Case Study

OMICRON

Attacks on energy utilities

Energy utilities are an integral part of critical infrastructure. They have recently become a unique target for adversaries aimed at disrupting their operations and the daily lives of those who depend on them.

IT and OT networks continue to grow and converge, increasing the attack surface for new threats within the utilities and industrial control system (ICS) environment.

OMICRON helps secure critical infrastructure with innovative devices and resilient processes.

Improving Operational Efficiency and OT Security for the German Power Grid

Building a new substation

As part of its digitalization roadmap, Stadtwerke Kempen has commissioned a new substation to develop a flexible, reliable, and resilient energy network that uses all available digital tools and technologies. The path to future-proofing the power grid proved to be demanding. During the planning and production process, technical challenges, project management, engineering challenges, and cybersecurity challenges had to be thought through and overcome.

Technical Challenges throughout the lifecycle of a new substation

The typical lifecycle of a substation project consists of three critical stages:

- Engineering design
- Testing and Commissioning
- Operation and Maintenance

For Stadtwerke Kempen's new substation, all three stages required new tools and processes for a seamless transition from conventional to digital practices – one of the main parts being the move from hard-wired communication to an Ethernet-based network as well as securing this communication.

Cybersecurity

To mitigate cybersecurity risks, Stadtwerke Kempen has deployed many of the controls recommended in three key risk mitigation and management frameworks:

> NIST
> IEC 62443
> German IT-Security Act 2.0 (“IT-Sicherheitsgesetz 2.0” in German)

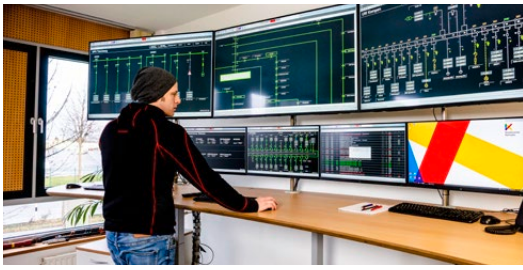
By deploying these frameworks as a guide Stadtwerke Kempen’s cybersecurity program improved significantly. The program adopted and recognized several key processes and technologies that efficiently defend and respond to various cyber-attack vectors.

At Stadtwerke Kempen, OMICRON’s team of digital substations and cybersecurity specialists guided the team through the project, helping them achieve their SAS audit and cybersecurity goal.

Taking a proactive, risk-based approach to cybersecurity

? The Challenge:
Lack of insight into OT-specific threats and how to respond to them in modern and conventional substations

The most common challenges faced by Stadtwerke Kempen are those our team continuously observes within power utilities throughout the industry. These challenges can be traced back to a lack of insight into OT assets and threats that specifically target the OT network, as well as a lack of knowledge about how to deal with them in modern and conventional substations with legacy systems.



OMICRON
Protecting OT and IT for energy utilities

Our OT cybersecurity professionals have a wealth of experience in OT security and SAS applications that comes from working with OT security systems.

In general, our Application Services team works with utilities and service providers around the world to share knowledge and best practices related to digital substations and innovative grid automation projects. We also actively participate in the development of international standards to ensure interoperability with multiple vendors. To foster industry dialog, we actively encourage utilities from around the world to exchange best practices and help facilitate an exchange of best practices.

Our Solution:
Gain insights with StationGuard's innovative approach to asset management and threat detection

Stadtwerke Kempen chose OMICRON's StationGuard solution because of its unique approach for detecting cyber assets communicating in IEC 60870-5-104 and IEC 61850 control centers, substations, and power plants using engineering file import and the SCL. StationGuard is a purpose-built IDS for utility automation and SCADA systems that monitors all communications in detail and detects cyber threats and communication errors. With this new approach, StationGuard reliably identifies anomalies in these networks with very few false positive alerts.

Since most of the network traffic in a modern substation is based on IEC 60870-5-104 and IEC 61850, we first used the detailed allow-listing approach. The function of each device was determined based on the SCL file or the engineering documentation. Unlike baseline or learning-based IDS, StationGuard supports the different phases of a substation's lifecycle with high selectivity in alerts.

With built-in support for commissioning and maintenance activities, the Stadtwerke Kempen team, thus, controlled

a) What the devices communicate and when.

b) All the assets, protocols, and services they use.

