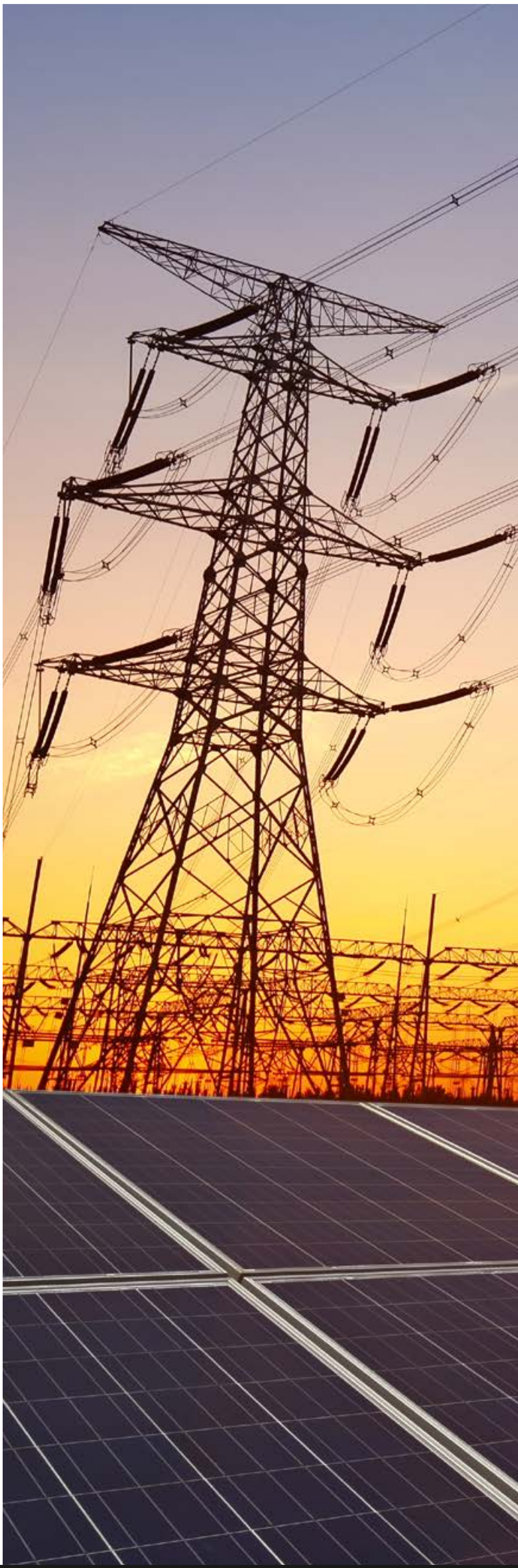
Transforming Powergrid Communication

Solutions for substation networking

2023/2024

Table of Contents



Introduction

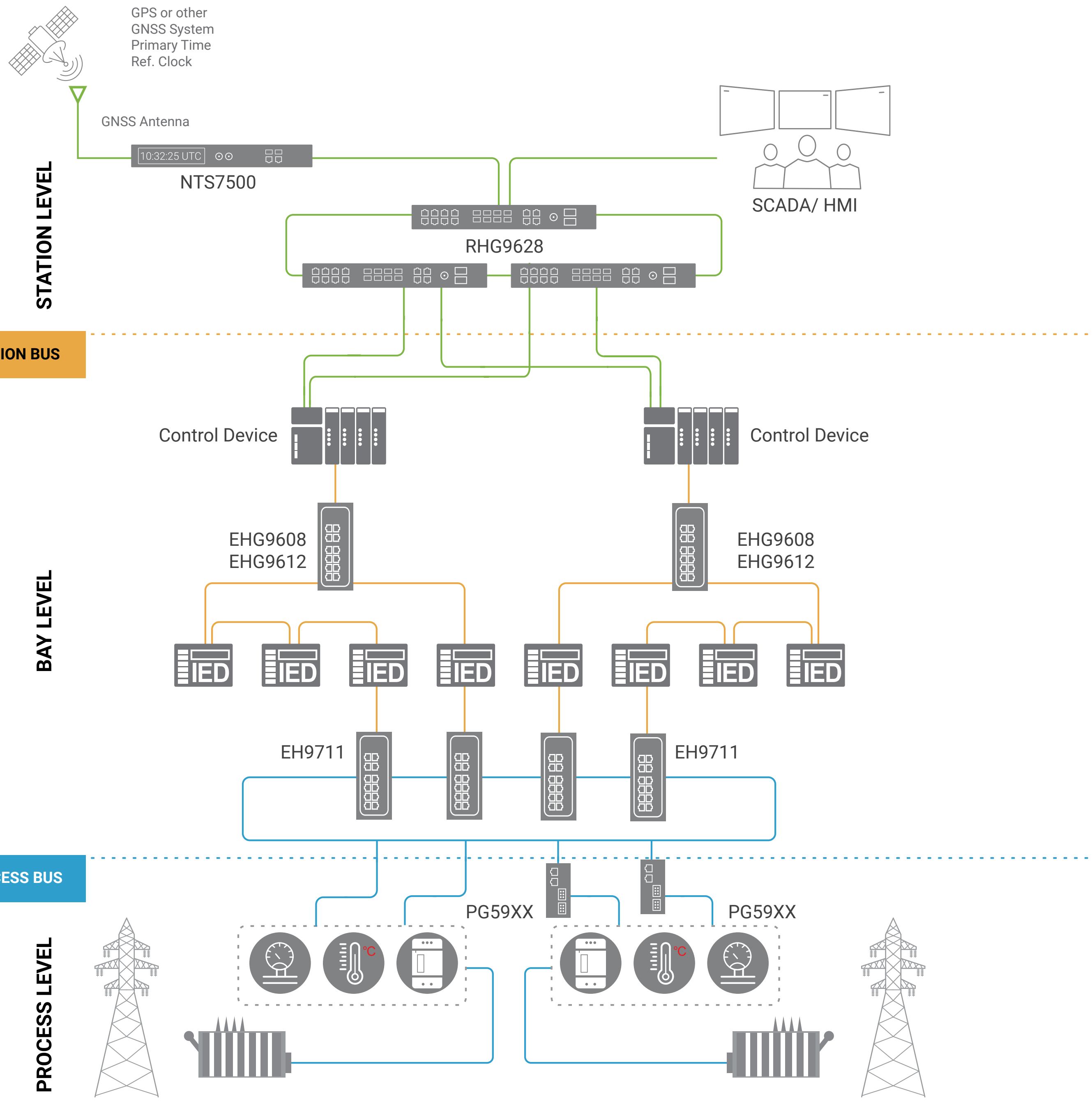
Many power grids throughout the world are in dire need of upgrade to accommodate clean energy production. Also, extreme weather can cause major disruptions to power transmission, just when it is needed most desperately by people. Modernizing the electricity grid is essential to achieving a future with fewer blackouts, more energy and economic security, and healthier communities.

