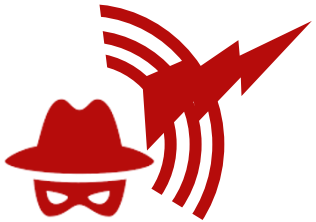
GPS/GNSS Jamming & Spoofing Mitigation Best Practices & Strategies

WSTS 2021

Nino De Falcis, Sr Director, Business Development Americas

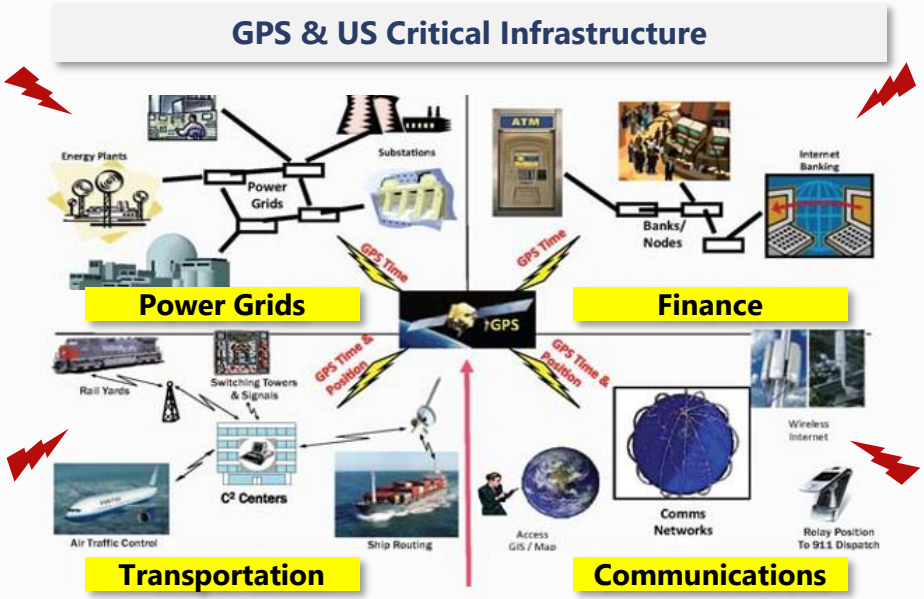
OSCILLOQUARTZ
An ADVA Company

The Problem



PNT Cyberthreats

Protecting US Critical Infrastructure from PNT Disruptions*



Homeland Security

***Economic Cost: $1B/day**[1]

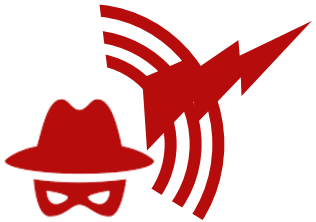
All supported by

Data Centers

[1]Source: RTI & NIST 2019

OSCILLOQUARTZ An ADVA Company

PNT Vulnerabilities



PNT Cyberthreats

GPS/GNSS Level

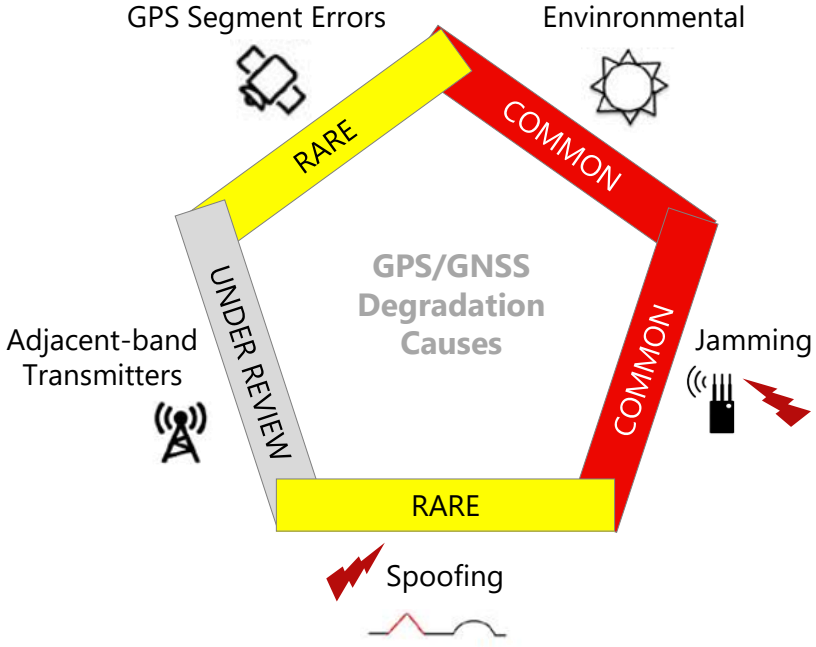
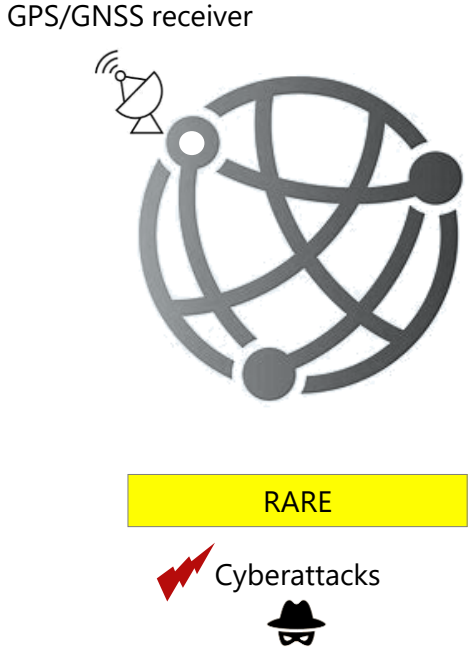


Figure 4.1 – Known GPS vulnerabilities to telecom

Network Level



OSCILLOQUARTZ
An ADVA Company

