NOZOMI NETWORKS

OT and IoT Security and Visibility for Substations & Power Grids & The Threat to the SME.

Ensuring high levels of security and privacy for remote supplier access to your IT and OT infrastructure

Securing the World's Largest Organizations

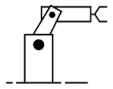
9 of Top 20
Oil & Gas

7 of Top 10
Pharma

5 of Top 10
Mining

5 of Top 10
Utilities

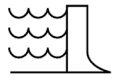
Chemicals



Manufacturing

Automotive

Airports



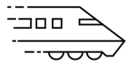
Water

Building Automation

Food & Retail

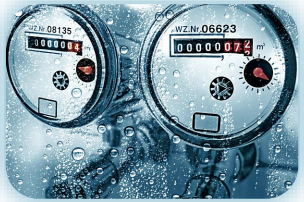
Logistics

Smart Cities



Transportation

Customer Spotlight



UTILITY

National Electricity Utility

Cybersecurity and anomaly monitoring of **>13M smart meters** at 10 OT SOCs for high resiliency and operational visibility.

UTILITY

National Electric Utility

Centralized visibility and monitoring to protect critical infrastructure across **112 substations** through improved security monitoring.

UTILITY

National Electric Utility

Modernized and enabled digital transformation of **298 substations** with a central management solution, helping meet compliance requirements.

UTILITY

Power and Telecommunications

Full visibility and monitoring across across OT/IoT networks, meeting regulatory guidelines and providing deep understanding of anomalies and threats.

Cyberattacks on Energy Infrastructure are Increasing

The Global Risk Report 2020
January 2020
Cyberattacks on critical infrastructure— rated the fifth top risk in 2020…—have become the new normal across sectors such as energy.

Ransomware Operators Demand $14 Million from Power Company
July 2020
The threat actor behind the Sodinokibi (REvil) ransomware is demanding a $14 million ransom from Brazilian-based electrical energy company Light S.A.

Key Part of Electricity Network Hit by Cyber Attack
May 2020
Staff at key energy market player Elexon were locked out of its systems by the cyberattack.

LookBack Malware Attacked Energy Utilities Across 18 States
January 2020
The Wall Street Journal has identified facilities that were hit, a few located near dams, locks and other critical infrastructure.

Energy: #3 Most Targeted Industry in 2020

Top 10 industries by attack volume, 2020 vs. 2019

Sector	2020 rank	2019 rank	Change
Finance and insurance (23.0%)	1	1	-
Manufacturing (17.7%)	2	8	6
Energy (11.1%)	3	9	6
Retail (10.2%)	4	2	-2
Professional services (8.7%)	5	5	-
Government (7.9%)	6	6	-
Healthcare (6.6%)	7	10	3
Media (5.7%)	8	4	-4
Transportation (5.1%)	9	3	-6
Education (4.0%)	10	7	-3

Source: IBM Security X-Force Threat Intelligence Index 2021

”

At a virtual press briefing, North American Electric Reliability Corporation (NERC) Senior VP Manny Cancel said that **the electricity sector has faced an “unprecedented” increase in cyber threats** over the past year and a half.

Cancel noted that **nearly 25 percent of the 1,500 electric utilities that share information with NERC said they had downloaded the tainted SolarWinds software.** A smaller subset of those said they used SolarWinds in their operational technology networks.

Source: IBM Security X-Force Threat Intelligence Index 2021


How can utilities improve cyber resilience ?

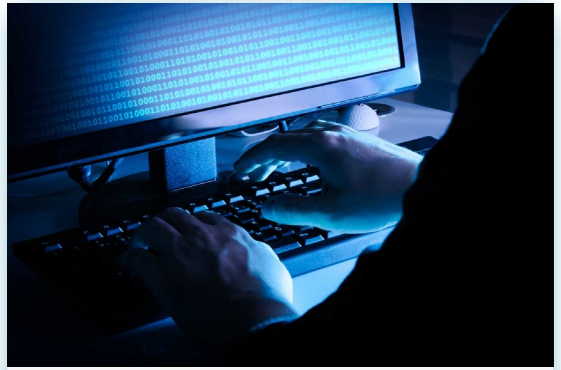
Common Operational & Cyber Challenges for Power & Electric Systems

Scalability

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, for very large volumes.

Bandwidth

Continuous monitoring of substations is difficult. Need for a solid network infrastructure with Quality of Service (QoS) and an integrated and interoperating IEC 61850 process bus.



Time Synchronization

Cyberattacks that affect IEEE 1588 / SNTP communication or the master clock/GPS can disrupt operations or be used for malicious purposes..

Mitigating OT/IoT Cyber Incidents

Power grid networks are susceptible to the same cybersecurity risks as IT systems, only with the potential for more damaging consequences

Conclusions

Improving OT and IoT Security for Substations and Power Grids

- OT/IoT Expertise is Essential
- Availability and safety are paramount
- Different sectors have different challenges but common threats
- Critical systems operations run 24/7/365 with significant safety risks
- Industrial networks contain heterogeneous and legacy systems, diverse assets and multiple connected architectures
- Industrial protocols are inherently insecure and often obscure to the IT world
- Deep experience with OT required in mixed OT/IoT/IT environments
- Unified visibility and security across OT, IoT and IT is essential
- Solutions must be easy to deploy, non intrusive and has multiple integrations

Considerations & Questions.

OT Cyber Security & Your Supply Chain.

- What effect would an extended power outage have on my business?
- Do we have an SLA with my power Utility?
- Do we have a contingency plan for Power outage?
- What can I do?

NOZOMI NETWORKS

Thank You!

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

nozominetworks.com