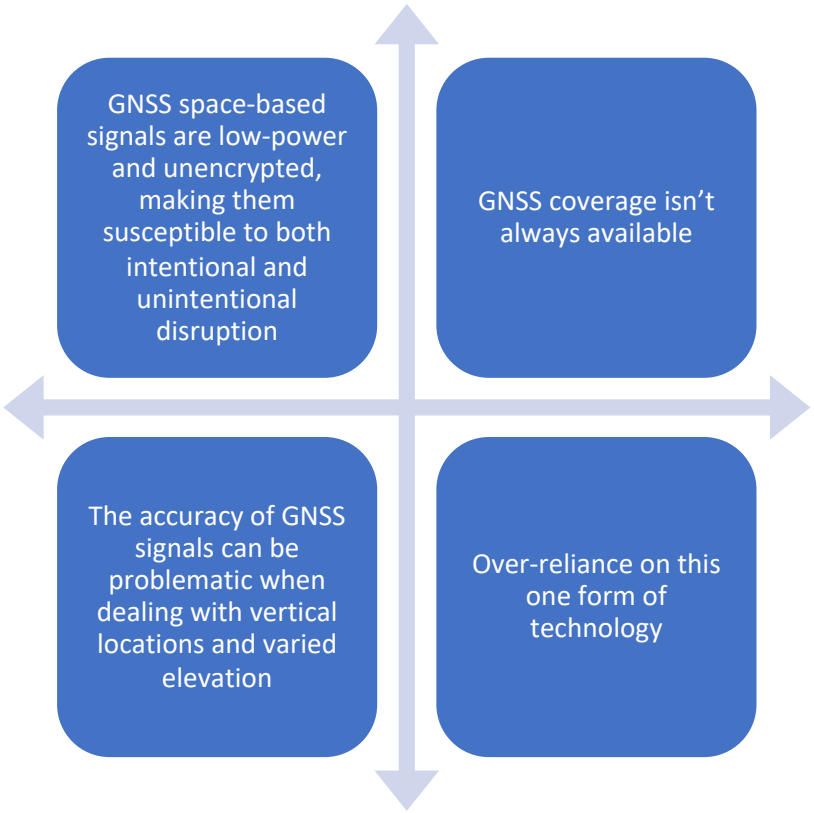
Energy Partner

iea International Energy Agency

PNT – An Invisible Utility

- Accurate and reliable positioning, timing and navigation (PNT) technologies enable many critical applications, including the electric grid, telecommunications, agriculture and port operations
- GNSS - primary source of PNT information via a constellation of orbiting satellites working in conjunction with a network of ground stations
- Resilient positioning, navigation and timing (RPNT) - Convergence of traditional PNT technology with non-traditional and emerging technology to improve the reliability, performance and safety of mission-critical applications
- The European Commission has estimated that 6-7 % of GDP in Western countries depends on GNSS

Need for Resilient PNT – Vulnerabilities and Impact



- A UK Government research in 2017 identified that a five-day loss of GNSS would cost the UK economy over £12 billion
- Most disruption to GNSS-dependent systems is caused by unpredictable threats on the ground, like radio frequency interference (RFI) from jammers or faulty equipment, multipath signals reflecting off buildings, and noise in adjacent frequency bands; increasing events of signal spoofing, or the transmission of fake GNSS signals

Threat vectors to PNT by Risk Score

14. Criminal + Privacy 1 Yr Total	125
16. Terrorist Jamming	125
18. Military-style Jamming	125
11. Unintentional RF	25 - 100
7. Human Error/software	15 - 75
13. Criminal Jamming (1 event)	75
12. Privacy seeker (1 event)	75
17. Terrorist Spoofing	55
6. Solar Activity - powerful	50
19. Nat. Agent Spoofing	48
15. Criminal Spoofing (1 event)	48
20. Attack on Satellites	25
9. Control Segment Failure	25
22. Cyber Attack Control Segment	24
5. Solar Activity - moderate	24
2. Terrain obstruction	10
1. Built structure obstruction	10
10. Space Debris	8
3. Foliage (pines, hvy canopy)	5
4. Solar Activity – mild	5
8. Satellite malfunction	4
21. Attack on Control Segment	1.4