DHS Resilient PNT Guidelines

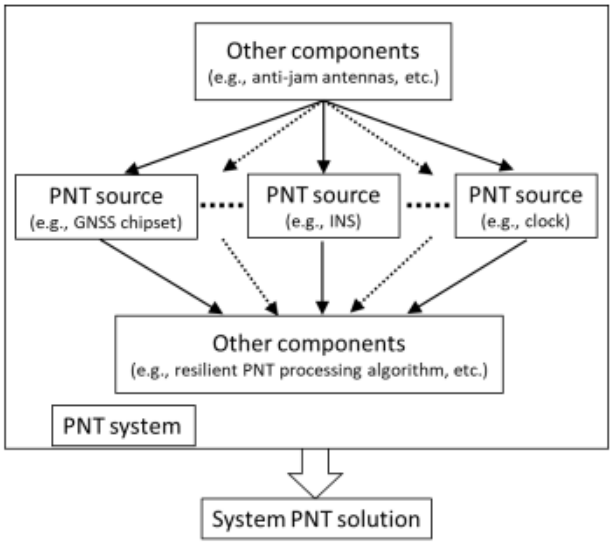
Driven by US Federal Executive Order 13905 of Feb 2020

Resilient PNT Conformance Framework*

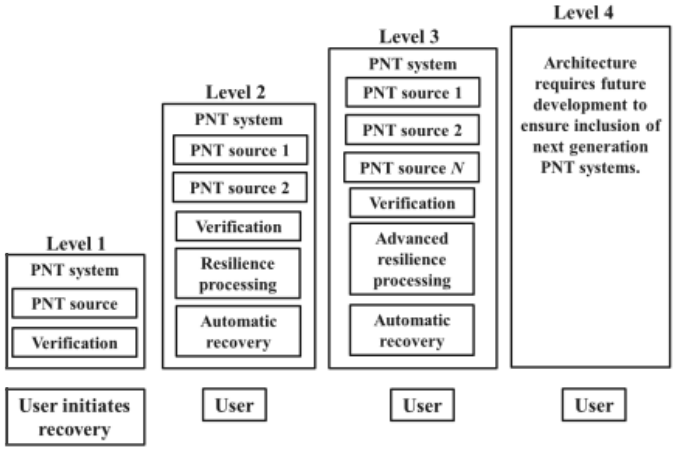
PNT Defense in Depth

Core Functions

Functional Diagram



Resiliency Levels



*source: DHS

OSCILLOQUARTZ An ADVA Company

DHS Anti-Spoofing Open-Source Resources

Released on Feb 26, 2021

PNT Integrity Library & Epsilon Algorithm Suite*

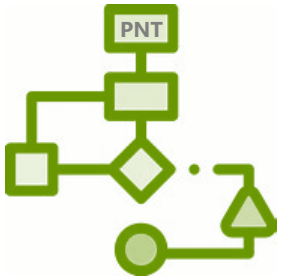
PNT Defense in Depth

Spoofing Detection Library

- Designed for GNSS receiver/time server OEMs
- Provides spoofing detection capabilities for GNSS PNT sources
- Provides scalable framework for GNSS PNT manipulation detection
- Allows additional checks to be added as new threats arise