One of OMICRON's recommended hardware setups for StationGuard is the 19" RBX1 IDS sensor platform. It offers several advantages: The RBX1 provides real-time visibility into OT networks for continuous cybersecurity monitoring and reliability in harsh power grid environments. Combined with our software, it provides powerful intrusion detection and visualization capabilities. The system can operate autonomously without a connection to a central server.

StationGuard combines cybersecurity monitoring with functional monitoring of the Substation Automation System (SAS) itself. With this intrusion detection system, the team at Stadtwerke Kempen correctly identified cyber threats, prohibited activities, and various malfunctions in the SAS and were able to respond to them in the most effective manner.

The binary output contacts of the RBX1 platform were used to signal alerts and the software's different states.

Stadtwerke Kempen GmbH profile

When building a new 10 kV medium-voltage substation, the energy supplier Stadtwerke Kempen GmbH (Germany) not only wanted to meet the highest possible safety standard but also to be prepared for the operating conditions in the future. To meet this requirement, the company opted for modern digital substation communication in accordance with the IEC 61850 standard.

Achieved Customer Goals:

The Stadtwerke Kempen team conducted validation tests that certified that StationGuard meets its cybersecurity control requirements in conventional and modern substations.

In addition, they gained a compliance advantage by implementing the digital station bus in compliance with regulations, such as the German IT-Security Act 2, which requires intrusion detection systems to be installed by May 2023.

Security risk assessment

With our IDS in place, we also commissioned a full OT cybersecurity risk assessment. This allowed us to provide the team at Stadtwerke Kempen with insights into the cybersecurity and functional aspects of the automation system. The assessment was designed to reveal security risks, such as attack surfaces, vulnerabilities, and functional issues in networks or automation devices.

By the end of the security assessment process, we shared the following information with Stadtwerke Kempen:

- Network diagram with IDS sensors' location.
- Graphical visualization of OT networks and their zones.
- Asset inventory of all devices communicating within the network.
- Protocols and services active in the network.
- Cyber risk overview.
- List of external connections.
- List of unnecessary installed services.
- Overview of functional issues.

The in-depth security assessment, weaknesses detection, and operational transparency led to fully implementing the newly developed substation at Stadtwerke Kempen.

"Our partnership with OMICRON has changed how we perceive and manage our Grid. OMICRON's StationGuard Solution has dramatically improved our security posture and shed light on our operating environment, third-party systems, and more."

Reinhard Bretzke
Head of Power Supply
Stadtwerke Kempen GmbH

The road ahead:
A leading-edge vulnerability management approach for enhanced visibility into power grid networks

While the team at Stadtwerke Kempen had a good understanding of the types and quantities of devices in their infrastructure, they were still concerned about remaining cyber risks. Stadtwerke Kempen wanted to continuously monitor their OT network for vulnerabilities that could disrupt power operations and quickly fix any issues that were discovered. However, matching vulnerabilities reported for protection and automation devices with those installed on-site using existing vulnerability management tools was a difficult task.

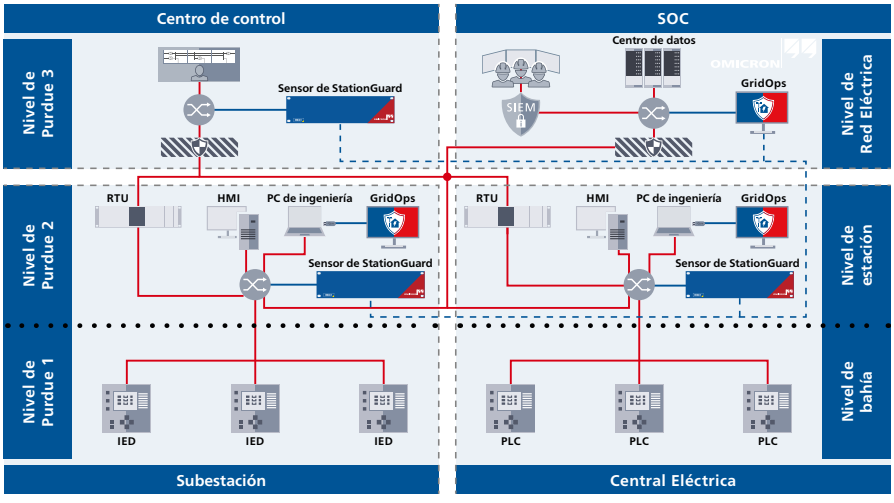
Therefore, Stadtwerke Kempen team was very excited when they learned that GridOps, StationGuard's central management system, was under development.

