NOZOMI NETWORKS

WHITE PAPER

# Improving ICS Cyber Security for Substations and Power Grids

## Real-time ICS Threat Detection and Operational Visibility Use Cases

*August 2019*

# Table of Contents

# 1. Read this Paper to Learn

- **The main issues facing power grid cyber security today**
- **Sample architectures to improve cyber security**
- **Specific use cases for securing electric power systems**
- **Detailed operational visibility uses cases for enhancing power grid reliability**
- **How passive ICS anomaly detection and monitoring works**
- **Expert insights on securing and monitoring power systems**

# 2. Introduction

Many electric utilities around the world are increasing the interconnectedness and digitization of their systems to gain operational efficiencies and meet changing customer demands. For example, improved smart grid connectedness, utilizing standards-based Ethernet and TCP/IP communications, is enabling efficient energy management. It also, however, increases concerns about cyber security.

Over the last few years, attacks on energy infrastructure have greatly increased[1] and cyberattacks have resulted in power outages in Ukraine in both 2015[2] and 2016[3]. Power system cyber threats are now recognized as core risks to safely functioning societies, economic stability and business continuity. They are also cited among the top issues keeping energy leaders around the world awake at night. Indeed, the World Economic Forum lists cyberattacks on critical infrastructure as one of the top five global risks. The 2019 Global Risk Report highlights that an attack on a country's electricity system could potentially have devastating effects[4,5].

To improve cyber resiliency many utilities are evaluating options for augmenting the cyber security of their industrial control system (ICS) networks. One fundamental security best practice is having real-time visibility into cyber security attacks, risks and incidents. Previously, the technology to provide such visibility for large, heterogeneous, high availability (HA) industrial systems, did not exist.

New solutions are now available. This paper paints a picture of how such a solution improves the cyber security and operational reliability of power generation, transmission and distribution systems.

It first describes the technical difficulties involved, starting at the substation level and expanding to include grid-wide challenges. Then, using four to five cyber security and operational scenarios, it examines how real-time threat detection and monitoring mitigates or solves issues that threaten security and availability.

When addressing today's escalating threat environment and government cyber security policies, it is important to know that solutions are available that reduce cyber risk while improving operational excellence and reliability.

© 2017 Nozomi Networks, Inc. / www.nozominetworks.com

# 3. Cyber Security and Monitoring: Technical Challenges

## I. Substations

Many electric utilities have hundreds or even thousands of substations and they are critical for realizing the efficiency and adaptability vision of the 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. This requires two-way communication of data, something that has typically not been possible in the past.

Thus, the communications networks of substations are being 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 resembling the one shown in Figure 1.