For reliable and efficient operation of the grid, power substations which transform, switch, and distribute electrical power to users are interconnected not only electrically, but also by a network of communication links and control systems. These networks are designed to enable real-time monitoring, control, and protection of the power system, allowing operators to respond quickly to changes in power demand or disruptions to the grid. A modern substation communication network follows the IEC 61850 Standard to provide interoperability between various equipment, and enables advanced functionalities such as wide-area protection and control, fault location, and disturbance recording.

This brochure is a compilation of ATOP's *Transforming Powergrid Communication* article series, published on atoponline.com. The series offer basic knowledge as well as application insights, to help you make informed decisions on how to build efficient, secure, and sustainable communication networks for power systems. We encourage you to learn from this thoughtfully prepared content, but also welcome you to reach out directly to our experts for the latest and personalized technology and information.

Substation digitalization based on the IEC 61850 standard

The IEC 61850 Standard defines substation communication in three levels: *Process Level* functions interface with electricity processes like switching and monitoring. These processes are controlled from the *Bay Level* by intelligent electronic units (IEDs), such as protection relays, meters, and controllers. Data acquired from the process level also passes through the bay level to inform station actions at the *Station Level*, or to be further aggregated and sent to monitoring systems like SCADA.



Several aspects must be considered to achieve maximal substation network reliability:

Electromagnetic compatibility (EMC) is definitely one of the first priorities to think about when building a substation network. Situated near power equipment and cables, devices in substations require better EMC than normal industrial facilities do. IEC61850-3 defines the construction, design and environmental conditions that substation devices must meet, and only when fully compliant and certified does ATOP present a device as "for substations."

Rugged housing that withstands demanding weather and heavy use is also indispensable in power applications. Especially with the rise of clean energy, substations are often located in remote and severe environments, so ATOP IEC 61850-3 certified devices make sure to deliver optimal performance even under harsh temperature and humidity conditions.

Redundancy is important to ensure that the substation network can continue to operate even if some equipment or systems fail. This can be achieved through the use of redundant power supplies, redundant control systems, and backup communication systems.

The EH9711 managed switch, designed specifically for substation access, enables both power and communication redundancy through dual power inputs as well as ring topology support. In the event of node failure, ring topologies like RSTP and ERPS allow traffic to self-recover in milliseconds. In addition to RSTP and ERPS, the Gigabit backbone switch RHG9628 also supports HSR/PRP to guarantee zero packet loss for critical substation information.

Interoperability is one of the key points of IEC 61850. Substations contain a variety of devices that use different protocols to communicate with each other. Some may even be legacy or proprietary. Protocol gateways act as a bridge between these different protocols, allowing devices to exchange information and operate together seamlessly. ATOP takes this concept a step further with diverse media options, such as optional SFP slots or cellular connections.

Precise timing, as first mention, may not seem closely related to power transmission—what is a nanosecond's difference in receiving electricity? But in truth, the impact of timing in substations is more critical than many imagine. Accurate synchronization of devices enables control systems to operate more efficiently and effectively, reducing the risk of errors or failures. All events on the network are logged with the same time reference, and protection devices can operate in the correct sequence, regardless of where they occur. This not only maintains the safety and reliability of operations, but also allows determination of the exact sequence of events, which is crucial in performance control and troubleshooting.
ATOP offers comprehensive solutions for precise timing in the nanosecond level, from grandmaster clocks which sync with a GNSS reference, to a range of powerful switches that support precise hardware-based boundary and transparent clocks, assuring the accuracy of events throughout the network.

Cybersecurity has been a growing focus of substation networks in recent years, as the more interconnected and digitized these systems grew, the more vulnerable they became to cyberattacks which could potentially cause significant damage. High availability requirements, wide geographic spread, and often legacy equipment pose unique challenges in securing power networks.
ATOP cybersecurity is certified for IEC 62443-4-1 and in the process to receive IEC 62443-4-2, which means that all products are developed and created with the highest awareness of cyber-risk consequences. Our substation solutions encompass numerous forms of protection including access control, network segmentation, and encryption, to serve different scenarios and needs.

Finally, a reliable network benefits from **remote management** and monitoring. ATOP solutions come with user-friendly management software that allow real-time visualization of topologies, remote control and troubleshooting, smart alarms, and more. Operators can quickly and easily onboard new devices, scale network systems, find bugs and errors, and resolve issues from off site, improving efficiency while lowering the costs of maintenance.

