Rhebo Industrial Protector in Industry 4.0

Rhebo Industrial Protector seamlessly protects industrial control systems against downtimes and cyber attacks in real-time.

PREVENT DOWNTIMES NOW

Rhebo Industrial Protector reports and prioritizes real-time anomalies in the ICS communication that can lead to disruptions and production downtimes and acts in accordance to key industry standards such as IEC 62443 and ISO 27001.

DETECT CYBER ATTACKS IN REAL-TIME

Rhebo Industrial Protector detects both known and unknown cyber threats and reports them immediately to plant operations.

INCREASE OEE AND PRODUCTIVITY

Rhebo Industrial Protector supports cross-system data integration for the effective implementation of your continuous improvement strategies.

Enable an Efficient and Secure ICS

Industrial Control Systems (ICS) are the nervous system of highly efficient manufacturing in Industry 4.0. They are also characterized by increasing complexity and links to networks outside the industrial environment (i.e. internet). The key to efficient and secure manufacturing is **effective management of the ICS** and the maintenance of high network quality. Only those who ensure digital transparency can **protect their production against technical malfunctions, network failures, and advanced cyber threats.** Rhebo Industrial Protector supports you in effectively controlling, optimizing and protecting complex ICS according to industry standards such as **IEC 62443 and ISO 27001.**

Rhebo Industrial Protector **monitors, analyzes and visualizes the complete data traffic** in your ICS to the deepest content level. Individual commands between the components of the industrial control systems details are available and checked for changes. Rhebo Industrial Protector **comprehensively detects and reports in real-time** anomalies that could change or disrupt existing processes. As part of any defense-in-depth strategy, you gain 100% digital transparency and ability to react immediately to potential malfunctions before the supply processes are affected. **This ensures productivity and continuity** for your industrial operations.

MEETING THE CHALLENGES OF INDUSTRIAL INTERNET OF THINGS (IIOT)

- Achieve transparency of complex network behavior
- Avoid downtimes
- Quickly troubleshoot errors and reduce MTTR
- Ensure system integrity
- Ensure data integration
- Detect advanced persistent threats and vulnerabilities

IDENTIFY THREATS EARLY & PREVENT PRODUCTION DOWNTIMES

•

INCREASE PLANT PRODUCTIVITY & LOWER MEAN TIME TO REPAIR (MTTR)

•

STANDARDS AND NORMS COMPLIANCE

Rhebo Industrial Protector Benefits

The productivity and continuity in Industry 4.0 and IIoT rises and falls with the uninterrupted operation of the ICS. Rhebo Industrial Protector registers, analyzes and visualizes all devices, assets and their communication relationships. You achieve digital transparency in your ICS thus achieving a complete network asset mapping along with a **risk analysis for your ICS** in accordance with **IEC 62443** and related standards.

CLARITY
•
AVAILABILITY
•
OVERALL EQUIPMENT EFFECTIVENESS

Technical failures and hidden cyber threats (e.g. via vulnerabilities) endanger plant availability and productivity. Rhebo Industrial Protector analyzes the complete communication in the ICS at content level and reports in real-time anomalies that may cause a malfunction. The protocol types commonly used in industrial automation such as Profinet, CIP and fieldbus are fully supported. This not only creates a **clear picture of your ICS communication** across all levels of the ICS architecture, but also **process stability and security.**

REAL-TIME
•
VISIBILITY
•
SECURITY

In order to identify disruptions quickly and systematically, a risk-based view of the respective anomalies are required. Rhebo Industrial Protector assigns risk scores to each anomaly notification. Notifications can additionally be sorted according to defined filters. This guarantees **fast actionability,** efficient troubleshooting, and supports you in implementing your ISMS in accordance with the ISO 27000 family and the basic requirements of IEC 62443.

EFFICIENCY
•
ACTIONABILITY
•
STABILITY

Modern production methods thrive on data. Rhebo Industrial Protector allows the **full integration of all anomaly reports into existing backend systems** – from the control station to the MES. Even the raw data of each anomaly is provided in PCAP format and can be analyzed in detail. This ensures that incident information not only optimizes your cyber security but also supports process control and preventive maintenance with critical data.

LEAN PROCESSES
•
SAVINGS
•
CLARIFICATION

Rhebo has the TeleTrusT seal »IT Security Made in Germany« and is committed to producing trustworthy industrial security with **no backdoors** as a German company based in Leipzig. Rhebo also complies with the strict requirements of German data protection laws.

