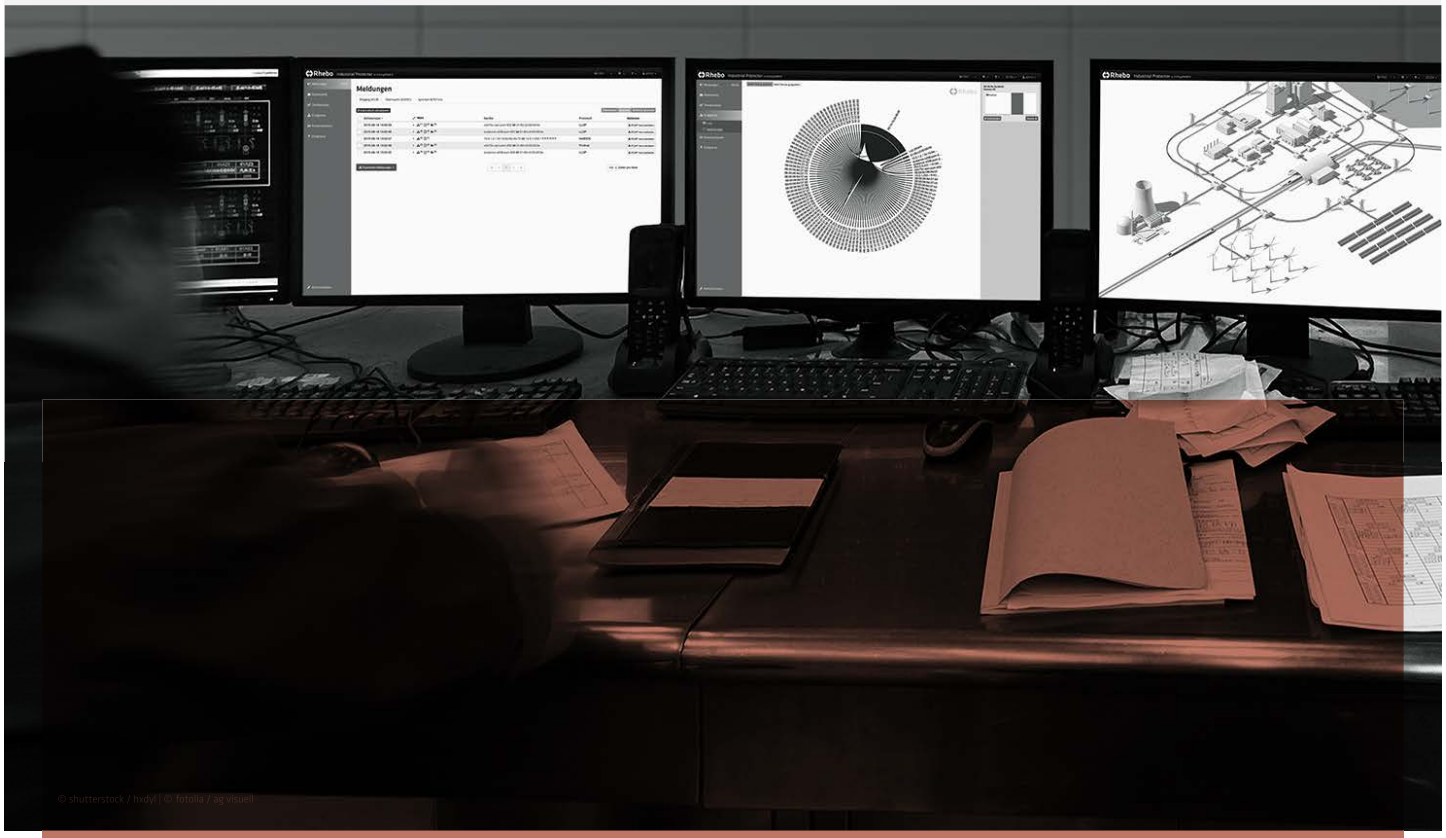
Anforderungen an industrielle Steuernetze in automatisierten Produktionen für 2017

Im Zuge fortschreitender Digitalisierung industrieller Steuernetze eröffnen sich produzierenden Unternehmen neue Chancen, aber auch Risiken. Beide sind Medaille ein und derselben Entwicklung, die prägend für die Industrie 4.0 ist: die Vernetzung von Steuernetzen untereinander und die Integration in die Office-IT.

