Pushing the limits of ePRTC

100 nsec holdover over 100 days

Alon Stern, Senior Manager of Technology, Oscilloquartz

WSTS 2024

GPS/PNT threats became a real concern

Russia's Advances on Space-Based Nuclear Weapon Draw U.S. Concerns

A congressman's cryptic statement about new intelligence set Washington abuzz and infuriated White House officials.

NY Times, Jan 2024

As Threats in Space Mount, U.S. Lags in Protecting Key Services

GPS has become essential for modern life, but its satellites and signals are vulnerable to attack. China is years ahead in developing alternatives.

NY Times, March 2024

The Russians Installed A GPS-Jammer In Ukraine. The Ukrainians Blew It Up – With A GPS-Guided Bomb: Forbes

by Editor | Nov 1, 2023 | Blog

Senior US official warns of security threat amid reports of Russian nuclear capability in space

The Gaudian, Feb 2024

House Intel chair's cryptic warning about "serious national security threat" prompts officials to urge calm

CBCNews, Feb 2024

Electronic Warfare Confounds Civilian Pilots, Far From Any Battlefield – NY Times

by Editor | Nov 23, 2023 | Blog

UK government PNT plan focuses on policy, timing center, eLoran, defense time and SBAS

October 18, 2023 - By Dana Goward

Russia is starting to make its superiority in electronic warfare count – The Economist