GridOps has been developed in response to the requests of many StationGuard customers over time. The GridOps platform will be released at the beginning of 2023 and, unfortunately, wasn't available during the time we worked on the Stadtwerke Kempen substation.

The first version of GridOps consists of four main modules:

- Asset Inventory Management
- Vulnerability Management
- Event and Alerts Management
- Reporting

By using Stadtwerke Kempen as an example, GridOps can overcome the challenges that arise in the substation. GridOps' vulnerability management addresses all the wishes and concerns outlined above.

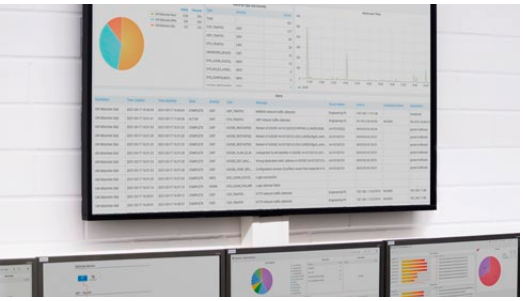


"The team behind StationGuard is made up of cybersecurity experts working side by side with protection and control experts. This bundling of know-how from both worlds makes StationGuard successful"

Andreas Klien
Product Manager
OMICRON

Case Study

The Challenge:
Identify vulnerabilities in OT devices to increase cybersecurity resilience and maturity



Security management and maintenance are very complex. It can sometimes be difficult to determine whether vulnerabilities pose a real risk to the system. Additionally, patches and upgrades for OT devices are limited and many security advisories are inaccurate.

Furthermore, there is an undeniable shortage of experienced OT cybersecurity professionals. It is also likely that IT security does not have the resources or the experience to adequately augment OT security.

Our Solution:
GridOps addresses multiple OT security needs with a single platform for unprecedented transparency and efficiency

The GridOps deployment at Stadtwerke Kempen will enable the team to achieve the following goals:

Using GridOps, Stadtwerke Kempen's IT and OT teams can collaborate to quickly identify and respond to threats in a timely manner.

Efficient asset identification processes reduce staff workload, which translates into lower financial expenses.

Thorough asset identification eases compliance by allowing Stadtwerke Kempen's team to classify and track critical information.

By prioritizing assets and budgets and developing mitigation action plans for unexpected incidents, the Stadtwerke Kempen team can plan efficient and effective incident response strategies.

By correctly identifying OT assets and their vulnerabilities, the Stadtwerke Kempen team can allocate resources to ensure that critical data, processes, and systems are optimally protected and resilient.

"The StationGuard Solution has helped us establish our cybersecurity baseline for OT networks and has given us the confidence to develop a security maturity level that demonstrates compliance with the German IT-Security Act 2.0."

Michael Schottner
Control Center Technician
Stadtwerke Kempen GmbH

New confidence for accelerating the adoption of new technologies

This case study examined how the StationGuard OT cybersecurity solution enables utilities to comprehensively identify OT assets and vulnerabilities, detect threats, address poor visibility of OT assets and environments, and provide purpose-built OT security solutions to gain a deeper understanding of cyber threats.

Summary of achieved goals:

- Addressing multiple needs of OT security with one comprehensive solution.
- Implementing a proven solution that "significantly improves the security profile".
- Improved operational efficiency by reducing time spent on OT management and cybersecurity.
- Improved cyber security to help Stadtwerke Kempen extend the useful life of its control systems.
- Maintaining 24/7 visibility and cybersecurity monitoring for operational networks.
- Immediate identification, investigation, and response to cybersecurity risks and incidents.
- Accurate mapping of the OT network and robust inventory of connected assets.
- A complete security risk assessment which leads to weaknesses detection and operational transparency.

As a result, the team at Stadtwerke Kempen received an overview of all the threats that specifically target the electrical industry and recommendations on how they can best identify and respond to them.