

Rhebo Industrial Protector in Industrie 4.0




Rhebo Industrial Protector sichert Ihre Steuerungsnetze gegen betriebliche Störungen und Cyberangriffe – lückenlos und in Echtzeit.

BETRIEBSAUSFÄLLE SOFORT VERHINDERN



Rhebo Industrial Protector meldet und priorisiert in Echtzeit jede Anomalie in der ICS-Kommunikation, die zu Störungen oder Ausfällen der Fertigung führen kann entsprechend der Industriestandards wie IEC 62443, ISO 27001 und VDI/VDE 2182.

CYBERANGRIFFE IN ECHTZEIT ERKENNEN



Rhebo Industrial Protector erkennt Cyberangriffe – bekannt oder unbekannt – und meldet sie umgehend an den Anlagenbetreiber.

GAE UND SYSTEMEFFIZIENZ STEIGERN



Rhebo Industrial Protector unterstützt die systemübergreifende Datenintegration für die effektive Umsetzung Ihrer Big-Data-Strategie.

Industrial Control Systems stabil und effizient steuern

Industrial Control Systems (ICS, deutsch Steuerungsnetze) sind in der Industrie 4.0 und dem Industriellen Internet der Dinge (IIoT) die Nervensysteme einer hocheffizienten Fertigung. Sie sind jedoch auch durch eine zunehmende Komplexität und Verknüpfung mit fertigungsfremden Netzen gekennzeichnet. Der Schlüssel zu einer stabilen und sicheren Fertigung liegt deshalb in einem **effektiven Management** des ICS zur Aufrechterhaltung einer hohen Netzwerkqualität. Nur wer digitale Transparenz sicherstellt, kann seine Fertigung gegen technischer Fehlerzustände, Netzwerkstörungen und moderne Cyberbedrohungen **absichern**. Rhebo Industrial Protector unterstützt Sie dabei, selbst komplexe ICS effektiv zu steuern, zu optimieren und entsprechend der Industriestandards wie **IEC 62443, ISO 27001 und VDI/VDE 2182** abzusichern.

Rhebo Industrial Protector **überwacht, analysiert und visualisiert den kompletten Datenverkehr in Ihrem Steuerungsnetz** bis auf Inhaltsebene. Selbst einzelne Befehle zwischen den Komponenten und übermittelte Prozess- oder Anlagenwerte werden detailliert ausgelesen und auf verdächtige Veränderungen überprüft. So kann Rhebo Industrial Protector alle auftretenden Anomalien, die Ihre Prozesse verändern oder stören könnten, lückenlos erkennen und **in Echtzeit** melden. Sie erhalten als Teil Ihrer Defense-In-Depth-Strategie vollständige digitale Transparenz und können sofort auf potentielle Störungen reagieren, bevor die Fertigungsprozesse betroffen sind. **So stellen Sie Produktivität und Kontinuität sicher.**



HERAUSFORDERUNGEN DES INDUSTRIAL INTERNET OF THINGS (IIOT) BEGEGNEN

- Anlagenausfälle vermeiden
- Komplexität übersichtlich machen
- Fehlerzustände schnell beheben
- Systemintegrität sicherstellen
- Datenintegration gewährleisten
- Cyberangriffe und Exploits von Schwachstellen erkennen



GEFAHREN FRÜHZEITIG ERKENNEN & PRODUKTIONSAUSFÄLLE VERHINDERN

ANLAGENVERFÜGBARKEIT ERHÖHEN & SYSTEMEFFIZIENZ STEIGERN

NORMEN UND STANDARDS EINHALTEN

Rhebo Industrial Protector Vorteile



STEUERUNGSNETZE VISUALISIEREN

Die Produktivität und Kontinuität in Industrie 4.0 steht und fällt mit dem störungsfreien Betrieb der Steuerungsnetze. Rhebo Industrial Protector registriert, analysiert und visualisiert alle Netzwerkteilnehmer und deren Kommunikationsbeziehungen. Sie schaffen digitale Transparenz in Ihrem ICS. So können Sie entsprechend IEC 62443 und verwandten Normen wie VDI/VDE 2182 ein lückenloses Network Mapping und eine fundierte **Risikoanalyse für Ihr ICS** vornehmen.

KLARHEIT
•
VERFÜGBARKEIT
•
**GESAMTANLAGENEFF-
FEKTIVITÄT**



EFFIZIENT UND PROAKTIV AUF VORFÄLLE REAGIEREN

Technische Fehlerzustände und verdeckte Cyberbedrohungen (zum Beispiel über Schwachstellen) gefährden die Anlagenverfügbarkeit und Produktivität. Rhebo Industrial Protector analysiert die komplette Kommunikation im ICS auf Inhaltsebene und meldet in Echtzeit jeden Anomalie, die eine Störung verursachen kann. Die in der industriellen Automatisierung gängigen Protokolltypen wie Feldbus, Profinet und CIP werden vollständig unterstützt. Das schafft nicht nur ein **detailliertes Abbild Ihrer ICS-Kommunikation** über alle Ebenen der ICS-Architektur, sondern auch **Prozessstabilität und Sicherheit**.

