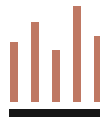


IEC 62443 in Practice

How Rhebo supports Industrial Control System monitoring and security



MONITOR
ICS COMMUNICATION



INCREASE
PRODUCTIVITY



REDUCE
CYBER RISK

This guide illustrates the technical requirements of the IEC 62443 industrial standard for security and stable operation of Industrial Control Systems. The guide explains how the industrial anomaly detection system Rhebo Industrial Protector enables companies with automated production to sustainably implement the requirements and ensure industrial network continuity.

Core Elements of IEC 62443

The international standard family IEC 62443 »Industrial communication networks – Network and system security« is a fundamental framework for industrial companies to protect their IT (office) and OT (production) against failures. The standard focuses on network security against attacks, advanced persistent threats, internal manipulation, and malware. However, the requirements of the standard are also employed to identify technical failures and misconfigurations that can affect productivity. The family comprises of four main chapters:

1. General Concept, Glossary, Metrics and Use Cases
2. Management requirements and processes
3. Technical and organisational requirements for the overall system
4. Technical and organisational requirements for components

In particular **the chapters 3 and 4** define different technical-organizational requirements for the system architecture, the component management and basic processes. The chapters differentiate between:

FR (Foundational Requirement) Basic requirement, which can be applied both at system level (Section 3.3) and component level (Section 4.2).

ZCR (Zones and Conduits Requirement) Requirements for separate network zones and communication channels within the ICS (Section 3.2)

DRAR (Detailed Risk Assessment Requirement) Requirements for a detailed risk assessment at system and component level (Section 3.2, ZCR 4).

This guide describes how Rhebo Industrial Protector helps industrial companies meet the requirements of Chapters 3 and 4 and avoid ICS disruption from cyber attacks, tampering, or technical faults.

NOTES

This document refers to the current standard documents ISA/IEC 62443-3-2 (Draft 06, 2015), IEC 62443-3-3: 2013-08 and IEC 62443-4-2 (Ed1, 2017) at the time of preparation.

For reasons of readability, the Foundational Requirements (FR) for the components according to Chapter 4.2 are not listed separately on the following pages. However, they are largely in concordance with the listed system level (SR) requirements according to Chapter 3.3 and can be applied to components accordingly.

Industrial Anomaly Detection in Industrial Control Systems

The Rhebo Industrial Protector industrial anomaly detection monitors and analyzes all communication **within** Industrial Control Systems (ICS) **in real-time**. The system functions as a non-intrusive, continuous network monitoring system and is an integral part of the concept for the fault-free operation of networked production facilities.

Rhebo Industrial Protector **decodes all communication at content level** and **reports any suspicious event within the networks as**