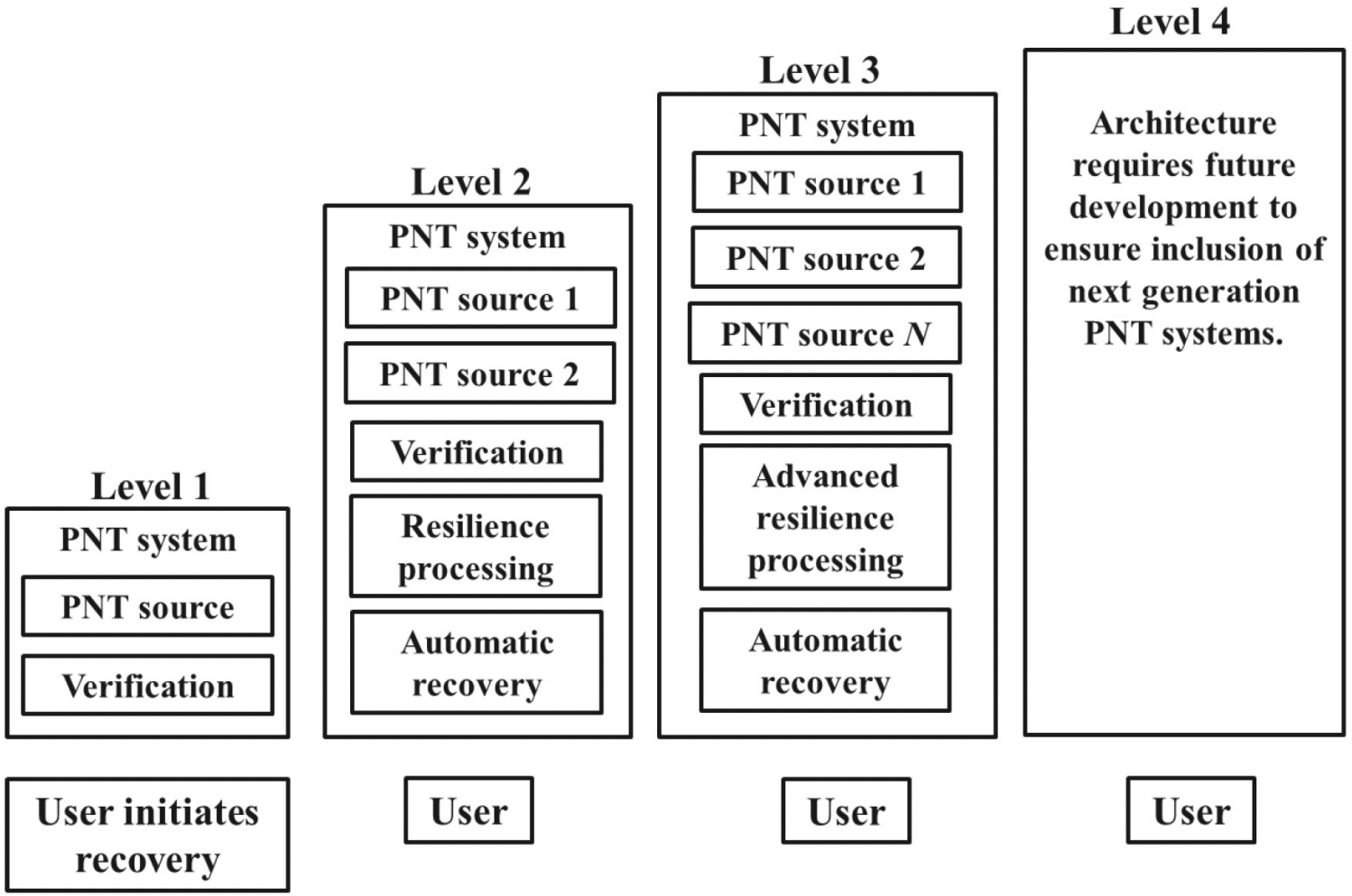
Risk Assessment and Categorization

- Need for a commonly accepted way of categorizing a system's level of resilience, and commonly agreed test methodologies for evaluating whether a system exhibits the required level of resilience
- United States Department of Homeland Security has drawn up a **Resilient PNT Conformance Framework**
- Sets out five levels of resilience, from 0 (not resilient) to 4 (most resilient), and describes what the outcome should be at levels 1–4 in terms of the system's ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions
- A Level 1 system may not function while an incident is occurring (and thus is not robust), but can be manually reset to its normal working state afterwards. A Level 4 system, by contrast, should continue to provide a PNT solution with no degradation of performance throughout the incident, and any affected components will auto-recover with no need for manual intervention

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.

Risk Assessment and Categorization

High-level system architectures corresponding to resilience levels



Risk Assessment and Categorization

- Resilient PNT Conformance Framework doesn't define how resilience should be practically measured, or provide any test methodologies or scenarios to help regulators, buyers and users establish the resilience of a given system
- The Institute of Electrical and Electronics Engineers (IEEE) is in the process of defining technical standards for PNT resilience – but creating standards that work everywhere and for everyone will be a difficult task
- By creating common definitions for different levels of resilient PNT systems, this new standard will enable vendors to differentiate their products from non-resilient PNT systems, as well as enable end-users to make deliberate, risk-informed decisions as to which systems are most appropriate for their applications and needs.

Function and design of PNT systems vary enormously - IEEE and its industry partners need to define test methodologies that allow the resilience of any given PNT system to be reliably measured

Threats to PNT systems are highly variable and constantly evolving - A GNSS receiver that conforms to Level 4 resilience in 2022 may be less resilient by 2025 if a previously unknown type of spoofing emerges in the interim – need to constantly evolve

As many critical PNT systems will be used internationally gaining international consensus on resilience standards and test methodologies is required

Way Forward

- The most obvious step is to upgrade what is already in place. GPS III is a next-gen form of GPS being developed, based on new GPS Block IIIA satellites which include sophisticated anti-jamming features and allows accuracy up to 3 times greater than that of GPS satellites currently in use
- Hybrid PNT with terrestrial/ ground-based PNT systems - RF spectrum is filled with signals intended for other purposes like mobile phone service, Wi-Fi, etc. These signals are lower frequency and more difficult to jam than GPS signals. By using them for navigation, these ground-based systems can also act as an effective redundant PNT system, providing backup for areas where GPS signals are unavailable
- The ultimate goal at some point in the future is to have a completely autonomous PNT source within a device or vehicle that doesn’t require positioning and timing from external sources but still offers PNT at the same or higher quality than existing systems

References

- Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework v 1.0

(https://www.dhs.gov/sites/default/files/publications/2020_12_resilient_pnt_conformance_framework.pdf)

- Prioritizing Dangers to the United States from Threats to GPS – Ranking Risks and Proposed Mitigations

(https://rntfnd.org/wp-content/uploads/12-7-Prioritizing-Dangers-to-US-fm-Threats-to-GPS-RNTFoundation.pdf)