

## Assured PNT sync planning for smart digital grids

### Protecting smart grids from PNT disruptions

Cyber threats are at an all-time high, putting critical energy infrastructure at risk, including positioning, navigation and timing (PNT) services. The “T” in PNT is often the least understood parameter, despite being the most valuable. The GNSS system, consisting of multiple satellite constellations, such as GPS, Galileo, Beidou and GLONASS, delivers accurate time across the globe, while enabling “P” and “N” solutions to work effectively. Like ground and power in electricity, timing is a critical asset used for precise network time synchronization, including accurately locating power line faults, synchronizing distributed control processes and load flows, and timestamping network grid data records. No matter how well power grids protect themselves, PNT cyber threats will continue, and some attacks may prevail like the Colonial Pipeline cyberattack on May 7, 2021. Both RTI International and NIST have estimated that the US economic cost of a GPS outage would be [1 billion USD per day](#).

ADVA, with its comprehensive portfolio of Oscilloquartz timing and synchronization solutions, has responded to the PNT cyber threats and developed innovative assured PNT (aPNT+™) technology to augment the resilience, security and robustness of timing for critical infrastructure. Our aPNT solution builds on expertise and products applied for decades in most mission-critical applications with operators and enterprises.

This sync planning guide provides an in-depth understanding of PNT cyber threats and vulnerabilities. It explains mitigating controls and outlines how the comprehensive Oscilloquartz solution portfolio assures

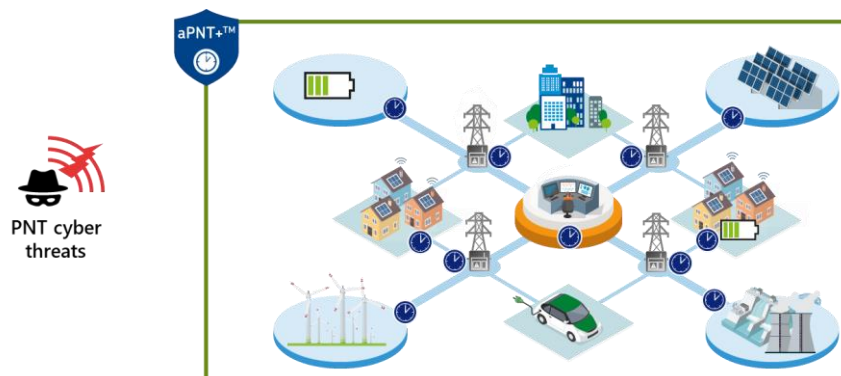


Figure 1: Smart grid overview and aPNT platform

precise and reliable synchronization even under the most unfavorable conditions such as malicious cyberattacks, unintentional GNSS jamming, failing components or communication network unavailability. Figure 1 shows our aPNT+™ solution effectively time-synchronizing a distributed smart grid network.

### Understanding growing PNT cyber threats and GNSS vulnerabilities

In response to growing PNT cyber threats and GNSS vulnerabilities, the US government issued [Federal Executive Order 13905](#) in February 2020 to protect critical infrastructure, such as energy, transportation, finance, communications, and supporting data centers, from PNT service disruptions. Other government entities, such as

the [UK government](#) and the [European Commission](#), have followed similar steps by launching various PNT assurance initiatives.

PNT cyber threats and GNSS vulnerabilities can be categorized into the following two groups of events:

- 1) **External**, including environmental, jamming, spoofing, adjacent-band transmitters, and GPS/GNSS segment errors. Their frequency is indicated in Figure 2.
- 2) **Internal**, including network assets, such as GPS/GNSS receivers and PTP network feeds. Their frequency is also indicated in Figure 2.