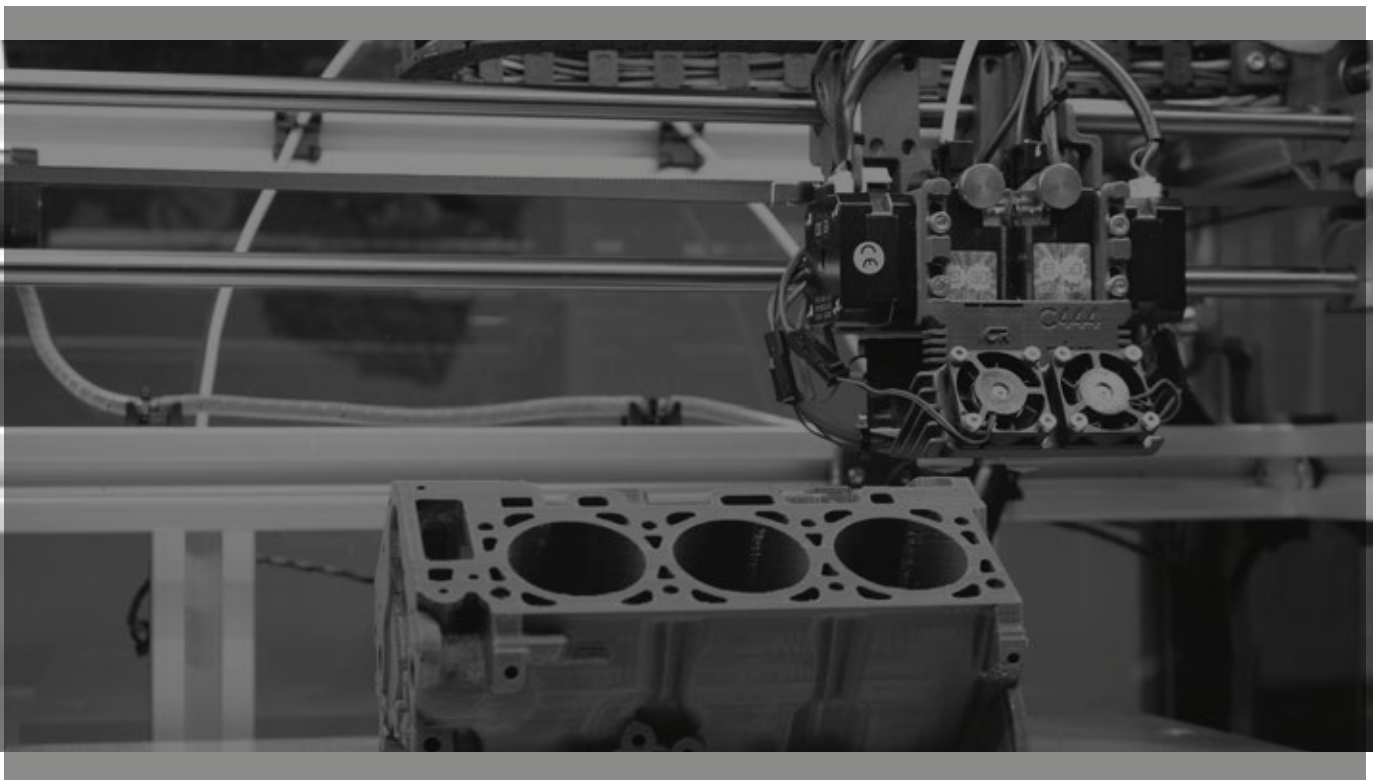
an anomaly in real-time. It reliably detects cybersecurity-relevant events as well as deviating operation sequences and technical error states, such as network and component errors. With various functions such as risk assessment, storage of forensic data, filters and interface integration, the anomaly detection actively supports the efficient analysis and elimination of anomalies. Operators can thus react actively to risk, eliminate errors more quickly and avoid unplanned downtimes.

Fundamental Requirements (FR) for System and Components in IEC 62443

FR 1	Identification and authentication control	4
FR 2	Use control	6
FR 3	System integrity	7
FR 4	Data confidentiality	11
FR 5	Restricted data flow	12
FR 6	Timely response to events	13
FR 7	Resource availability	14

Zones and Conduits Requirements (ZCR) and Detailed Risk Assessment Requirements (DRAR) in IEC 62443

ZCR 1	Identification of the System under Consideration (SuC)	16
ZCR 2	High-level cyber security risk assessment	17
ZCR 3	Partition of the SuC into zones and conduits	18
ZCR 4	Detailed cybersecurity risk assessment	19
ZCR 5	Documentation of cybersecurity requirements, assumptions and constraints	20



Fundamental Requirements (FR) for System and Components in IEC 62443

FR 1 – Identification and authentication control

SR 1.1 / 1.2 – Human user, software process and device identification and authentication
SR 1.6 – Wireless access management



Requirements according to IEC 62443

The system requirements (SR) 1.1 and 1.2 require the ability to clearly identify and confirm all users, software processes, and devices. Core principles such as segregation of duties and limitation of access

(Least Privilege, PoLP) should be observed accordingly. This requirement also applies to the management of wireless access mechanisms (SR 1.6).



How Rhebo Industrial Protector supports implementation

The foundation for planning and ensuring the requirements for »identification and authentication« is the transparency of the network asset structure and the details of the communication taking place within it. Both aspects provide relevant conclusions about the respective status of the individual endpoint device assets and applications in the ICS.

Rhebo Industrial Protector identifies and visualizes in real-time all network connections and their communication parameters for a complete digital asset inventory by network endpoint and connections. The operator can filter and evaluate the results as required by,

for example, network segment, device type, firmware version, protocol, data volume etc.

Furthermore, Rhebo Industrial Protector monitors all communication in the network and analyzes the type and content of that communication. All relevant protocols such as Profinet, S7, EtherCAT, Modbus, LLDP and PTP are supported along with hundreds of others. The passive sensors can be integrated at any number of points into the ICS and includes both wire and wireless communication segments.



SR 1.8 – Public key infrastructure (PKI) certificates



Requirements according to IEC 62443

When using a public key infrastructure (PKI), the control system shall be able to manage PKI according to accepted best practices or request public key certificates from existing PKIs.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector identifies encrypted communication and the encryption method used including encryption type and ciphers. The software learns the patterns of allowed encrypted communi-

cation and alerts the operators when these patterns or the type of encryption change.

SR 1.13 – Access via untrusted networks



Requirements according to IEC 62443

The control system is designed to monitor and control all access methods to the ICS which use unsecured networks.