Precision Timing Protocol in power substations

Precise time synchronization is essential for the safe and reliable operation of power systems. Network faults can occur at any time, but especially for critical utilities, fault detection and isolation need to be fast and accurate to minimize the risk of damage.

Even under normal operation, the stability and control of power systems depend on coordination and synchronization of various devices and systems, such as generators, transformers, and switches. Precise time synchronization allows for coordinated operation and control of these devices, ensuring grid stability and minimizing the risk of power outages. For renewable energy sources such as solar and wind power, where energy resources are often distributed, time synchronization is particularly important for coordination of multiple sources to maximize their contribution to the grid.

Monitoring and analysis of power grids also require precise time synchronization to accurately correlate data from various sources, such as sensors and meters. With event data in the correct sequence, managers can perform real-time and offline analysis of grid performance and faults.

Why use Precision Time Protocol?

Precision Time Protocol (PTP) is a protocol that is used to synchronize clocks in a network to a common time reference. Key features of PTP include:

High accuracy

PTP's most defining feature is its ability to provide sub-microsecond accuracy, by exchanging hardware timestamped packets between devices. Because packets are timestamped when they enter and leave a device, inaccuracies that arise from software processing time are eliminated. The process doesn't require additional processing overhead, which can introduce jitter and delay in the time synchronization process. Thus PTP is suitable for applications that require precise timing, such as power systems and industrial automation, as well as for telecommunication networks and financial trading systems.

Dynamic adaptability

PTP is able to dynamically adjust its synchronization rate and algorithm to adapt to changes in network conditions, such as latency or packet delay variation. Accumulated delay calculations are used to provide an accuracy with 1 µs.

Fault tolerance

PTP includes mechanisms for fault tolerance and redundancy, such as backup grandmasters and boundary clocks, to ensure that the network continues to operate in the event of failures or disruptions.

Scalability

PTP can support large-scale networks with thousands of devices, making it suitable for power systems, which have many interconnected devices that require synchronized timing. A single grandmaster clock can synchronize the time of multiple devices on the network, so the cost of deploying and maintaining multiple timing sources is low.

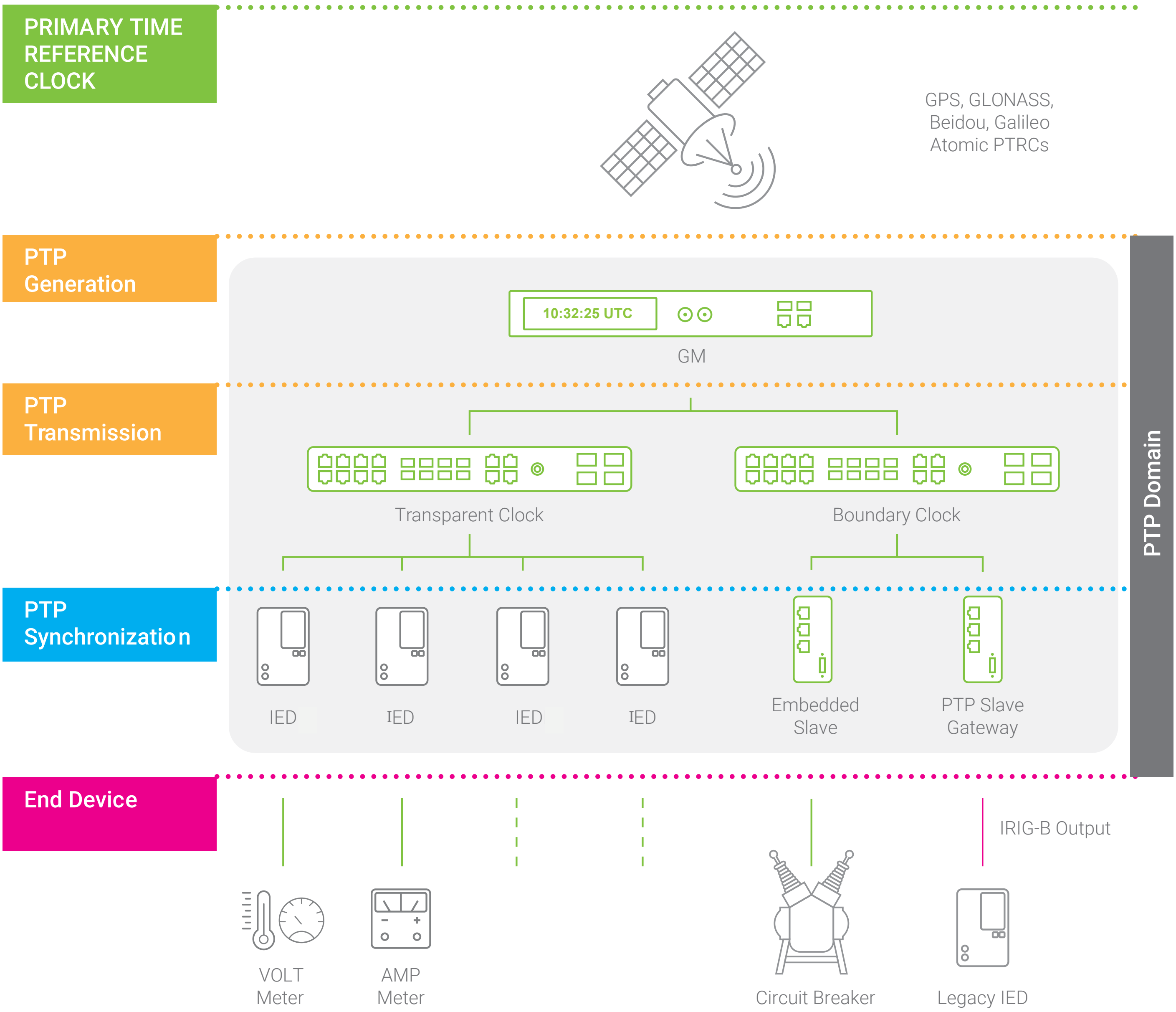
Cost effective

PTP can operate over Ethernet networks, eliminating the need for dedicated timing hardware. Therefore, it is a cost-effective solution to install and to maintain.

