NOZOMI NETWORKS

WHITE PAPER

Improving Cybersecurity & Reliability for Substations and Power Grids

With OT Continuous Monitoring

Table of Contents

1. Introduction

Many electric utilities around the world have increased the interconnectedness and digitization of their systems to gain operational efficiencies and reduce their carbon footprint. For example, improved smart grid connectedness, utilizing standards-based Ethernet and TCP/IP communications, is enabling efficient energy management. However, it also increases concerns about cybersecurity and reliability.

Electric utilities worldwide also face increasing regulatory mandates around cybersecurity. In the United States, the NERC CIP standards dictate strict and enforceable cybersecurity protections for bulk electric systems. The European Union's NIS2 Directive mandates cyber risk management, reporting, and resilience testing for essential sectors like energy. Australia's SOCI Act requires utilities to adopt cybersecurity best practices and report incidents, or face penalties.

To improve cyber resiliency and prepare to meet these new requirements, many utilities are evaluating options for enhancing the cybersecurity of their operational technology (OT) systems. One fundamental security best practice is having real-time visibility into assets, network traffic, and vulnerabilities.

This paper illustrates how an OT continuous monitoring platform improves the cybersecurity and operational reliability of power generation, transmission and distribution systems.

Read this paper to learn:

- The challenges facing power grid operators today
- How OT continuous monitoring technology works
- Sample architectures to improve cybersecurity
- Specific use cases for securing electric power systems
- Detailed operational visibility use cases for enhancing power grid reliability
- Expert insights on security and monitoring power systems

2. The Digital Transformation of Substations for the Smart Grid

Many electric utilities have hundreds or even thousands of substations which are critical for maintaining efficiency and adaptability in a smart grid. Their main role is to step down power from the transmission grid to the distribution grid with infrastructure that is closest to electricity consumers.

With the smart grid, information about consumption and operations needs to be sent back to a central point for analysis by energy management systems and substation automation systems, which requires two-way communication of data.

Thus, the communications networks of substations have been retooled to facilitate connectivity with multiple systems. The preferred networking technologies are based on Ethernet and TCP/IP and adhere to the IEC 61850 standards. This international family of standards defines the architecture of electrical substations and has the benefit of allowing devices from multiple vendors to communicate and work together seamlessly. It covers areas such as modeling, configuration, and low-level communications protocols. The protocols used are primarily the IEC 61850-8-1 (GOOSE and MMS) and secondarily the IEC 61850-9 protocols, or SV (Sampled Values).

Most substations include a mixture of equipment, with some using IEC 61850 communications and others using serial communications schemes (such as the one standardized in IEC 60870-5-101).

The typical substation may have a system architecture that looks like the one shown in Figure 1.