DATA SECURITY
•
TRUST
•
CONTROL

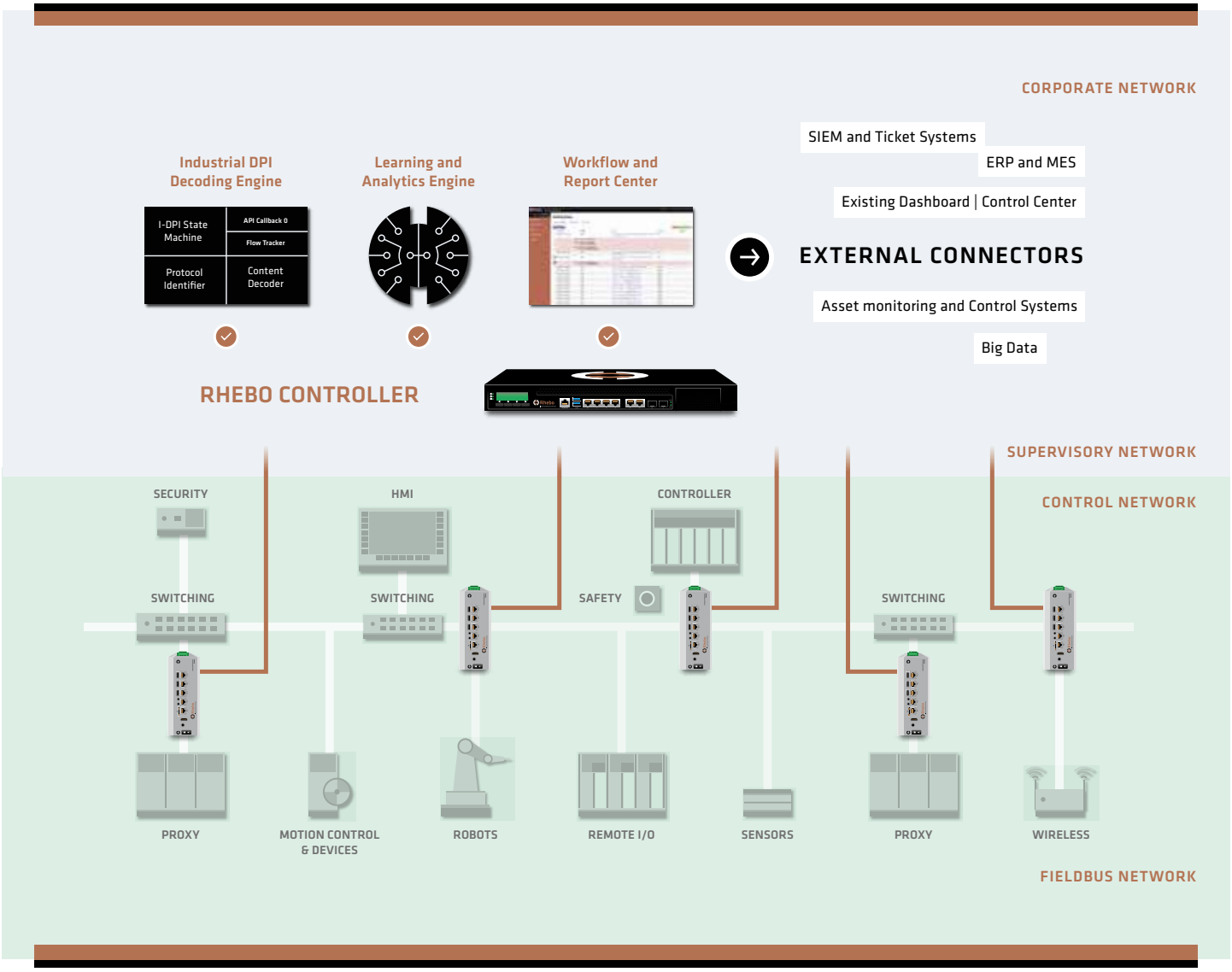
Technical Brief: Analyze, Learn, Report, Secure

Complete analysis of the ICS communication

Rhebo Industrial Protector monitors your ICS seamlessly, passively and non-intrusively. Network taps or mirror ports send each data packet exchanged in the process control system to Rhebo Industrial Protector. There, the data packets are decoded, analyzed and compared with the authorized communication patterns down to command level using deep packet inspection technology. For this purpose, the anomaly detection automatically learns the prevailing communication pattern of your ICS within a very short time without impairing the processes and defines this as plant-typical communication. During operation, Rhebo Industrial Protector registers any deviation from standard network behavior as an anomaly and notifies the system administrator in real-time.

This allows for the detection of any change in the network behavior that might have an effect in the security of supply, e.g.:

- two or more PLC / PAC communicate with a new protocol;
- a component changes the chain of command and sends new commands or requests;
- a network user (e.g. maintenance laptop) accesses a controller that he has never accessed before;
- malware on a computer or maintenance laptop scans the network control technology for open ports and possible targets;
- the data volume and packet sizes between certain PLC components change unexpectedly over time;
- data packets are delayed, sent in the wrong order, repeatedly or not at all;
- data packets are sent incorrectly (fragmented or with an incorrect checksum);
- a sensor suddenly delivers measured values outside a defined range.



Integration of Rhebo Industrial Protector in industrial conrol systems

Visualization and error diagnosis

The recorded communication data is visualized graphically and in tabular form. They provide a complete overview of all network nodes and the communication taking place between them. Deviations in the behavior of communication protocols such as Profinet, EtherCAT, EtherNet/IP, Modbus etc. are detected as anomalies and reported in real-time. The anomaly reports are assigned with a risk score that takes into account both the risk of the suspicious data packet and the relevance of the affected components for the availability and system integrity. The more disruptive the suspicious action and the more system-relevant the affected components are, the higher the risk score.

The Rhebo Industrial Protector user can display anomaly notifications by risk score or any of the filterable categories (e.g. protocol type, device) and prioritize according to countermeasures. Data from the system can be shared programmatically via standards-based APIs to external systems and raw forensic traffic data is stored in connection to each anomaly notification. Problems of the manufacturing systems and ICS can thus be identified and address systematically and efficiently.

Industrial Protector Controller

Industrial Protector Sensor

About Rhebo

Rhebo is a German technology company specializing in the reliability of industrial control systems and critical infrastructures by means of detailed monitoring of data communication within the industrial network. IT market analyst Gartner Inc. named Rhebo as the only German manufacturer of an industrial anomaly detection among the top 30 suppliers in the international »Market Guide for Operational Technology Security 2017«. The company is a member of Teletrust – IT Security Association Germany.