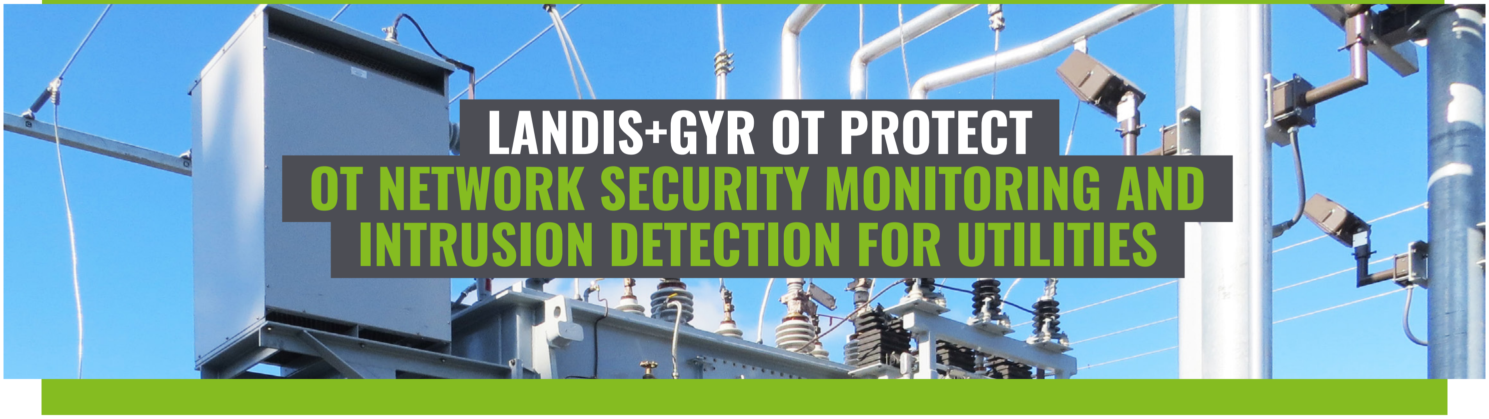
Landis+Gyr

Solution Brief OT Protect



LANDIS+GYR OT PROTECT
OT NETWORK SECURITY MONITORING AND INTRUSION DETECTION FOR UTILITIES

REDUCE THE RISK OF OT CYBER INCIDENTS
through asset discovery, network monitoring and anomaly detection

ENABLE FAST MITIGATION OF OT ATTACKS
through logging and early warning of suspicious network activity

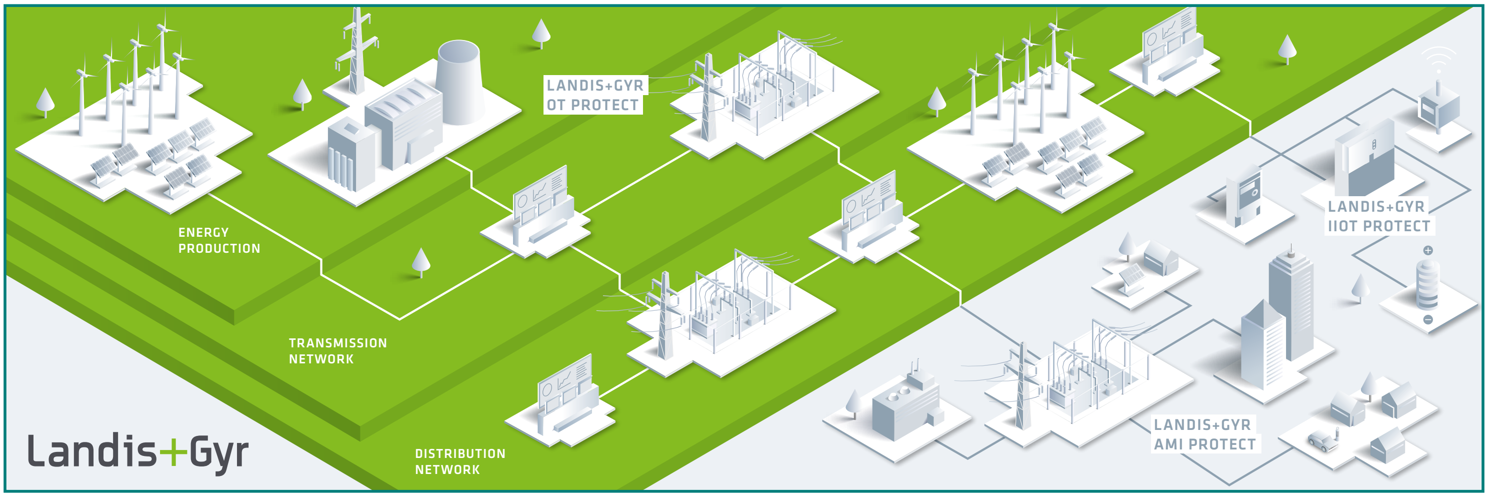
BRIDGE THE OT SECURITY SKILLS GAP
with services tailored to your needs