GNSS Spoofing Detection Algorithm

- Detects inconsistencies in position/velocity/ clock observables provided by GPS receivers
- Enables end-users to have basic spoofing detection capabilities without any modifications to the existing GPS receiver



*source: DHS

OSCILLOQUARTZ An ADVA Company

NIST Resilient PNT Guidelines

Driven by US Federal Executive Order 13905 of Feb 2020

Cybersecurity Profile for PNT Services*

PNT Defense in Depth

Goals

Framework

Core
- Guidance & controls

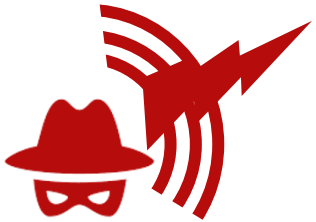
Implementation Tiers
- Qualitative measurement of cybersecurity risk management practices

Profile
- Alignment of requirements & objectives, risk appetite, & resources

*sources: NIST.IR.8323 & NIST

OSCILLOQUARTZ An ADVA Company

Best Practice Approaches against PNT Cyberthreats



PNT Cyberthreats

Multilayer Detection

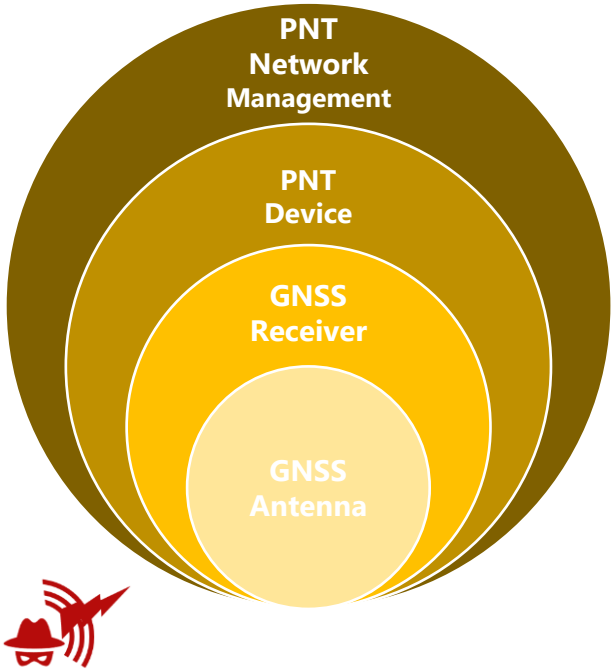
Multisource Backup

Fault-Tolerant Mitigation

Resilience/Robustness/Cybersecurity Augmentation

OSCILLOQUARTZ
An ADVA Company

Multilayer Detection Approach



Level 1: GNSS Antenna

- Use anti-jam/spoof antennas, with threat alarms
- Add in-line anti-jam/spoof accessories, with threat alarms

Level 2: GNSS Receiver

- Use smarter multi-constellation/-band receivers, with jam/spoof & satellite count monitoring, jam mitigation, spoof detection, etc., and threat alarms