How Rhebo Industrial Protector supports implementation

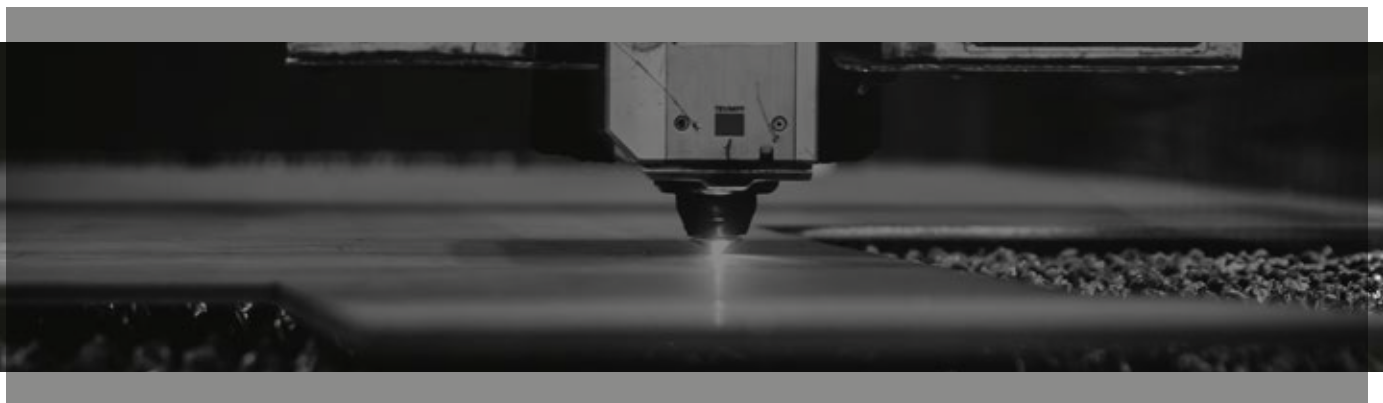
Rhebo Industrial Protector monitors both internal and remote access (via gateway or otherwise) to the ICS. Unauthorized access is reported in real-time as an anomaly and stored to the ICS including all traffic details and packets for later forensic analysis.

Anomalies include among others:

- unknown devices,
- new connections,
- communication across different zones and conduits,
- changed function of the communication.

With the additional real-time network map, operators can check the current status of logical and physical connections at any time.

Rhebo Industrial Protector registers every successful or failed login operation. Logins that use non-encrypted protocols such as HTTP, FTP, SMB or Telnet are reported. In addition, regular time synchronization is identified (PTP, NTP, SNTP, etc.), which provides operators with an overview of the status and performance of the logging functions.



FR 2 – Use control

SR 2.8 – Auditable events



Requirements according to IEC 62443

The control system shall provide audit records relevant to security. These shall take into account the following security categories: access control, request errors, operating system and control system

events, backup and recovery, configuration changes, potential attack activity (e.g. port scans), and audit logs.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector reports any events in the ICS that indicate covert attacks, malware, espionage, exploits of vulnerabilities or Internet access, technical failures and network changes and does this in real-time.

Each anomaly is stored with timestamp and transaction details (metadata and copy of actual communication packets). The anomaly notifications can be filtered according to user preferences. Operators can immediately analyze the incident and plan actions.

SR 2.11 – Timestamps



Requirements according to IEC 62443

The control system shall generate and provide timestamps for the creation of audit reports.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector stores all anomaly notifications with industry standard time-synchronized timestamps. By integrating the

anomaly detection with a trusted service provider, the validity of anomaly notifications for compensation claims can be secured.

FR 3 – System integrity

SR 3.1 – Communication integrity



Requirements according to IEC 62443

The control system is designed to ensure the integrity of the information transmitted.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector analyzes the layers 2-7 of the transmitted communication and reports any deviation indicating damaged data integrity. These include, but are not limited to, TCP checksum

errors and transmission errors indicating fragmented data or other data errors.

SR 3.2 – Malicious code protection



Requirements according to IEC 62443

The control system shall use mechanisms to detect, report, prevent and contain the execution of malware or unauthorized software. As a Requirement Enhancement (RE), the control system should be

able to execute the security measures at all access and exit points (SR 3.2 RE1) and manage the mechanisms (SR 3.2 RE2).



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector continuously analyzes all endpoints device assets and their communication within the ICS. Communication deviating from known and confirmed communication patterns is reported in real-time as an anomaly. As a result, attacks are reliably detected at the earliest stage. Examples of this includes:

- a new network node;
- communication of endpoint device assets via a new protocol or insecure connections;
- bypassing security mechanisms with a physical or virtual component;
- change of the command hierarchy or dispatch of previously unused communication by a component;
- access by a network user (e.g. maintenance laptop) to a previously unused controller;
- scan of the network for addresses and ports.

