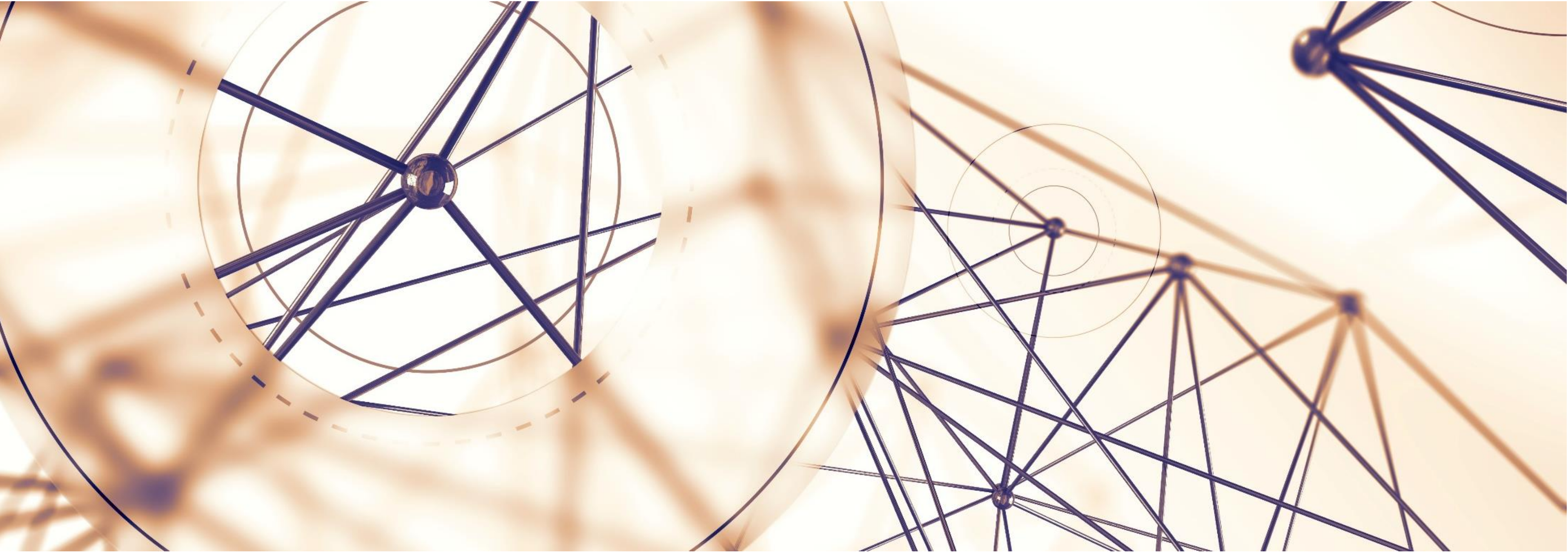


GPS/GNSS Jamming & Spoofing Mitigation Best Practices & Strategies

ITSF 2021

Nino De Falcis, Sr Director, Business Development Americas

OSCILLOQUARTZ
An ADVA Company

What is the aPNT mandate?

Driven by US federal gov's executive order 13905 of Feb 2020

- **Protect** critical gov & industry infrastructure against PNT disruptions from GPS/GNSS jamming/spoofing & cyberattacks

- **Define** critical infrastructure under national security threats
  - Power grid
  - Finance
  - Transportation
  - Communications
  - Data centers

- **Use** published PNT assurance guidelines in progress & evolving
  - DHS Resilient PNT Conformance Framework *(IEEE P1952 Resilient PNT UE working group)*
  - NIST Cybersecurity Framework for PNT Profile (*NISTIR 8323*)

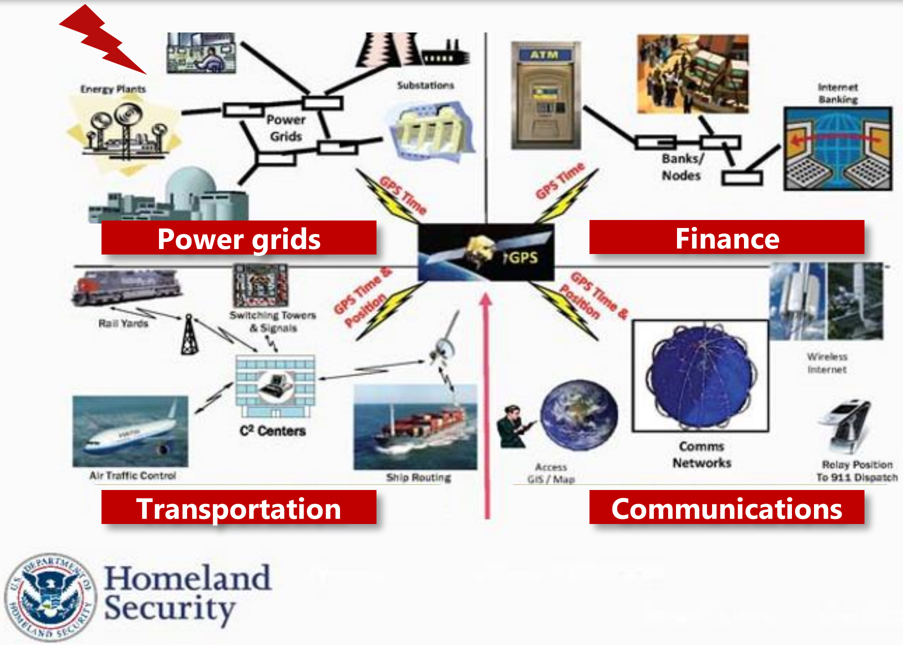
© 2021 ADVA. All rights reserved.