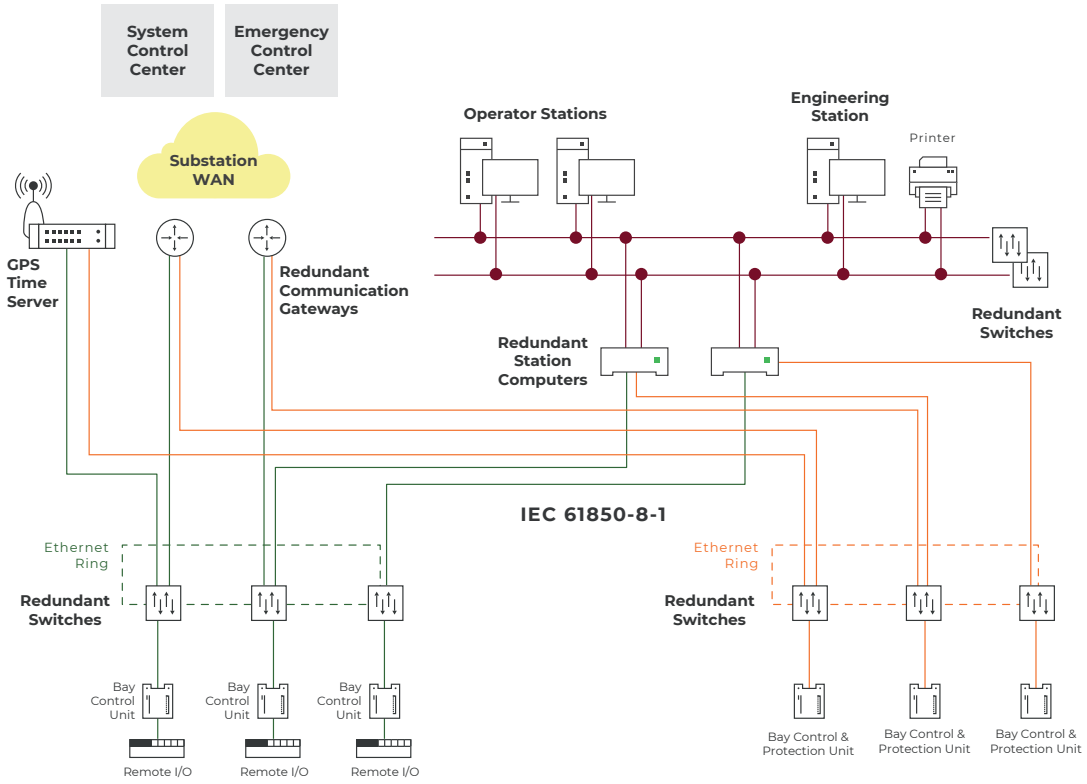



**Figure 1** - Sample deployment architecture of a substation automation system and control network.

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 an HA 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 that 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 need to address increasing concerns about cyber security.

## II. Cyber Resiliency Architecture

Building on the reference architecture presented in Figure 1, Figure 2 shows a typical deployment of ICS threat and anomaly detection implemented at different levels of the system.