Rhebo Industrial Protector also identifies hardware, firmware, and software vulnerabilities that are listed in the CVE database for each process and device.

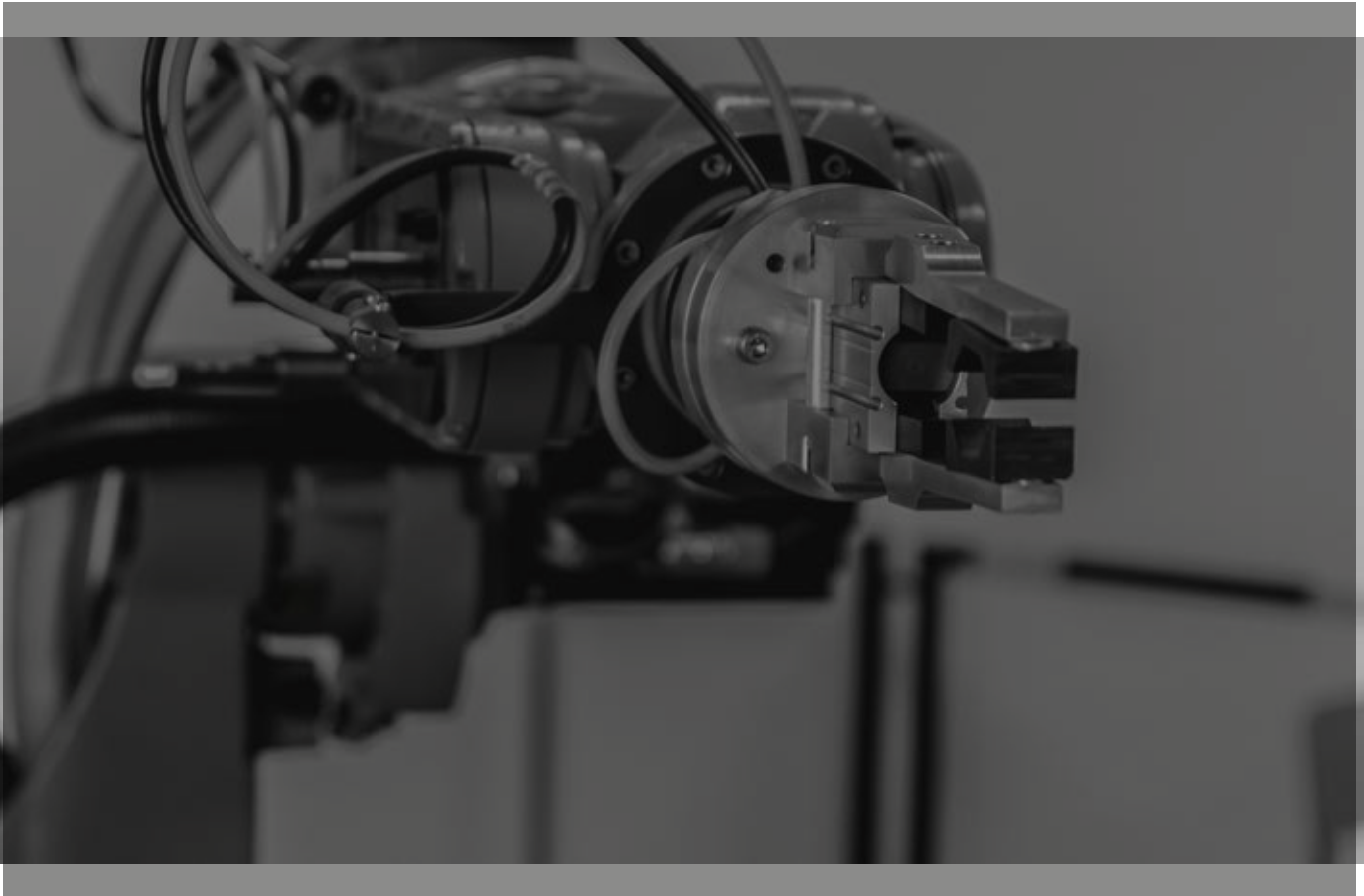
Recurring anomalies are displayed in the context of previous events (called »recurrences«) and can be correlated to investigate their causes.

Each anomaly notification is evaluated according to risk and takes into account both the communication and the devices involved. The basic data for the risk assessment can be configured by operators according to their specific requirements and infrastructure.