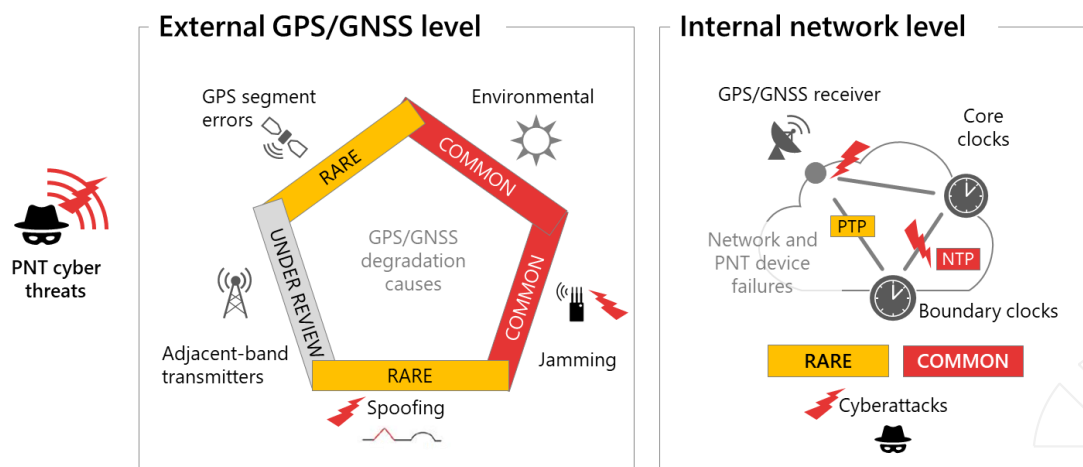


Figure 2: PNT threats and GNSS vulnerabilities

Unlike PTP, NTP has already been subject to multiple cyberattack events known as NTP amplification, which is a type of distributed denial of service attack.

## Time-synchronizing new smart grids

The traditional way that an energy supply chain is generated, transmitted, and distributed is changing at a fast pace, from a centralized grid architecture to a new smart, distributed grid architecture, as depicted in Figure 3.

As today's large power plants are boosted by growing distributed energy resource systems (DERs), from wind farms, solar plants and battery storage systems to microgrids, smart solar homes and DERMS (DER management systems), traditional grid operational strategies require a major rethink in network planning architecture, especially time synchronization and PNT service assurance. Moreover, keeping up with the influx of data from DERs can be daunting.

Timing is an enabler of the digital transformation of integrated smart grids. It is not only needed for real-time control, visibility, and management of integrated grid networks, but also for accurately timestamping network data points, driving the need for energy efficiency and price control, by both synchronizing and streamlining distributed energy flows in overloaded networks. All active energy sites across the smart grid network must be integrated into the operational control system, and both substations and DERs are essential monitoring and control data points. For secure, robust, and reliable operation of smart grids, operators need real-time control of its health, with immediate alarm, threat, and mitigation notifications. Moreover, precise timestamped measurements enable real-time network analytics, visualization and fault location.

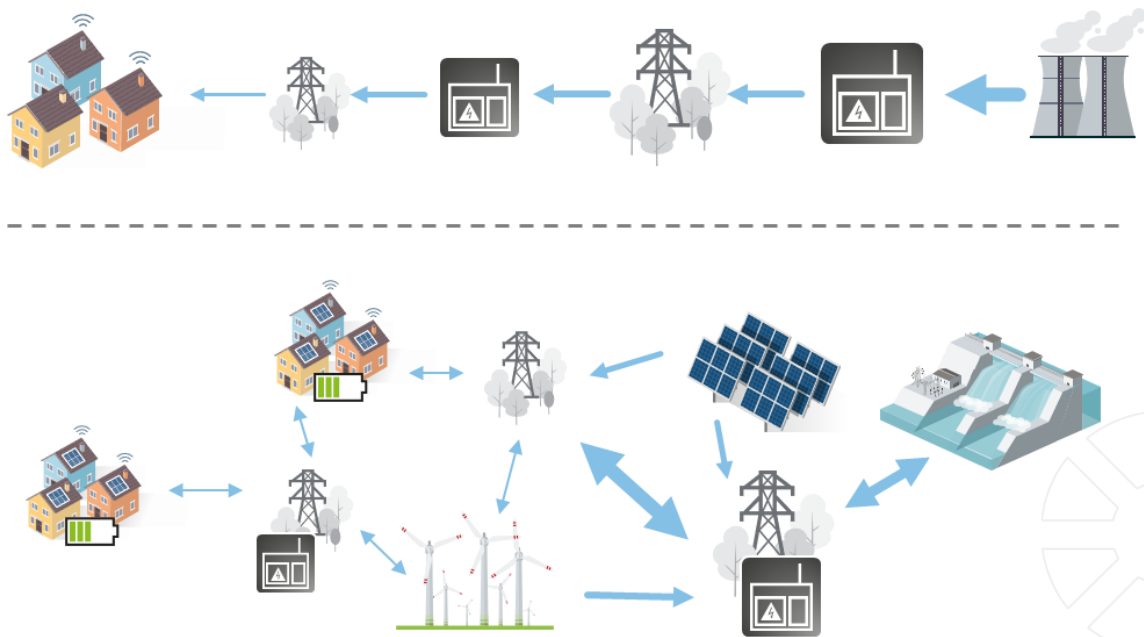


Figure 3: Centralized power generation and distributed smart grid

### Higher data timestamping accuracy requirements in smart grids

Higher levels of accuracy are required to tightly timestamp the growing influx of distributed energy data points, which must also be traceable to UTC time standard. GNSS is the widely used technology today to deploy UTC-traceable timing, but other backup sources are used like an independent cesium atomic clock and PTP network feeds. Table 1 provides a summary of timing requirements in smart grid applications. With the advent of new DER edge and access networks like microgrids being connected to smart grid networks, and the migration from low-speed legacy SCADA to real-time timestamped WAMS data management, such requirements are tightened for enhanced control, fault localization and visibility, especially in balancing power generation and load, with smart time-synchronized PMUs, in microgrids during islanding.