The problem

PNT
cyberthreats

$1B/day in economic cost if PNT is disrupted*

GPS & US critical infrastructure under national security threats



Power grids

Finance

Transportation

Communications

All supported by

Data centers

*source: RTI & NIST 2019

© 2021 ADVA. All rights reserved.

PNT cyberthreats & GNSS vulnerabilities

PNT cyberthreats

External GPS/GNSS level

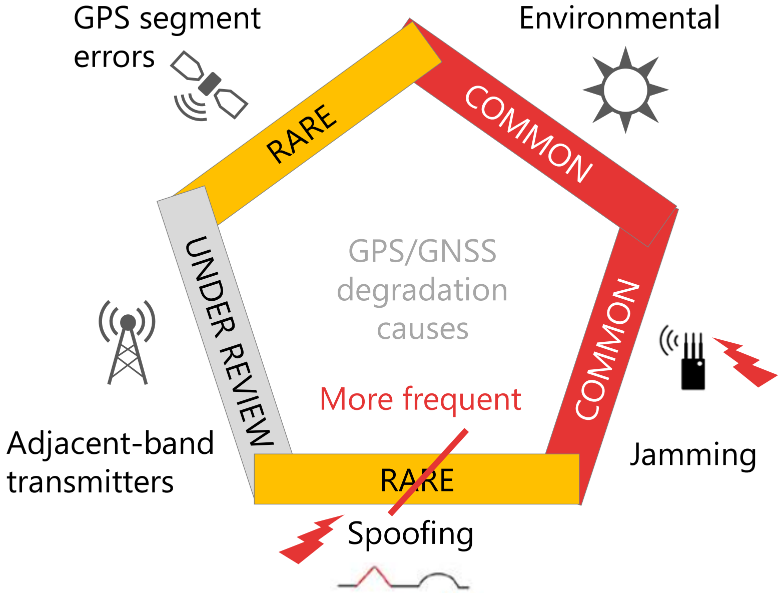
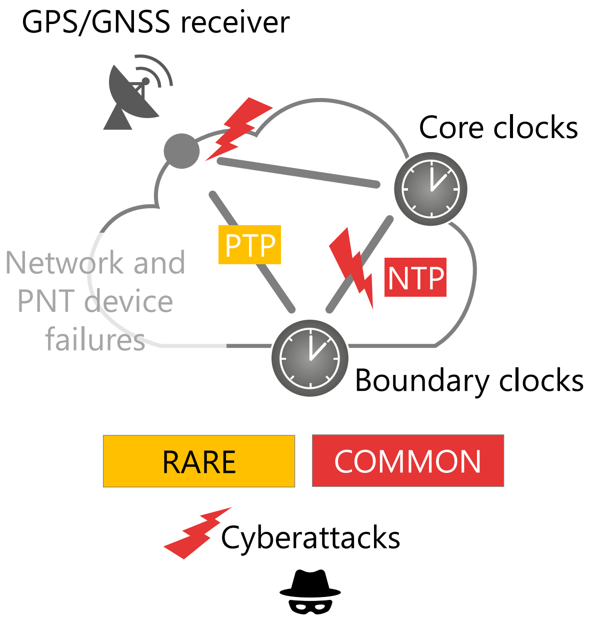


Figure 4.1 – Known GPS vulnerabilities to telecom

Internal network level

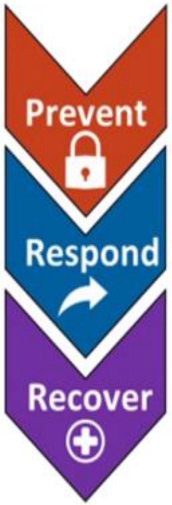


© 2021 ADVA. All rights reserved.

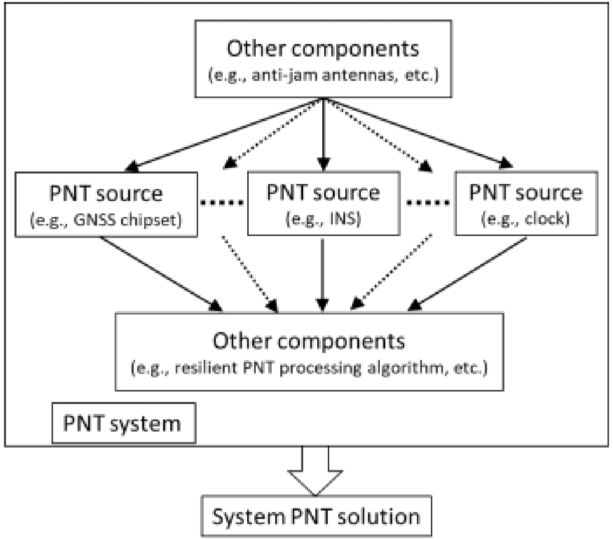
What are DHS' resilient PNT assurance guidelines?