ECHTZEIT
•
SICHTBARKEIT
•
**NETWORK CONDITION
MONITORING**



ANLAGEN- VERFÜGBARKEIT SICHERN

Um Störungen schnell und gezielt zu verhindern, bedarf es einer Risikoeinschätzung der jeweiligen Anomalie. Rhebo Industrial Protector weist jeder Anomalie-meldung einen Risk Score zu. Zusätzlich können Meldungen nach eigens definierten Filtern sortiert werden. Das garantiert eine schnelle Handlungsfähigkeit, die effiziente Beseitigung von Störungen und unterstützt Sie bei der Umsetzung ihres ISMS entsprechend der **ISO 27000-Familie** und der Grundanforderungen der **IEC 62443**.

EFFIZIENZ
•
HANDLUNGSFÄHIGKEIT
•
STABILITÄT



PRODUKTIVITÄT OPTIMIEREN

Moderne Fertigungen leben von Big Data. Rhebo Industrial Protector erlaubt die volle **Integration aller Anomalie-meldungen in bestehende Backendsysteme** – vom Leitstand bis zum MES. Die Rohdaten jeder Anomalie werden im PCAP-Format abgespeichert und können detailliert analysiert werden. So stellen Sie sicher, dass Informationen zu Vorfällen nicht nur Ihre Cybersicherheit optimieren, sondern auch die Prozesssteuerung und präventive Instandhaltung gezielt mit wichtigen Daten unterstützen.

SCHLANKE PROZESSE
•
EINSPARUNG
•
AUFKLÄRUNG



SICHER SEIN MIT MADE IN GERMANY

Rhebo ist Träger des TeleTrusT-Siegels »IT Security Made in Germany« und verpflichtet sich damit als deutsches Unternehmen mit Sitz in Leipzig zur Herstellung **vertrauenswürdiger IT-Sicherheit ohne Hintertüren**. Rhebo trägt zudem den Anforderungen des deutschen Datenschutzrechtes Rechnung.

DATENSICHERHEIT
•
VERTRAUEN
•
KONTROLLE

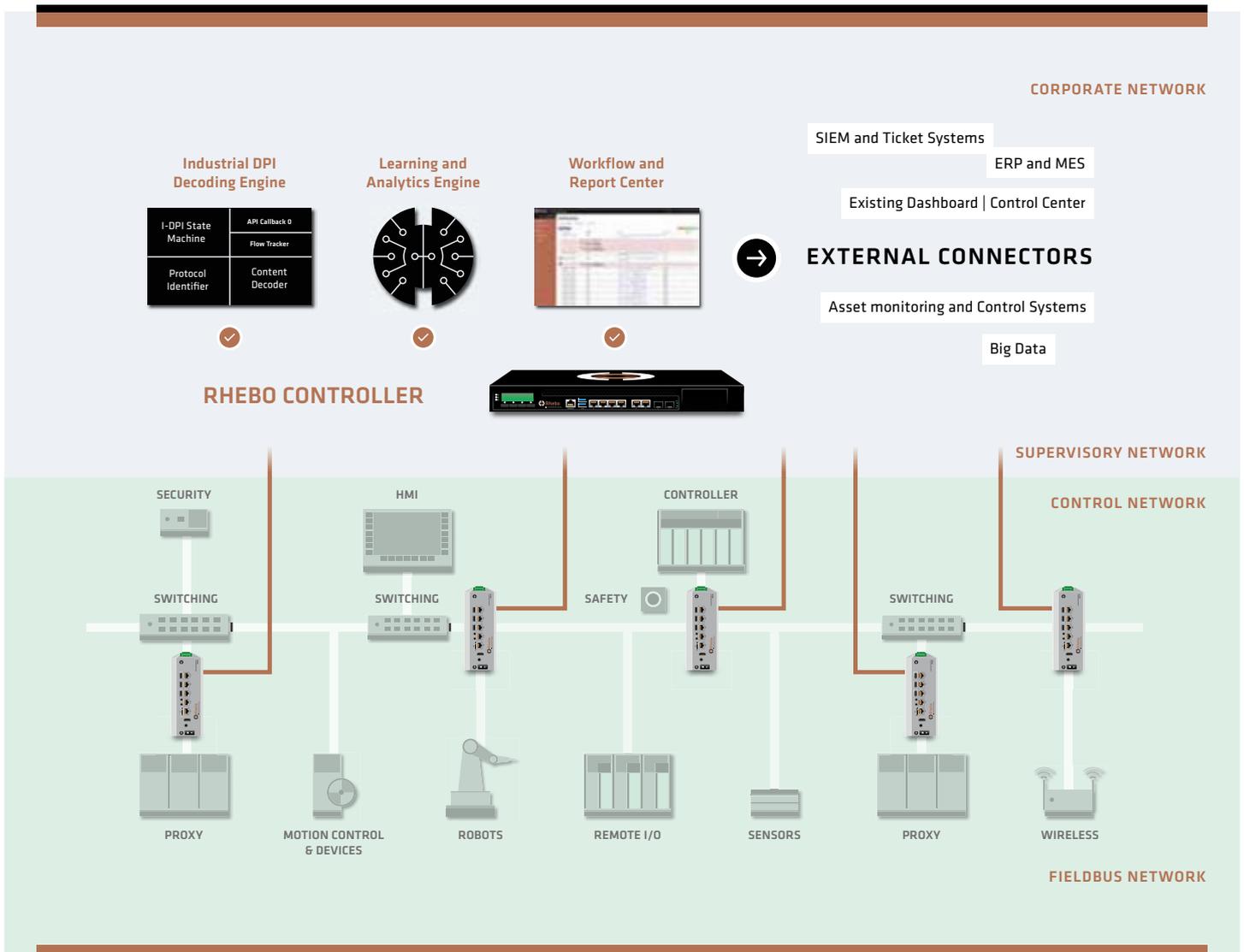
Technischer Exkurs: Analysieren, Lernen, Melden, Schützen