Level 3: PNT Device

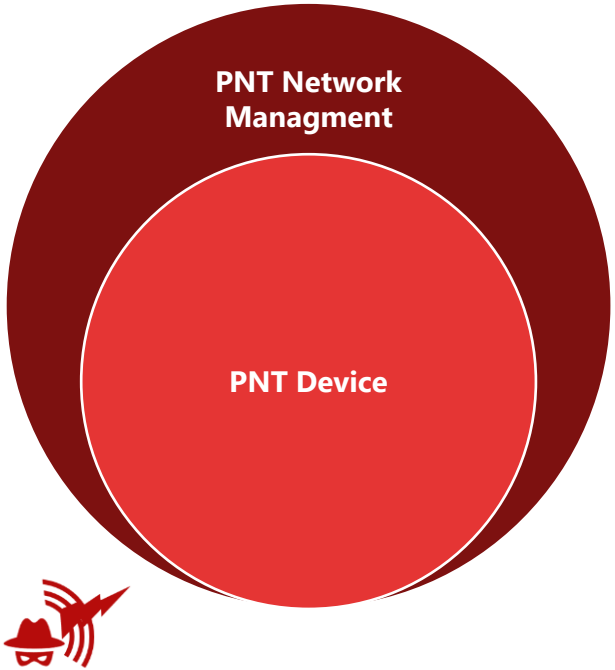
- Use/compare 2 GNSS receivers, in fixed & nav mode, to detect location/phase/time change, with spoof alarms
- Monitor/compare/verify multisources (GNSS/PTP), with jam alarms

Level 4: PNT Network Management

- Manage/monitor/compare/verify all network devices (GNSS/PTP/ etc.) in real-time, with AI/ML-based threat analytics/alarms

4 Levels of Jamming/Spoofing Detection

Multisource Backup Approach



Level 1: PNT Device

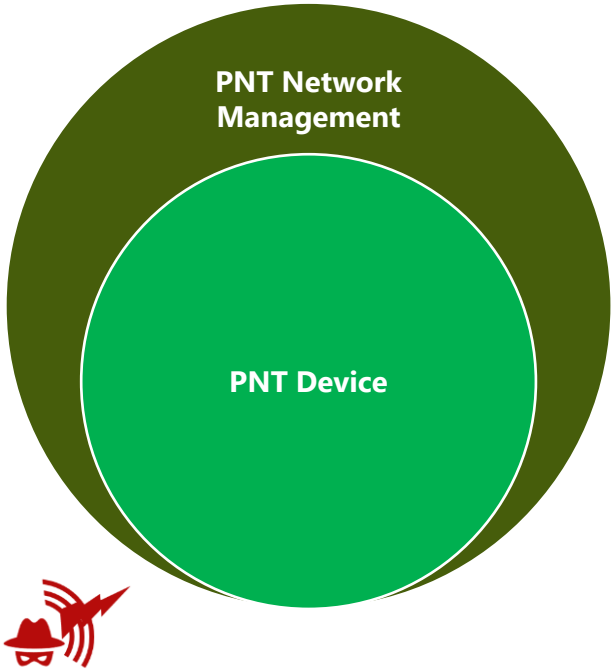
- **Source 1**: Use GNSS receiver(s) or DoD M-code receiver
- **Source 2**: Use local holdover clock (super Crystal or Rubidium atomic)
- **Source 3**: Use external standalone (no antenna) Cesium atomic clock, to provide a trusted ePRTC (enhanced Primary Reference Time Clock) with verified GNSS/PTP sources
- **Source N**: Use other sources/clocks of opportunity like White Rabbit (SyncE+PTP), etc.

Level 2: PNT Network Management

- **Source 4:** Use/manage network NTP/PTP time feeds
- **Source N**: Use/manage other sources/clocks of opportunity like White Rabbit (SyncE+PTP), etc.

Augmented PNT Resilience & Robustness

Fault-Tolerant Mitigation Approach



Level 1: PNT Device

- Monitor/compare/verify multisources (GNSS/PTP), with fault-tolerant failover based on detected GNSS jamming/spoofing & network cyberthreat alarms

Level 2: PNT Network Management

- Manage/gather/analyze/visualize all network device data in real-time, then use AI/ML analytics to detect, mitigate & prevent:
  - Jamming/spoofing based on GNSS receiver observables, with threat alarms
  - GNSS environmental obstruction, with threat alarms
- Use a centralized, fault-tolerant network management & monitoring system at scale, with multisource failover in case of jamming/spoofing threats
- Gain complete control/visibility of threats across the network, with a geo map showing compromised/mitigated PNT devices