Grid applications	Timing requirements (min reporting resolution accuracy relative to UTC)
Advanced time-of-use meters	15-, 30- and 60-minute intervals are commonly specified (ANSI C12.1)
Non-TOU meters	Ongoing, with monthly reads or estimates
SCADA	Every 4-6 seconds reporting rate
Sequence of events recorder	50µs to 2ms
Digital fault recorder	50µs to 1ms

Protective relays	1ms or better
Synchrophasor / phasor measurement unit - PMU (30-120 samples/second)	Better than 1µs for 30 to 120Hz
Traveling wave fault location	100ns
Micro-PMUs (sample at 512 samples/cycle)	Better than 1µs
Communications protocols	
Substation local area network communication protocols (IEC 61850 GOOSE)	100µs to 1ms synchronization
Substation LANs (IEC 61850 sample values)	1µs

Table 1: Timing accuracy requirement in smart grids  
Source: NASPI's report - [TSTF: Time Synchronization in the Electric Power System March 2017](#)

## Oscilloquartz's intelligent aPNT+™ platform for smart grids

Based on the initial guidelines provided by the US Department of Homeland Security (DHS) and National Institute of Standards and Technology (NIST), with their [Resilient PNT Conformance Framework](#) and [NISTIR 8323 Foundational PNT Profile](#), respectively, Oscilloquartz has developed an intelligent aPNT+™ platform. The aPNT+™ platform is a leading-edge, assured-PNT grandmaster clock architecture at scale, integrating Oscilloquartz's best-practice aPNT framework against PNT cyber threats and GNSS vulnerabilities. The aPNT framework includes these three fundamental building blocks, all working together as an integrated function for augmented PNT assurance, including resilience, robustness, and security:

- 1) Multi-layer detection
- 2) Multi-source backup
- 3) Multi-level fault-tolerant mitigation

The threefold aPNT framework in Figure 4 features not only augmented resilience but also robustness and cybersecurity, all equally essential features for full PNT assurance.



Figure 4: aPNT+™ platform overview

**Multi-layer detection**

Initially, it is vital to identify any malicious and unintentional disturbance of GNSS signals. As a first shield of defense, this is performed through specialized GNSS antennas and in-line accessory options, which are able to detect jamming and spoofing cyberattacks. For a second shield of defense, the GNSS receiver can compare signals from several constellations and can be enhanced with multi-band capability to detect (and also mitigate) malicious or disturbed signals. Also, Oscilloquartz uses dual GNSS receivers in most products, one in fixed mode and the other in nav mode, to detect (and mitigate) spoofing events when the coordinates of the nav receiver change compared to the ones of the fixed receiver. For a third shield of defense, the PNT device processing the GNSS timing signal can further detect (and mitigate) any issues by comparing it with multiple sources like network PTP timing and a standalone, GNSS-backup cesium clock if collocated with the PNT device. As a fourth shield of defense, an intelligent, AI-assisted PNT network management system can monitor, compare, verify, and analyze sync information in real-time from multiple sources across the network and can detect (and mitigate) any anomalies. Such a multi-layer detection system is performed through a combination of these four functional components working together dynamically, as depicted in Figure 5.