How does PTP work?

The architecture of a PTP network involves a hierarchical system of master and slave clocks. Masters serve as the source of time, distributing the time to different segments, while slave clocks receive PTP messages from masters and adjust their own time to synchronize with the network time. This strata system allows for easier network management and troubleshooting of issues when they arise.

A common substation PTP network includes a grandmaster (GM) clock, boundary clocks (BC) and transparent clocks (TC) as intermediary slaves, and end slave clocks, as depicted in the following figure. Below we will take a deeper look into the features and requirements of each clock type.



The grandmaster clock

NTS7500

NTS8600

Stratum 1 in the PTP hierarchy contains the grandmaster clock, which is the source of accurate time for the entire PTP network. The grandmaster is typically synchronized to a reference (Stratum 0) time source such as a GPS clock. Based on the reference time, it generates PTP messages and distributes them to lower-tier clocks in the network. The reliability of the grandmaster ensures accuracy for the whole system, and redundancy is essential as a fault-tolerant precaution.

As a power-grade grandmaster clock, ATOP NTS series incorporates a high-precision GNSS module and PTP hardware support, including for IEEE/IEC 61850 Power Profiles as well as for legacy ones like IRIG-B, BJT, BCD, ST, and ST with checksum. The industrial fanless design, wide operation temperature, and high EMC ensure maximal availability under harsh conditions, while PRP and power redundancy further safeguard the PTP network against failures.

Boundary clocks

Boundary clocks receive time information from the grandmaster clock and act as new masters to redistribute it to other devices in the network. They also perform time stamping and packet forwarding functions. Boundary clocks reduce the load on the grandmaster clock and improve time accuracy by minimizing the propagation delay of PTP messages.

RHG9528

RHG9728

Capacity is an important feature of boundary clocks, as they are often used to connect multiple PTP domains or in complex network topologies. The ATOP RHG9X28 hardware-based boundary clock supplies up to 24 Gigabit ports to handle large numbers of PTP clients with simple architecture, while additional 10G uplinks allow fast transmission to upper level management. Its modular configuration provides flexibility and scalability. Support for multiple profiles ensure compatibility with various PTP devices.

Transparent clocks

Transparent clocks also receive PTP time packets from the grandmaster, but while they measure the propagation delay of PTP messages and compensate for it, they do not modify the PTP messages in any way—they forward the messages transparently between network segments. Transparent clocks are used in large networks with multiple network segments, and provide a way to mitigate the effects of network latency and delay variation.

EHG9508

A good transparent clock, like ATOP EHG9508 and EHG9512, supports multiple network segments to provide accurate time synchronization across large networks. It integrates easily into existing network infrastructure without causing disruption, and its low latency minimizes propagation delay to establish accurate time synchronization.

EHG9512

Transparent clocks calculate link delay time within a network by two methods, end-to-end (E2E) or peer-to-peer (P2P). With E2E, timestamps for delay calculation are collected when the clock receives the time packet from the grandmaster, and when the packet reaches the end of the network. Any other transparent clocks in between simply forward the packet, achieving maximal efficiency. ATOP EHG95xx and EHG96xx series are of this type.

With P2P, timestamps are collected and the delay calculated from each transmission (or hop) between a sequence of transparent clocks. ATOP RHG9X28 series can work as this type of transparent clock, which, compared to E2E, may generate higher loading but also higher accuracy.

Ordinary clocks

The final level in a PTP network is ordinary clocks, or PTP-enabled devices, which are those that receive PTP time packets from the boundary clocks or transparent clocks, and use the information for operation. In a power substation, ordinary clocks can be part of protection relays, meters, switches, and others. They do not pass on the PTP packets to other devices, but may use the time information to control other end devices.

ATOP's range of PTP-enabled devices are rugged for harsh environments, easy to manage through web UI or dedicated software, and most importantly, cyber secure. The EH9711 managed switch, for example, is compliant with IEC62443-4-2. Security-assuring features include network monitoring with port mirroring and access control with 802.1x, AAA, ACL, and IP Source Guard.