DHS Resilient PNT Conformance Framework

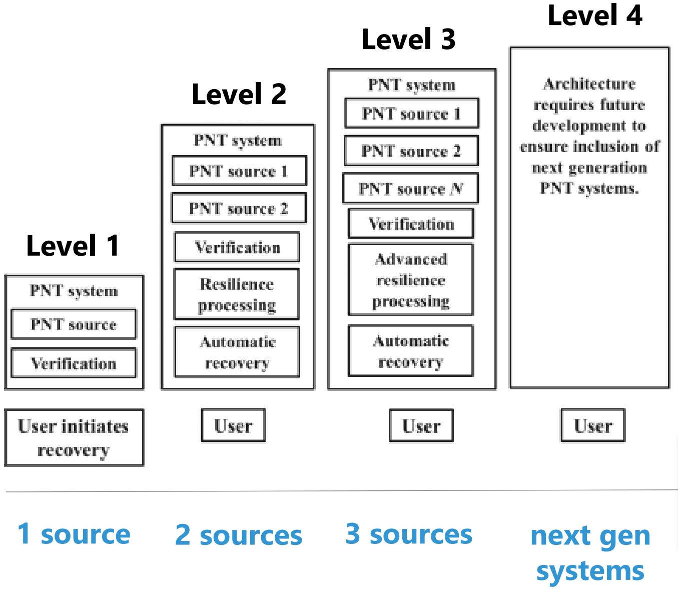
Core functions



Functional diagram



PNT Resiliency levels



© 2021 ADVA. All rights reserved.

DHS anti-spoofing open-source resources

Released on Feb 26, 2021

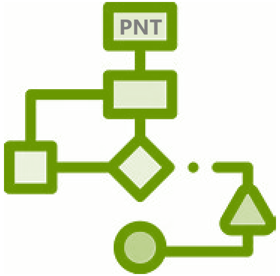
PNT Integrity Library & Epsilon Algorithm Suite*

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

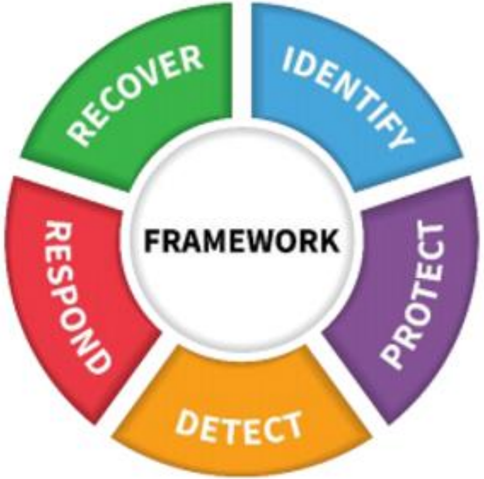
© 2021 ADVA. All rights reserved.

What are NIST's cybersecurity assurance guidelines?