Dieses Whitepaper analysiert die daraus entstehenden Herausforderungen für Unternehmen mit automatisierter Produktion und definiert die notwendigen Schritte zu einem integrierten kontinuierlichen Network Monitoring.



Neue Herausforderungen an die Cybersicherheit durch Integration in Office-IT

Der Übergang von serieller Kommunikation zu Ethernet und Co. in der Produktion bedeutet vor allem neue Herausforderungen an die Absicherung der Steuernetze. In der Vergangenheit ermöglichte die serielle (direkte) Anbindung der Produktionskomponenten eine verhältnismäßig hohe Sicherheit gegen äußere Eingriffe. Die Cybersicherheit nahm daher keinen besonders großen Raum in der Strategie der Produktionsplanung ein.

Aufgrund der Ablösung serieller Verbindungen durch Ethernet-basierende Technologien, sowie der Integration der Produktions-IT, in manchen Bereichen auch Operational Technology (OT) genannt, in die Office-IT, entstehen neue Anforderungen an die Cybersicherheit in der Produktion. Die einst isolierten Steuer- und Kontrollnetze sind nun potentiellen Gefahren aus dem Netz, über WLAN oder aus der Office-IT, ausgesetzt. Dies beeinflusst insbesondere Aspekte des Verfügbarkeitsmanagements sowie die IT-Sicherheitsstrategie in den Betrieben.

Gängige Sicherheitslösungen sind jedoch bislang auf die Office-IT optimiert. So können weder Firewalls, noch Intrusion-Detection- oder SIEM-Systeme die notwendige Transparenz in industriellen Steuernetzen liefern, die für die Ausrichtung der Maßnahmen im Bereich Cybersicherheit erforderlich ist.
Um bestehende Sicherheitsinfrastrukturen weiterhin nutzen zu können, sollten deshalb industrielle Monitoring- und Cybersicherheitslösungen in diese integriert werden. So könnten z. B. Ereignisdaten und Netzwerkinformationen an vorhandene SIEM-Systeme weitergegeben und in der Analyse berücksichtigt werden.

Produktivitätssteigerung durch höhere Anlagenverfügbarkeit und umfassende Qualitätssicherung

Neben dem Sicherheitsaspekt eröffnen sich für Unternehmen neue betriebswirtschaftliche Vorteile. Diese werden in Zukunft Treiber für den langfristigen Erfolg eines Unternehmens sein:

- Erhöhung der Produktivität durch schnelleren Eingriff in die Produktion und durch individuelle Fertigung ohne zusätzliche Kosten;
- Steigerung der Qualität und Anlagenverfügbarkeit durch Integration der Steuernetz-Daten in MES und ERP;
- Verbesserung der Six Sigma- und Kaizen-Methoden durch ganzheitliche Einblicke in die Produktionsprozesse und Anlagenkonfiguration;
- deutliche Kostenersparnis und Reduzierung der Ausfallzeiten durch Predictive Maintenance.

Entscheidend für den Unternehmenserfolg sind drei Ziele von Industrie 4.0

1

Leichterer Zugriff auf das Steuernetz und Umsetzung agiler Produktionsprozesse

Durch die Konvergenz von OT und IT können Unternehmen schneller und gesamtheitlicher die Produktion steuern und z. B. an Kundenwünsche anpassen. Das wird vor allem durch die Integration der aktuellen Anlagenkommunikation in das MES und ERP ermöglicht. Als Ziel wird in diesem Bereich gerne von der Losgröße 1 geredet, also einer Unikatproduktion. Zugleich ermöglicht die Verschmelzung der Infrastrukturen und die Vernetzung der Anlagen untereinander die ganzheitliche Prozessoptimierung.

2

Echtzeit-Monitoring der Anlagen für Predictive und Prescriptive Maintenance

Anlagendaten werden gebündelt, in Echtzeit gesammelt und übersichtlich aufbereitet. Dadurch können Instandhaltungszeiten besser geplant und Ausfallzeiten signifikant reduziert werden.

3

Integration der Steuerkommunikation in die Qualitätssicherung und das Betriebliche Verfügbarkeitsmanagement

Der Zugriff vom Unternehmensnetz auf die Automatisierungsumgebung (OT) sowie die Echtzeitanalyse der Steuernetze stellen Daten bereit, die sowohl eine ganzheitliche Qualitätssicherung als auch die konsequente Umsetzung eines betrieblichen Verfügbarkeitsmanagements ermöglichen. Bislang hört die Qualitätssicherung an der Anlage und den Produktionsparametern auf. Die Integration der Steuernetzkommunikation und Netzwerkfunktionalität in das Qualitätsmanagementsystem sowie Kaizen- und Six-Sigma-Methoden steigert die Anlagenverfügbarkeit sowie die Produktqualität und reduziert Betriebsausfälle und Stillstände.