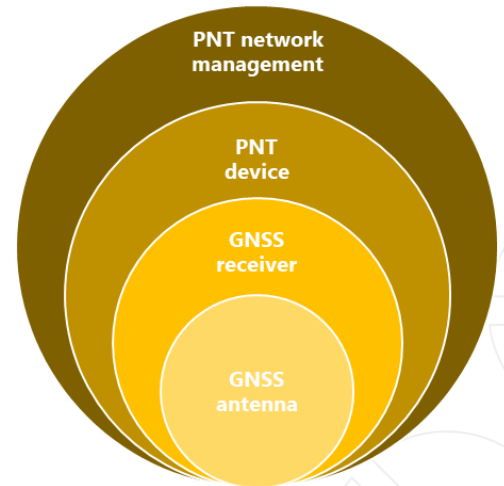


Figure 5: Multi-layer detection

**Multi-source backup**

Multi-source backup is achieved through a combination of available sources. As a first shield of defense, the PNT device can automatically failover to a backup source if a GNSS source is compromised based on the above multi-layer detection system. Typical backup sources at the PNT device level are a standalone cesium (Cs) clock, a crystal (Xo) or a rubidium (Rb) holdover oscillator, and other sources of opportunity like white rabbit (WR). At the PNT network management level, typical backup sources are PTP/NTP and legacy sources like SyncE and BITS. As a second shield of defense, an intelligent, AI-based management system can monitor, compare, verify, and analyze sync information from multiple sources across the end-to-end network and provide an automatic backup source if one or multiple PNT devices are compromised. Such a multi-source backup system is performed through these two functional components working together dynamically, as depicted in Figure 6.

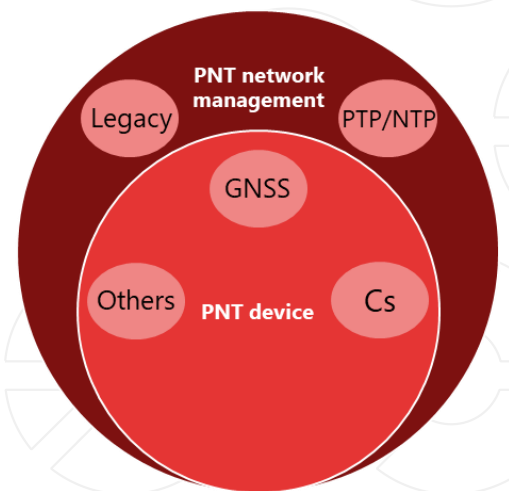


Figure 6: aPNT backup opportunities

**Multi-level fault-tolerant mitigation**

Multi-level fault-tolerant mitigation is achieved through the aggregation of sync data in real-time from the above multi-layer detection and multi-source backup systems, to provide PNT cyber threat detection, mitigation, protection, and analytics across the end-to-end sync network. As a first shield of defense, the PNT device monitors, compares, verifies, and analyzes sync information from multiple sources, with automatic failover to a backup source if a GNSS source is compromised. As a second shield of defense, an intelligent, AI-based PNT network management system can monitor, compare, verify, visualize, and analyze sync information from all the PNT devices and network timing sources to provide resilient, robust, and secure fault-tolerant mitigation, including self-reconfiguring the sync network sources. Moreover, the sync chain topology and its geo map can be visualized with location-based alarms for full control and visibility of PNT assurance. Such a multi-level fault-tolerant mitigation system is designed to provide trusted PNT assurance, including sync, GNSS, and NTP/PTP, through these two functional levels, working together dynamically, as depicted in Figure 7.

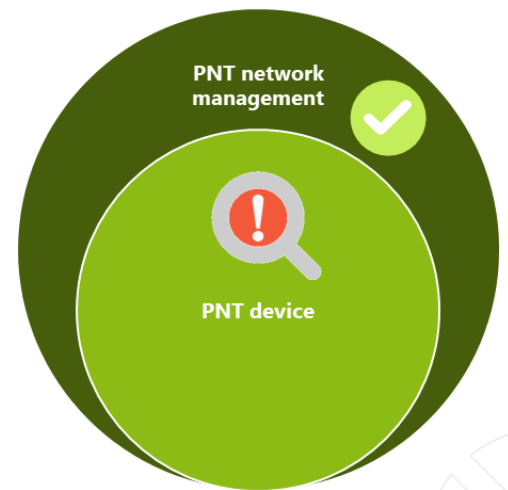


Figure 7: aPNT fault mitigation

Oscilloquartz’s scalable aPNT+™ intelligence platform in Figure 8 is integrated into the company’s innovative product portfolio. It not only integrates the four resiliency levels of the DHS’s guidelines but also provides an enhanced level 4 resiliency, which is the highest resiliency level for trusted PNT assurance, by being able to self-