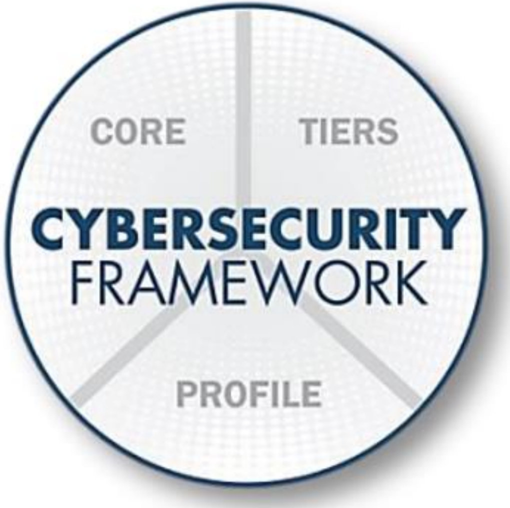
PNT Defense in Depth

NIST Cybersecurity Framework for PNT Profile

Goals



Framework



Core

- Guidance & controls

Implementation tiers

- Cybersecurity risk measurement & management practices

Profile

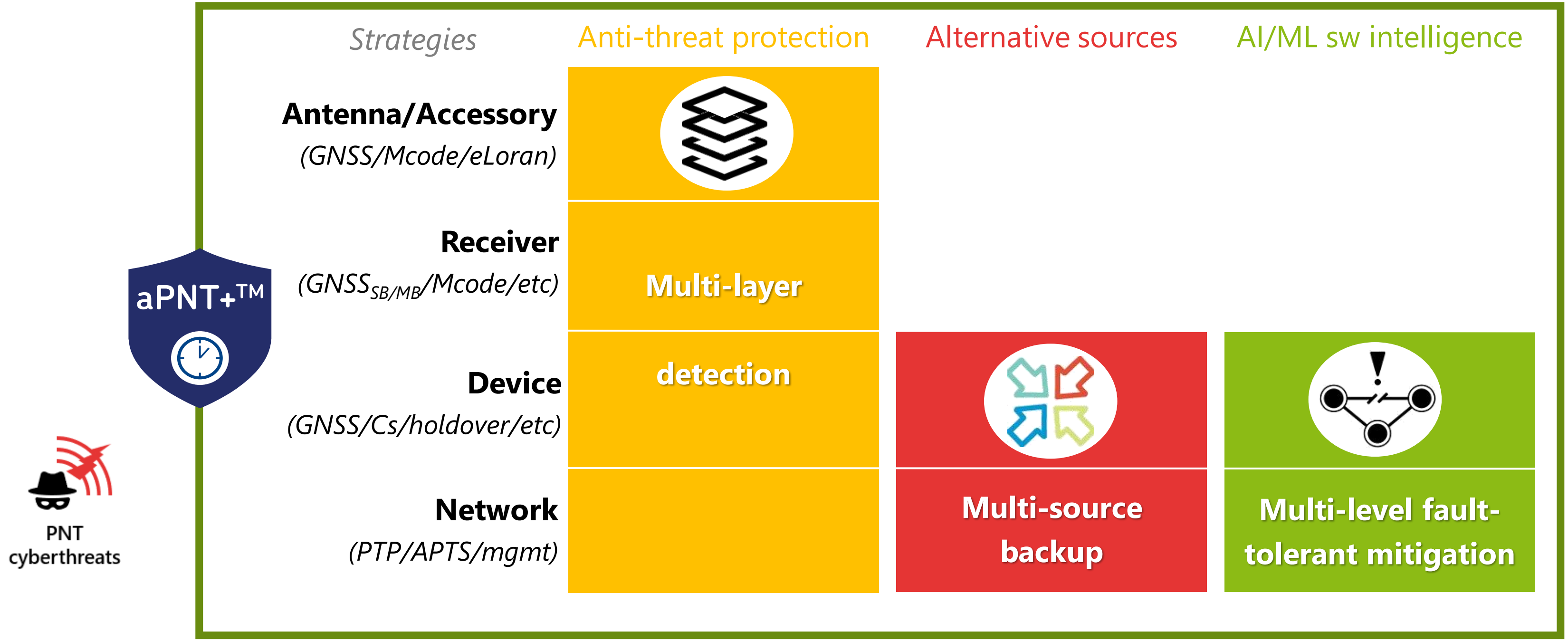
- Requirements & objectives alignment, including risk appetite & resources

© 2021 ADVA. All rights reserved.

OSCILLOQUARTZ
An ADVA Company

Best practice aPNT+ framework with zero-trust PNT sources

3 building blocks



Strategies

Anti-threat protection

Alternative sources

AI/ML sw intelligence

Antenna/Accessory *(GNSS/Mcode/eLoran)*

Receiver *($GNSS_{SB/MB}$/Mcode/etc)*

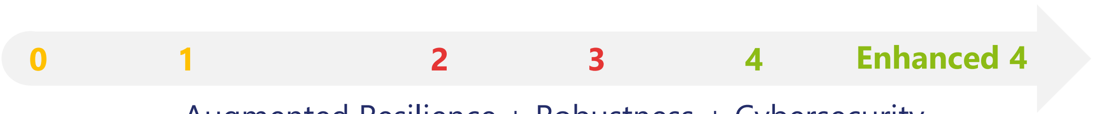
Device *(GNSS/Cs/holdover/etc)*

Network *(PTP/APTS/mgmt)*

Multi-layer detection

Multi-source backup

Multi-level fault-tolerant mitigation



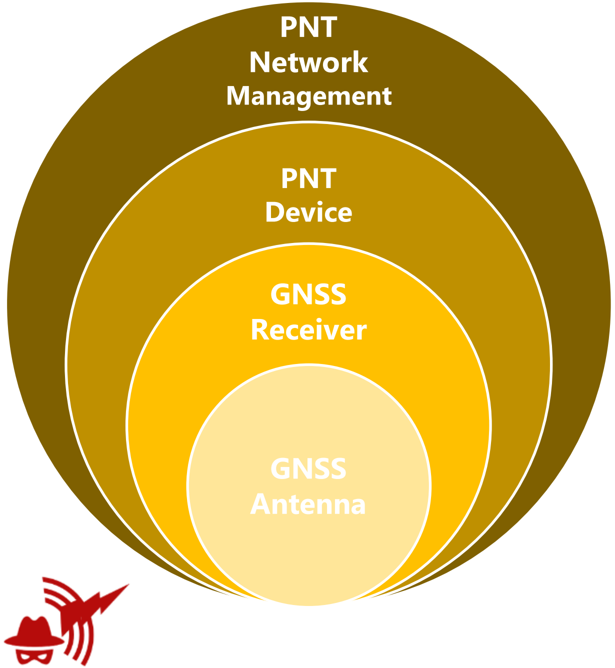
DHS PNT resiliency level 0 1 2 3 4 Enhanced 4

Augmented Resilience + Robustness + Cybersecurity

PNT Defense in Depth

© 2021 ADVA. All rights reserved.