All anomaly notifications, including all process details, are stored as PCAP for immediate forensic analysis.

Rhebo Industrial Protector allows for the manual or rule-based forwarding of anomaly notifications to active security systems (firewall, SIEM, IDS) or the control room which allows for the centralized

orchestration of countermeasures as well as consolidation of security mechanisms.



SR 3.3 – Security functionality verification



Requirements according to IEC 62443

The control system shall have the ability to verify the planned behavior of devices and components, especially in the context of FAT

(Factory Acceptance Testing), SAT (Site Acceptance Testing) and planned maintenance, and to detect anomalies.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector analyzes the network behavior of each network participant in real-time. In addition, any unexpected external access into the ICS such as during maintenance intervals (especially remote maintenance) is detected and flagged as an anomaly. New or modified communication processes that deviate from the

learned and approved pattern are immediately reported as an anomaly – even when performed by an already authorized device or system. With these abilities, Rhebo Industrial Protector supports the verification of the planned behaviour of new or modified devices within the scope of FAT, SAT and planned maintenance measures.

SR 3.4 – Software and information integrity



Requirements according to IEC 62443

The control system shall detect and record unauthorized changes to software and information. The basic objective is to protect software and information from manipulation and misuse.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector reports any attempts to manipulate information and software when such attempts are made via the ICS network or affect a device's communication pattern. Access and write attempts by malware or remote control servers are thus reliably detected, rated with a correspondingly high risk factor and reported to the operators in real-time.

SR 3.5 – Input validation



Requirements according to IEC 62443

The control system is designed to validate the form and content of any input that may affect the control system.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector specializes in industrial communication protocols and uses deep packet inspection technology to validate the legitimacy and accuracy of the communication transmitted in the ICS. 6 categories of questions are analyzed:

1. Who is communicating (and are the devices authorized to do so)?
2. Which protocols are used (and is the communication relationship normal)?
3. What is being communicated (and is the communication legitimate)?

4. Is the communication packet correct and error-free (and if not which error occurred)?
5. Does the communication process fit into the typical communication pattern (and if not, what is anomalous)?
6. What content is being transmitted (and are those values normal / correct)?

Deviations from the standard pattern are reported as an anomaly in real-time.

SR 3.6 – Deterministic output



Requirements according to IEC 62443

The control system shall provide the ability to set the output to a predetermined value if normal operation cannot be maintained due to an attack.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector is completely passively deployed in the ICS and does not disrupt or otherwise affect operation production devices in any way. This deployment has the unique advantage

of preventing manipulation of the monitored data as well as the Rhebo Industrial Protector control system, even if the ICS itself is attacked or disrupted.

SR 3.7 – Error handling



Requirements according to IEC 62443

The control system shall detect and handle error conditions in such a way that an effective and timely troubleshooting can be carried out.

The information must be treated as confidential as possible in order to avoid the exploitation by attackers.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector reports error states in real-time that indicate system or network errors or quality degradation. These include various quality and continuity anomalies such as:

- protocol errors
- missing or delayed cyclic messages
- communication interruptions
- degrading round-trip times
- TCP window sizes falling
- missing TCP handshakes
- low TTL of packets indicating routing problems
- out of order packets etc.

Recurring anomalies are displayed in the same context of previous notifications («recurrences») and can be easily correlated with their source anomaly data for forensic investigations.

Each anomaly report is evaluated according to risk and takes into account both the communication and the endpoint devices involved. The basic data for the risk assessment can be configured by operators according to their specific requirements and infrastructure.

The error condition anomalies are listed separately from security-relevant anomalies on the graphical user interface. This enables fast prioritization. All anomaly notifications and their corresponding event details are stored as PCAP for immediate forensic analysis. Information can be transmitted to other systems in encrypted form.

Rhebo Industrial Protector thus offers operators the knowledge base and the time advantage to react to error conditions before they have serious consequences.

FR 4 – Data confidentiality

SR 4.1 – Information confidentiality

SR 4.3 – Use of cryptography



Requirements according to IEC 62443

The control system shall protect the confidentiality of information at rest and during transport. When using cryptographic methods, in-

ternationally recognized and proven security practices shall be used.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector supports ICS operators in verifying their encryption mechanisms and communication security. Protocols used, encrypted communication, encryption methods are all identified and analyzed. The system learns the patterns of permitted encrypted communication and alerts operators when the patterns or encryption types change. Rhebo Industrial Protector also reports any communication that:

- uses outdated encryption methods,
- uses insecure protocols (such as SMB, NetBIOS, HTTP),
- uses encryption certificates from untrusted providers.

Depending on the trustworthiness of the certificate provider and the devices involved, the anomaly notifications receive an equivalent risk assessment.