by Editor | Nov 27, 2023 | Blog

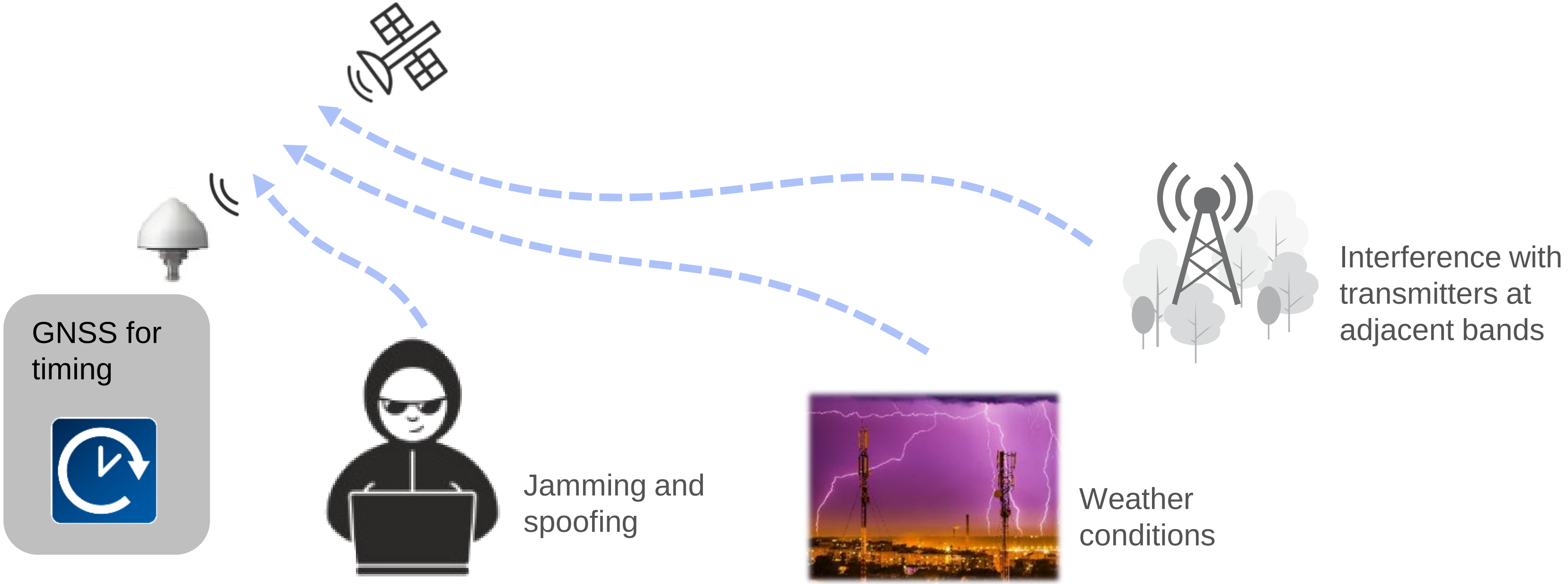
DAILY HONKER

Mysterious GPS Disruptions Spread Across Texas; FAA Issues Warning to Pilots

Oct 19, 2022

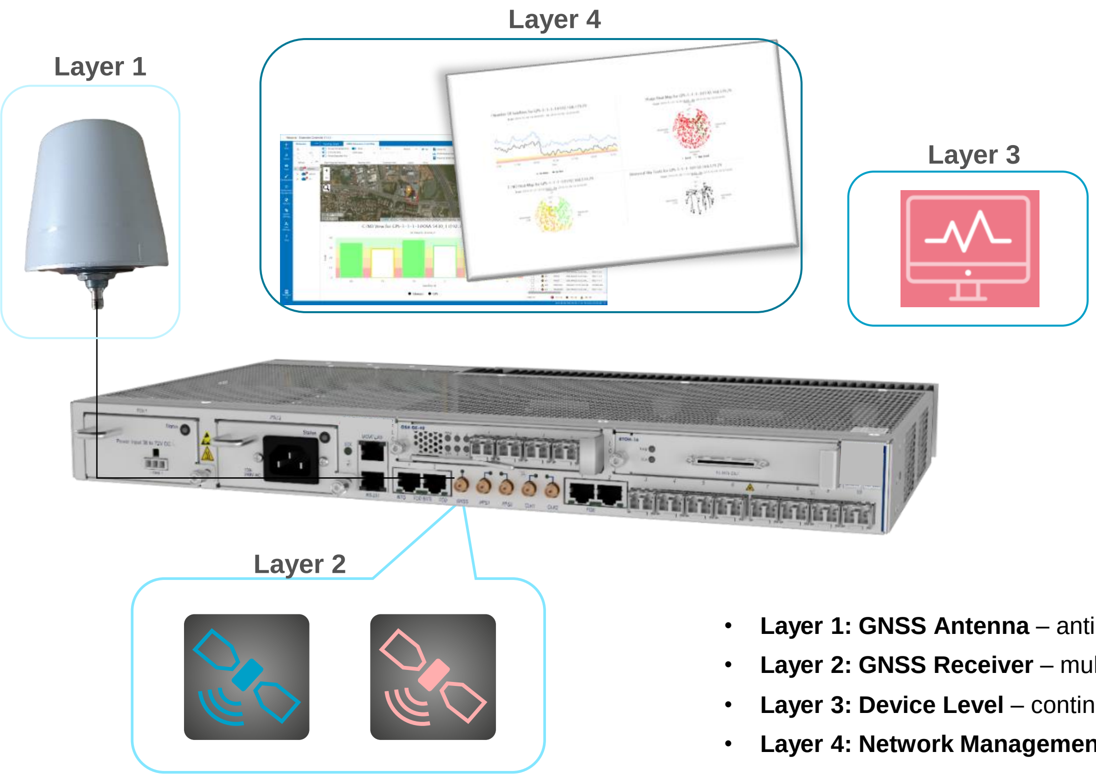
What would happen if GPS was attacked?