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

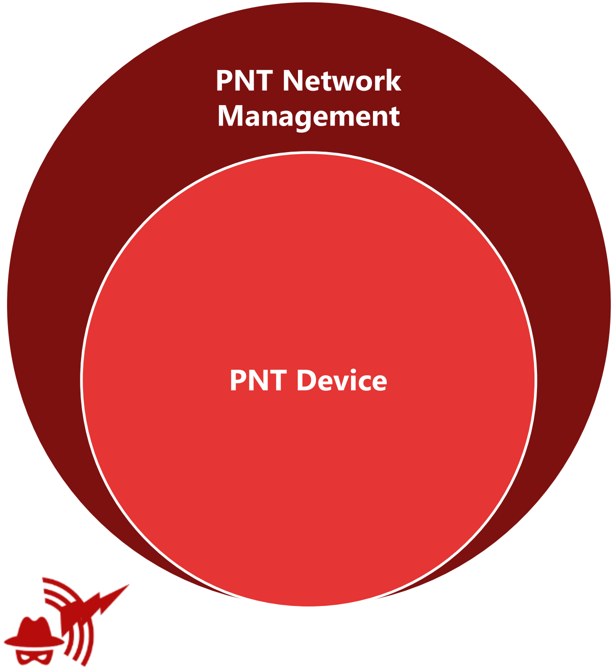
Level 4: PNT Network Management

- 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

© 2021 ADVA. All rights reserved.

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.

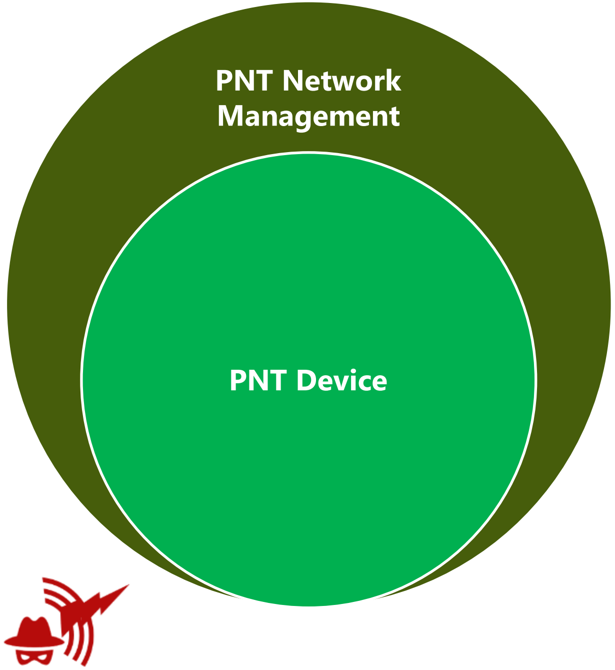
Level 2: PNT Network Management

- **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

© 2021 ADVA. All rights reserved.

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

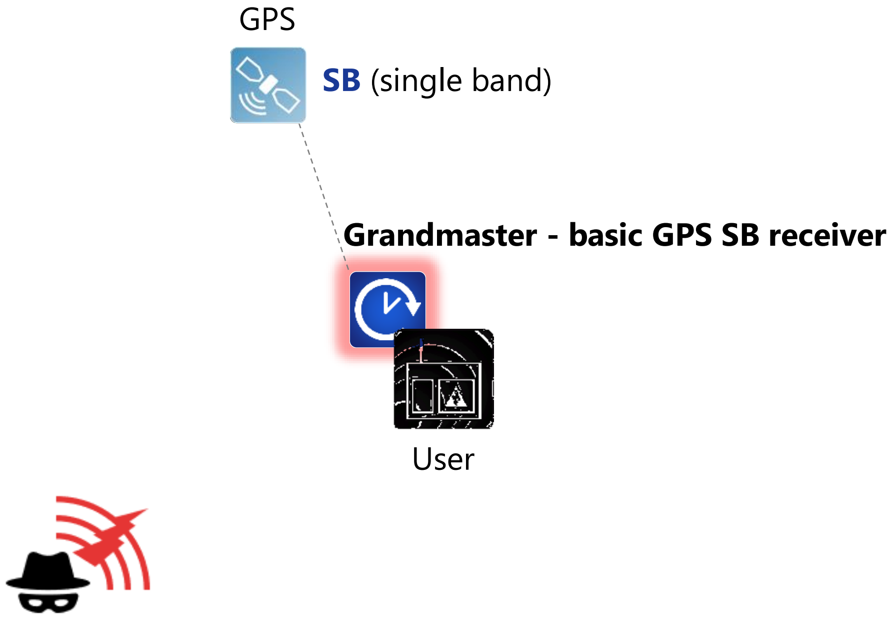
© 2021 ADVA. All rights reserved.

Best architecture strategies against PNT cyberthreats

Level 1 resiliency

Problem

User **level 0** PNT disruptions



GPS

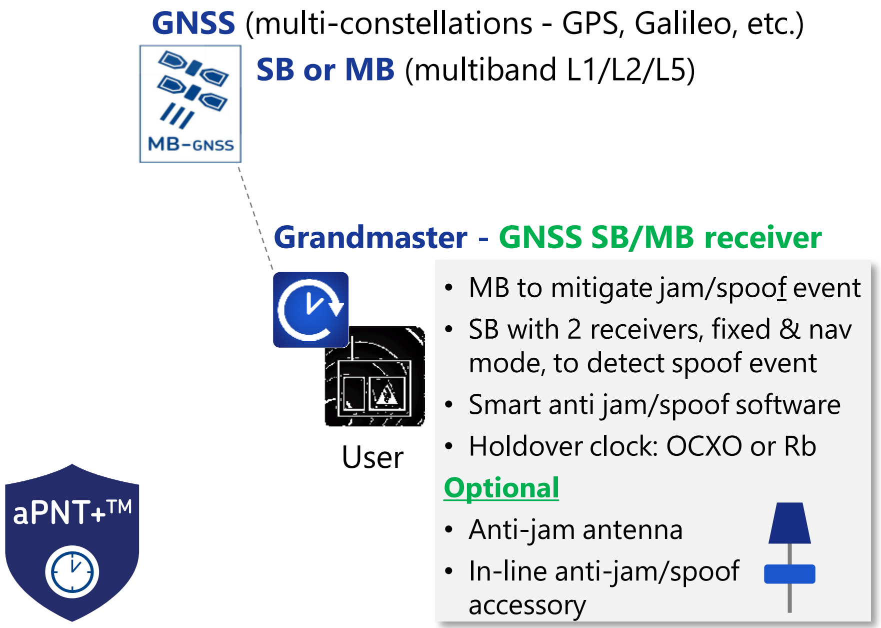
SB (single band)