FR 5 – Restricted data flow

SR 5.1 – Network segmentation

SR 5.2 – Zone boundary protection

SR 5.3 – General purpose person-to-person communication restrictions



Requirements according to IEC 62443

The control system shall provide the capability to logically separate control system networks and non-control system networks and critical control system networks from other control system networks (SR 5.1). The boundaries of segments and zones shall be monitored and

protected (SR 5.2). In particular, general messages from users or systems outside the control system (email, social media, etc.) that allow the transmission of executable files (SR 5.3) shall be prevented.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector analyzes communication entering or leaving the ICS. The sensors can be integrated at any number of points passively within the ICS and includes wireless routing points. Any communication that deviates from the defined or desired network segmentation rules is reported in real-time as a security-rele-

vant anomaly. Anomalies in this context can include new protocols, protocols untypical for ICS, new connections, new network endpoint participants, as well as function changes, and suspicious processes such as port scans or execution instructions.



FR 6 – Timely response to events

SR 6.1 – Audit log accessibility



Requirements according to IEC 62443

The control system shall provide authorized persons and/or tools with read-only access to audit logs. This access should be provided

as automatical as possible via programming interfaces (API) (SR 6.1 RE 1).



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector stores all details of an anomaly including metadata describing the anomaly notification and the raw packet data as a PCAP. These can be inspected by the operator at any time and are intuitively displayed and filterable. Standard interfaces (e.g. REST-API, Syslog CEF or SNMP) allow (manual or automated) forwarding

of anomaly notifications to other backend systems such as firewalls, SIEM, MES or the control room. Through the integration of an trust service provider, the anomaly notifications can also be assigned with certified timestamps to prevent subsequent manipulation.

SR 6.2 – Continuous monitoring



Requirements according to IEC 62443

The control system shall be able to continuously monitor the performance of all security mechanisms. By means of generally accepted

practices and recommendations of the security industry, security breaches shall be detected, evaluated and reported in a timely manner.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector continuously and seamlessly monitors all communication in the ICS network. Violations of other security mechanisms (e.g. firewall, virus scanner, IDS, SIEMs) are also identified

and reported as network behavior anomalies but optionally with higher risk profile score. Recurring anomalies are flagged separately.

FR 7 – Resource availability

SR 7.1 – Denial of service protection



Requirements according to IEC 62443

The control system shall remain functional even under deteriorated conditions during a DoS event. Communication loads shall be re-

duced (SR 7.1 RE 1) and the risk that ICS users (humans, software, devices) can trigger DoS events shall be limited (SR 7.1 RE 2).



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector detects communication that indicates a breach of security rules or could affect the optimal functionality of network components or operational continuity. This includes new communication processes and increases in network activity among

others. Rhebo Industrial Protector itself is not affected by external events. The passive, non-intrusive integration prevents its attack and manipulation in case of a successful penetration of the ICS.

SR 7.7 – Least functionality



Requirements according to IEC 62443

The control system shall restrict the use of unnecessary functions, ports, protocols and/or services.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector supports operators in managing the ICS with a complete visualization of all endpoint device assets, ports, connections and their network behavior in terms of functions, protocols and content. Any change in network behavior as well as any

new connection and component are reported as an anomaly in real-time. This allows operators to continuously check whether unnecessary or harmful functions, ports, protocols and services exist in the ICS – and remove them.

SR 7.8 - Control system component inventory



Requirements according to IEC 62443

The control system shall provide an up-to-date list of installed endpoint device assets. In addition, the specific properties of each component shall be fully documented.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector automatically creates and updates a complete list of all endpoint device and services in the ICS for a continuous and complete digital asset inventory. Using the interactive network map, vendor list, and connection views, all details of the physical and logical components can be displayed and filtered, including:

- IP and MAC address
- vendor
- connections and data flows between endpoint devices
- communication volume with other endpoint devices
- protocols and functions with values exchanged and used over time
- operating system and firmware version
- known CVE vulnerabilities according to the endpoint device including firmware version.



Zones and Conduits Requirements (ZCR) and Detailed Risk Assessment Requirements (DRAR)

ZCR 1 – Identification of the System under Consideration (SuC)



Requirements according to IEC 62443

The organization shall clearly define the system under consideration (SuC). Any boundaries to other systems and their access points shall be identified and documented.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector automatically generates a complete list of all endpoint device assets in the system under consideration (see SR 7.8). Operators can thus continuously create an automated digital asset inventory in order to:

- define the SuC in the planning phase (e.g. for network segmentation)
- optimize the SuC in terms of security rules and production effectiveness
- review the SuC at any time to ensure compliance with the permitted communication procedures.