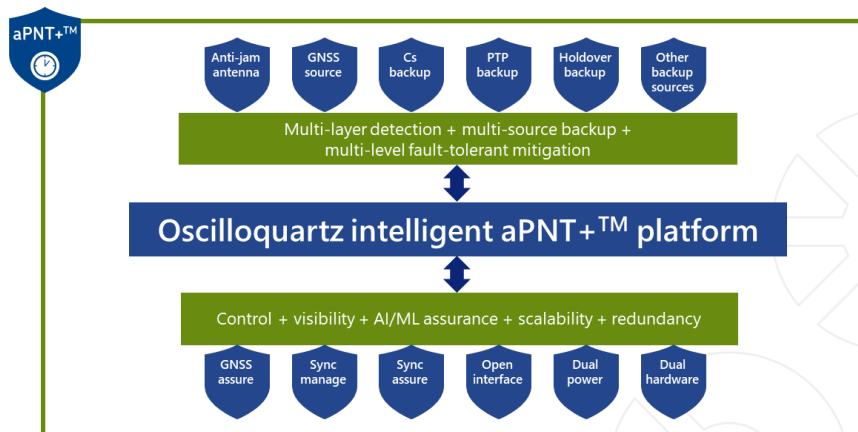












Figure 8: aPNT+™ components

reconfigure the sync network sources like a “system of systems.” Such resiliency could be used in core networks, for instance, to build a trusted time-as-a-service infrastructure, serving edge and access grids and DER networks.



Moreover, the aPNT+™ platform integrates the suite of components in Table 2, some of which are optional, starting from the primary GNSS source and based on a mix of users' requirements, including PNT cyber threat risk appetite:

aPNT+™ components	Resiliency levels (pictures not to scale)	Description
<p><b>PNT devices with sophisticated GNSS receivers</b></p>	<p><b>Level 1 source</b></p> 	<p>coreSync, accessSync, edgeSync products families support up to two multi-band (MB) or single-band (SB), multi-constellation (GPS/GLONASS/BEIDOU/GALILEO) GNSS receivers.</p> <p>Advanced jamming and spoofing detection on PNT device and network management levels.</p>
<p><b>Anti-jam antenna</b></p>	<p><b>Level 1 source enhanced</b></p> 	<p>Jamming and spoofing signals typically originate at low elevations. An optional anti-jamming, anti-spoofing antenna can mitigate such events by modifying the radiation pattern of the GNSS antenna such that it is "deaf" to signals arriving from 10° below and 15° above the horizon while slightly increasing the gain of the antenna at zenith.</p> <p>The antenna can be coupled with coreSync, accessSync, edgeSync product families.</p>
<p><b>Cesium atomic clock backup</b></p>	<p><b>Level 2 source backup</b></p> 	<p>The cesium atomic clocks provide extremely stable and accurate frequency autonomous reference which can be used as backup to GNSS.</p> <p>Oscilloquartz offer a range of standalone cesium atomic clocks, magnetic cesium clocks that provide ePRC and optical cesium clocks that provide ePRC+ performance. These create an enhanced primary reference time clock (ePRTC) when combined with any coreSync and edgeSync+ products, providing an accurate, robust and secured synchronization source.</p>
<p><b>PTP backup</b></p>	<p><b>Level 3 source backup</b></p>	<p>All Oscilloquartz products families can utilize PTP and SyncE inputs which can be used as backup to GNSS.</p>

<p><b>Other sources</b></p>	<p><b>Level N source backup enhanced</b></p> 	<p>Multiple external sources (such as eLORAN) can be connected to Oscilloquartz products by utilizing the PPS/CLK and ToD inputs</p>
<p><b>Holdover backup</b></p>	<p><b>Level 4 source backup</b></p> 	<p>Oscilloquartz products use a range of high-quality oscillators, from oven-controlled oscillators (OCXO) through to high-quality double-oven-controlled oscillators (DOCXO) to rubidium miniature atomic clock oscillators. These high-quality oscillators provide extended holdover when external synchronization references are not available.</p>
<p><b>Dual-power and redundant hardware</b></p>	<p><b>All level sources enhanced</b></p>  	<p>Oscilloquartz coreSync, accessSync product families provide two redundant, hot-swappable power supplies for increased MTBF and fast MTTR.</p> <p>coreSync also provides optional carrier-grade hardware redundancy of all management and synchronization modules</p>
<p><b>Sync management, monitoring, and assurance</b></p>	 	<p>All Oscilloquartz product families are equipped with Syncjack™ – a comprehensive synchronization monitoring and assurance toolkit which enables the quality of synchronization across the network to be monitored. The data collected by Syncjack™ can be collected by ADVA’s Ensemble Controller and Sync Director network management system for additional analysis and troubleshooting.</p>
<p><b>AI/ML-assisted GNSS assurance</b></p>	<p><b>All level sources enhanced</b></p> 	<p>GNSS assurance is provided by a centralized GNSS monitoring, and assurance system integrated into ADVA’s Ensemble Controller network management system.</p> <p>The GNSS assurance system collects data from all Oscilloquartz product families, which is analyzed and used for the following:</p> <ul style="list-style-type: none"> <li>- Smart GNSS jamming/spoofing/obstruction detection, mitigation and prevention, using AI technology with alarm events provided</li> <li>- GNSS antenna installation health monitoring</li> </ul> <p>The GNSS assurance can also read performance data from third-party GNSS receivers.</p>