Das bestätigt neben der aktuellen Überarbeitung der Norm IEC 62443 auch der »Industrial Analytics 2016/2017 Report« der Digital Analytics Association (DAA). Die Studie basiert auf einer Befragung von 151 Analyseexperten und Entscheidungsträgern aus Industrieunternehmen zu den Chancen und Herausforderungen von Industrie 4.0 sowie des Industriellen Internet of Things (IIoT).

Voraussetzungen für das Erreichen von mehr Cybersicherheit und Produktivitätssteigerung

Die Integration und Analyse von Daten aus verschiedenen Systemen zur Steigerung der Produktivität ist immer nur so gut und aussagekräftig, wie:

- die Qualität der Daten;
- die Strategie der Datensammlung;
- das Wissen über die Wechselwirkungen und Kommunikation zwischen den Anlagen (Assets);
- das Verständnis über die Rollen der einzelnen Anlagen innerhalb der Gesamtkonfiguration.

Gleichzeitig ist die Cybersicherheit davon abhängig:

- wie zuverlässig ungewöhnliche Veränderungen und Anomalien im Steuernetz entdeckt werden;
- wie schnell diese Veränderungen gemeldet werden;
- wie gut die Daten über Ereignisse visualisiert und priorisiert werden.

Die erfolgreiche Umsetzung der beiden Kernziele Cybersicherheit und Produktivitätssteigerung ist nur möglich, wenn die folgenden Voraussetzungen erfüllt werden

1

Alle Assets in der Produktion sowie deren Verknüpfungen sind bekannt

Um eine klare Aussage sowohl zu Qualitätsthemen als auch zu Sicherheitsproblematiken geben zu können, ist die Grundvoraussetzung, Steuernetze mit all ihren Eigenschaften zu verstehen. Hier reicht eine Liste der Geräte, die im Steuernetz aktiv sind, nicht aus.

Viel wichtiger ist eine Übersicht der Vernetzungs- und Kommunikationsstrukturen. Welche Geräte kommunizieren miteinander? Welche Protokolle und Funktionen werden verwendet?

Die Überwachung der partizipierenden Geräte in einem Steuernetz muss kontinuierlich erfolgen. So können selbst nur zeitweise verbundene Geräte wie z. B. Wartungsrechner oder andere Fremdgeräte zuverlässig erkannt und deren Auswirkung auf das Steuernetz nachvollzogen werden. Letzteres erhält insbesondere dadurch Gewicht, dass längst nicht mehr alle Geräte an einer Anlage von ein und demselben Hersteller stammen. Jedes Gerät kann daher auch potentiell in Konflikt mit anderen Geräten treten, wenn diese nicht aufeinander abgestimmt sind.

Anfertigen eines Live-Mitschnitt des gesamten Netzwerkverkehrs

2

Die verschiedenen Rollen der einzelnen Anlagen und Geräte innerhalb eines Steuernetzes sind bekannt

Basierend auf der Liste der Assets und deren Verknüpfungen müssen die Rollen der einzelnen Geräte und Anlagen untereinander verstanden werden. Wie ist die Hierarchie unter den Geräten? Wer gibt Befehle? Welche Feedbackschleifen bestehen? Wie beeinflussen sich die Geräte untereinander?

In aktuellen Profinet-Umgebungen umfasst die Identifikation vor allem die Rollenzuweisungen auf den drei Ebenen I/O-Supervisor, I/O-Controller und I/O-Device (z. B. Roboterarm). Mit der zunehmenden Vernetzung und Ausweitung von IIoT-Strukturen werden sich die Wechselwirkungen weiter verkomplizieren. Wichtig ist hier, dass Konflikten in den Rollenzuweisungen vorgebeugt wird.

