Rhebo AMI Security
Effective Cybersecurity For The Advanced Metering Infrastructure

REAL-TIME VISIBILITY OF THE AMI

through asset discovery and communications monitoring.

EARLY AMI INTRUSION DETECTION

through OT anomaly detection and HES integration for fast threat mitigation without changing the AMI architecture.

AMI SECURITY SERVICES

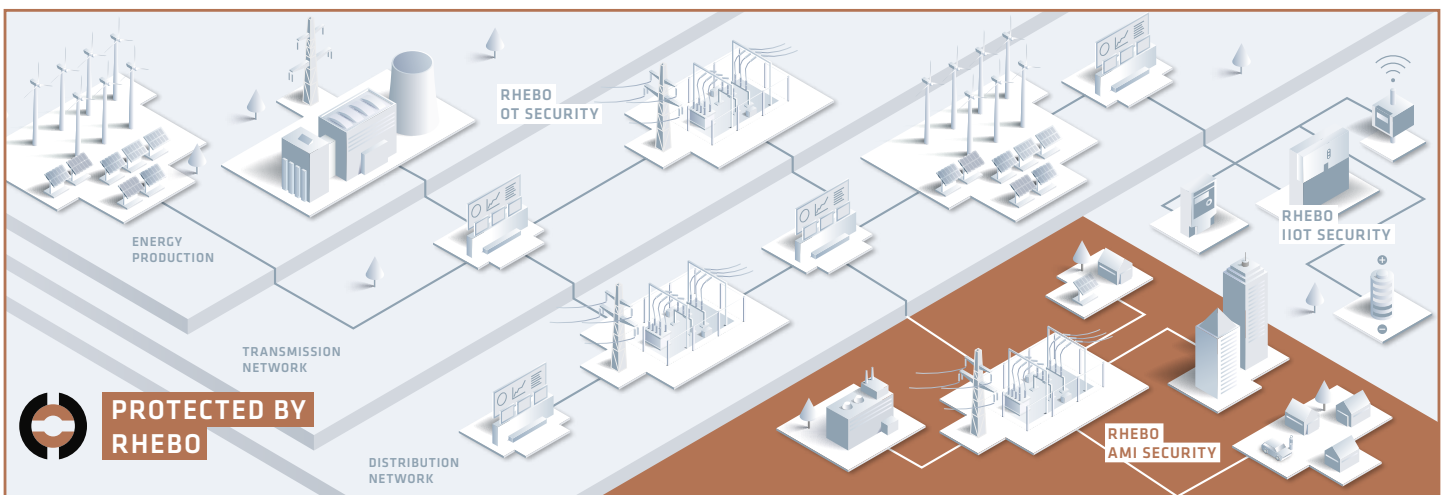from infrastructure risk analysis to continuous AMI monitoring and forensic analysis.

»Our goal is to provide our customers with a powerful and secure Advanced Metering Infrastructure. Rhebo AMI Security offers a simple and effective tool which we can add to our system's application through a highly cost-efficient subscription license«.

Juha Torstensson | Vice President for Software, Service & Solution | Landis+Gyr

Rhebo AMI Security integrates with Head End Systems (HES) and continuously monitors the network communications of the Advanced Metering Infrastructure (AMI) without requiring any change to the AMI architecture or devices. Any anomaly within the AMI is detected, assessed and reported in real time. Rhebo fully supports companies from the energy sector along the industrial security lifecycle from the initial risk analysis to managed AMI monitoring with intrusion and anomaly detection.

