ELECTRONICS & DEFENSE

(Resilient)^{2}PNT

A Robust Solution Combining Device & Network Resiliency

The dependency on Position, Navigation and Timing (PNT) services for critical infrastructure has continuously increased in the last decades. It is widely accepted that GNSS vulnerabilities represent a real threat for critical infrastructures mainly depending on GNSS as timing source. Recently, the EU commission launched an initiative (AltPNT) to evaluate technologies to enhance the resiliency of PNT to GNSS vulnerabilities. Rather than a single technology, we illustrate how diverse technologies can complement each other to enhance resiliency.

#Trustable #Resilient #rPNT #HighAccuracy #FollowTheWhiteRabbit

Device based resiliency

- Resiliency to Jamming (GNSS denied scenario):
  - Multi-band & multi-constellation for cross-validation
  - IDM suite for early detection of threats
  - External passive hydrogen maser (PHM) or local holdover (DOCXO, mini-Rubidium mRO)
  - Optional LEO STL (Satelles) tracking if GNSS L1/E1 bands are jammed
- Resiliency to Spoofing:
  - Open Service Navigation Message Authentication (OSNMA) for Galileo allows spoofing detection
  - STL is fully encrypted to protect against spoofing

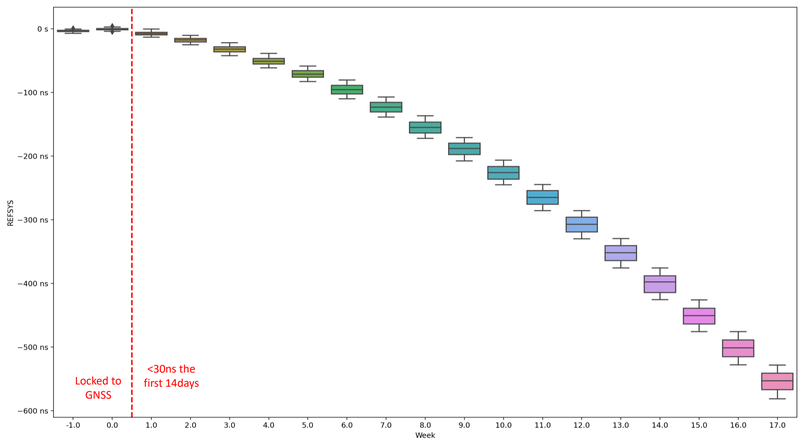
Network based resiliency

- WR/PTP-HighAccuracy (sub-ns time transfer capability) allows measuring and comparing distributed GNSS spread at tens of km.
- Smooth switching mechanism from one timing source to the other with no degradation in case the majority differs from actual timing source (voting scheme as trust metric).
- PTP might be used as backup PNT source with bounded degraded performance

→ Resilient^{2}PNT=(Device Resiliency x Network Resiliency)

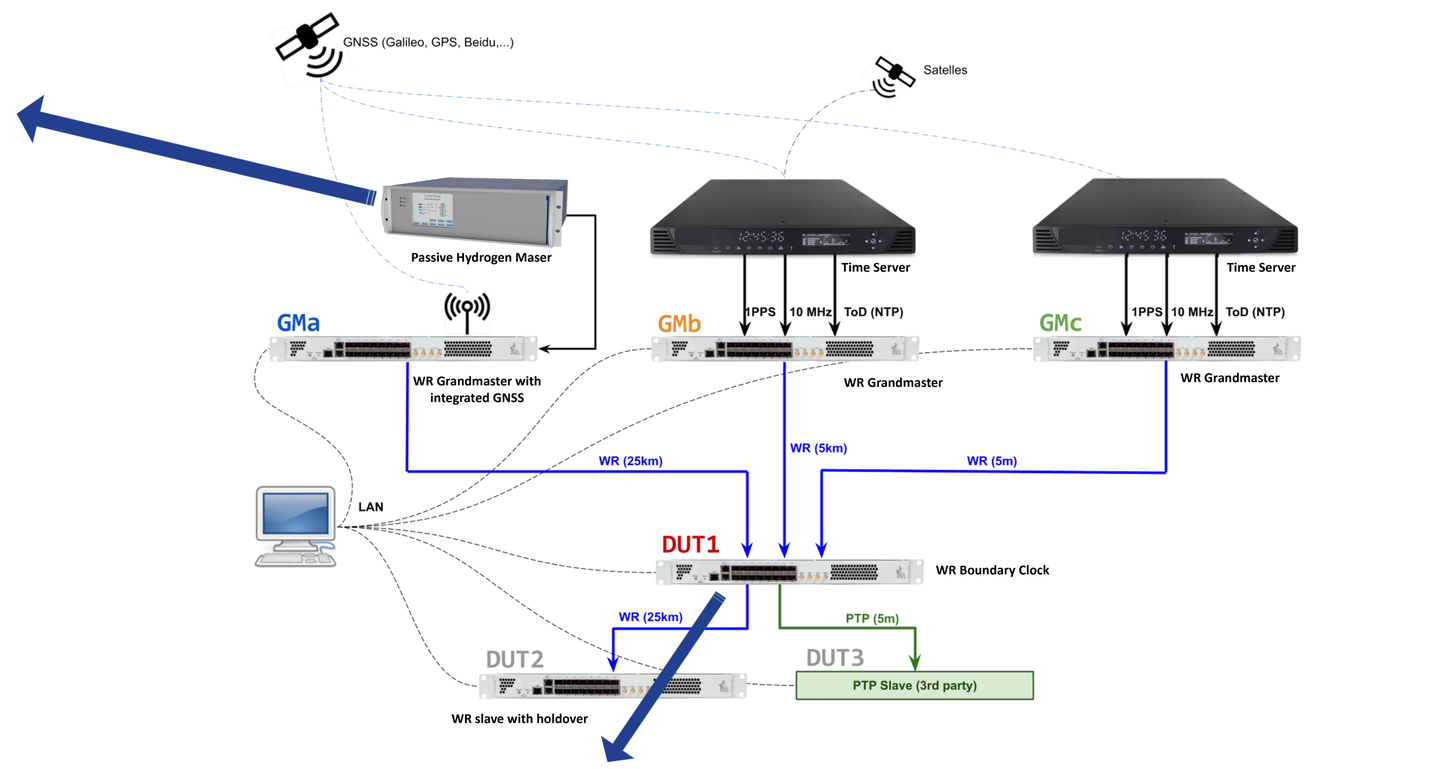
Level 1	Level 2	Level 3	Level 4
✓ User initiates recovery	✓ Identify and isolate possible threats ✓ Continue operating with degraded performance	✓ At least 3 cross-verified PNT sources ✓ Continue operating with bounded performance	✓ Cross-connected PNT sources ✓ Continue operating with no degradation