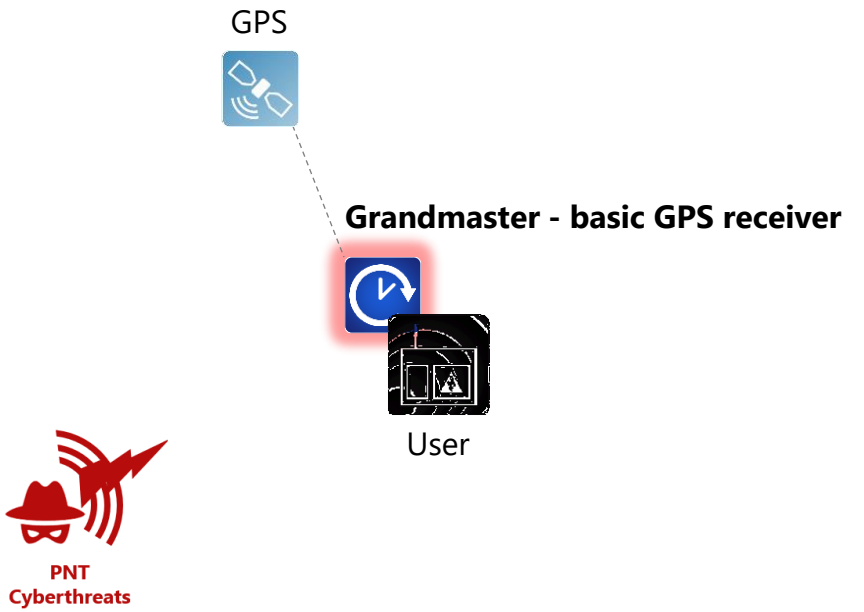
Complete PNT Control, Visibility & Assurance

Best Architecture Strategies against PNT Cyberthreats

Level 1 Resiliency

Problem

User **Level 0** PNT Disruptions



Solution

User **Level 1** PNT Resiliency

GNSS (multi-constellations - GPS, Galileo, etc.)

SB (single band) or

MB (multiband L1/L2/L5)

Grandmaster - 2 GNSS SB/MB receivers

- Fixed & Nav mode receivers to detect spoof events
- MB to mitigate jam events
- Holdover clock: super XO or Rb
- Anti jam/spoof software