ZCR 2 – High-level cybersecurity risk assessment



Requirements according to IEC 62443

The organization shall perform a high-level cybersecurity risk assessment of the SuC (according to ISA99.02.01: 2009 paragraph

4.2.3.1-4) to identify the unforeseen risk that the SuC poses to the organization.



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector provides the information necessary for a risk assessment (see SR 7.8). This information can be collected both initially as part of a Rhebo Industry 4.0 Stability and Security Audit (RISSA) or continuously with long-term integration of Rhebo Industrial Protector.

Long-term installation ensures continuous risk assessment and complete reporting of anomalies.

The RISSA delivers:

- an initial recording and documentation of the infrastructure
- analysis and evaluation of the status of the ICS
- identification and evaluation of possible existing security gaps and error conditions
- recommendations for improvement.



ZCR 3 – Partition of the SuC into zones and conduits



Requirements according to IEC 62443

The grouping of zones and conduits including the affected endpoint device assets of the ICS shall consider different aspects:

- results of the general cybersecurity risk assessment according to ZCR 2 (3.1)
- logical and physical separation from the enterprise network (3.2)
- relevance for occupational safety (3.3)
- temporary integration into the ICS (3.4)
- wireless communication (3.5)
- connection to networks outside the SuC (3.6).

The components shall be assigned to individual zones and conduits and the distribution shall be visualized (3.7).

For each zone and each conduit the properties shall be documented in detail. This includes full information on components and their function, boundaries, access points, communication flows, connections, security level objective, applicable security rules and assumptions and dependencies (3.8).



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector supports ICS operators in setting up groups, zones and conduits with a complete list of all endpoint device assets in the system under consideration.

Rhebo Industrial Protector can be integrated into any number of SuCs and at any number of points within them using non-intrusive, passive network taps or mirror ports. This allows operators to ensure a complete and consistent interior view and monitoring of their seg-

ments (groups, zones, conduits) and to continuously monitor them.

Rhebo Industrial Protector creates and updates a complete list of all ICS components in real-time for documentation purposes (3.7 / 3.8). Using the interactive network map, connection overview and vendor list, all details of the respective endpoint device assets can be accessed and filtered (see SR 7.8).



ZCR 4 – Detailed cybersecurity risk assessment



Requirements according to IEC 62443

On the basis of ZCR 3, a detailed risk assessment shall be carried out for each zone & each conduit. This follows 12 requirements (DRAR):

- DRAR 1: Identify threats
- DRAR 2: Identify vulnerabilities
- DRAR 3: Determine consequences and impact
- DRAR 4: Determine unmitigated likelihood
- DRAR 5: Calculate unmitigated cybersecurity risk
- DRAR 6: Determine security level target
- DRAR 7: Identify and evaluate existing countermeasures
- DRAR 8: Re-evaluate likelihood and impact
- DRAR 9: Calculate residual risk
- DRAR 10: Evaluate, if residual risk is at or below tolerable risk
- DRAR 11: Define and apply additional cybersecurity countermeasures
- DRAR 12: Document and communicate results



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector provides detailed insight into the properties, functionality, and network behavior of each individual endpoint device assets that affects the monitored ICS with its communication.

This allows operators to analyze individual zones and conduits with respect to their specific Detailed Risk Assessment Requirement (DRAR). In addition, vulnerabilities from the CVE database are taken into account. In the network map each endpoint device asset can be examined individually and in relation to the connected endpoint device assets in a SuC.

Operators thus gain a transparent picture of all activities within a zone or a conduit to answer to the respective DRAR.

Within the scope of an initial evaluation, the Rhebo Industry 4.0 Stability and Security Audit (RISSA) supports operators to conduct an initial analysis to get a complete picture of the structure, network nodes and the inherent processes (see ZCR 2) for the first time.

ZCR 5 – Documentation of cybersecurity requirements, assumptions and constraints



Requirements according to IEC 62443

The documentation shall provide a clear understanding of the networks, information technology, protocols and ICS systems that may be associated with the SuC (5.3). The Cyber Security Requirement

Specification (CSRS) shall include a description of the threat environment and vectors. This should include both sources of knowledge about threats and possible future threats (5.4).



How Rhebo Industrial Protector supports implementation

Rhebo Industrial Protector creates and updates a complete daily list of all endpoint device assets that communicate with the SuC endpoint device assets both inside and from outside the SuC. This allows the digital asset inventory to be extended in real-time to the physical and logical environment in which the SuC is embedded. Using

the interactive network map, vendor list and connection overview, all details of the respective endpoint device assets can be accessed and filtered (see SR 7.8). Rhebo Industrial Protector is therefore also an integral source providing knowledge about anomalies and vulnerabilities as part of a defense-in-depth strategy.