»Security and availability are at the heart of the Landis+Gyr offerings. With Landis+Gyr OT Protect we provide our energy sector customers a dedicated and easy-to-use OT network security monitoring with anomaly detection that increases the cyber resilience of US energy distribution operations.«

Zeek Muratovic | Director Security Solutions | Landis+Gyr

Landis+Gyr OT Protect provides companies with a powerful network-based intrusion detection system (NIDS) specifically designed for OT environments and energy distribution infrastructure. The tried-and-tested OT network security monitoring system developed by the Landis+Gyr security portfolio Rhebo gives operators and security managers full OT visibility, real-time anomaly detection and notification. This enables your company to prevent the disruption of industrial processes as well as to mitigate cyber attacks fast and targeted. Landis+Gyr also supports you in bridging the prevailing skills gap by (optionally) operating the OT Protect solution as a managed service for you.

OT PROTECT DEDICATED & SIMPLE



NEW SECURITY CHALLENGES FOR COMPLEX ENERGY SUPPLY SYSTEMS

The power grid is becoming increasingly fragmented due to the integration of municipal utilities, renewable energy resources and the construction of new substations. The individual stations are often located far away from the central control room. Therefore, control is increasingly carried out digitally via remote access. To secure these peripheral systems, distribution and transmission system operators often rely exclusively on firewalls. These reliably detect known malware. However, firewalls are blind to novel attack patterns, zero-day vulnerabilities and attacks utilizing stolen credentials. With several hundred of thousands of new malware variants each day cybersecurity limited to identifying known signatures becomes highly unreliable. Protection mechanisms in OT components are notoriously minimal. On-site personnel is rarely trained and authorized to handle OT security issues. Communication within the plants often is a black box the central control room. Incorrect or corrupted communications within substations and other remotely controlled power systems can not be detected until they have already impacted the power supply. This makes it easy for cybercriminals to scout OT networks as part of the reconnaissance, move laterally within the infrastructure, advance threat propagation as well as cause and sustain disruption.

»The network security monitoring provides us with specific support in monitoring remote maintenance and network access points. It helps us detect defects and anomalies in the OT before disruptions occur in our energy or water supply.«

Rainer Fuhrmann | Head of I&C Systems | muti-utility energy and water supplier EWR Netz

END-TO-END OT CYBERSECURITY FOR CRITICAL INFRASTRUCTURES

Together, Landis+Gyr and Rhebo support sectors such as energy, water and renewables along the entire lifecycle of establishing and maintaining OT cybersecurity. With our OT security solution, critical infrastructures can rely on our strong expertise from the initial OT risk analysis to integrating an OT intrusion and anomaly detection system to (optionally) the continuous operation of the security system coming from Landis+Gyr and Rhebo. OT network security monitoring Rhebo Industrial Protector combines passive OT monitoring with non-intrusive anomaly detection. The system is a dedicated solution for OT cybersecurity covering the infrastructure from the control rooms and central power plants to substations and renewable energy resources to enable reliable end-to-end monitoring of the distributed infrastructure. Cyberattacks, manipulation, scans and technical error states occurring in the facilities are detected and reported in real time on the basis of the associated communication changes.

The OT security solution supports all common platforms and can be integrated cost-efficiently into any industrial automated networks and IT cybersecurity via:

- dedicated industrial hardware for physical setups;
- virtual appliances for the operation in VMware, Hyper-V and other virtual environments;
- integration in common SIEM systems like Splunk and IBM QRadar.

The solution fully supports specific substation protocols such as OPC and DNP3, amongst others. With our OT security solution, resilience and system hardening of the OT are improved as threats can be mitigated quickly, and attacks can be prevented from spreading to other sites or the central systems.

SECURE IN NO TIME
3 STEPS TO UNCOMPROMISING OT SECURITY

1

The first easy step to OT security: **Rhebo Industrial Security Assessment**

Cybersecurity starts with visibility. The Rhebo Industrial Security Assessment is an OT cyberrisk and vulnerabillity analysis that provides a deep understanding of your OT assets, risk exposure as well as recommendations for effective measures for hardening the systems.

You profit from

- the identification of all devices and systems within the OT including their properties, firmware versions, protocols, connections and communication behavior (Asset Discovery & Inventory);
- an in-depth analysis of existing CVE-documented vulnerabilities;
- the identification of risk exposure, security gaps and technical error states;
- a detailed audit report and workshop with actionable recommendations.