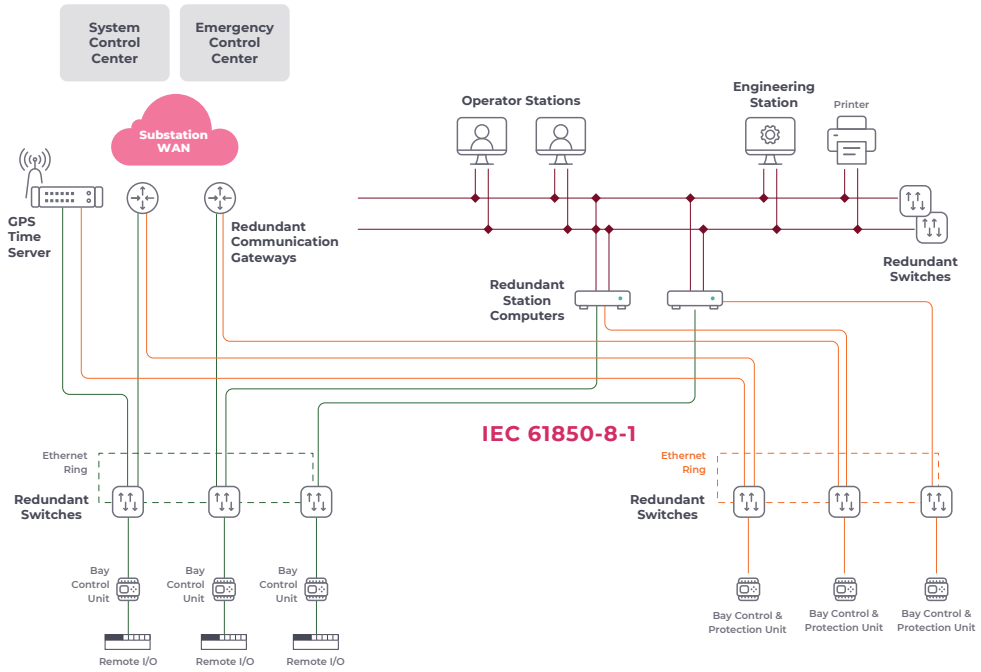

Figure 1 - Sample deployment architecture of a substation automation system and control network.

Figure 1 shows a sample network architecture diagram for a substation automation system where the station level includes operation and engineering stations that are connected to a redundant LAN managed by two dedicated switches. Two station computers, in a high availability configuration, act as IEC 61850 communications gateways between the station level and the bay level.

The lower part of the figure shows two different redundant IEC 61850-8-1 based networks, one dedicated to the control units and the other to control and protection units.

These are critical networks that require high throughput speeds and redundant, dedicated, equipment to meet the substation's operating requirements. For example, communications that use the GOOSE protocol and are essential for protecting substation functioning must be delivered in <4ms. Similarly, phasors that regulate transmission systems voltage (SV) require high bandwidth.

The IEC 61850 bus, ultimately based on Ethernet technologies and primarily using fiber media, is crucial for substation operations, having replaced analog wires. Its performance is key to ensuring high digital substation functionality and availability.

Communication between the substation and the Control Centers is managed through dedicated gateway and modems that map the data to different protocols for transmission over dedicated WANs (Wide Area Networks). The WANs utilize a variety of communications media such as leased lines, MPLS, power line-based communications, satellite, radio microwave or cellular.

The protocols used for the WAN communications vary depending on the substation and the communications architecture. Examples include mapping the IEC 60870-5-104 protocol over IP, or the IEC 60870-5-101 over serial, or DNP3 either over IP or serial. In the case shown in Figure 1, the gateway devices decouple the IEC 61850 station bus from the IEC 60870-5-101 or IEC 60870-5-104 WAN, as per the IEC 61850-80-1 standard.

Modern substation systems, such as this example, need to support interoperability and deliver high reliability and availability. They also must address increasing concerns about cybersecurity. This is where OT continuous monitoring technology comes in.

3. How Does OT Continuous Monitoring Technology Work?

Many electric utilities around the world have increased the interconnectedness and digitization of their systems to gain operational efficiencies and reduce their carbon footprint. For example, improved smart grid connectedness, utilizing standards-based Ethernet and TCP/IP communications, is enabling efficient energy management. However, it also increases concerns about cybersecurity and reliability.

Electric utilities worldwide also face increasing regulatory mandates around cybersecurity. In the United States, the NERC CIP standards dictate strict and enforceable cybersecurity protections for bulk electric systems. The European Union's NIS2 Directive mandates cyber risk management, reporting, and resilience testing for essential sectors like energy. Australia's SOCI Act requires utilities to adopt cybersecurity best practices and report incidents, or face penalties.

To improve cyber resiliency and prepare to meet these new requirements, many utilities are evaluating options for enhancing the cybersecurity of their operational technology (OT) systems. One fundamental security best practice is having real-time visibility into assets, network traffic, and vulnerabilities.