Rhebo AMI Security Dedicated & Simple

RHEBO OT SECURITY

ENERGY PRODUCTION

TRANSMISSION NETWORK

DISTRIBUTION NETWORK

RHEBO IIOT SECURITY

RHEBO AMI SECURITY

PROTECTED BY RHEBO

New Security Challenges
For Energy Providers

The smart meter rollout is an integral part of the energy transition and digitization. In Europe, the number of smart meters is expected to rise to **227 million by 2026.** In the USA alone, 103 million smart meters were already installed in 2020, 88 % of them in the residential sector. For attackers, this creates **hundreds of millions of potential access points into local and national power grids.** In particular, the fact that smart meters are installed in uncontrolled environments like people's homes and public spaces makes it difficult for energy companies to monitor and secure infrastructure perimeters against unauthorized access and disruption. This new risk exposure is fuelled by the fundamental architecture of AMI. Not only are millions of smart meters connected with each other as well as with downstream systems such as home energy management systems (HEMS) and data collectors. They also store sensitive information for smart grid communications. Both increase the **risk of threat propagation, lateral movement and spill-over effects** to the critical infrastructure's OT. Utilities have strategically invested in IT security over the years and now threats are pivoting to the next weakest link, the industrial infrastructure and devices, which **require an immediate hardening to increase resilience.**

»Sophisticated cyber attacks on advanced metering infrastructures are a clear and present danger. The most devastating scenario involves a computer worm that traverses advanced metering infrastructures and permanently disables millions of smart meters.«

Aaran Hanson et al. in »International Journal of Critical Infrastructure Protection«, 2017

Extending Cybersecurity
To The Edge

Rhebo's solutions and services have been securing energy companies' industrial control systems and operational technology from cyberattacks for nearly ten years – from the central control room to substations and renewable energy plants. With Rhebo AMI Security, Rhebo **extends the industrial cybersecurity shield of energy suppliers and utilities to the edge of their operations.** Rhebo AMI Security monitors all communication processes of smart meters, data collectors and HES for anomalies in the anticipated behavior without the need to modify the AMI.

Malicious activities such as lateral movements and scans, malware and data manipulation, but also technical error conditions, are **detected and reported in real time.** Rhebo provides the operation of the AMI monitoring and the integrated **intrusion & anomaly detection** as a managed protection service. Our experts track the anomaly alerts, assess their criticality and define mitigation measures. This **allows utilities to focus on their core business** without losing sight of the security of their AMI.

Rhebo 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,
Advanced Metering Infrastructure
and IIoT cybersecurity.

COMPREHENSIVE SUPPORT
for increasing industrial resilience
fast and uncomplicated.

**AMI SECURITY MADE
SIMPLE**
through OT-focused analysis &
intelligent event visualization
without the need to modify the AMI.

**SECURITY AGAINST KNOWN AND
NOVEL ATTACKS**
through monitoring, asset discovery
and threat detection as well as
event correlation of smart meters,
HES and network.

END-2-END SECURITY
through anomaly detection to prevent
threat propagation across OT, IIoT and
Advanced Metering Infrastructure.

»With Rhebo we can be sure that any anomaly in our operational technology networks will be
reported in real time enabling us to react immediately«.

Dirk Hollmach | Head of Net Operations | Mitnetz Strom

**SECURITY AGAINST
PREVAILING VULNERABILITIES**
through recurrent AMI
cyber risk analysis
and maturity assessments.

SECURING ACTIONABILITY
through Rhebo expert support
for risk analysis, operations and
forensic analysis.

SYSTEM SECURITY
through flexible and cost-efficient
integration of Rhebo solutions
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.

**SECURITY OF
TRUST MADE IN GERMANY**
compliant with European Cyber Security
Organisation (ECSO) and GDPR.

Simple & Effective
3 Steps To A Secure Advanced Metering Infrastructure

1

AMI RISK ANALYSIS AND MATURITY ASSESSMENT

The first easy step to AMI security

AMI security starts with visibility.

The Rhebo AMI risk analysis and maturity assessment provides a deep understanding of your AMI assets, network and communication structure, 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 AMI 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

CONTINUOUS AMI MONITORING AND THREAT DETECTION

The seamless transition to continuous AMI monitoring & threat detection

AMI security does not end at the network perimeters.

The Rhebo AMI monitoring with intrusion and anomaly detection provides AMI-dedicated security. It advances the existing perimeter firewall security by extending anomaly detection to communications between the smart meters / data concentrators and the head end system.

You profit from

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

3

MANAGED DETECTION AND RESPONSE

The recipe to peace of mind: We monitor so you don't have to

AMI security needs resources and know-how.