<b>AI/ML assisted network management</b>	<b>All level sources enhanced</b>	Smart global network sync control and visibility in real-time, using fault-tolerant mitigation technologies, with alarm/threats events and a geo map displaying compromised and mitigated PNT devices and sites, are provided by Ensemble Controller, Ensemble Sync Director and the GNSS assurance application.
------------------------------------------	-----------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Table 2: aPNT+™ component overview

### Smart grid timing architecture with PNT assurance

Timing needs to be provided at central power plants, primary and secondary substations as well as with DERs. Each site has different requirements in regard to timing interface types, number of client clocks, resilience and redundancy, as well as space restrictions and environmental requirements. Our aPNT portfolio is optimized for these use cases and provides optimized solutions for any smart grid timing application.

Planning and architecting timing for smart digital substations including aPNT, while integrating legacy systems to protect existing investments, can be a daunting task. However, the Oscilloquartz aPNT+™ platform makes the process easy, seamless, and cost-effective.

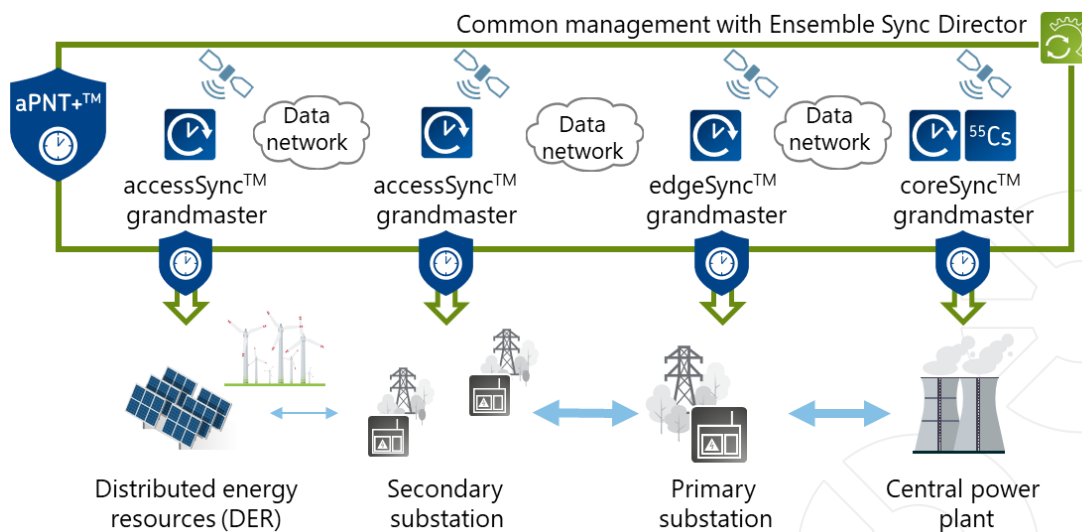


Figure 9: Overview on smart grid timing with aPNT

Figure 9 shows a smart power grid with our aPNT+™ solution for delivering accurate and resilient timing. Each site is equipped with a PTP grandmaster with integrated NTP server, GNSS receiver and PTP network backup. It provides sophisticated jamming/spoofing cyberattack detection for immediate mitigation through automatic failover to one of multiple PTP backup feeds from an upstream trusted coreSync™ grandmaster.

Any attack, disturbance or device failure is immediately notified to the network management system. The Ensemble Controller and Ensemble Sync Director use AI/ML technologies for root-cause analysis and predictive maintenance. With a comprehensive set of management features, the complete synchronization and data network is managed, monitored and controlled with a single solution. Any problem is immediately visualized on a geo map, providing the location of the compromised site and enabling fast and efficient reaction to any threat.

The resilient and robust design of our aPNT+™ platform will survive deliberate attacks as well as unintentional jamming or shadowing of antennas. It will mitigate any technical failure such as defects of PNT devices or outages of underlying communication networks. The automated management system will minimize human error and, with a high degree of automation and AI/ML-assisted assurance, operational problems are avoided. Our aPNT+™ platform assures PNT services even in the most adverse conditions.

### Distributing timing inside primary and secondary digital substations

Figure 10 shows how timing is distributed within a secondary substation, with legacy interfaces, such as IRIG-B, NTP, and 1PPS, to protect existing investments, once PNT cyber threats have been mitigated as discussed above. In this configuration, a new indoor, ultra-compact accessSync™ OSA 5405 SyncGrid™ grandmaster is used.