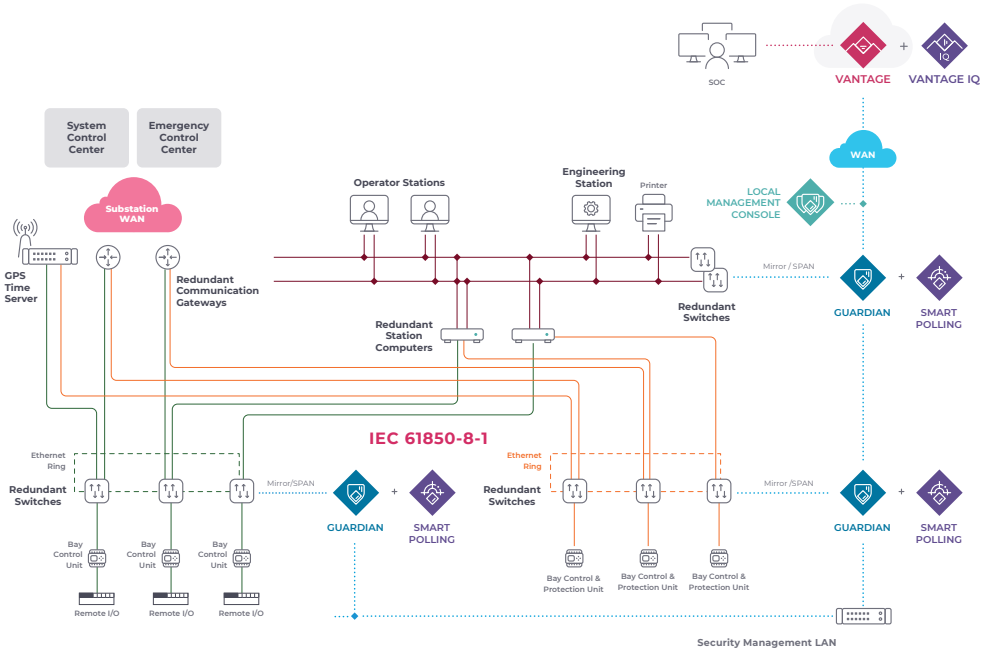

Figure 2 - Cyber resiliency architecture with OT with OT continuous monitoring.

The anomaly detection appliances should be available in a range of options, providing flexible deployment scenarios. Figure 2 shows two rugged DIN rail mounted appliances installed at the bay level, while a rack mounted appliance is used on the station LAN. The cybersecurity appliances should communicate with local or central management consoles through a dedicated management LAN, completely separated from the production environment. This ensures that the transmission of IEC 61850 communications is not disturbed in any way.

In this scenario, a hierarchical management console architecture is used. A local management console (LMC) aggregates the data and the alerts produced by the continuous monitoring appliances at a substation. This information is forwarded, through a TCP/IP WAN, to a central management console (CMC). The CMC can receive and aggregate information from multiple, geographically distributed LMCs or appliances. The CMC should have the flexibility to work at multiple levels in the architecture, for example, collecting data from local or regional substations and then forwarding it to a CMC located in the SOC.

These monitoring platforms solve an important part of the SCADA (supervisory control and data acquisition) security problems by automatically identifying industrial assets and providing comprehensive, real-time cybersecurity and visibility of industrial control networks. They should provide optimal performance while monitoring thousands of substations and assets across low bandwidth networks.

Delivering this functionality requires overcoming significant technical challenges. These challenges, and how a state-of-the-art OT continuous monitoring platform solves them, are described in the next section.

4. Challenges of Securing Electric Power Systems

Electric power generation systems and grids are characterized by large geographic areas and a substantial amount of infrastructure. This large scale creates challenges in managing and monitoring the industrial control network and its devices. Some of the technical challenges are described below, along with example solutions for addressing them.

4.1 Scalability

Challenge

- The solution needs to be operational at up to thousands of substations, each of which has many assets.
- Asset tracking, including their real-time status, requires a solution that can handle very large volumes, and do so with excellent performance.