Rhebo supports you in operating the AMI security monitoring with anomaly detection, in particular in evaluating and responding to incidents, as well as continuously reviewing and improving mitigation mechanisms.

You profit from

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

Sample Controller & Sensor Deployment
In The Advanced Metering Infrastructure
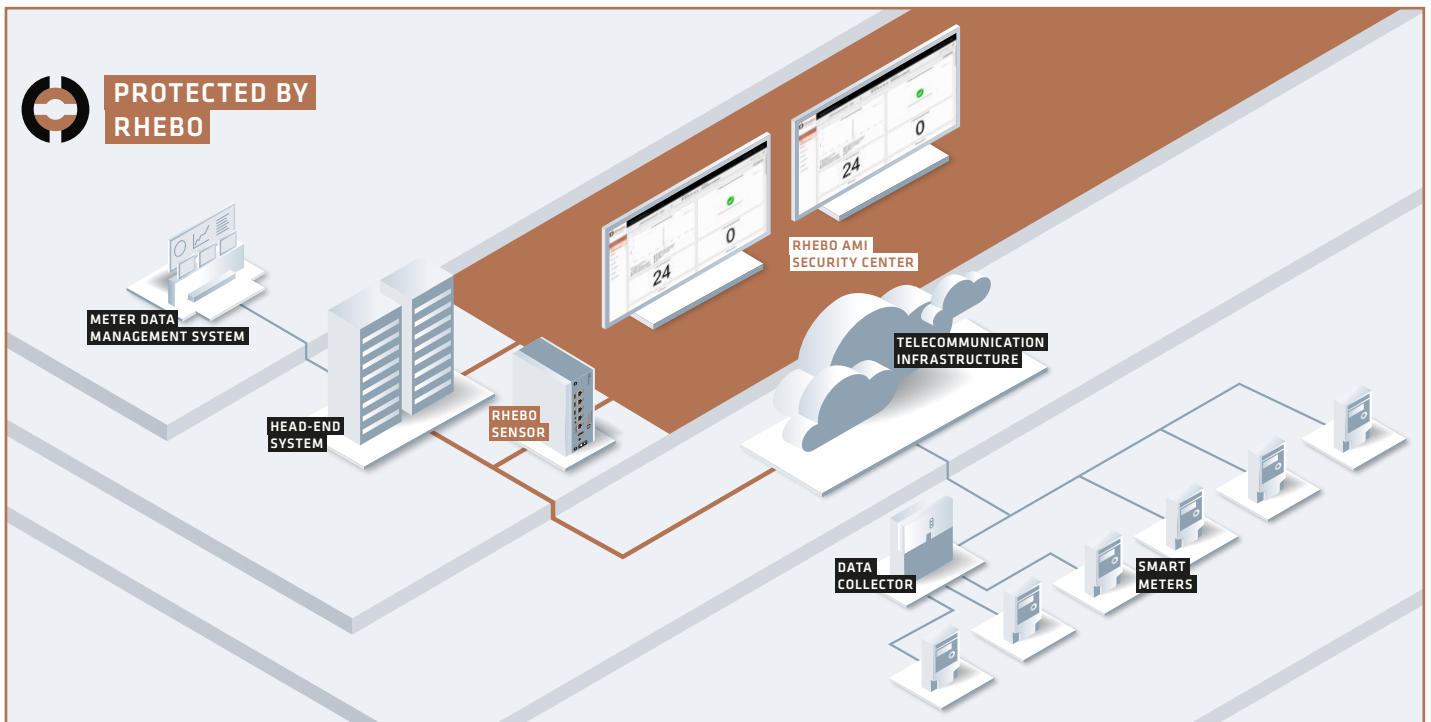
Literacy Means Knowledge
Protocols Detected & Analyzed With Rhebo AMI Security*

ABB Redundant Network
  Routing Protocol
Acronis Backup
Adobe Server
ARP
AXIS Camera-Management
BACnet
Boot Service Discovery
  Protocol
Canon BJNP
CIP
Cisco
Cisco CDP
Cisco CGMP
Cisco DCE
Cisco DTP
Cisco EIGRP
Cisco WLCCP
Codesys
COTP
DCE/RPC
DECnet
DHCP
DLMS / Cosem **
DNP3
DNS
EAP over LA
ECTP
EGP
ELCOM-90