Vollständige Analyse der Steuernetzkommunikation

Rhebo Industrial Protector überwacht Ihr Industrial Control System (ICS) lückenlos, passiv und rückwirkungsfrei. Netzwerk-Taps oder Spiegelports senden jedes im Steuerungsnetz ausgetauschte Datenpaket an Rhebo Industrial Protector. Dort werden die Datenpakete mittels Deep-Packet-Inspection-Technologie bis auf Befehlsebene dekodiert, analysiert und mit den autorisierten Kommunikationsmustern abgeglichen. Dazu erlernt die Anomalieerkennung binnen kürzester Zeit und ohne Beeinträchtigung der Fertigung vollautomatisch die vorherrschende Kommunikationsstruktur Ihres ICS und definiert diese als anlagentypische Kommunikation. Im laufenden Betrieb registriert Rhebo Industrial Protector jede Abweichung von diesem Normverhalten als Anomalie und meldet diese in Echtzeit an den Anlagenbetreiber.

Damit werden alle die Fertigung beeinflussenden Veränderungen vollständig erkannt, zum Beispiel:

- zwei oder mehr Steuerkomponenten kommunizieren über ein neues Protokoll;
- eine Komponente ändert die Befehlshierarchie oder sendet bislang nicht verwendete Befehle;
- ein Netzwerkteilnehmer (z. B. Wartungslaptop) greift auf eine Steuerung zu, auf die er zuvor nie zugegriffen hat;
- eine Malware auf einem Computer oder Wartungslaptop scannt die Fernwirktechnik nach offenen Ports und möglichen Angriffszielen;
- das Datenaufkommen und die Paketgrößen zwischen bestimmten Steuerkomponenten ändern sich unerwartet über die Zeit;
- Datenpakete werden verzögert, in falscher Reihenfolge, wiederholt oder gar nicht gesendet;
- Datenpakete werden fehlerhaft (fragmentiert oder mit falscher Prüfsumme) gesendet;
- ein Sensor liefert plötzlich Messwerte außerhalb eines definierten Bereichs.



Integration von Rhebo Industrial Protector im industriellen Steuerungsnetz

Visualisierung & Fehlerdiagnose

Die aufgezeichneten Kommunikationsdaten werden grafisch und tabellarisch aufbereitet. Sie geben damit einen vollständigen Überblick aller Netzwerkteilnehmer und der zwischen ihnen stattfindenden Kommunikation. Abweichungen im Verhalten der Kommunikationsprotokolle wie Feldbus, CIP, Profibus, Profinet, CC-Link, Modbus u.a. werden als Anomalie erkannt und in Echtzeit gemeldet. Die Anomaliemeldungen werden mit einem Risk Score versehen. Dieser berücksichtigt sowohl das Risiko des verdächtigen Datenpakets als auch die Relevanz der betroffenen Komponenten für die Verfügbarkeit und Systemintegrität. Je verdächtiger die Kommunikation und je systemrelevanter die betroffenen Komponenten sind, desto höher fällt der Risk Score aus.

Der Anlagenbetreiber kann die Anomaliemeldungen nach Risk Score oder anderen Kategorien (z. B. Protokolltyp, Komponenten) ordnen und erhält eine umgehende Priorisierung der Maßnahmen. In Verbindung mit der Speicherung der Rohdaten eines Vorfalls und der vollen Integration der Daten in bestehende Backendsysteme können Probleme in der Fertigung sowie der Konfiguration der ICS-Architektur gezielt analysiert und behoben werden.



Industrial Protector Controller



Industrial Protector Sensor

Über Rhebo

Rhebo ist ein deutsches Technologieunternehmen, das sich auf Ausfallsicherheit industrieller Steuerungssysteme und Kritischer Infrastrukturen mittels Detailüberwachung der Datenkommunikation spezialisiert hat. Das Unternehmen wird im internationalen »Markt-

fürher für betriebstechnische Sicherheit 2017« des IT-Marktanalysten Gartner Inc. als einziger deutscher Hersteller einer industriellen Anomalieerkennung unter den Top-30-Anbietern genannt. Das Unternehmen ist Mitglied im Teletrust – Bundesverband IT-Sicherheit e. V.