Solution

- OT continuous monitoring should be designed to easily manage large scale substation deployments in terms of setup, configuration, and maintenance. A simplified standardized setup process should be used to automatically provision each environment with a common configuration, possibly a custom one.
- The implementation should have a hierarchical architecture with monitoring appliances at substations communicating with layers of the CMC above them. Grouping substations and appliance deployments makes system management easier and allows operators to easily obtain substation and global level views.
- The learning functionality of the system should be dynamic, allowing the system to automatically switch from learning to protection mode. Two-phase anomaly detection systems, where one must manually switch from learning to protection mode for the whole instance, can be problematic and difficult to implement. Good continuous monitoring platforms cut deployment and maintenance costs by using an intelligent one-phase approach that:
  - Eliminates the need for operators to know when to switch into protection mode.
  - Accommodates networks that might have sub-segments that need different learning time periods. For example, there might be some parts of the system that are easy to learn, and other data-oriented parts that are more complex, requiring a longer learning time frame.
- The solution should include an asset management capability that automatically identifies the thousands of devices in the system and, over time, their subparts. For example, it should recognize:
  - The inner components of modular PLCs (programmable logic controllers)
  - Logical node subsystems such as:
    - Circuit breakers (represented in IEC 61850 as the XCBR logical nodes)
    - Circuit switches (represented in IEC 61850 as the XSWI logical nodes)
    - Measurement points (IEC 61850 MMXU logical nodes), etc.
  - The LMC and CMC should show the status and attributes of each device and subpart, such as firmware version, OS, role, configuration, etc.

4.2 Bandwidth

Challenge

- The network bandwidth connecting substations to the main control center is usually low and might be active only “on demand”. For example, secondary substations in the distribution domain might only communicate as needed.
- Continuous monitoring of substations is therefore difficult. A solid network infrastructure with Quality of Service (QoS) policies in place is needed, as well as an integrated and interoperating IEC 61850 process bus. The process bus must be able to optimize traffic under various conditions to guarantee adequate grid resilience.

Solution

- Communications between the continuous monitoring appliances located in substations and the CMCs should be heavily optimized for bandwidth. It should also integrate with the bandwidth policies set in the digital substation bus for a more advanced level of QoS.
- Communications should also be regulated based on fixed bandwidth constraints. For example, it can be set to occur only at night, or to synchronize with just some parts of the system, depending on the overall requirements and the substations’ specific needs.

4.3 Time Synchronization

Challenge

- Equipment on the control network such as IEDs (intelligent electronic devices), merging units, control units and Ethernet devices need to be time synchronized with high accuracy, often to less than one microsecond. The preferred fast and safe timing system uses the IEEE 1588 protocol and a master clock or global positioning system (GPS). However, SNTP (simple network time protocol) is also very common even though it is less accurate and was created with an IT environment in mind.
- Time synchronization allows events such as faults to be replayed, detailing what happened when and to what equipment, throughout the event.
- Cyberattacks that affect IEEE 1588/SNTP communication, or the master clock/GPS can disrupt operations or be used for malicious purposes.

Solution

- The continuous monitoring platform should rapidly detect any changes to communication baselines or device status, facilitating preemptive or fast correction of time synchronization-related threats.
- The system should also readily identify specific attacks to SNTP sources.

4.4 Complexity

Challenge

- In the past, the protocols used for substation communication were mainly IEC 60870-5-104, DNP3 and Modbus. The packets sent using these protocols are easy to understand. For example, a moderately experienced technician could use Wireshark to decipher the data that endpoints sent across the wire. All the bits and bytes of the protocol are clearly shown and represented.
- New (or updated) substations use IEC 61850 and its underlying protocols for communications, and this approach is much more complex. For example, a command sent through the ACSI stack (MMS based) is far more difficult to comprehend than a single IEC 60870-5-104 command. With IEC 61850 protocols a significant amount of context must be known to correctly evaluate a single read or write logical node property.
- Complex payloads with multiple layers (like ACSI over MMS) require stateful analysis and comprehensive context recognition capabilities. Moreover, the system must keep and maintain a coherent state of each IED even as it is controlled by commands from multiple protocols, such as GOOSE and ACSI.