2

The seamless transition to comprehensive OT security: **Rhebo Industrial Protector**

Cybersecurity does not end at the network perimeters. The OT monitoring with next generation OT threat and intrusion detection Rhebo Industrial Protector provides enterprise-ready OT-dedicated security. It advances the existing perimeter firewall security by integrating holistic anomaly detection that does not interfere with the critical industrial processes.

You profit from

- real-time visibility of communication behavior of all OT assets (protocols, connections, frequencies);
- real-time reporting and localization of events (anomalies) that indicate cyberattacks, manipulation or technical error states;
- early identification of attacks via backdoors, previously unknown vulnerabilities and internal adversaries that firewalls fail to detect (defense-in-depth).

3

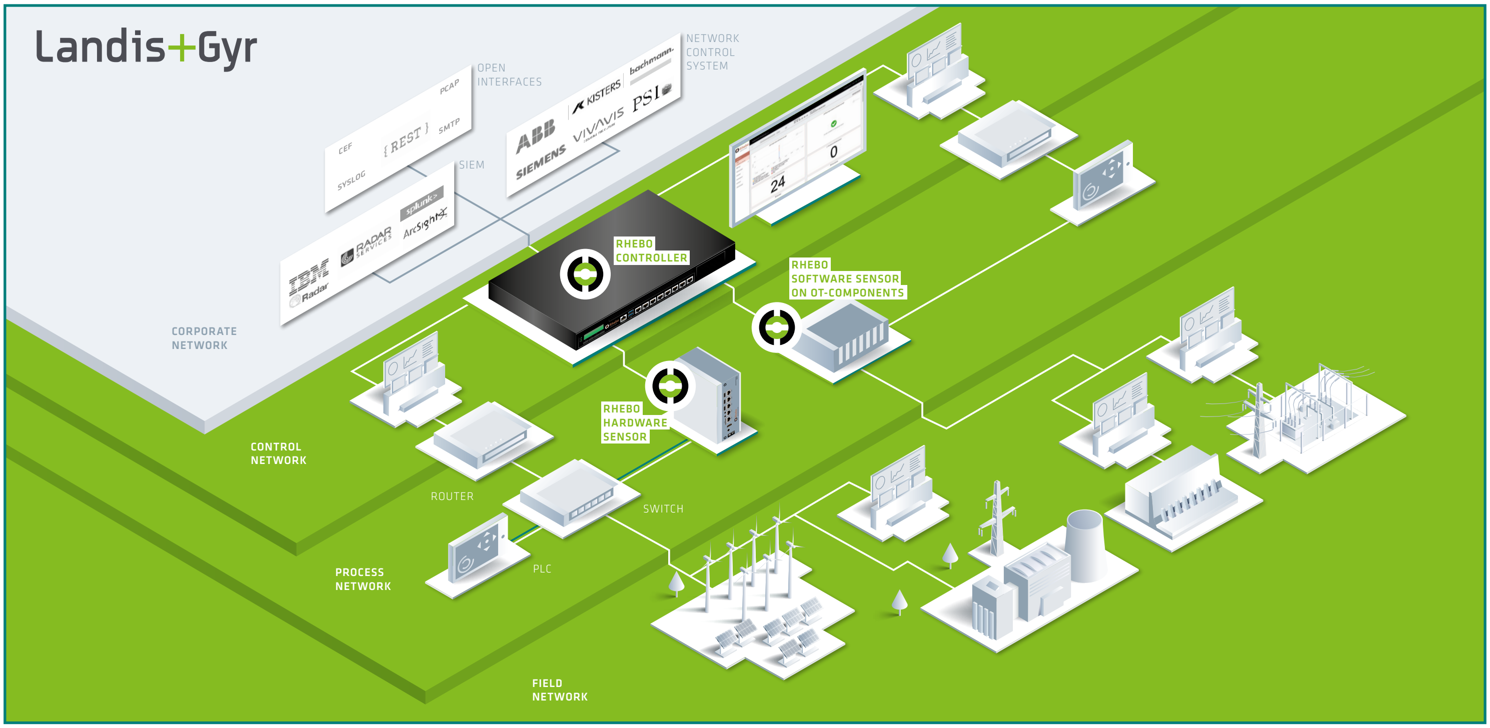
The recipe to peace of mind. We monitor so you don't have to: **Rhebo Managed Protection**

Cybersecurity needs resources. With Rhebo Managed Protection, we support you with operating the OT security monitoring system, evaluating incidents, as well as reviewing mitigation mechanisms. You can book our OT experts for regular sparring sessions on new findings, or have Landis+Gyr operate your OT network security monitoring for you.