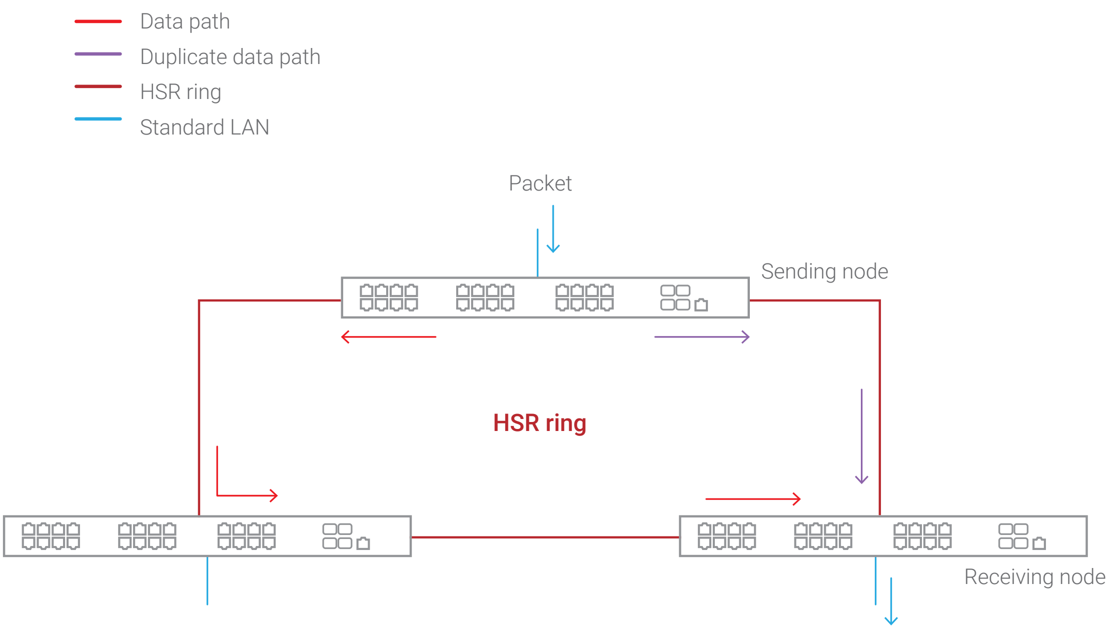
EH9711

Adopting PTP can help substations achieve highly precise and stable time synchronization, enabling efficient and reliable operation of critical power system applications. To ensure successful implementation of PTP in power substations, one must consider various factors such as clock selection, network architecture, and hardware and software requirements. Reach out to our experts for discussions on your specific project, or read our earlier whitepaper, *PTP Best Practices for Industrial Networking,* for more in-depth knowledge on PTP.

HSR and PRP: what high-availability means for power substations

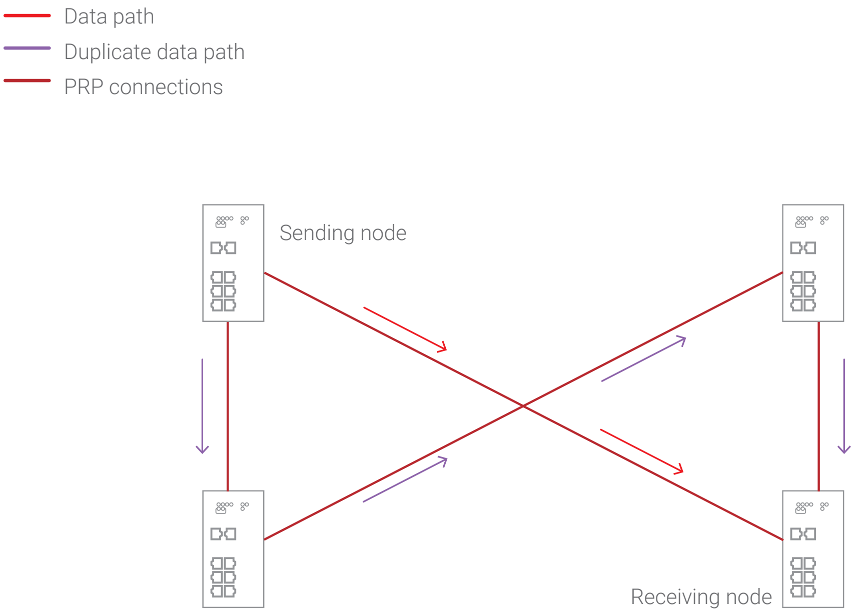
To avoid errors and blackouts, substation automation must ensure strict data integrity and the least latency or downtime. Therefore, the IEC 61850 Standard adopts High-availability Seamless Redundancy and Parallel Redundancy Protocols to achieve fault-tolerant communication between devices within the power grid infrastructure. These redundancy techniques are known as hot redundancy, where redundant links are simultaneously active, thus enabling minimal switchover time.

High-availability Seamless Redundancy (HSR; IEC 62439-3 Clause 5) is a protocol designed to provide seamless and uninterrupted communication in the event of a network failure or equipment malfunction. The HSR topology is typically a ring, with each device connected by two ports to the ring. When a device sends data, it duplicates the packet and transmits it simultaneously in both directions of the ring. At the receiving end, the first arriving correct version is selected for further processing, and the duplicate or corrupted packet is discarded. In this way, HSR attains zero packet loss and high reliability.



A differentiation point of HSR from other redundancy mechanisms is that the dual ring topology allows sub-millisecond switchover without impacting real-time control and protection functions, which are crucial for the continuous operation in critical applications. Additionally, HSR's deterministic nature ensures that data transmission occurs within predictable timeframes, making it suitable for applications where downtime or communication failures can have severe consequences for the power grid's operation and safety, such as protection relay coordination or real-time control of substation equipment. In short, wherever precise timing is necessary on top of data integrity.

Parallel Redundancy Protocol (PRP; IEC 62439-3 Clause 4) is another redundancy protocol used in power grid communications. It also creates a redundant network topology, but instead of rings, it uses a double star topology to send duplicate data packets over two independent network paths.



The benefit of PRP is that the load on each individual connection is as of a non-redundant connection. Therefore, PRP is valuable in large-scale communication networks, such as one that involves multiple substations or interconnected systems spread over a wide area, where the primary concern may be the scalability and flexibility of the network.

PRP can easily accommodate a higher number of devices and network segments by leveraging parallel paths. Each device or network segment can have its own redundant communication path, allowing for more extensive and complex network topologies. This flexibility makes PRP suitable where the network infrastructure needs to be scalable and adaptable to changing requirements.

HSR and PRP can share the same nodes, and operate invisibly to the application, meaning that they are independent of the application-protocol and compatible with most Industrial Ethernet protocols. Yet, building an IEC 61850 network with HSR and PRP still calls for careful planning and device selection. Both protocols utilize specialized hardware that contain redundant network interfaces, are capable of duplicating and forwarding packets, and provide redundancy and seamless switchover functionalities. HSR, in particular, requires support for ring topology and usually Precision Time Protocol (PTP).