Solution

- OT cybersecurity requires a powerful deep packet inspection (DPI) data model with in-depth knowledge of IEC 61850 that can readily evaluate IED interactions at both the network and process levels. This includes:
  - Examining packets in all 7 levels of the OSI model
  - Knowing the official syntax and grammar for each protocol
  - Understanding the customizations used by specific industry sectors, including electricity transmission and distribution systems
  - Providing a high-performance analysis algorithm to evaluate complex possibilities in real time
  - Having a way of handling encrypted communications
  - Alerting OT and IT staff of problematic situations quickly and clearly

4.5 Cybersecurity Risk

Challenge

- Before the adoption of standard IT technologies, such as Ethernet and TCP/IP based communications, and connections to external systems, power grid networks were protected by obscure communications protocols and isolation.
- Now power grid networks are susceptible to the same cybersecurity risks as IT systems, only with the potential for more damaging consequences.

Solution

- A comprehensive understanding of IEC 61850 networks is required to baseline a thorough set of behaviors and generate alerts when anomalies occur.
  - For example, a simple rogue node attaching to the network should be readily detected and reported, as well as unseen irregular communication between known nodes.
  - Even complex state changes within IEDs should be easily detected and evaluated. OT anomaly detection should be able to learn and analyze both network and process-level objects with high performance.
  - The IEC 61850 architecture is evolving to provide better cybersecurity. For example, IEC Technical Committee 57, Working Group 15 (WG15) is defining ways to strengthen global standards to improve the security of the world's power systems. Vendors of passive monitoring platform should have in-depth knowledge of advancing IEC 61850 standards and leading-edge secure substation architectures.
  - NERC CIP has recognized the functional value of the IEC 61850 communication protocols but, interestingly, it has also whitelisted GOOSE when it comes to compliance. The committee does, however, acknowledge that the simple GOOSE real-time protocol has limited ways of preventing cyberattacks.
  - The cybersecurity solution should perform in-depth DPI on GOOSE communications and have the high-performance necessary for evaluating complex possibilities in real-time. Any cybersecurity or process variable irregularities should be immediately recognized and communicated to operators.

5. Cybersecurity Use Cases

5.1 Responding to the Asset Inventory Mandate

Scenario

A fundamental cybersecurity best practice is to have a system inventory of all the electric power grid's network and OT assets. Creating such an inventory is often done in spreadsheets, which is extremely time consuming and difficult to maintain.

Solution

An OT continuous monitoring solution should automate the creation of an inventory of system assets and keep the inventory up to date. Asset metadata should be gathered and monitored, and additional data such as location or site, should be easy to add. The asset information collected should include:

- Asset and subpart properties: site, name, IP address, MAC address (and vendor), its state (is it there or not? Is it working or not?), etc.
- Embedded devices, for instance PLCs, including their inner components: device vendor, firmware version, product and model name
- Logical node subsystems such as:
  - Circuit breakers (represented in IEC 61850 as the XCBR logical nodes)
  - Circuit switches (represented in IEC 61850 as the XSWI logical nodes)
  - Measurement points (IEC 61850 MMXU logical nodes), etc.
- General PCs: operating system and installed software applications with their version numbers. Patch levels should also be available.
- Endpoint configurations and behavior, including USB activity, user activity and log file changes.

The asset inventory should be available in dedicated views in the LMCs and CMCs and it should be easy to find and drill down on each asset. Furthermore, alerts should be triggered when changes to hardware, software, and devices occur.

5.2 Managing Vulnerability Alerts

Scenario

NIST publishes a new critical CVE alert for a vulnerability for an automation vendor's device and information about how to exploit the vulnerability is available on the internet.

Solution

The continuous monitoring platform should automatically identify and score open vulnerabilities on OT assets with a variety of methods, including network monitoring, endpoint monitoring and smart polling, to provide continuous visibility into vulnerabilities and help operators respond with actionable intelligence.

5.3 Identifying and Remediating Insider Threats

Scenario 1

An employee or a supplier of the power system operator uses valid, anonymous credentials or provides them to a remote threat actor, to gain access to the industrial network. The local or remote threat actor inserts malware onto the control network and deletes log files to disguise the activity.

Scenario 2

The laptop of a maintenance worker is connected to the substation network and inadvertently introduces malware.

Solution

In both cases, an OT continuous monitoring platform should detect the threat, provide cyber resiliency, and accelerate forensics.