You profit from

- expert support for the operation of the OT security monitoring system;
- fast forensic analyses and assessment of OT anomalies;
- fast actionability in case of incidents;
- regular OT cyber risk analyses and maturity assessments for continuous improvement.

EASY AS PIE
NETWORK SECURITY MONITORING ACROSS YOUR OT



RHEBO INDUSTRIAL PROTECTOR
YOUR LEAN AND DEDICATED OT INTRUSION DETECTION

Rhebo Industrial Protector provides enterprise-ready OT-dedicated security. It advances the existing perimeter firewall security by integrating network-based OT monitoring with anomaly detection. Any communication that indicates cyberattacks, tampering, espionage or technical error conditions is reported in real time. This allows early detection of multi-step attack patterns as outlined by the MITRE ATT&CK for ICS framework.

WHAT?

- real-time detection of cyber attacks and technical error states within the OT and SCS,
- full visibility of OT components for asset inventory,
- documentation of asset properties incl. protocols, connections and vulnerabilities,
- optional managed services.

HOW?

- continuous network-based monitoring of communication in, to and from the OT*,
- behavioral analysis of network traffic using deep packet inspection,
- immediate notification about any communication anomaly including pcap files for forensic analysis,
- passive, non-intrusive monitoring and detection.

WHY?

- tried-and-tested OT cybersecurity against sophisticated threat actors and zero-day exploits,
- OT security made simple even for small teams,
- easily scalable to multiple sites with one central point of control,
- comprehensive support from initial risk analysis to IDS operation.

* for complete list of supported protocols, see Rhebo Industrial Protector spec sheet

OT SECURITY MADE SIMPLE

✓

STRONG TRACK RECORD

of industrial security solutions for the energy and water sector.

✓

DEDICATED AND SIMPLE SOLUTION

for cost efficient implementation of OT, head-end system and grid edge cybersecurity.

✓

COMPREHENSIVE SUPPORT

for increasing industrial resilience fast and uncomplicated.

✓

SECURITY AGAINST PREVAILING VULNERABILITIES

through periodic OT cyber risk and maturity assessments.

✓

SECURITY AGAINST KNOWN AND NOVEL ATTACKS

through continuous OT monitoring, asset discovery and anomaly detection.

✓

SECURITY AGAINST INTRUSION SPILL-OVER

through end-2-end security monitoring with anomaly detection in energy distribution infrastructure.

✓

OT SECURITY MADE SIMPLE

through OT-focused analysis & intelligent event visualization.

✓

SECURING ACTIONABILITY

through expert support for risk analysis, operations and forensic analysis.

✓

SYSTEM SECURITY

through flexible and cost-efficient integration on IIoT devices and network components.

✓

SECURITY AGAINST UNPREDICTABLE TCO

through simple license schemes and easy, low-footprint installations.

✓

SECURING COMPLIANCE

through Next Generation IDS for OT based on national security laws and international security standards.

»With Rhebo, we can centrally and reliably secure our energy supply as well as the municipal utilities and over 16,000 decentralized energy producers we serve. The newly gained transparency and continuous monitoring visibly increases our network quality«.

Florian Wenzel | ICS manager
German multi-utility energy company TEN

ORDER YOUR CUSTOM OT NETWORK SECURITY ASSESSMENT OR BOOK A DEMO

EXPLORE THE LANDIS+GYR SECURITY SOLUTIONS

SECURITY@LANDISGYR.COM | +1 855 3455 454
WWW.LANDISGYR.COM/SOLUTION/CYBERSECURITY

ABOUT LANDIS+GYR

Landis+Gyr is the leading global provider of integrated energy management solutions for the utility sector. Offering one of the broadest portfolios, we deliver innovative and flexible solutions to help utilities solve their complex challenges in smart metering, grid edge intelligence and smart infrastructure. With sales of USD 1.8 billion, Landis+Gyr employs approximately 5,600 people in over 30 countries across five continents, with the sole mission of helping the world manage energy better.

www.landisgyr.com

ABOUT RHEBO

Rhebo provides simple and effective cybersecurity solutions for Operational Technology and distributed industrial assets for the energy sector, critical infrastructure and manufacturing. The company supports customers with OT security from the initial risk analysis to managed OT monitoring with intrusion & anomaly detection. As a trustworthy cybersecurity provider, Rhebo is ISO 27001 certified Since 2021, Rhebo is part of the Landis+Gyr AG.

www.rhebo.com

INFORMATION SECURITY MANAGEMENT SYSTEM
DNV
ISO/IEC 27001

Solution brief OT Protect 2025-02 v02

Pictures: tbc, AdobeStock