**Sample Deployment Architecture**

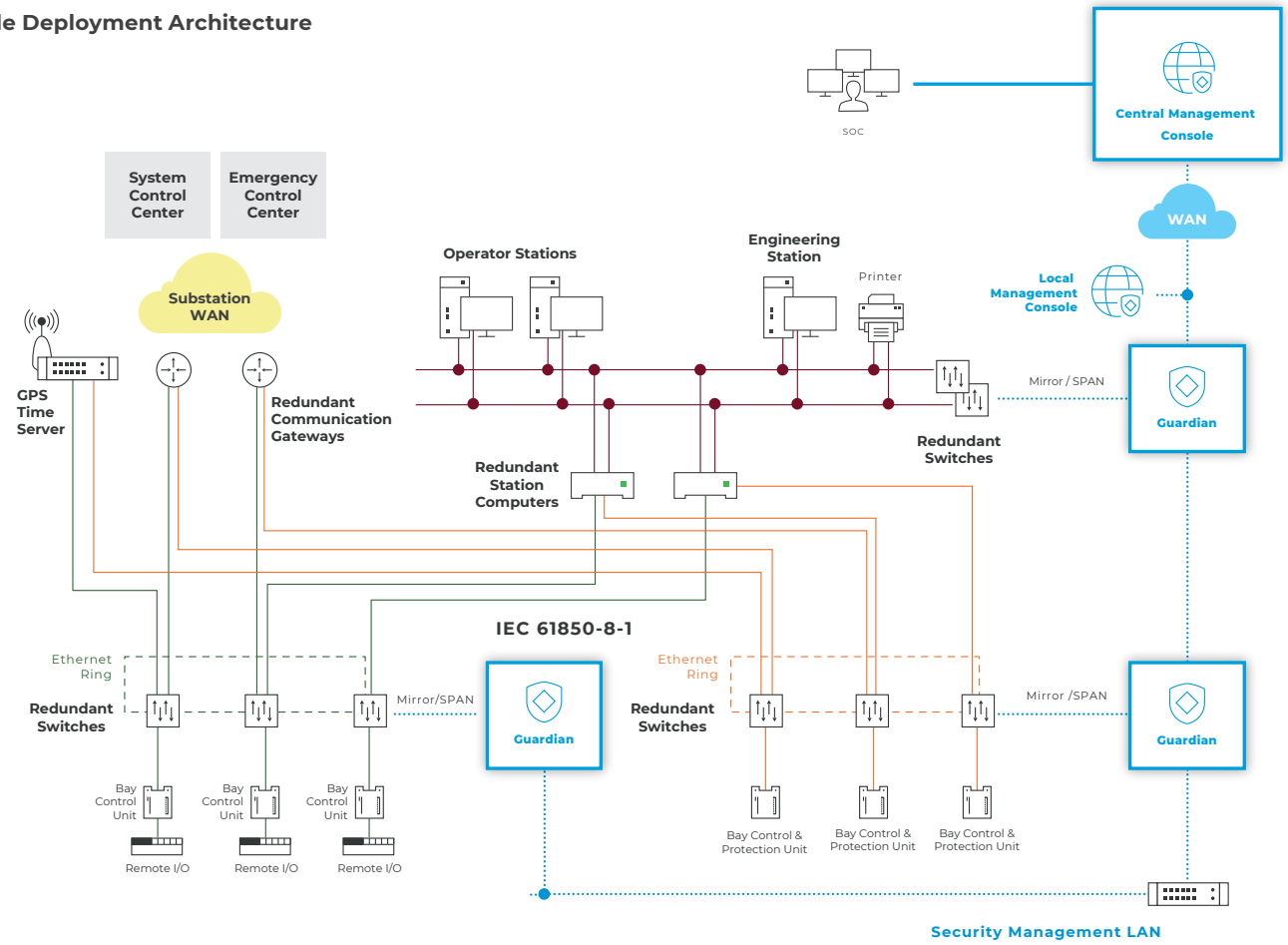



**Figure 2** - Example substation and SOC architecture showing the deployment of an ICS threat detection and monitoring solution.

The cyber security 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.

- Since the approach is passive, the installation is non-intrusive, with no downtime or network disruption.
- Deployment simply requires configuring the network monitoring devices on SPAN or mirror monitoring ports.
- The cyber security 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 passive monitoring appliances at a substation. This information is

forwarded, through a TCP/IP WAN, to the CMC located in the Security Operation Center (SOC). 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.

If needed, the alerts collected by the CMC should be forwarded to a SIEM (security information and event management) and and correlated with other IT events occurring on the enterprise infrastructure. Ideally the solution also integrates with popular user authentication systems, thereby integrating with the utility's end-to-end IT systems.

The passive monitoring devices solve an important part of the supervisory control and data acquisition (SCADA) security problem by automatically identifying industrial assets and providing comprehensive, real-time cyber security 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 state-of-the-art ICS cyber security solves them, are described in the next section.

## III. 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.

## IV. Scalability

**The 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.

**The Solution**

- ICS network 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 threat detection systems, where one must manually switch from learning to protection mode for the whole instance, can be problematic and difficult to implement. Good passive monitoring solutions cut deployment and maintenance costs by using an intelligent one-phase approach that:
  - Eliminates the need for operators to know when it's the right time to switch to 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 timeframe.
- 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 programmable logic controllers (PLCs)
  - 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.

## V. Bandwidth

**The 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.

**The Solution**

- Communications between the cyber security 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.

## VI. Time Synchronization

**The 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.

**The Solution**

- The network security monitoring solution 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.

© 2017 Nozomi Networks, Inc. / www.nozominetworks.com

## VII. Complexity

**The 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.
- Nowadays, 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.
- Today, an advanced Deep Packet Inspection (DPI) implementation is required to effectively analyze IEC 61850-8 communications. The DPI technology must deal with complex payloads with multiple layers (like ACSI over MMS), and requires 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.

**The Solution**

- ICS cyber security requires a powerful 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

## VIII. Cyber Security Risk

**The 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 cyber security risks as IT systems, only with the potential for more damaging consequences.
- Recently cyberattacks caused power outages in Ukraine both in 2015 and 2016. Fortunately, the outages were fixed within a few hours, though the damage to the control network and systems took much longer to repair.