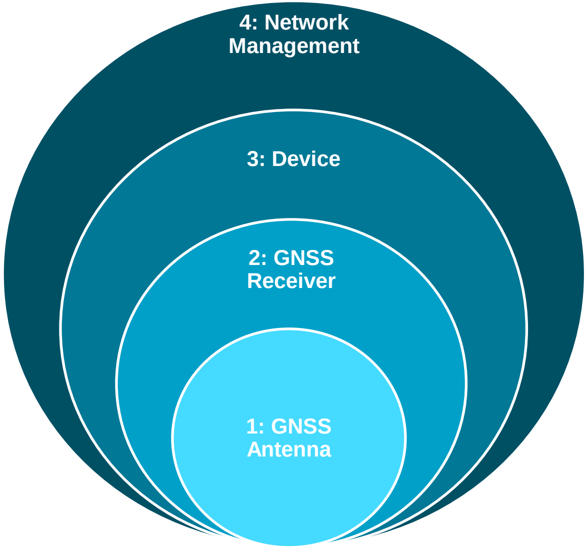
We heavily rely on GNSS - but it is very vulnerable



Department of Homeland Security (DHS) : GPS is a single point of failure risk & unreliable for PNT services

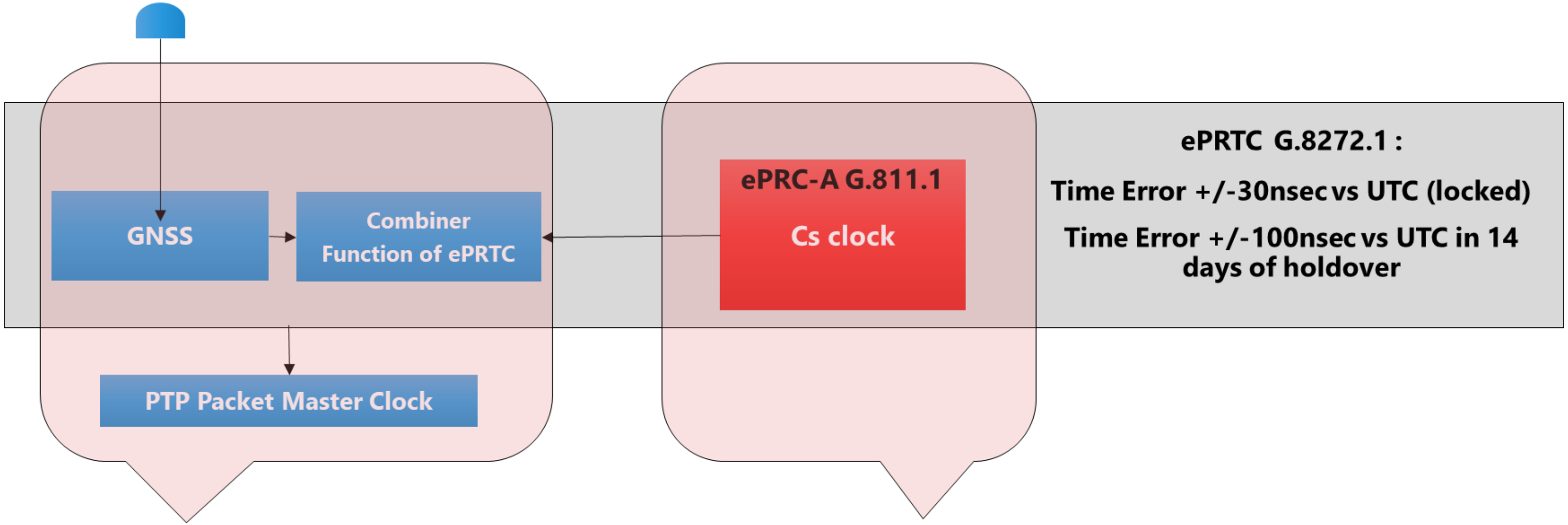
Multilayer threat detection





- **Layer 1: GNSS Antenna** – anti-jam/spoof antennas
- **Layer 2: GNSS Receiver** – multi-constellation / multi-band receivers with jam/spoof detection
- **Layer 3: Device Level** – continuous monitoring to mitigate spoofed GNSS vs PTP signals
- **Layer 4: Network Management** – Monitor all network clocks (GNSS/PTP/ etc.)