Optional

- Anti-jam antenna
- In-line anti-jam/spoof accessory

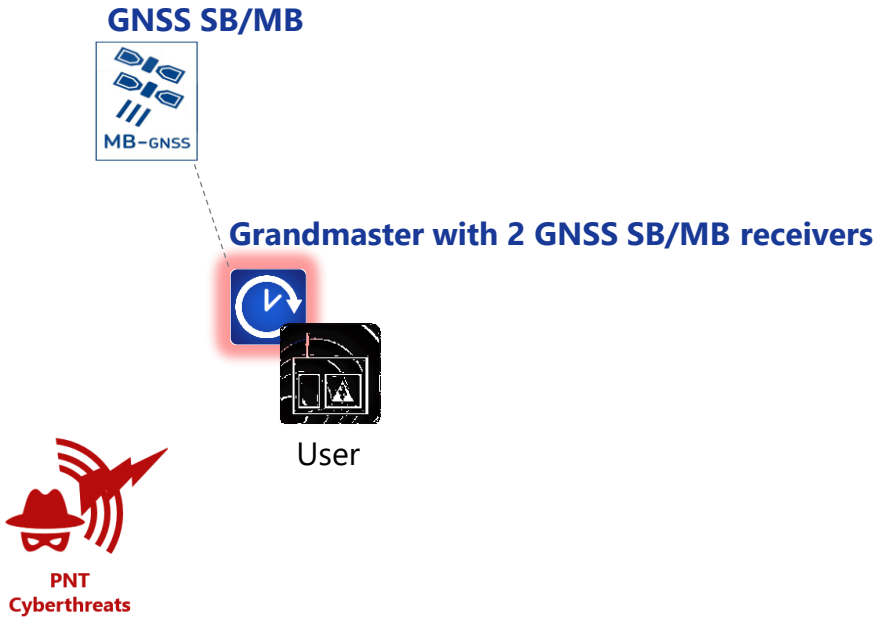
OSCILLOQUARTZ
An ADVA Company

Best Architecture Strategies against PNT Cyberthreats

Level 2 Resiliency

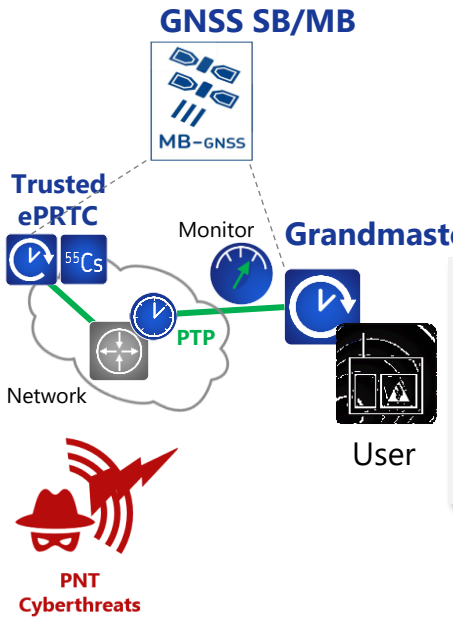
Problem

User **Level 1** PNT Disruptions



Solution

User **Level 2** PNT Resiliency



- Config same as level 1 resiliency

PLUS

- **PTP network time backup from ePRTC source**
- **PTP network time monitor**, with threat alarms

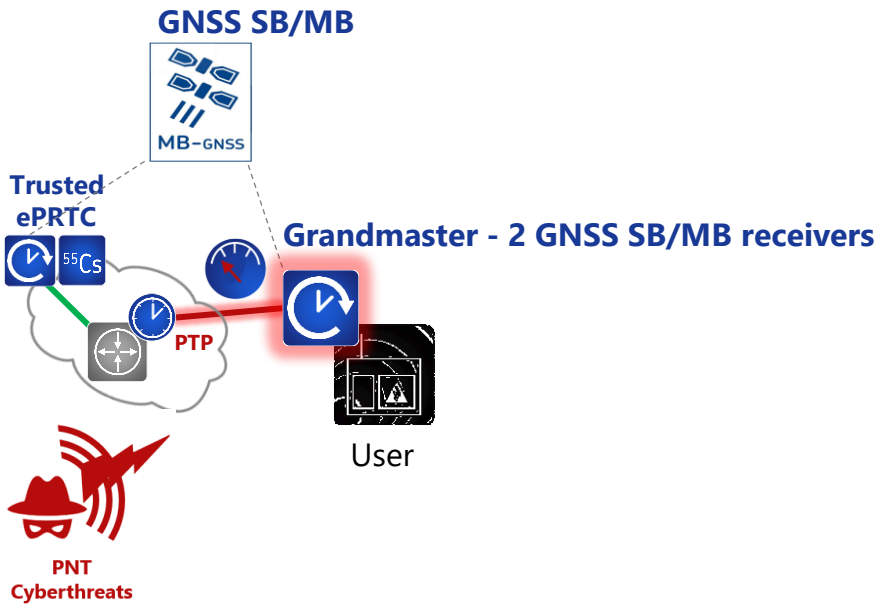
OSCILLOQUARTZ
An ADVA Company

Best Architecture Strategies against PNT Cyberthreats

Level 3 Resiliency

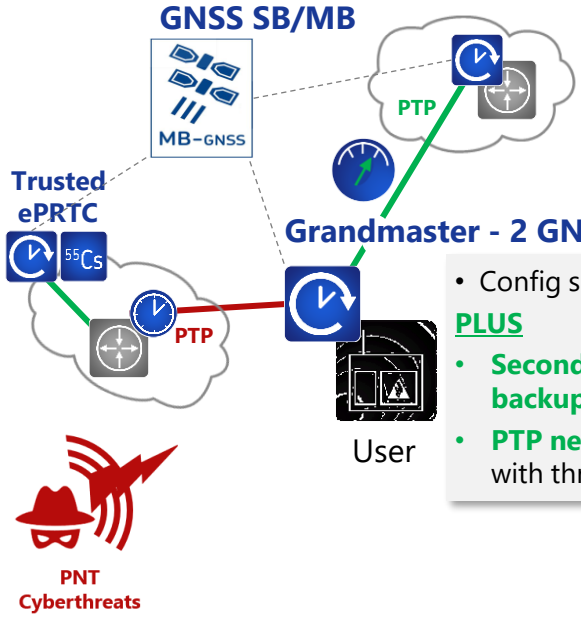
Problem

User **Level 2** PNT Disruptions



Solution

User **Level 3** PNT Resiliency



- Config same as level 2 resiliency

PLUS

- **Secondary PTP network time backup**
- **PTP network time monitor**, with threat alarms