**The 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. ICS threat 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 cyber security. 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 solution should have in-depth knowledge of advancing IEC 61850 standards and leading edge secure substation architectures.[6]
- The NERC CIP[7] committee 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 cyber security solution should perform in-depth DPI on GOOSE communications and have the high-performance necessary for evaluating complex possibilities in real-time. Any cyber security or process variable irregularities should be immediately recognized and communicated to operators.

# How ICS Network Monitoring Works

**TECHNOLOGY OVERVIEW**

Power plants or substations typically use equipment from a heterogeneous assortment of vendors and this equipment runs thousands of real-time processes generating a huge volume of data. Analyzing and monitoring this data to detect threats and anomalies that might be caused by a cyberattack is akin to mission impossible.

This is where ICS network monitoring that employs AI and machine learning comes in. Typically, an appliance is attached to a SPAN or mirror port of a switch in a substation or operations center. The application on the appliance observes network traffic and rapidly analyzes the high volumes of ICS data that are impossible to evaluate any other way.

This data analysis is used to develop process and security profiles specific for each ICS. Once baselines are established, behavioral analytics and threat signatures are used to constantly monitor them. The result is the rapid identification and alerting of cyberattacks, cyber incidents and critical process anomalies. This information can be used to prevent, contain or mitigate cyber threats or process incidents before significant damage can occur. The data analysis is also invaluable in reducing troubleshooting and remediation efforts.