Solutions for Productivity and Cybersecurity in IIoT

Rhebo Industry 4.0 Stability and Security Audit

INSTALLATION OF RHEBO INDUSTRIAL PROTECTOR



IMMEDIATE TRANSPARENCY



MONITORING



DATA ANALYSIS



WORKSHOP



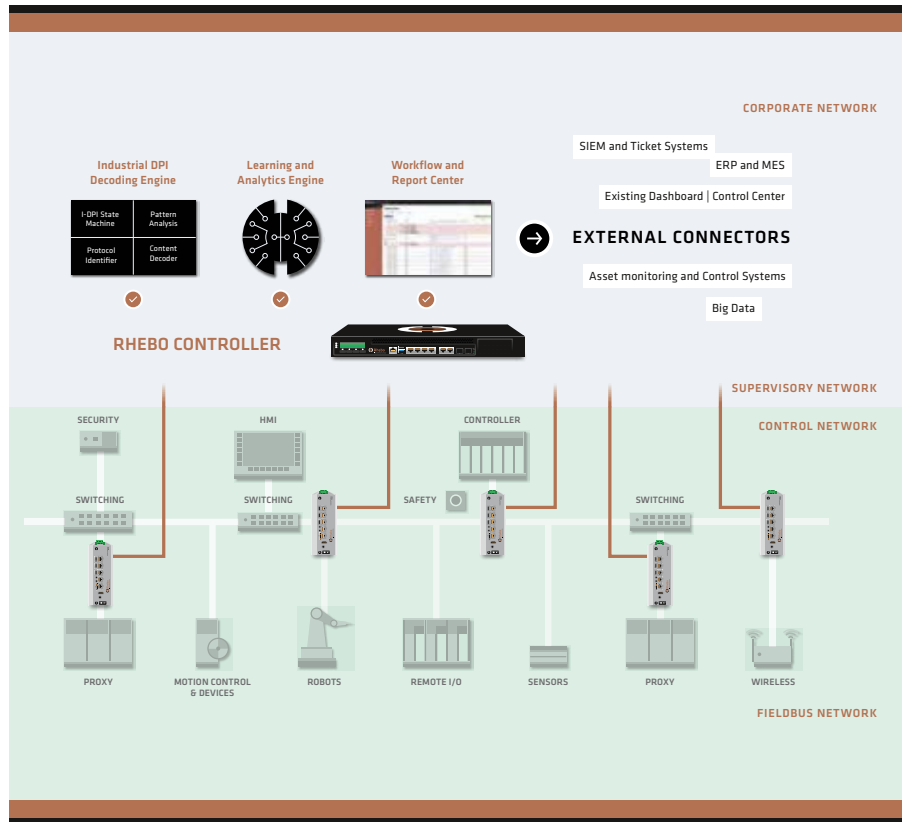
REPORT



CONTINUOUS IMPROVEMENT

2 WEEKS

Rhebo Industrial Protector



Integration of Rhebo Industrial Protector in an Industrial Control System.

Benefits

- REDUCE CYBERSECURITY AND PRODUCTIVITY RISK** through complete transparency of the Industrial Control System as well as real-time anomaly detection
- PREVENT DOWNTIME COSTS** through early mitigation of errors before the infrastructure is affected
- SUPPORT CONTINUOUS IMPROVEMENT PROCESS** through detailed logging of all ICS events including forensic data
- PROTECT YOUR DATA** through technology »Made in Germany«
- ESTABLISH CENTRAL MONITORING OF ICS** through standardized interfaces to SCADA, control room, MES, SIEM and other relevant systems

How secure is your Industrial Control System?

Put your network through
its paces.

Contact us

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

Gartner Security

Trust Seal
made
in
Germany
www.teletrust.de/itsec

About Rhebo

Rhebo develops and markets innovative industrial monitoring solutions and services for energy suppliers, industrial companies and critical infrastructures. The company enables its customers to guarantee both cybersecurity and the availability of their OT and IoT infrastructures and thus master the complex challenges of securing industrial networks and smart infrastructures. Since 2021 Rhebo has been a 100% subsidiary of

Landis+Gyr AG, a leading global provider of integrated energy management solutions for the energy industry with around 5,500 employees worldwide. Rhebo is a partner of the Alliance for Cyber Security of the Federal Office for Information Security and is actively involved in Teletrust – IT Security Association Germany and Bitkom Working Group on Security Management for the development of security standards.

www.rhebo.com