Grandmaster - basic GPS SB receiver

User

Solution

User **level 1** PNT resiliency



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

SB or MB (multiband L1/L2/L5)

Grandmaster - GNSS SB/MB receiver

- MB to mitigate jam/spoof event
- SB with 2 receivers, fixed & nav mode, to detect spoof event
- Smart anti jam/spoof software
- Holdover clock: OCXO or Rb

Optional

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

User

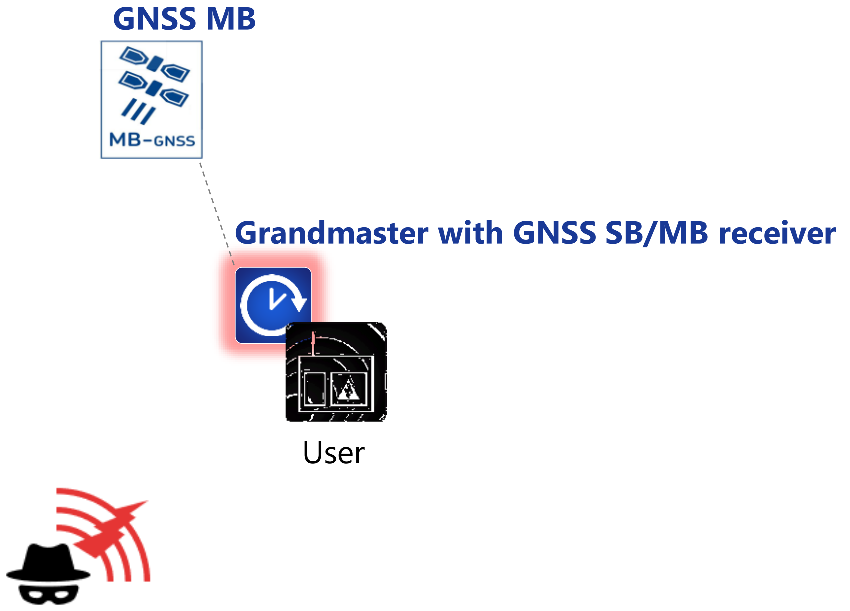
© 2021 ADVA. All rights reserved.

Best architecture strategies against PNT cyberthreats

Level 2 resiliency

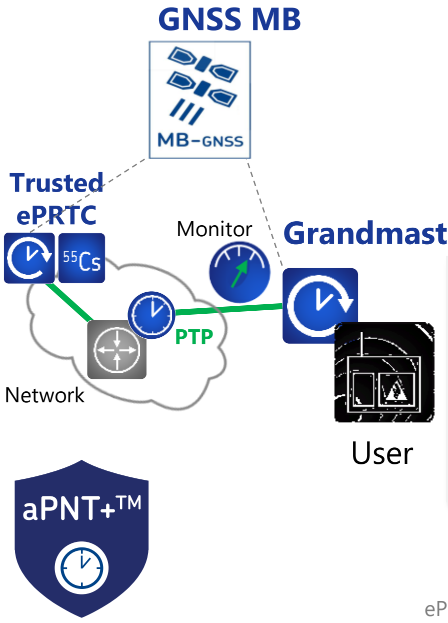
Problem

User **level 1** PNT disruptions



Solution

User **level 2** PNT resiliency



- Same config as level 1 resiliency

PLUS

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

ePRTC - enhanced Primary Reference Time Clock

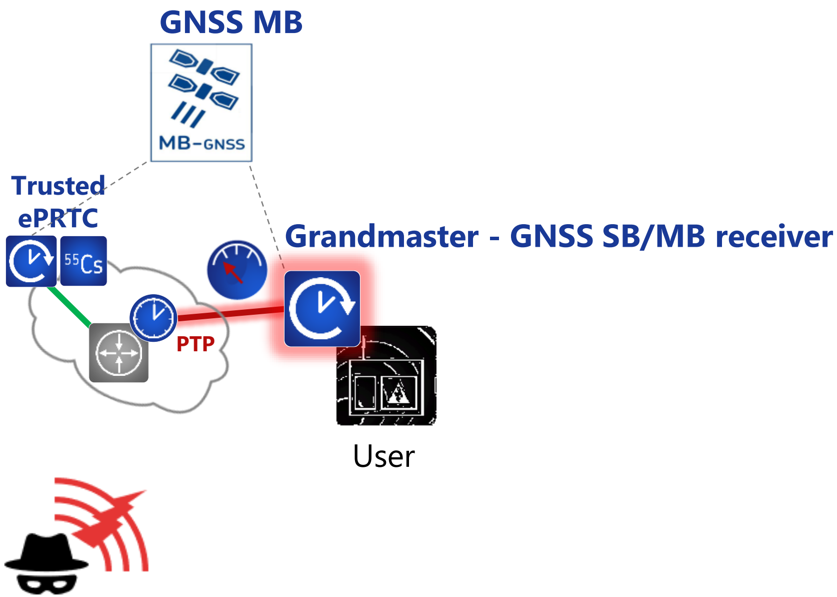
© 2021 ADVA. All rights reserved.