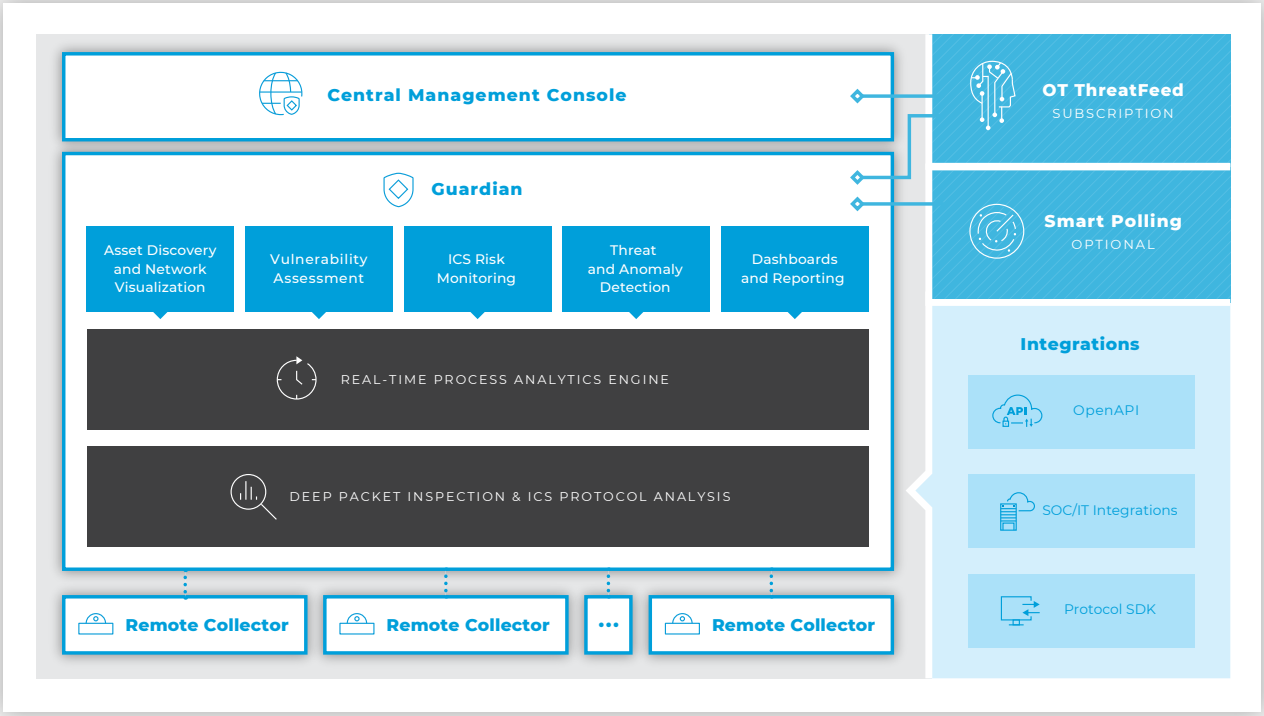



**Figure 3** - The architecture of the Nozomi Networks product line provides an example of the key components of a real-time ICS network monitoring, visibility and cyber security solution.

# 4. Use Cases - Cyber Security

## I. Responding to Mandate for Up-to-Date System Inventory

**Scenario**

A fundamental cyber security best practice is to have a system inventory of all the electric power grid's network and ICS assets. Creating such an inventory is typically extremely time consuming and difficult to maintain

**The Solution**

The ICS 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, as far as passive traffic analysis allows.

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.

## II. Managing Vulnerability Alerts

**Scenario**

The U.S. Department of Homeland Security issues an ICS-CERT alert for a vulnerability for an automation vendor's device and information about how to exploit the vulnerability is available on the Internet.

**The Solution**

The ICS real-time monitoring solution should automatically collect and maintain an inventory of all OT assets. On a user-defined schedule, assets should be checked against a state-of-the art vulnerability repository. This approach automatically determines that devices with the vulnerability exist on the utility's power grid network and generates an incident alert including a dashboard item with a high score.

Field technicians or SOC staff responsible for utility structures security receive the alert, and check it in the vulnerability dashboard. They are easily able to identify and locate the devices that have the vulnerability. Action on the vulnerability can then be triaged, and if needed, remediation can be scheduled and verified.

## III. Detecting / Countering a Cyberattack on Regional Control Center

**Scenario**

A threat actor conducts a cyberattack on a regional control center and gains access to its LAN. From this vantage point the attacker has visibility to hundreds of RTUs and can possibly control them, threatening or causing a power outage.

**The Solution**

ICS network monitoring 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 baselines should have been checked with system experts who have identified network peculiarities, such as VPN access, or IP ranges that are assigned to vendors. Pre-existing anomalies such as rogue PCs or dual-homed devices should also be incorporated into the baselines.
- The ICS cyber security solution should rapidly identify the suspicious activity associated with a threat actor accessing the LAN.
- A high-level incident 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 ICS threat detection system.
- ICS 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.

## IV. Identifying / Remediating a Malicious Insider Threat

**Scenario**

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.

**The Solution**

ICS network monitoring 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 baselines should have been checked with system experts who have identified network peculiarities, such as VPN access, or IP ranges that are assigned to vendors. Pre-existing anomalies such as rogue PCs or dual-homed devices should also be incorporated into the baselines.

The ICS v solution 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 ICS threat detection system.
- ICS 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.

## V. Discovering / Triaging Malware Introduced by a Maintenance Worker

**Scenario**

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

**The Solution**

ICS network monitoring 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 baselines should have been checked with system experts who have identified network peculiarities, such as VPN access, or IP ranges that are assigned to vendors. Pre-existing anomalies such as rogue PCs or dual-homed devices should also be incorporated into the baselines.
- The ICS cyber security solution should rapidly identify the suspicious activity of someone accessing the substation network and inadvertently introducing malware.
- High-level incidents should be immediately sent to the appropriate operators and SOC staff.
- Staff would then execute incident response plan utilizing network diagrams, asset inventories and process information available from the threat detection system.
- ICS 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.

# 5. Use Cases - Operational Visibility

## I. Recognizing Malfunctioning Devices

**Scenario**

Interactions between a substation RTU and the control center SCADA can be troublesome and often hide several sources of failure. The inspection/troubleshooting tools available with the SCADA are often cumbersome to setup and are not necessarily enabled. Important information like trace logs may not be available. Moreover, if the logs are available, they tend to differ between vendors, making them difficult to interpret.