Übersicht aller Geräte im Netzwerk

3

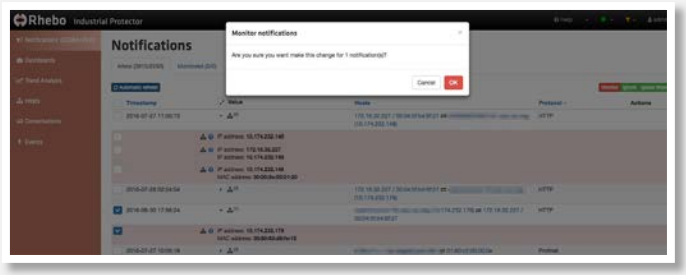
Fehlerhafte und sicherheitsgefährdende Geräte werden zuverlässig detektiert

Nach dem initialen Identifizieren aller Geräte innerhalb eines Steuernetzes müssen diese Geräte kontinuierlich überwacht werden, um eine fehlerfreie Funktion zu gewährleisten.
Durch die kontinuierliche Analyse kann sichergestellt werden, dass die identifizierten Geräte keine Fehlfunktionen herbeiführen, beispielsweise entstanden durch:

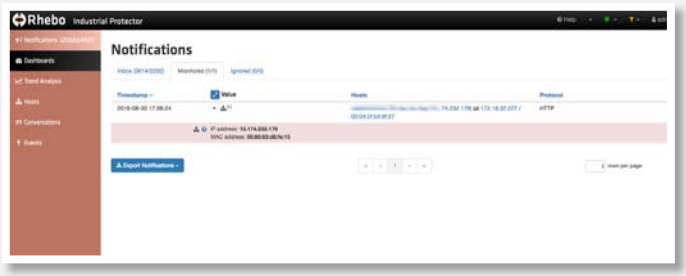
- (beabsichtigte und unbeabsichtigte) Fehlkonfigurationen;
- fehlerhaftes Verhalten aufgrund von Programmierfehlern oder Verschleiß;
- »Man-in-the-middle«-Angriffe;
- interne oder externe Kompromittierungen oder
- IPs mit multiplen MAC-Adressen.

Neue Geräte werden in Echtzeit erkannt und gemeldet

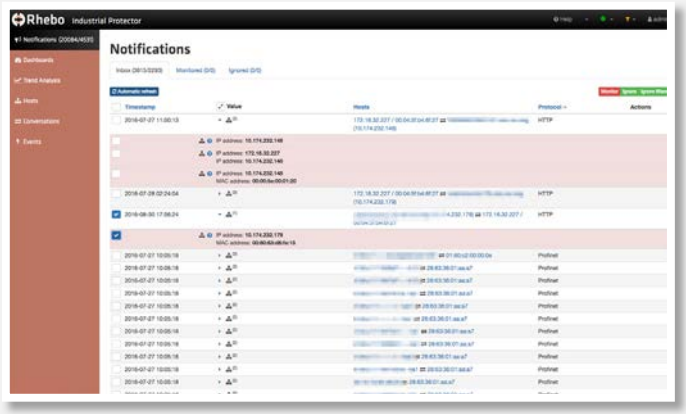
Genauso wie die Fehlfunktion oder Kompromittierung von bereits identifizierten Geräten müssen grundsätzlich alle neuen Geräte in einem Steuernetz in Echtzeit gemeldet werden.



Ein Netzwerkgerät wird überwacht



Meldungen neuer Geräte im Netzwerk

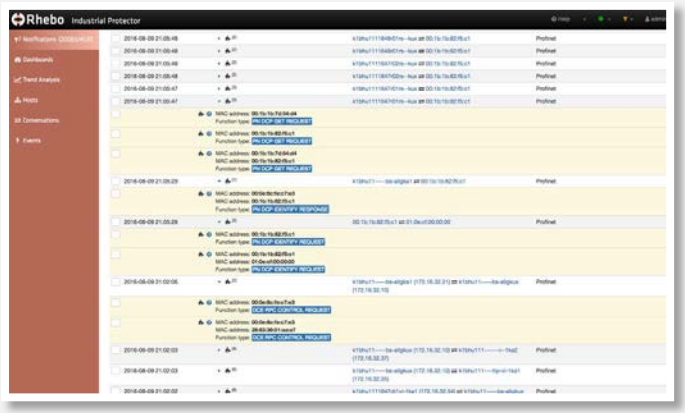


Bestätigung vor dem Überwachen einer neuen Meldung

4

Risikobehaftete oder verdächtige Befehle auf Geräten werden in Echtzeit erkannt

Neben der reinen Hardwareerkennung müssen auch Veränderungen bzw. Anomalien innerhalb der Kommunikationsstruktur lückenlos aufgespürt werden. Ein Gerät innerhalb eines Steuernetzes kann nach wie vor dieselbe Rolle und dieselben Verknüpfungen zu anderen Geräten besitzen. Entscheidend ist die Kommunikation des Geräts zu anderen Geräten. Das gilt explizit, wenn die Kommunikation eine Befehlsfunktion hat, also über das Verhalten anderer Geräte bestimmt. Die Erkennung und Meldung muss in Echtzeit stattfinden.