Solution: Mitigation using ePRTC implementation



ePRTC combiner + PTP GM

Cesium Atomic clock

Growing need to maintain normal timing performance during extended GNSS outages

30 days locked ➔14 days in holdover

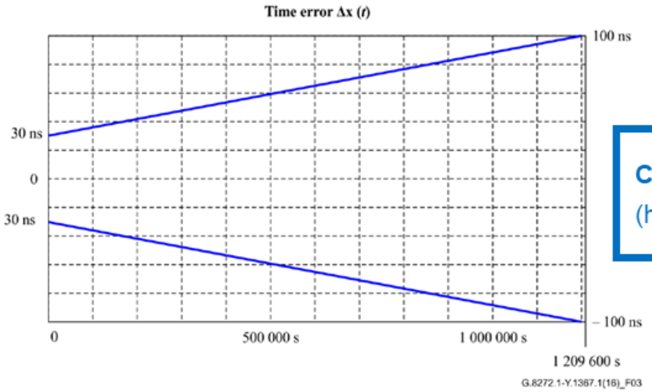


Figure 3 – ePRTC-A phase/time holdover requirements

Changed to Parametric Holdover

(holdover time depends on locked period)

6 days locked ➔6 days in holdover

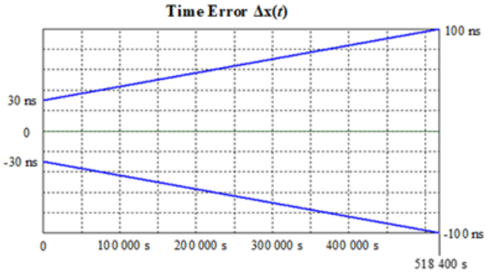
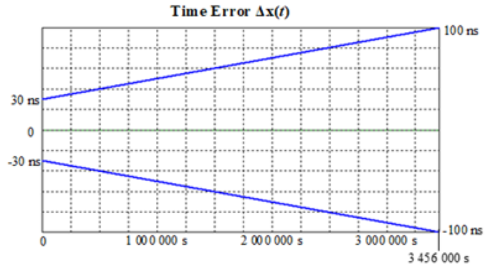


Figure V.2 – ePRTC-A phase/time holdover requirements for L = 6 days

40 days locked ➔40 days in holdover



Does 40 holdover days are enough for PNT?

New ePRTC standard provides up-to 40 days in holdover during GNSS outages

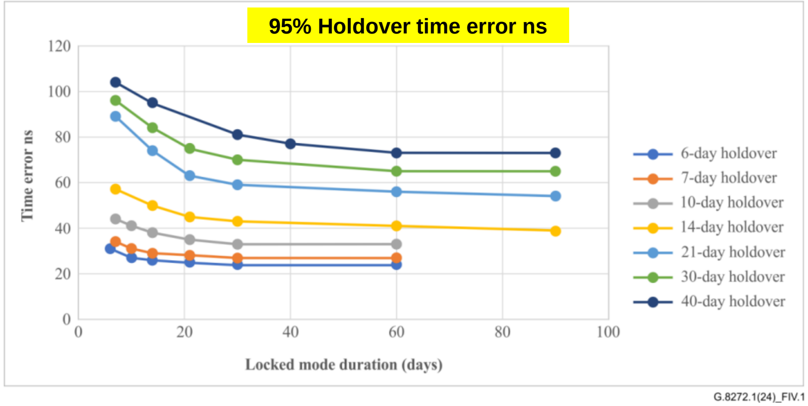


Figure IV.1 – Holdover time error vs locked-mode duration for various holdover periods ranging from 6-day holdover to 40-day holdover