**The Solution**

ICS network monitoring should reduce 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 ICS threat detection 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 the 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.

## II. Validating "Permit to Work" Maintenance

**Scenario**

The maintenance contractor of an automation system vendor is approved to visit five substations on an 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.

**The Solution**

- The day after the update work is scheduled, the maintenance manager for the region of the substations concerned reviews the dashboard of his ICS 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 of 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.

## III. 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.

**The Solution**

By analyzing system parameters using the ICS network monitoring solution's real-time query engine, checks and correlations should 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 ICS threat detection with flexible rule capabilities. This functionality can be used to verify complex states of the system, both for operational and security purposes.

## IV. 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.

**The Solution**

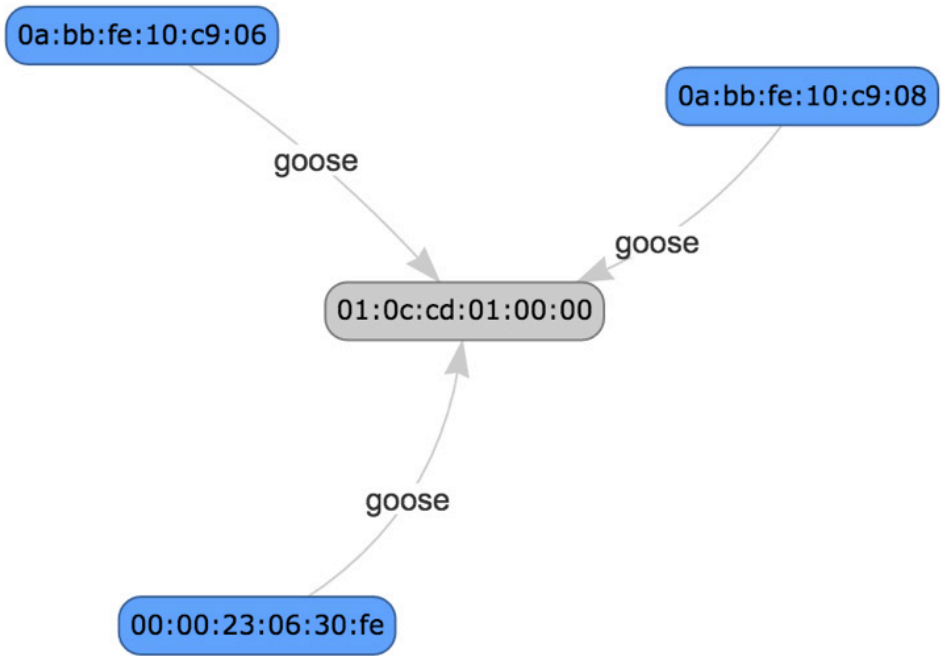
By observing the system with the process or variables view of a passive network monitoring solution, operators should have a clear synthesis of the events occurring in the network, and be able to keep track of all changes.

**Example**

A digital substation enabled by IEC 61850 is a complex and interoperable system. In particular, inside each substation, GOOSE messages quickly notify the system of events to and from IEDs with strict time constraints (< 4ms).

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 ICS network monitoring solution 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.

CONCLUSION

# Improving ICS Cyber Security for Substations and Power Grids

Increasing cyber threats, management fears and government policies are driving power generation, substation and electric grid operations to improve the resiliency of their systems with enhancements to ICS cyber security programs.

An important part of this effort is the implementation of innovative solutions that improve ICS visibility, cyber resiliency and availability.

Without ICS visibility, it's difficult to stay on top of what's happening at the grid or substation level. One small change or networking issue can impact reliability, safety and revenue. While a fast response to threats and anomalies is critical, spotting issues requires real-time visibility into assets, connections, communications and more. Unfortunately, these are capabilities that many power transmission and distribution systems lack.