Best architecture strategies against PNT cyberthreats

Level 3 resiliency

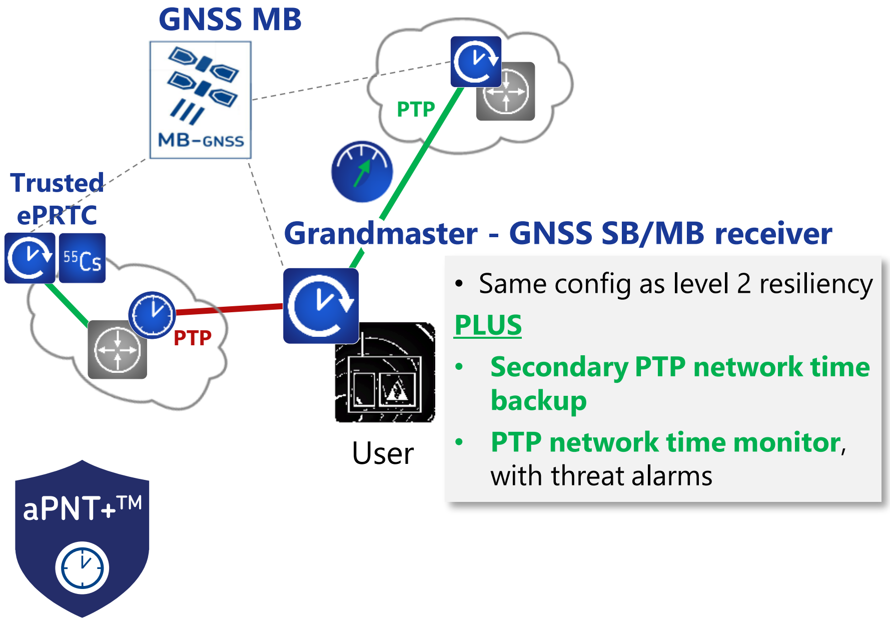
Problem

User **level 2** PNT disruptions



Solution

User **level 3** PNT resiliency



- Same config as level 2 resiliency

PLUS

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

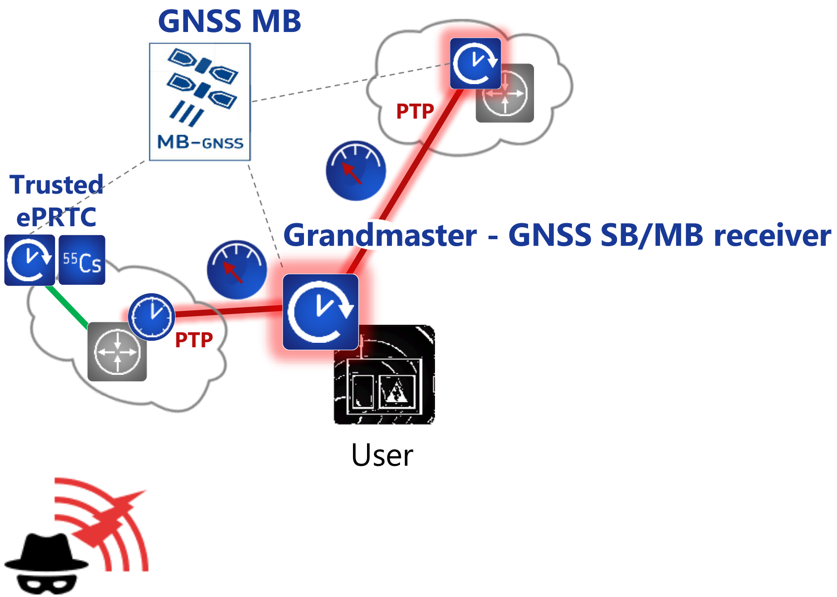
© 2021 ADVA. All rights reserved.