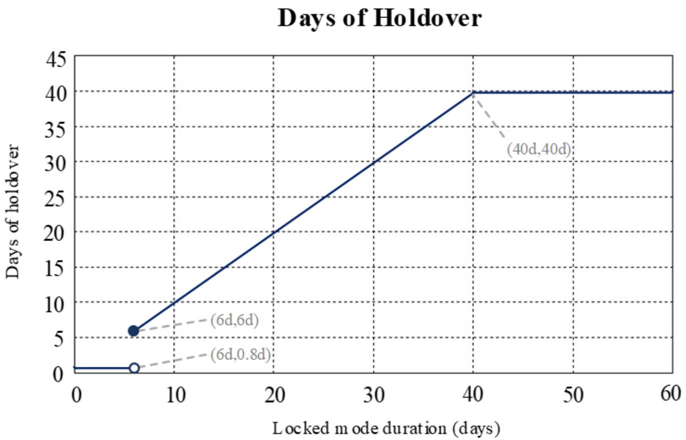


Figure V.1 – Days of holdover as a function of locked mode duration (graphical representation of Table 3)

Parametric holdover is based on simulations with 95% (2σ) confidence intervals

Pushing the limits of ePRTC - Improving resiliency in the face of increasing GNSS vulnerabilities

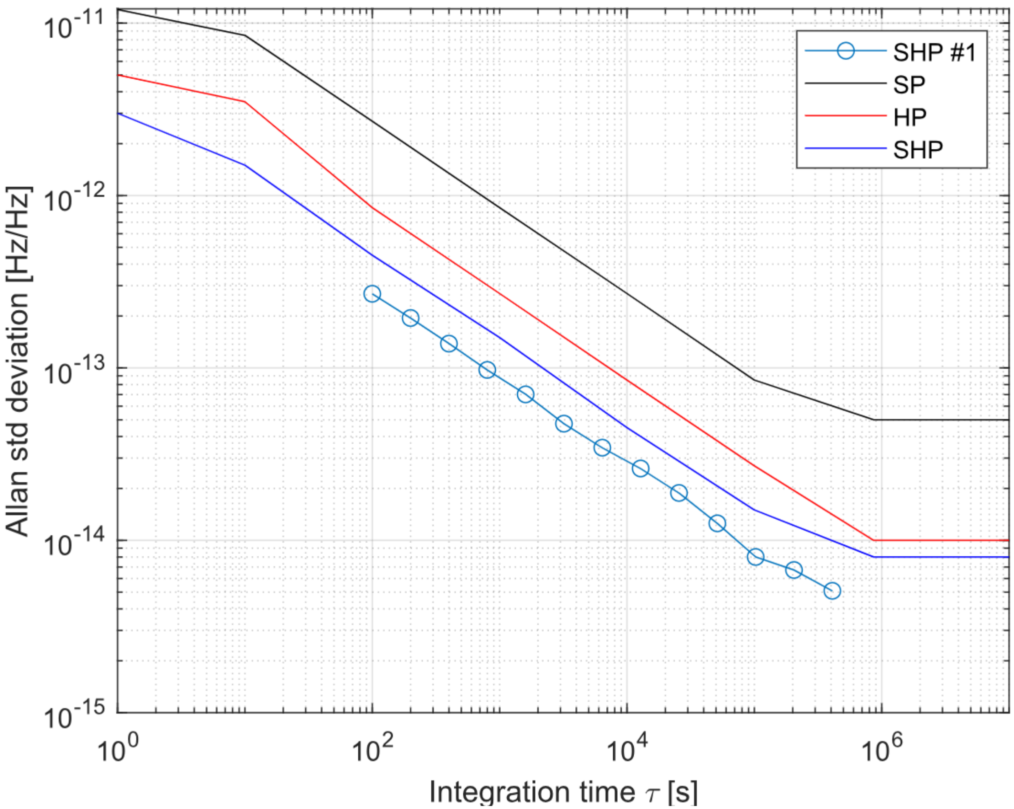
Can the industry accommodate longer holdover period that is required by the market?

Why not 100 days if possible?