Meldungen neuer Profinet-Funktionen im Netzwerk

5

Die Netzwerkdynamik wird analysiert und Kommunikationsflüsse gelenkt

Aktuell gilt in IT-Umgebungen: jeder kann jederzeit mit jedem kommunizieren. Abhängig von der Bandbreite des Steuernetzes und der Leistung der Endgeräte kann das zu Kapazitätsengpässen führen. Das kann wiederum die Anlagenverfügbarkeit und Funktionalität beeinträchtigen. Kollidieren Kommunikationsflüsse im Steuernetz, kann dies negative Auswirkungen nach sich ziehen:

- Information geht verloren;
- Information wird wiederholt und damit redundant geliefert;
- die Verarbeitung akuter Information wird verzögert;
- Fehlfunktionen, Qualitätsprobleme oder Betriebsausfälle.

Netzwerkstabilität ist entscheidend für die fehlerfreie Produktion und eine maximale Anlagenverfügbarkeit.
Effektives Kontinuitätsmanagement braucht deshalb eine Priorisierung und Taktung jeglicher Kommunikation in Steuernetzen. So kann z. B. abhängig vom Produktionsablauf klar definiert werden, wann und was Anlage A mit Anlage B kommunizieren darf.

Um dies zu erreichen, sollten zwei Voraussetzungen erfüllt sein:

1. **Echtzeit-Analyse jeglicher Kommunikation im Steuernetz;**
2. **Verständnis der Kommunikationsflüsse und Abhängigkeiten im Steuernetz (siehe oben).**

Verteilung von Meldungstypen und des Durchsatzes über die Zeit

Verteilung von HTTP- und Modbus-Kommunikation über die Zeit

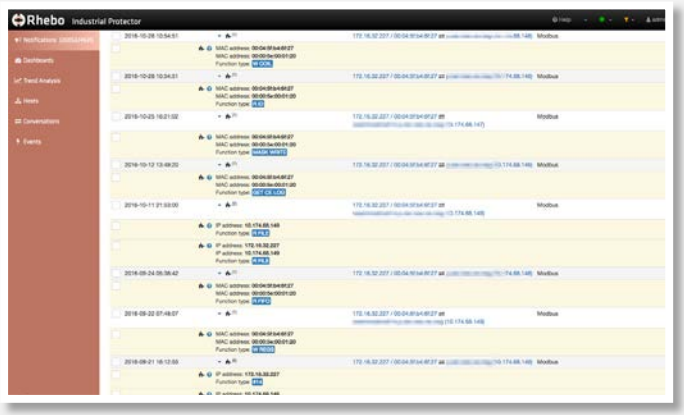
6

Die gesamte Steuernetzkommunikation wird lückenlos überwacht und ausgelesen

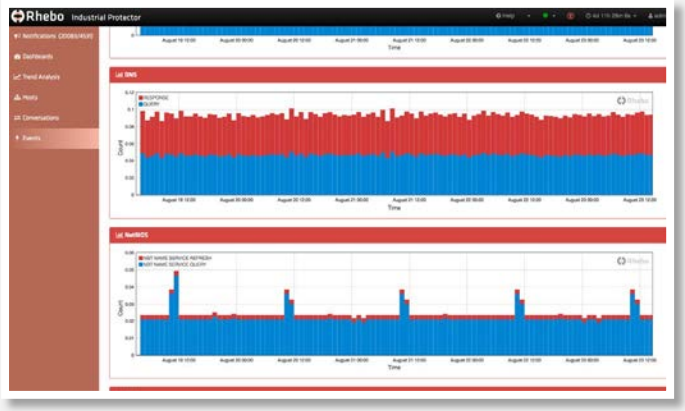
Um sowohl eine maximale Datenqualität als auch die maximale Systemabsicherung in Bezug auf Cybersicherheit und Verfügbarkeit zu erreichen, muss das Monitoring sowohl zeitlich als auch inhaltlich lückenlos sein.