ESET Remote
  Administrator
EtherCAT
FTP Control
FTP Data
General Electric
General Inter-ORB Protocol
GigE Vision Control Protocol
GigE Vision Streaming
  Protocol
Haag Damon
HART
HP
HP DTC
HP Extended LLC
HP PROBE
HSR
HSRP
HTTP/S
iba Device Configuration
  Protocol
ICMP
IEC60870-5-104
IEC61850-GOOSE
IEC61850-GSSE
IEC61850-MMS
IEC61850-SMV
IGMP
Intel Advanced-Network-
  Services

Internet Printing Protocol
Internet Small Computer
  Systems Interface
Inter-Switch Message
  Protocol
IPsec Authentication
  Header
IPsec Encapsulating
  Security Payload
IPv6
Java Remote Method
  Invocation
Kerberos
Landis+Gyr Outside Data
  Exchange Protocol
Line Printer Daemon
  Protocol (LPD)
Link Aggregation Control
  Protocol
Link Aggregation Marker
  Protocol
LDAP
LLC
LLDP
LLMNR
LonTalk
McAfee ePO
mDNS
Modbus
MQTT

MRP
Munin Data Exchange
  Protocol
MySQL Client-Server
  Protocol
Nagios
NetBIOS
NFS
NTP
Omicron OMFind
ONVIF Simple Object
  Access Protocol
OPC_UA
OpenProtocol
Operation, Administration,
  Maintenance
OSPF
PIM
Powerlink
Proficy iFix
Profinet
Profinet-IO CM
PSI
PTP
QNX Qnet
QUIC
Realtek Remote Control
  Protocol
Real Time Streaming
  Protocol

Remote Desktop Protocol
Remote Shell
Rhebo
RK 512
Routing Information
  Protocol
S7 / S7+
SentinelSRM
Sercos III
Siemens Spectrum
  Power TG
Siemens SICAM PAS/PQS
Simple Object Access
  Protocol
Sinec H1
SKINNY
Slow Protocol
SMA
SMB
SMTP
SNMP
SqlNet2
SQL Server Resolution
  Protocol
SSDP
SSH
SSL
STOMP
STP

Stream Control
  Transmission Protocol
Symantec Endpoint
  Protection Manager
Syslog
TCP Keep-Alive
TDS
Telnet
TFTP
Tivoli Storage Manager
TNS
Undo License Manager
Veritas Backup Exec Client
VMWare-Lab-Manager
VMware Server Console
VNC
VRRP
Web-Based Enterprise
  Management
Web Services Discovery
WinCC
X11
.NET TCP Binary Protocol

Highlighted protocols:
industry-specific protocols

* as of June 2022
** available in January 2023

Order your custom AMI network security assessment or book a demo

www.rhebo.com | sales@rhebo.com | +49 341 3937900

Explore More Rhebo Solutions

↗ Rhebo OT Security

↗ Rhebo IIoT Security

Secured By Rhebo

Stromnetz Hamburg

Leipziger Wasserwerke

Thüringer Energienetze

Landis+Gyr

BayWa r.e.

MITNETZ STROM

OT Security Made In Germany

TeleTrusT Pioneers in IT security.

CYBERSECURITY MADE IN EUROPE™
Initiated by ECSO. Issued by eurobits e.V.

Allianz für Cyber-Sicherheit

PLATTFORM INDUSTRIE 4.0

SecurITy
made in Germany
Trust Seal
www.teletrust.de/itsmig

Rhebo OT Security Made Simple

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. Since 2021, Rhebo is part of the Landis+Gyr AG, a leading global provider of integrated energy management solutions for the energy industry with around 5,000 employees in over 30 countries worldwide. Rhebo is a partner of the Alliance for Cyber Security of the Federal Office for Information Security (BSI) as well as the Teletrust – IT Security Association Germany. The company was awarded the »IT Security Made in Germany« and »Cybersecurity Made In Europe« labels for its strict data protection and data security policies. *www.rhebo.com*