Security profiles should have previously learned the behavior of the SCADA LAN and established baselines.

- The platform should rapidly identify suspicious activity such as malware that has been inserted onto the control network and the deletion of log files.
- High-level incidents should be immediately sent to the appropriate operators and SOC staff.
- Staff would then execute the incident response plan utilizing network diagrams, asset inventories and process information available from the continuous monitoring system.
- Incident replay and archiving capabilities (“time machine”) should be available to hunt for advanced attacks that cover their tracks and to accelerate forensic analysis post incident.

6. Operational Visibility Use Cases

6.1 Recognizing Malfunctioning Devices

Scenario

Interactions between a substation Remote Terminal Unit (RTU) and the control center Supervisory Control and Data Acquisition (SCADA) system are often complex, making setting up troubleshooting tools within SCADA challenging. These tools also lack important information like trace logs. Moreover, if the logs are available, they tend to differ between vendors, making them difficult to interpret.

Solution

Continuous monitoring platforms reduce time spent on troubleshooting efforts and the maintenance costs related to this situation.

- The solution should analyze traffic using a multi-dimensional approach that considers both network connections and the process state.
- It should proactively identify and isolate network problems and other types of failures.
- Operators should be provided with advance notice of failing equipment so they can conduct less costly preventative maintenance.

Example 1

The continuous monitoring solution analyzed IEC 60870-5-104 ASDUs (application service data units) with Cause of Transmission = Spontaneous and grouped them by RTU. This revealed that three of the RTUs were flapping from alarm states related to their power status. The power grid operator solved the problem by replacing the power supplies of the affected RTUs.

Going forward this utility could use the query within a monitoring dashboard to prevent extraordinary maintenance and keep all RTUs in good operating condition.

Example 2

By evaluating several statistics for each link, it is possible to identify the links with the most problematic network performance. Combining this information with the TCP retransmission percentage, the number of successful handshakes and connection attempts, it should be easy to track the link behavior over time.

For example, if a link's retransmission rate is not very high (5.5%) but it requires four SYNs (connection attempts) to complete the three-way handshake, it is a problematic link.

This information is used to remediate problematic links before there is a connection problem.

6.2 Validating "Permit to Work" Maintenance

Scenario

The maintenance contractor of an automation system vendor is approved to visit five substations on a scheduled date and update the firmware on the IEDs at each site. The contractor does the maintenance one day late and at Site C only updates the firmware of three of five IEDs.

Solution

- The day after the update work is scheduled, the maintenance manager for the region of the substations concerned reviews the dashboard of his continuous monitoring system and sees that the updates have not been done. He telephones the vendor who explains the work will be done today.
- The next day, the maintenance manager reviews his dashboard again and sees that at Site C, not all the updates are done. He contacts the vendor and reviews the situation. The vendor agrees to send the maintenance worker out again, at no charge to the electric utility.

6.3 Identifying and Documenting Device Bugs

Scenario

Complex bugs in RTUs are often difficult to reproduce and thus difficult to submit to the vendor. The operator has clues about how the bug is triggered but has a hard time finding real evidence.

Solution

By analyzing system parameters using the continuous monitoring platform's real-time query engine, checks and correlations can be quickly done. Both network and process parameters can then be used to identify the bug.

The solution should be able to create one or more rules to constantly verify that constraints and conditions of the system are verified. When something goes bad, a specific alert should be created to track failures over time.

Example

A bug in the RTU firmware causes the TCP connection to be RST'd near an IEC 60870-5-104 ASDU with Type Ident 126 (Directory). This is very unproductive because this is used to send the daily energy plan to the RTU. The operator experiences this annoying situation several times but is never able to collect evidence of the problem since it seemed to occur randomly.

The utility should be able to overcome this problem by using a custom rule capability that checks where:

- An ASDU with type 126 has been sent to a specific IOA and
- A TCP link reset happened to the RTU that had received the ASDU described above

This process should help provide a large set of evidence for the RTU vendor, and once a fix is implemented, verify that it works.