Das Erreichen der Voraussetzungen 1–6 bedingt deshalb ein Überwachungssystem mit drei Grundfunktionen:

1. Echtzeit-Monitoring und Analyse;
2. Dynamische Weiterentwicklung der Monitoring-Algorithmen mittels maschinellen Lernens und
3. Auslesen aller Datenpakete im Steuernetz bis auf Inhaltsebene.



Meldungen neuer Modbus-Funktionen im Netzwerk



Verteilung von DNS- und NetBIOS-Kommunikation über die Zeit

7

Events und Anomalien werden automatisch zugeordnet, priorisiert und visualisiert

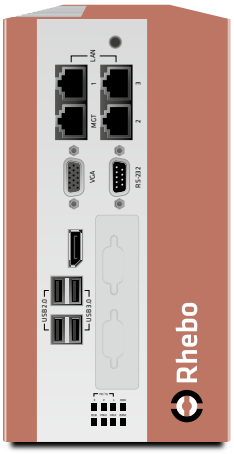
Ein Monitoring- und Sicherheitssystem ist nur so gut, wie die Nutzer ihre Daten verstehen und auslesen können. Das System muss deshalb in der Lage sein, im ersten Schritt gemeldete Ereignisse bzw. Anomalien einzuordnen und zu gewichten. Dabei bleiben alle Daten zu den Ereignissen erhalten. Sie müssen jedoch vorsortiert und verständlich visualisiert werden.

Zudem muss der Export der Daten reibungslos erfolgen. Das ist nicht nur für verschiedene interne und externe Berichtspflichten relevant. Der Export und nachfolgende Import in andere Backend-Systeme (SIEM, MES, ERP) ist auch die Voraussetzung, um Daten effektiv verknüpfen und weiterverarbeiten zu können. Nur so können die industriellen Daten für weitere Anwendungen wie forensische Analyse, Qualitätssicherung und Business Continuity sicher und aussagekräftig verwendet werden.

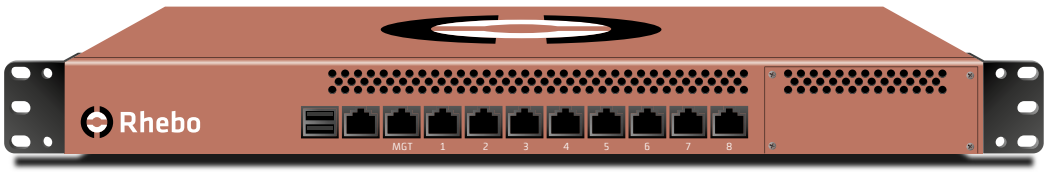
Kontinuierliches Network Monitoring für die Optimierung und Sicherung industrieller Steuernetze

Rhebo Industrial Protector überwacht lückenlos und rückwirkungsfrei die vernetzte Steuerkommunikation einschließlich der Schaltanlagen-, Fernwirk- und Netzleittechnik.
Alle Datenpakete werden auf Inhaltsebene dekodiert und jeglicher verdächtige Vorgang wird in Echtzeit gemeldet. Selbst abweichende Operationsverläufe, die zu Anlagenausfällen führen können, wie z. B. Netzwerkprobleme und Maschinenstörungen, werden zuverlässig erkannt. Die Administration behält dabei die komplette Kontrolle über die Anlagenfunktionalität. Alle Daten über verdächtige Operationen (inklusive Metadaten und Paketinhalte) werden gespeichert. Das ermöglicht eine detaillierte Analyse jedes verdächtigen Vorgangs.

- Komplette Kontrolle und Transparenz Ihres Steuernetzes
- Erkennen aller unzulässigen Vorgänge in Steuernetzen in Echtzeit
- Früherkennung und Vermeiden von Ausfällen
- Vollautomatischer und selbstlernender Betrieb



Industrial Protector Sensor



Industrial Protector Controller

Über Rhebo

Rhebo ist ein Technologieunternehmen, das sich auf die Ausfallsicherheit von Industrial Control Systems mittels Überwachung der Steuerkommunikation spezialisiert hat. Wir tragen dem Industrial Internet of Things Rechnung und schützen vernetzte industrielle Steuersysteme und kritische Infrastrukturen. Unser Anspruch ist die lückenlose Absicherung von Steuernetzen gegen Ausfälle, Netzwerkanomalien und Cyberattacken mittels vollständiger Analyse aller Datenströme auf Inhaltsebene.

Rhebo GmbH Spinnereistraße 7 | 04179 Leipzig | Deutschland
Rhebo.com

Whitepaper 03-2017 | © Rhebo GmbH