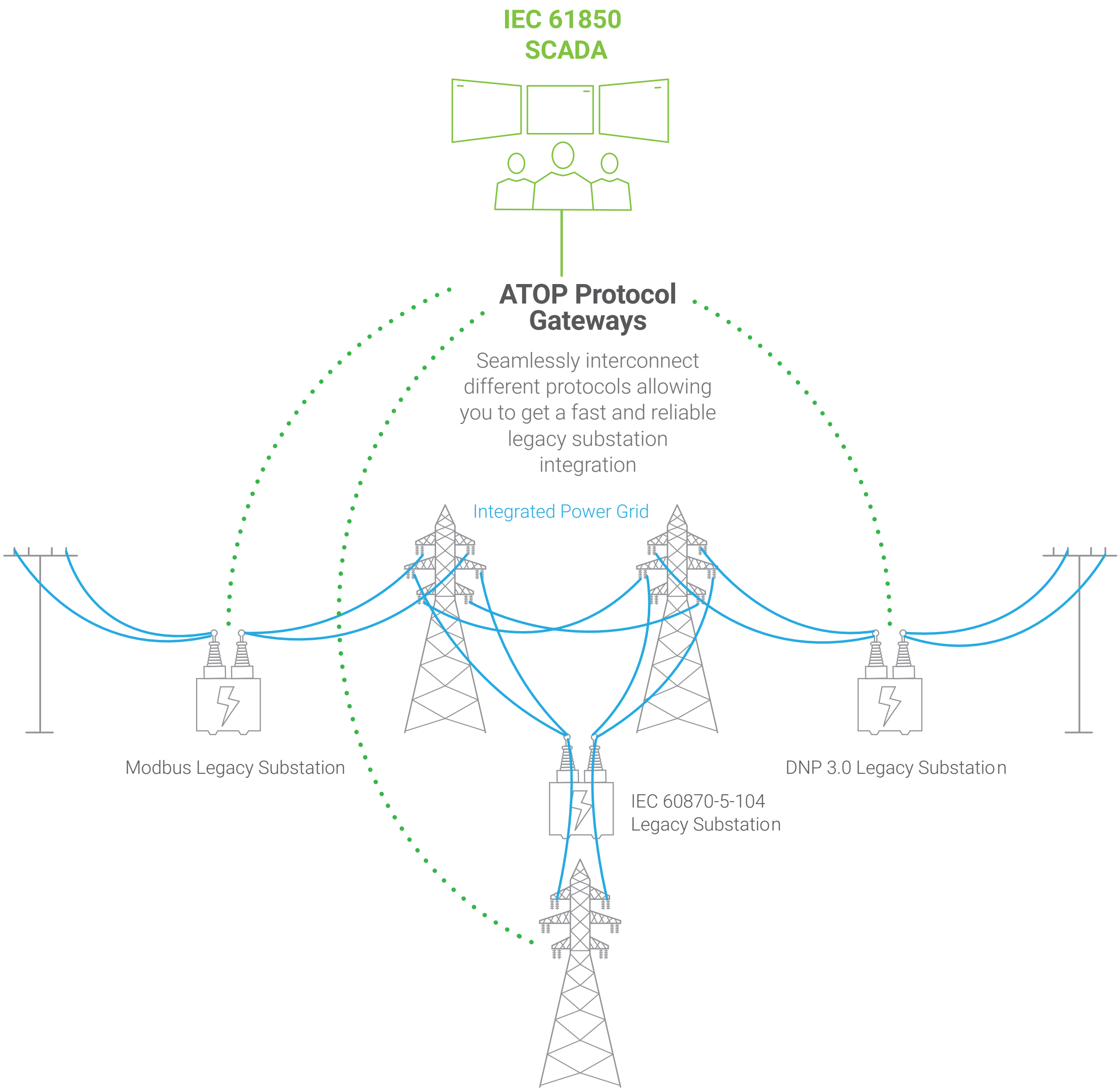
Previously, we talked about achieving precision timing in power substations through PTP. Used in conjunction with HSR/PRP, PTP helps synchronize redundant paths and ensure that all devices involved have a consistent and accurate time reference. In certain scenarios, HSR/PRP networks may require precise time-triggered operations for critical tasks, of which the effectiveness relies on PTP time alignment. PTP in these networks may need to operate separately within multiple synchronization domains, or be redundant in itself, to maintain precise time alignment within each redundant or parallel path. On the other hand, timestamping by clock nodes in a PTP network can complicate the HSR/PRP handling process, as duplicate packets are no longer identical as they move along different data paths. So, much consideration is needed to build a reliable and robust system that meets IEC 61850 standards.

For substation backbone communication, ATOP RHG9628 and RHG9528 High-Availability Managed Gigabit Switches are ideal nodes as they support HSR/PRP ports as well as PTP and advanced management features. The high-availability functions are basically plug-and-play, and the large number of modulated slots enable large-scale, flexible networks. For communication with non-HSR/PRP supporting IEDs, connect each IED to the HSR/PRP topology through a redundancy box (RedBox), and you're good to go.

Protocol gateways and data concentrators in substation application

At the time of building, power utilities typically invest in the latest available technologies. Yet, equipment in the grid system has a long lifespan, lasting over 50 years. As a result, often both legacy and new technologies are present in the power grid. A challenge of implementing IEC61850, therefore, is to integrate all technologies seamlessly to enable this enhanced system.

For substations utilizing legacy process protocols such as through IEC 60870, DNP 3.0, and Modbus, ATOP provides protocol gateways of powerful hardware platforms paired with stable software, enabling transparent, highly reliable, and fault-tolerant protocol-to-protocol translation for integrating legacy equipment into modern network systems.