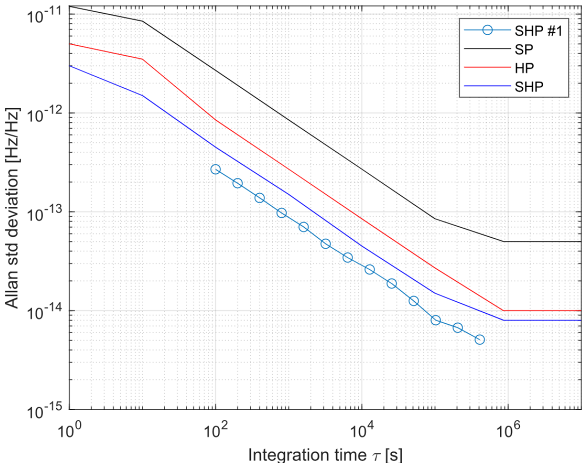
Target mission critical infrastructure sectors under national security threats

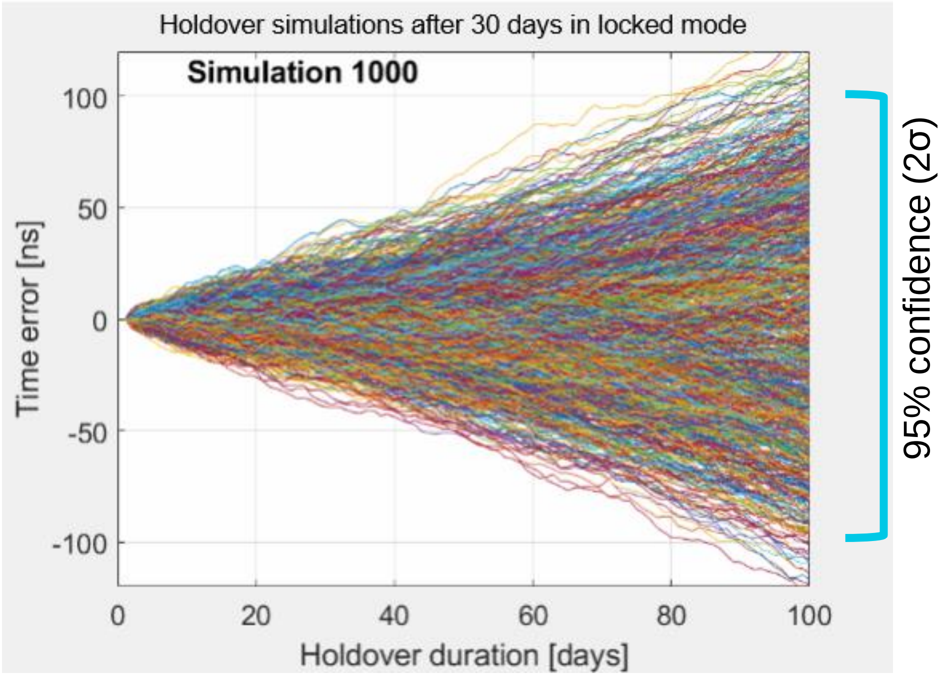
- Power grids
- Finance
- Transportation
- 5G Communications
- Defense Communications
- 5G/Defense Data centers

ePRTC holdover performance is starting from the Cesium's ADEV performance



Holdover simulations, based on real Cesium clocks, provides performance with confidence intervals





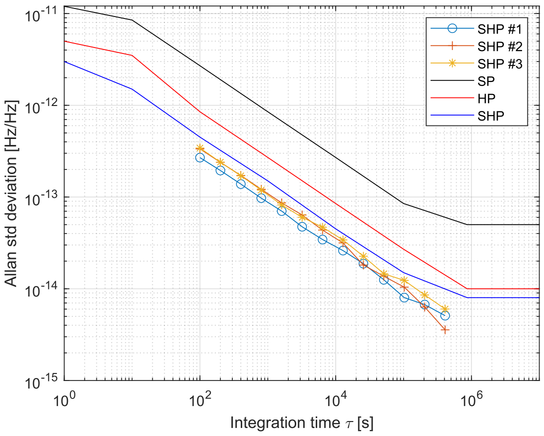
1000 simulations, 100 days for each simulation ➔ more than 250 years of simulation

