



CASE STUDY

Securing Global Power Generation Network



Enel improved the reliability, efficiency and cyber security of its power generation plants and networks in Italy.

Working together, Enel and Nozomi Networks achieved substantial, measurable improvements in control network reliability, efficiency, and cyber security.



Customer Profile

- A multinational energy company, operating in 30 countries across 4 continents
- One of the world's leading integrated electricity and gas operators



Goals & Challenges

- Improve reliability, efficiency, and cyber security
- Eliminate manual, time-consuming ICS monitoring, troubleshooting and correlation work
- In-depth support for SCADA protocol IEC 60870-5-104



Results

- Improved productivity, availability, and cyber resiliency
- Centralized monitoring, troubleshooting and securing of the industrial control network
- Reduced troubleshooting and remediation efforts



“Through this partnership, we have made a substantial improvement in our Remote Control System. Nozomi Networks’ Guardian is now a fundamental element of our network infrastructure and an essential tool for our daily activities. Nozomi Networks proved to us, through an extensive production pilot in Italy, that their non-intrusive in-depth technology was able to substantially improve the reliability, efficiency, and cybersecurity of our Remote Control System.”

FEDERICO BELLIO

Head of Power Generation, Remote Control System

Guardian Proves its Value and Is Implemented System-Wide

The Challenge: Enhancing Security Profile While Increasing Operational Efficiency

Electric energy operators around the world are working to increase the reliability and cyber resiliency of their systems. This includes Enel, a global power company that manages and monitors the Italian power grid.

This grid:

- Serves 31 million customers
- Has a net installed energy capacity exceeding 31 gigawatts
- Includes more than 500 power generation plants, including hydroelectric, thermoelectric, and wind
- Is managed and monitored by Enel 24/7/365
- Is operated by Terna, the Italian Transmission System Operator (TSO)

Enel is responsible for the availability of the grid's underlying ICS and industrial network. It also manages Regional Control Centers and Interconnection Centers which connect with the TSO. The TSO manages the flow of energy to the grid plus controls and remotely regulates the power generation of power plants, increasing and decreasing power production as required. The complex system of interaction and cooperation between Enel and the TSO has strong security implications as well as operational and business challenges.

Enel's Goals: Improved Efficiency, Reliability, and ICS Security

Initially Enel was using standard networking tools to manage, monitor and troubleshoot the ICS and the control network. However, operations were manual and time-consuming.

Information was difficult to gather and required human knowledge to be understood and correlated.

Enel wanted to improve efficiency as well as reliability and security with another approach. Plus, it required in-depth support of SCADA protocol IEC 60870-5-104, used for power system monitoring and control and support for the security requirements of IEC 62351.



“This project benefited from the combination of Enel's extensive experience operating distributed power production control networks and our unique, patented technology for non-intrusive in-depth analysis of Industrial Control Systems. Together we have improved the reliability, efficiency, and cybersecurity of Enel's power generation system in Italy, a national critical infrastructure.”

MORENO CARULLO

Chief Technology Officer of Nozomi Networks

Guardian: Proves its Value Throughout the Project Roll-Out

Working together, Enel and Nozomi Networks deployed **Guardian™** at one Regional Control Center first. Following extensive testing and fine-tuning the deployment proceeded to full-scale roll-out.

As a first step, Guardian probes were installed at all Regional Control Centers to monitor the Italian operational network. They were also installed at Interconnection Centers to monitor the connection between Enel and the TSO.

Next, the **Central Management Console™** was installed to operate, monitor, and update the probes from a central control room.

Finally, Guardian portable P500 appliances were introduced to monitor and analyze segments requiring investigation and troubleshooting.

The Results: Improved Productivity, Availability and Cyber Resiliency

Post deployment Enel uses the Nozomi Networks solution to monitor, troubleshoot, and protect its industrial control network from a central location. Gathering information has become an automated process and one that delivers correlated and meaningful information. This has improved efficiency and allowed Enel's staff to focus on protecting operations.

Tangible benefits include:

- Full visibility and monitoring of the Enel control network. Includes sites at remote, isolated locations as well as the connections between Enel and the TSO.
- Enhanced operational insight such as detecting misconfigurations, anomalous activities, critical states, and standard and advanced security attacks. Supervision utilizes in-depth understanding of Enel's ICS and supported SCADA application level protocols such as IEC 60870-5-104.
- Automatic real-time notification of industrial events of interest, including alerts triggered by custom-designed rules and constraints.
- Traffic analysis for current and future investigations thanks to Guardian's unique features.



"Enel Power Plants are a strategic asset we are committed to protect. Malfunctions or damage to this infrastructure would be a threat to our national security."

"With Nozomi Networks' Guardian we can now detect and collect operational and cybersecurity issues in real time, and take corrective actions before the threat can strike."

GIAN LUIGI PUGNI
Head of Cybersecurity Designs

The Nozomi Networks Advantage

Nozomi Networks helps power companies accelerate the pace of digital transformation by pioneering innovation for industrial cyber security and operational control. We make it possible for organizations to tackle escalating cyber risks to operational networks while modernizing their businesses to succeed in the future.

Nozomi Networks delivers OT visibility, threat detection and insight to thousands of the largest industrial sites around the world. Through the innovative use of artificial intelligence (AI), our solution automates the hard work of inventorying, visualizing and monitoring industrial control networks.

Energy operators benefit from the real-time visibility and threat detection needed to ensure high cyber resiliency and reliability.



About Enel



With more than 61 million users worldwide, Enel has the largest customer base among European competitors and figures among Europe's leading power companies in terms of installed capacity and reported EBITDA.

Enel manages a highly diverse network of power plants: hydroelectric, thermoelectric, nuclear, geothermal, wind, solar PV and other renewable sources. More than 47% of the electricity Enel produced in 2014 was free of carbon dioxide emissions, making it one of the world's major producers of clean energy.

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.



www.nozominetworks.com

 [@nozominetworks](https://twitter.com/nozominetworks)

© 2019 Nozomi Networks, Inc.

All Rights Reserved.

CS-ENEL-8.5x11-004