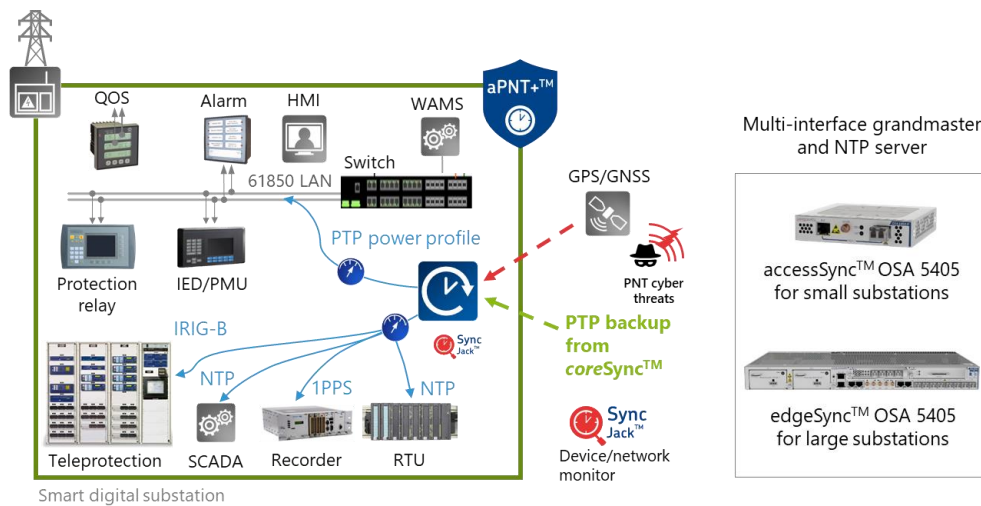


Figure 10: Assured and resilient substation timing

Our Syncjack™ solution provides real-time information about timing quality and performance monitoring on both incoming and distributed timing, such as GNSS/PTP backup and 1PPS/NTP/PTP, respectively.

Additionally, the OSA 5405 SyncGrid™ grandmaster provides various legacy I/O interfaces, as shown in Figure 10, as well as the PTP power profile.

For a larger, secondary digital substation, a modular OSA 5422 PTP grandmaster and NTP server can be used. It complements the same rich set of features with a modular design for scale and flexibility.

### Architecting timing for smart DERs with PNT assurance

Figure 11 shows a smart grid with multiple small to larger DERs, together with a centralized DERMs. Accurate time synchronization with PNT assurance is required to perfectly interconnect and balance the energy flows from overloaded DER networks to core grid networks, and vice versa.

We provide a range of cost-effective accessSync™ OSA grandmasters with this suite of Oscilloquartz aPNT+™ components.

Additionally, DERM visibility is provided through transparent GUIs and the unique Ensemble Sync Director topology view of the end-to-end timing network, simplifying control of the global synchronization network. Any

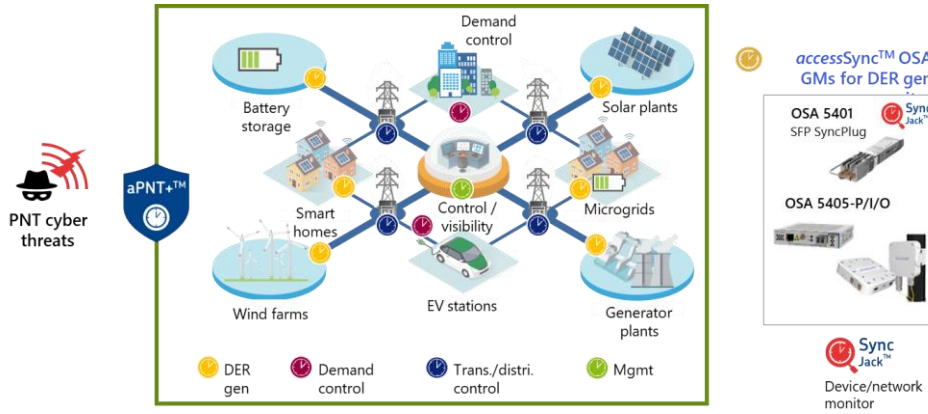


Figure 11: Timing of smart grids and DERs

threat is immediately visualized on a geo map, providing the location of any compromised site and notifying the user of any threat.