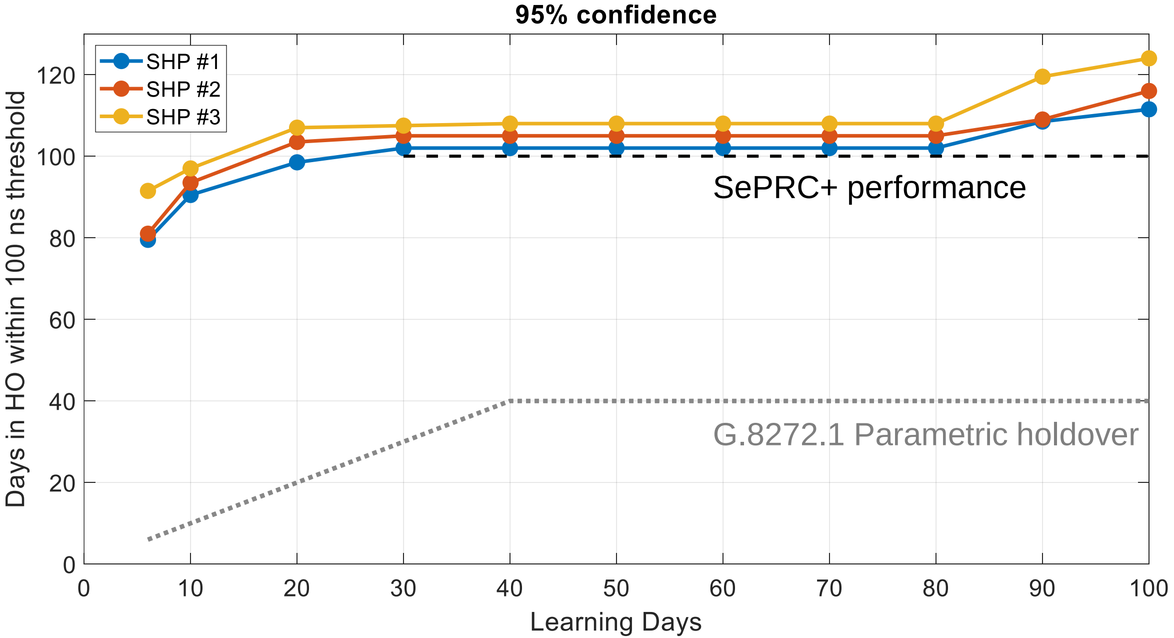
OSCILLOQUARTZ
A division of Adtran

Holdover estimations using simulations provides strong statistical confidence

- 1000 simulations for multiple SHP measured Cesium clocks, characterized by ADEV mask
- Perform simulations across a range of durations in locked mode to estimate holdover performance for different learning periods, from 6 to 100 days
  - More than 250 years of simulations
- Assess the holdover performance for each learning duration with a 95% confidence level (2σ), utilizing the 95th percentile from all simulations

SePRC+ exceeding holdover standard limits
<u>100nsec</u> holdover over <u>100 days</u> with 95% confidence (2σ)





100nsec over 100 days requires SHP clock

OSCILLOQUARTZ
A division of Adtran

Measured SePRTC+ performance with SHP tube

Summary

- GNSS provides 100nsec high time accuracy, but faces significant vulnerabilities
- G.8272.1 ePRTC parametric holdover mitigates against GNSS vulnerabilities, maintaining normal timing performance for up to 40 days during GNSS outages, depending on the learning period
- 100nsec holdover over 100 days is achievable and was proven today
- Pushing the limits of holdover performance above 100 days, remains a major technological challenge for the vendor to break, the more is better
- Simulating atomic clock holdover using data from actual Cesium clocks characterized by ADEV, provides performance insights with confidence intervals
- SePRC+ holdover limit exceeds G.8272.1 parametric holdover and achieves 100nsec over 100 days
- Longer holdover period will allow to set ePRC as primary source

Thank you

Pls contact me in case you have any comments or questions : alon.stern@adtran.com

oscilloquartz.com