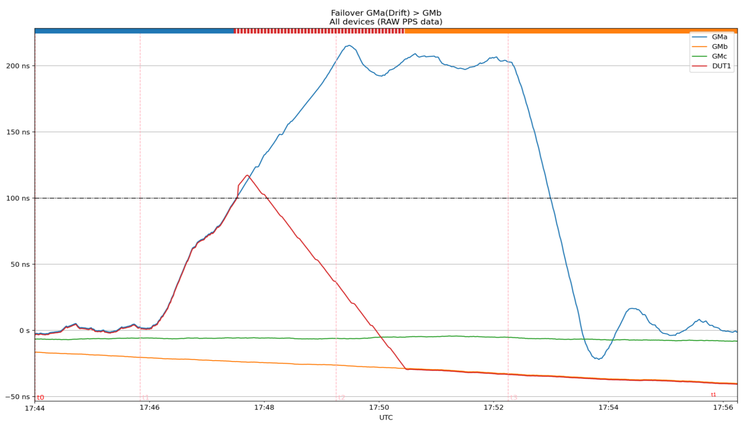
ResilientPNT solution fulfills all levels according to DHS



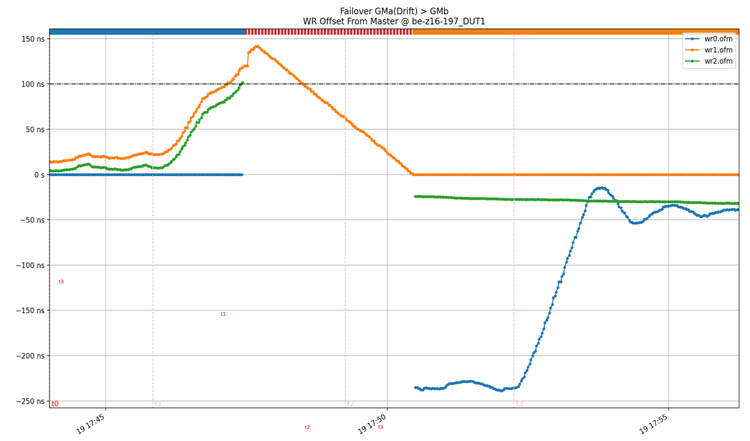
Long-term holdover (120days) of the passive hydrogen maser

Use case:
Setup presented during the altPNT demo day where multiple test scenarios run by JRC has been successfully fulfilled.

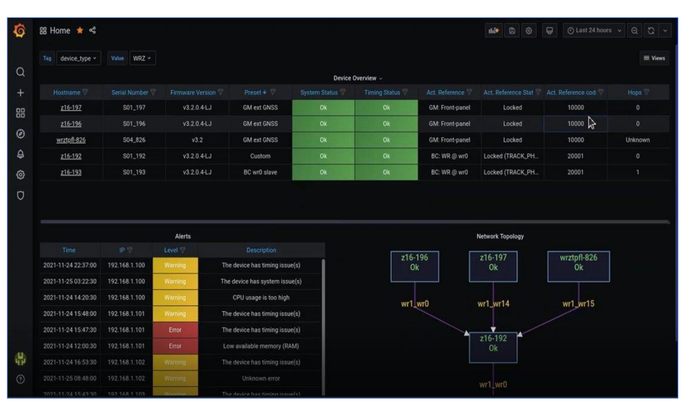




External PPS measurement in laboratory
At t1, a drift of 1ns/s is simulated on GMa . At t2, it is stopped and then reverted at t3. The device under test (DUT1) shows how it smoothly failing over GMa to GMb



Measuring at the device under test (DUT1)
Both GMb & GMc are drifting from the actual time reference (GMa) which means that GMa is under attack. The voting mechanism embedded in **DUT1** detect it and recover switching from GMa to GMb.



Monitoring framework
Main dashboard view of the **centralized monitoring system** installed in the monitoring server. It retrieve alerts from SNMP and SYSLOG. It also uses LLDP for topology discovery and reverse PTP.

SAFRAN