	DER site	Secondary substation	Primary substation	Core site
aPNT+™ components	GNSS SB Optional anti-jam antenna PTP backup OSC backup GNSS/sync assurance	GNSS SB (a single-band receiver) Optional anti-jam antenna PTP backup OSC backup AI-/ML assisted GNSS assurance Sync monitoring and assurance	Up to two GNSS MB/SB receivers Optional anti-jam antenna PTP backup OSC backup AI-/ML assisted GNSS assurance Sync monitoring and assurance Dual power supply and hardware redundancy Optional other sources	Up to two GNSS MB/SB receivers Optional anti-jam antenna Cs backup PTP backup OSC backup AI-/ML assisted GNSS assurance Sync monitoring and assurance Dual power supply and hardware redundancy Optional other sources
PTP grandmaster, NTP server	accessSync™ OSA 5401/05	accessSync™ OSA 5401/05	edgeSync™ OSA 5422	coreSync™ OSA 5430/40, cesium clock OSA 3350
Network management	Ensemble Controller with Ensemble Sync Director featuring Syncjack™ assurance for GNSS and PTP			

Table 3: Oscilloquartz aPNT+™ platform selection guide

## Innovative aPNT+™ solutions for smart grids

We provide a comprehensive portfolio of innovative aPNT+™ products for various smart grid and DER applications, from coreSync™ and edgeSync™ to accessSync™, as depicted in Figure 12. By integrating our market leading aPNT+™ technology into our products, we not only offer a range of cost-effective solutions for the smart grid ecosystem at scale, but also the industry's best and most comprehensive features in augmented resilience, robustness and cybersecurity.

Protecting smart grids from PNT disruptions with defense in-depth and AI/ML technologies is our aPNT motto.

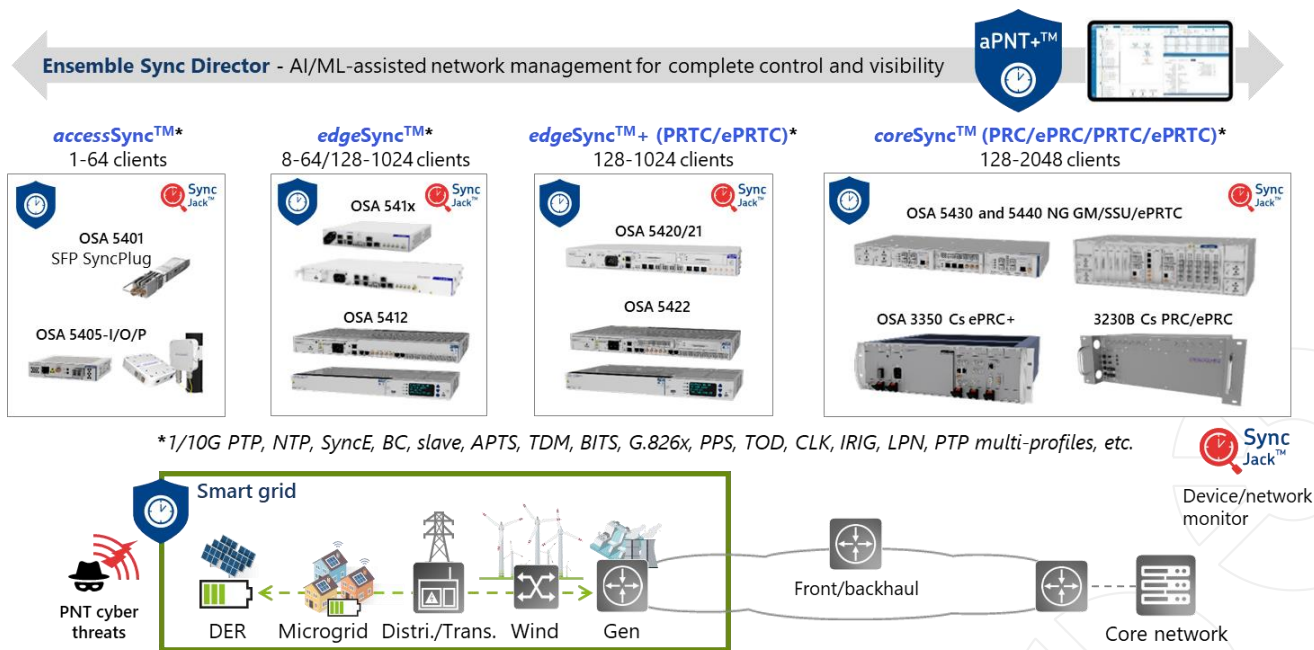


Figure 12: aPNT+™ platform for resilient smart grid timing

## Any questions?

We're here to help. Contact us by clicking [here](#) and refer to this aPNT sync planning guide in the form. Or perhaps you'd like an aPNT assessment audit? Simply email us at [info@adva.com](mailto:info@adva.com).