IEC 60870

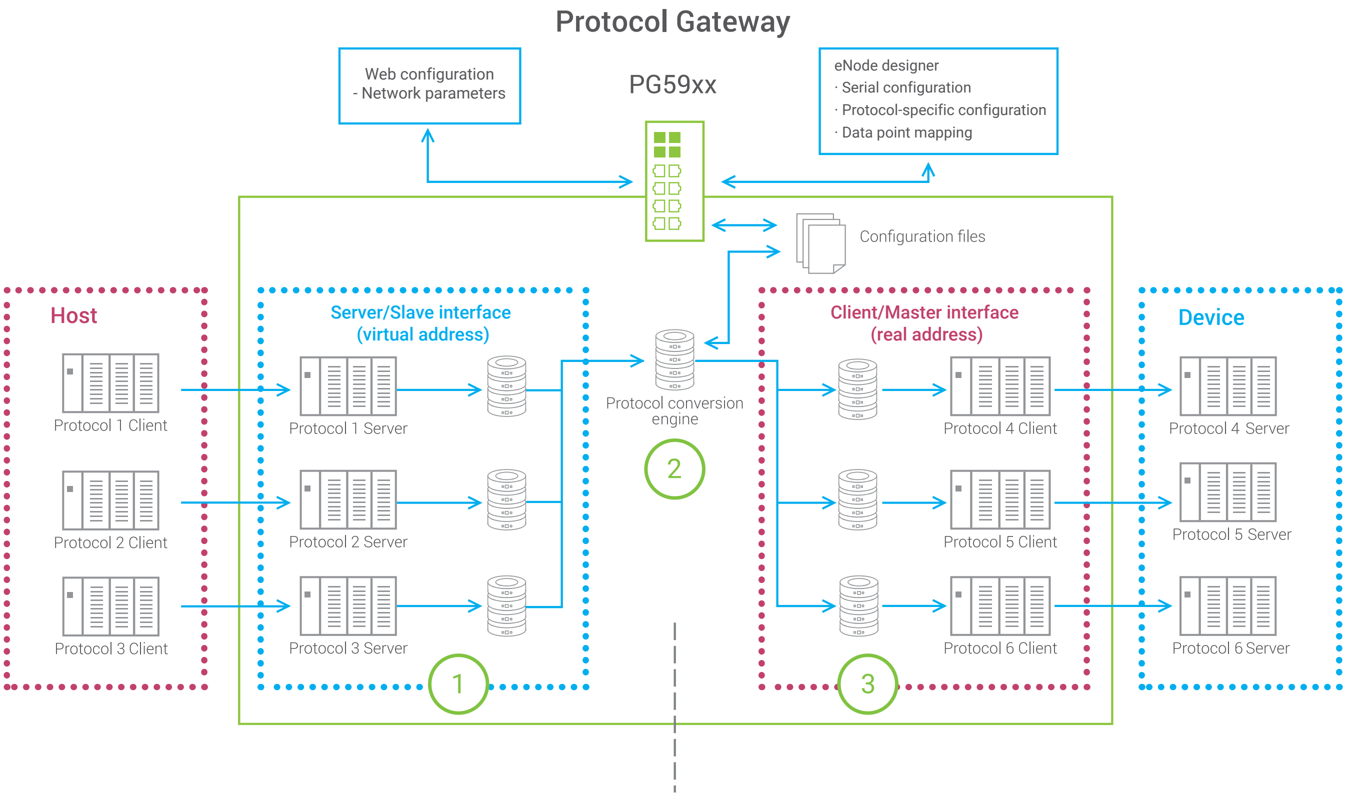
Architechture of protocol gateways

Architecture of a protocol gateway consists of three parts:

① A **server/slave interface**, which listens to an external host client/master, such as a PLC. The protocol gateway will act towards the host as a slave device according to the protocol used.

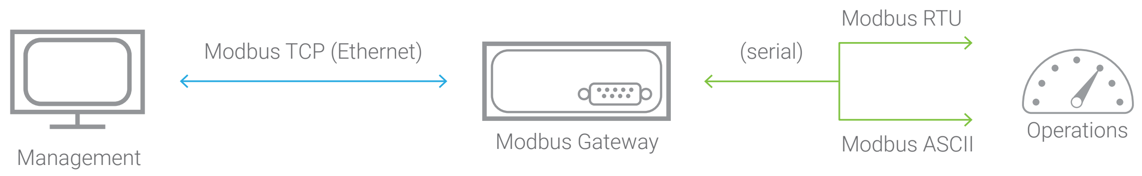
② A **protocol engine**, the core of the unit that moves, translates, and maps the data points, commands, and events between the client and server sides. Here, data, commands, and events are stored and mapped to other protocols. ATOP protocol gateways allow protocol mapping to any Serial or Ethernet port. Using the friendly eNode Designer tool, users can assign different protocols to different ports, configure serial port settings and protocol-specific parameters, and define real IDs or virtual addresses for the Master/Client or Slave/Server to work with, respectively.

③ A **client/master interface**, which actively polls or issues commands to an external server/slave device.