Best architecture strategies against PNT cyberthreats

Level 4 resiliency

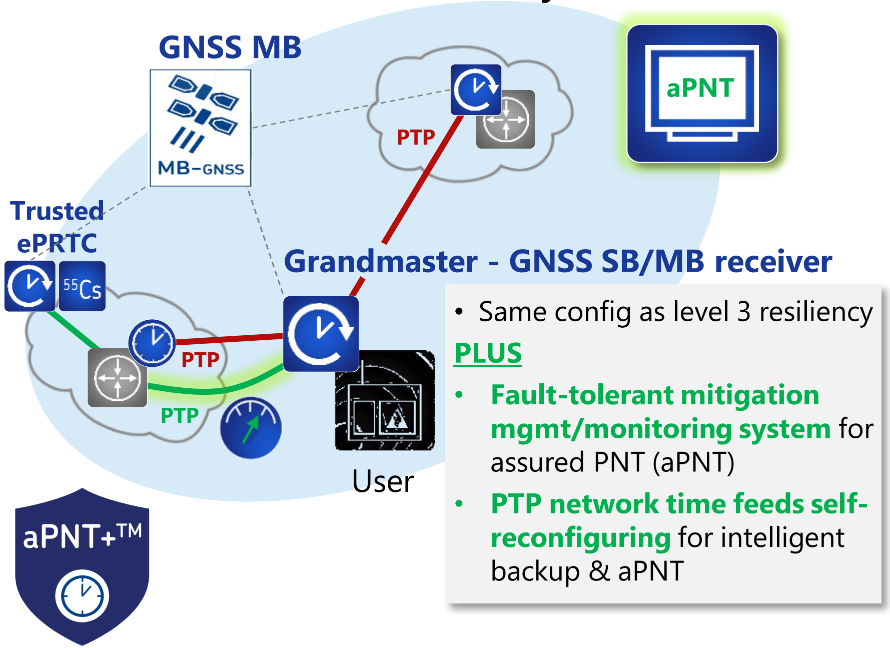
Problem

User **level 3** disruptions



Solution

User **level 4** PNT resiliency



- Same config as level 3 resiliency

PLUS

- **Fault-tolerant mitigation mgmt/monitoring system** for assured PNT (aPNT)
- **PTP network time feeds self-reconfiguring** for intelligent backup & aPNT

© 2021 ADVA. All rights reserved.

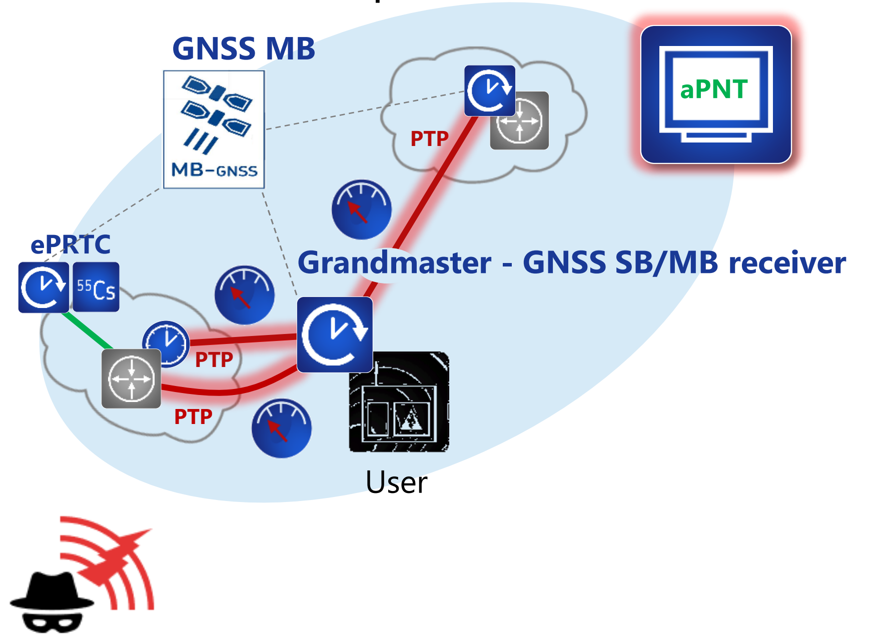
OSCILLOQUARTZ An ADVA Company

Best architecture strategies against PNT cyberthreats

Enhanced level 4 resiliency

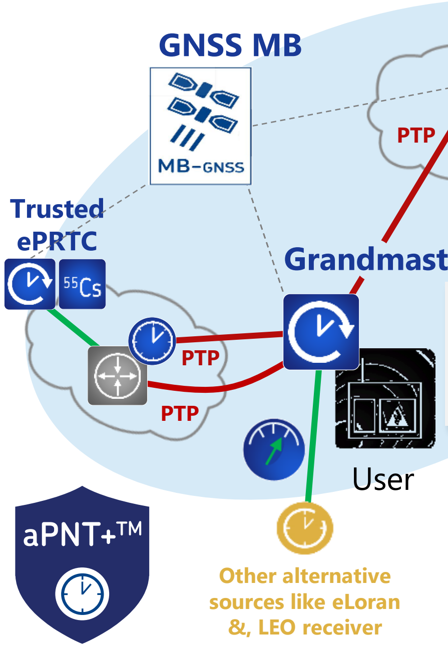
Problem

User **level 4** disruptions



Solution

User **enhanced level 4** PNT resiliency



Other alternative sources like eLoran &, LEO receiver

- Same config as level 4 resiliency

PLUS

- **Other sources of opportunity**

© 2021 ADVA. All rights reserved.

Thank you

NDeFalcis@adva.com

IMPORTANT NOTICE

The content of this presentation is strictly confidential. ADVA is the exclusive owner or licensee of the content, material, and information in this presentation. Any reproduction, publication or reprint, in whole or in part, is strictly prohibited.
The information in this presentation may not be accurate, complete or up to date, and is provided without warranties or representations of any kind, either express or implied. ADVA shall not be responsible for and disclaims any liability for any loss or damages, including without limitation, direct, indirect, incidental, consequential and special damages, alleged to have been caused by or in connection with using and/or relying on the information contained in this presentation.
Copyright © for the entire content of this presentation: ADVA.