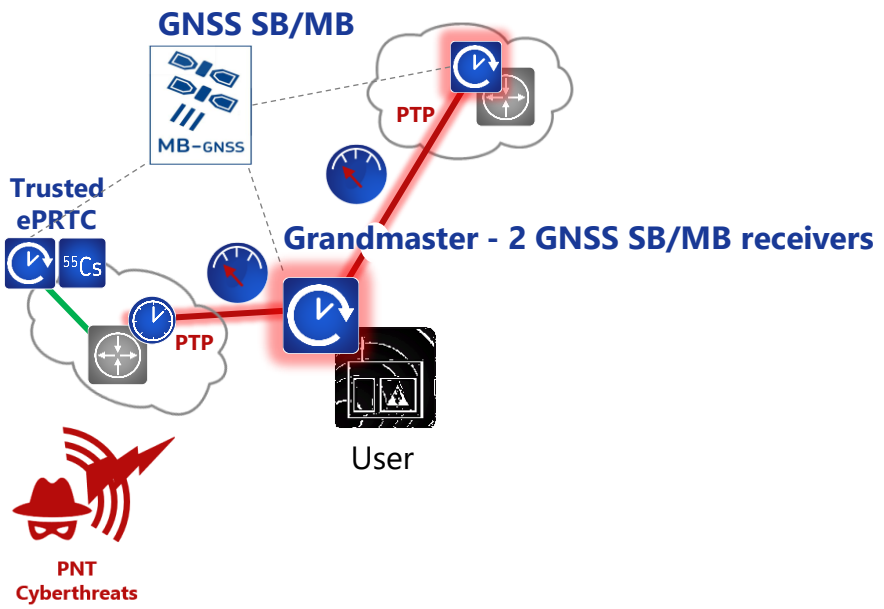
OSCILLOQUARTZ
An ADVA Company

Best Architecture Strategies against PNT Cyberthreats

Level 4 Resiliency

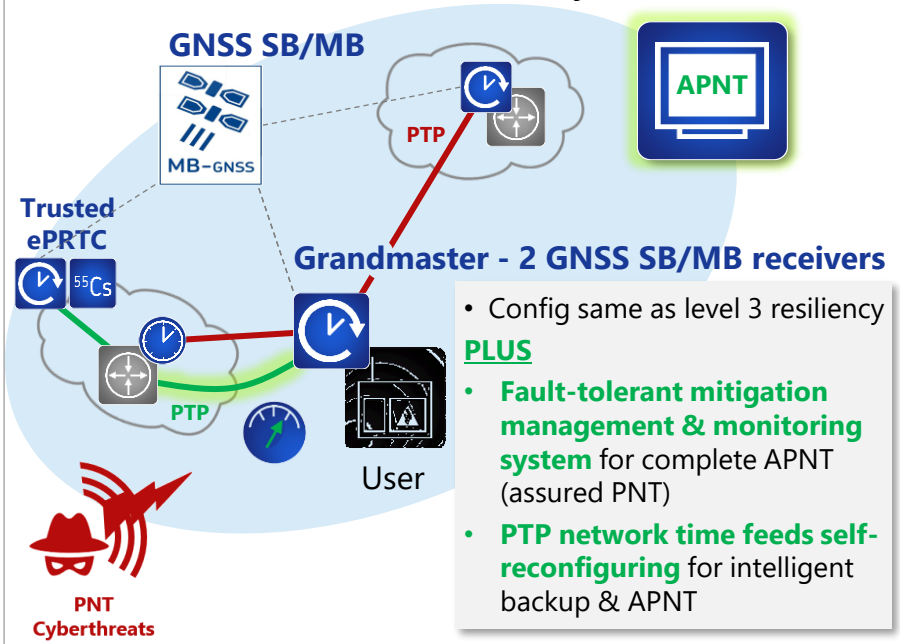
Problem

User **Level 3** Disruptions



Solution

User **Level 4** PNT Resiliency



- Config same as level 3 resiliency

PLUS

- **Fault-tolerant mitigation management & monitoring system** for complete APNT (assured PNT)
- **PTP network time feeds self-reconfiguring** for intelligent backup & APNT

OSCILLOQUARTZ
An ADVA Company

OSCILLOQUARTZ
An ADVA Company

Thank you

NDeFalcis@adva.com