Application of protocol gateways

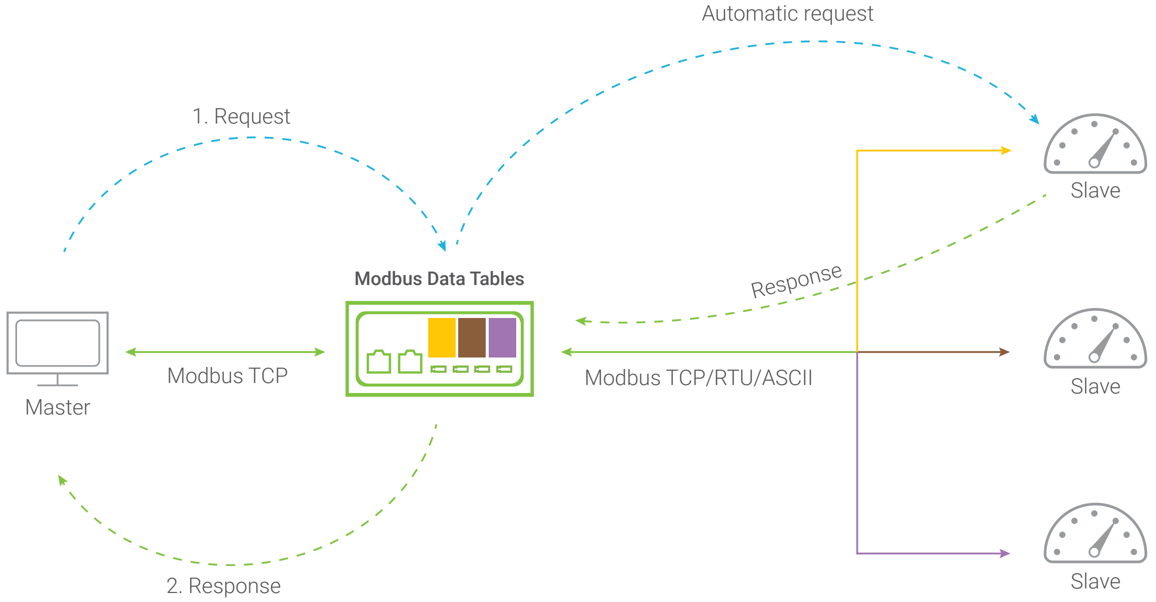
Choose and set up protocol gateways according to the host and equipment protocols required. A Modbus gateway, for example, converts Modbus RTU and ASCII to Modbus TCP. Modbus RTU is a compact binary protocol known for its efficiency and compactness, while Modbus ASCII uses human-readable ASCII characters, useful for debugging and testing purposes. By converting these serial protocols to Ethernet-based Modbus TCP, the Modbus gateway enables higher data rates as well as more advanced control and monitoring features. It is the key to bridging legacy devices with modern IEC61850 systems, allowing the high availability, reliability, and security that modern power grids need, without the cost and hassle of a full system renewal.



ATOP protocol gateways can serve more than simple protocol conversion. **Port isolation** and **VPN** features (such as provided by ATOP 5904D) protect against potential failures and attacks by ensuring that issues on one side of the gateway do not propagate across to critical devices. **Routing** and **filtering** functions help control the flow of information, managing data traffic and optimizing communication between devices. **Data mapping** assigns data points into memory, further improving communication efficiency.

A **data concentrator** (such as the ATOP MB5916-CT and MB5916A-CT) is an advanced machine suitable for frequent polling requests from multiple devices. ATOP Modbus concentrators perform pre-defined Modbus commands to read/write data automatically from slave devices. It then mirrors the obtained slave device data to its own memory, compartmenting those from different slaves in separate tables for easy access. Thus, requesting masters can receive responses in a shorter period, achieving better overall efficiency, even with a high density of devices.

Modbus concentrator register mapping can be customized for optimal performance where different masters need to access different data structures. Link status and data timestamp access allow high-level management, and for the most mission critical applications, redundant architecture can achieve automatic link recovery in case of Ethernet or serial link failure.



Case study: Robust and secured networking for substations

Requirements

To provide a full turnkey industrial networking solution for up to 32 substations, many which are far from each other. The overall network must comply with industrial cyber security standards as well as ensure high reliability. Some other required standards include:

- Traffic optimization and packet prioritization according to IEEE 802.1p/q
- Precision Time Protocol—time synchronization according to IEEE 1588v2
- HSR-PRP zero packet loss redundancy protocol

Solution

A comprehensive solution was provided by ATOP along with partners BlackBear TechHive and BlackBear Cyber Security. In total, more than 150 ATOP switches are used throughout these 32 substations. All are managed via BlackBear TechHive's network management tool. Specifically designed for efficient, portable, scalable, secure and consistent management of network communications systems, the BlackBear NIMBL is capable of, among other features, automatic device discovery, device monitoring and diagnostics, and alarm notifications in case of any anomalies.

A data diode solution by BlackBear Cyber Security provides hard defense through network segmentation between the operational technology (OT) side to information technology (IT) side, as IT is exposed to external environments and hence more susceptible to cyber-attacks. The BlackBear Intelligent Gateway (BIG) is an FPGA-based data diode. It ensures a strict data flow from OT to IT only, so any traffic from IT to OT will be blocked in its entirety. With a data diode, the user avoids a lot of maintenance work, and keeps safe from zero day vulnerabilities. Firewalls, on the other hand, are never safe from zero day vulnerabilities as they rely on known malware signatures to operate.

Moreover, data traffic must be encrypted to avoid eavesdropping. ATOP switches use MACsec to encrypt data from RTUs/VOIPs/AMRs/recorders to the central SCADA room, and the BIG encrypts data from and through SCADA. Therefore, SCADA data can be sent securely to uplinks via FTP/sFTP.

All networking devices are IEC62443 compliant to ensure sufficient cybersecurity robustness. Especially in critical environments like substations where the stakes are high, this feature is important indeed. And built with industrial-grade hardware and design, the whole system is able to perform reliably under harsh environments for a long period of time.

OFFICAL WEBSITE

LITERATURE LIBRARY

ATOP Technologies | by BlackBear TechHive

2F, No. 146, Sec. 1, Dongxing Rd., Zhubei City, Hsinchu County, Taiwan

+886-3-550-8137 +886-3-550-8131 info@atop.com.tw