This scenario demonstrates how useful it is to have an OT continuous monitoring platform with flexible rule capabilities. This functionality can be used to verify complex states of the system, both for operational and security purposes.

6.4 Taking Control of Complexity: Understanding IEC 61850 Networks

Scenario

The setup and configuration of GOOSE messages between IEDs in substations requires a powerful tool that can visualize, in real-time, what's happening in the network. A tool like Wireshark is useful, but it quickly becomes difficult to comprehend with a growing amount of data. An IED explorer is not suitable either, because it is not able to provide all the required communications-level details.

Solution

By observing the system with the process or variables view of a continuous monitoring solution, operators should have a clear synthesis of the events occurring in the network and be able to keep track of all changes.

Example

Using network and process views together, it should be possible to:

- Track down all GOOSE events
- View the current state of all data sets
- Verify all the events flowing in the different IEC 61850 VLANS

In the schema shown above it is simple to see which IEDs in the process bus are publishing and sending updates of their logical nodes to other parts of the system. Checking the VLAN tags involved, performing tailored traces, and inserting specific checks on these links should be quick and easy.

The process view of an OT continuous monitoring platform should allow operators to instantly know the state of the IEC 61850 substation without any active interaction with IEDs. By clicking on an IED from the previous schema, the operator should see the current state of logical node properties and whether they have been accessed via ACSI or broadcast via GOOSE messages. This greatly assists with monitoring, troubleshooting and recording the events that are exchanged in the process bus.

7. Choosing an OT Continuous Monitoring Platform

Increasing cybersecurity threats, management concerns and government regulations are driving power generation, substation and electric grid operators to improve the resiliency of their systems with enhancements to their OT cybersecurity programs.

An important part of this effort is the implementation of innovative solutions that improve cyber resiliency and availability. When considering a continuous monitoring solution, seek one that meets the use cases described in this document, and that can perform effectively despite the scale and complexity inherent in substation and power grid systems. The best solution will offer a wide range of capabilities for both cybersecurity and operational visibility in one integrated platform.

Look for a solution with the following capabilities:

- **Support for OT protocols** - This includes having comprehensive knowledge of power grid standards and protocols such as IEC 61850, DNP3, Modbus and IEC 60870-5-104. Without the ability to monitor traffic between control systems and field devices, utility cybersecurity and operations teams are blind to nearly 50% of their infrastructure.
- **AI-enhanced behavioral analysis** - A process analytics engine that creates detailed profiles for every device according to the process state over multiple cycles. The resulting model improves anomaly detection and classification by combining high-fidelity asset insights with contextual understanding and adaptive learning to detect anomalies with a very low false-positive error rate.
- **Network visualization and mapping** - An auto-discovery mode that creates an intuitive network diagram in real-time and is filterable by user role and network segment.
- **Real-time query engine** - A powerful query editor for ad-hoc questions on any aspect of network or process parameters.
- **Time Machine / Event correlation engine** - A time machine allows a user to go back in time to when an alert was generated and visualize, navigate, search, and query the entire system. Event correlation is important because it groups multiple alerts into actionable, context-aware incidents.
- **Option to enrich data with OT-safe active methods** - Discovering and understanding the assets on your OT networks requires a flexible range of tactics, such as passively listening to the network, running a polling process, and leveraging offline collection methods.
- **Scalable & flexible deployment options** - Look for a solution that can handle more than a two-tier architecture to give you scalable visibility and security across all your sites, assets and endpoints. Look for a multi-tier architecture, with options for either a cloud or on prem management console.

A solution should also offer a variety of form factors for the monitoring appliances to provide a device that is right for a range of substation and control center architectures.

With support for 200+ protocols, including DNP3, Modbus, and IEC 61850, the Nozomi Networks platform delivers robust network visibility to provide situational awareness for all assets and their communications—the foundation for effective cybersecurity. The detailed OT telemetry in our platform equips your team to assess risks, detect threats early, respond quickly, harden infrastructure, and improve system resilience.

NOZOMI NETWORKS

Cybersecurity for OT, IoT and Critical Infrastructure

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

nozominetworks.com

NN-WP-SUB-8.5x11-006