Security gaps related to people, processes and technology can have a big impact on operational resiliency too. For example, the traditional divide between IT and OT, at the same time as power grid networks are increasingly connected with business networks, can lead to cyber security blind spots. But, with a focus on training, best practices and the right technology, power grid operators can improve reliability and resiliency.

In fact, with the Nozomi Networks solution, ICS visibility and cyber security are easy to achieve. It delivers improved ICS visibility by automatically creating an up-to-date inventory of all assets on the network. It then monitors asset behavior and network traffic for threats and anomalies, alerting operators to changes that could indicate potential problems. The solution also provides advanced vulnerability and threat detection, along with detailed insights that lead to faster prioritization and remediation.

Capable of meeting the use cases described in this document and perform effectively despite the scale and complexity inherent in power grid systems, the Nozomi Networks solution improves cyber security, visibility and resiliency.

**FIND OUT MORE**

Electric utilities can benefit greatly from investing in a network visibility, monitoring and security solution. Find out for yourself how quickly the Nozomi Networks solution boosts cyber security and resiliency for substations and power grids.

## What to Look for in a Real-time ICS Visibility and Cyber Security Solution

While increasing cyber threats dominate the news, there is reason to be optimistic.

New technology, such as the Nozomi Networks solution, is easy and safe to deploy, dramatically improves OT cyber security and integrates seamlessly with IT infrastructure.

When choosing a cyber security solution and vendor for your organization, make sure they have the advantages shown here.

- **Accurate OT Operational Visibility**
- **Advanced ICS Threat Detection**
- **Proven, Large-Scale Global Installations**
- **Swift Deployment Across Many Sites**
- **Easy IT/OT Integration**
- **Global Partner Ecosystem**
- **Passion for Customer Success**

## See the Nozomi Networks Solution in Action

If you would like to see our solution in action, and experience how easy it is to work with Nozomi Networks, please contact us at **nozominetworks.com/contact**

# Additional Resources

SOLUTION BRIEF

**Nozomi Networks Real-time Cyber Security**

DOWNLOAD

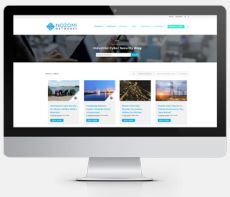
WEBPAGE

**Solution: Electric Utilities**

VISIT

WEBPAGE

**Blog: Electric Utilities**



VISIT

CASE STUDY

**Enel: An Energy Producer and Distributor**

DOWNLOAD

# References

1. "World Energy Perspectives – the road to resilience", World Energy Council, Sept. 29, 2016.
2. "Ukraine, Vermont Utility Cyberattacks Highlight Need for Robust ICS Security in 2017", Nozomi Networks blog, Jan. 2, 2017.
3. "The Ukrainian Power Grid Was Hacked Again", Motherboard, Jan. 10, 2017.
4. "The Global Risks Report 2019", World Economic Forum, 2019.
5. "U.S. Executive Order on Cyber security – What You Need to Know", Nozomi Networks blog, May 12, 2017.
6. "Advancing IEC Standards for Power Grid Cyber security", Nozomi Networks blog, Jan. 26, 2017.
7. "NERC CIP" is the North American Electric Reliability Corporation Critical Infrastructure Committee.

## About Nozomi Networks

Nozomi Networks is accelerating the pace of digital transformation by pioneering innovation for industrial cyber security and operational control. Leading the industry, we make it possible to tackle escalating cyber risks to operational networks. In a single solution, Nozomi Networks delivers OT visibility, threat detection and insight to thousands of the largest critical infrastructure, energy, manufacturing, mining, transportation and other industrial sites around the world.

For detailed information about our products, visit

**www.nozominetworks.com**

#thosewhoknowpicknozomi

NOZOMI NETWORKS

*#thosewhoknowpicknozomi*

© 2019 Nozomi Networks, Inc.
All Rights Reserved.

WP-SUB-8.5x11-004