



Rhebo und RAD SecFlow

Skalierbare Cybersicherheit für Umspannwerke und verteilte Energieressourcen



Mit der Integration von Rhebo Industrial Protector auf den RAD SecFlow-1v IoT-Gateways gewinnen Versorgungsunternehmen und Betreiber Kritischer Infrastrukturen vollständige Transparenz und Cybersicherheit für den Fernbetrieb ihrer Anlagen. Rhebo erweitert die Stateful-Firewall auf dem Gateway um ein leistungsfähiges

Netzwerkmonitoring mit Anomalieerkennung auf Umspannwerkebene. Neuartige Angriffe, Malware-Aktivitäten und technische Fehlerzustände können erkannt und korrigiert werden, bevor es zu Störungen kommt.

360°-Sicherheit gegen Störungen

Unternehmen im Energie- und Gassektor bedienen ihre Anlagen oft per Fernsteuerung. Die Kommunikation mit dem Network Operation Center (NOC) sowie innerhalb der ferngesteuerten Anlagen muss daher besonders abgesichert werden. Bei täglich mehr als 320.000 neuen Malware-Varianten und immer spezialisierteren Angriffsmethoden ist die Erkennung neuer Angriffsmustern umso wichtiger. Für eine schnelle Abwehr und das Verhindern eines Übergriffs auf andere Standorte oder das NOC muss dabei die Erkennung bereits an der betroffenen Anlage erfolgen.

Mit dem RAD SecFlow-1v Industrial IoT Gateway schaffen Unternehmen die Basis für eine sichere und ökonomische Anbindung ferngesteuerter Energiesysteme. Das Gateway ermöglicht die sichere Anbindung von RTUs, Smart-Meter-Aggregationsgeräten und IoT-Basisstationen über Funk- oder Glasfasernetze. Die vorinstallierte Stateful-Firewall von RAD analysiert die eingehende Kommunikation auf bekannte Angriffssignaturen und blockiert diese bei Bedarf. Mit Rhebo Industrial Protector wird die Firewall-Funktion um eine Überwachung der Fernwirk- und Netzleittechnik per Anomalieerkennung erweitert. Der Rhebo-Sensor läuft als eingebettete Funktion auf dem RAD-Gerät und nutzt die Edge-Computing-Fähigkeiten des SecFlow-1v. Rhebo Industrial Protector analysiert kontinuierlich die Kommunikation in der Fernwirk- und Netzleittechnik auf der

Ebene der einzelnen Standorte (zum Beispiel Umspannwerk, Solarpark, Windkraftanlagen, Wärmepumpen, Leitwarte). Jede Abweichung innerhalb der Kommunikation vom erwarteten Muster wird in Echtzeit erkannt, bewertet und gemeldet. Dies ermöglicht es den Betreibern, ihr System zur Angriffserkennung weiterzuentwickeln, um unter anderem folgende Anomalien zu erkennen:

- neue Geräte und Netzwerkteilnehmer
- verändertes Kommunikationsverhalten eines Geräts
- kritische Aktivitäten wie Firmware-Aktualisierungen und Änderungen in den Betriebsmodi der SPS
- Umgehung bestehender Sicherheitsmechanismen
- Spionageaktivitäten wie Scans und laterale Bewegungen
- bekannte Schwachstellen der Geräte
- technische Fehlerzustände (z. B. zyklische Telegramme, Kommunikationsabbrüche, Fehlkonfigurationen)

Detaillierte Netzwerkkarten und Verbindungsübersichten schaffen ein vollständiges Echtzeitbild des Netzwerks. Betreiber erhalten vollständige Transparenz über ihre Fernwirk- und Netzleittechnik sowie deren Sicherheitsstatus und Risikoexposition. Durch den Einsatz von Sensoren auf Feldebene kann der im SecFlow integrierte Rhebo Industrial Protector Angriffe auf Feldebene erkennen, die auf höheren Ebenen nicht sichtbar sind.

Ihre Vorteile mit Rhebo und RAD

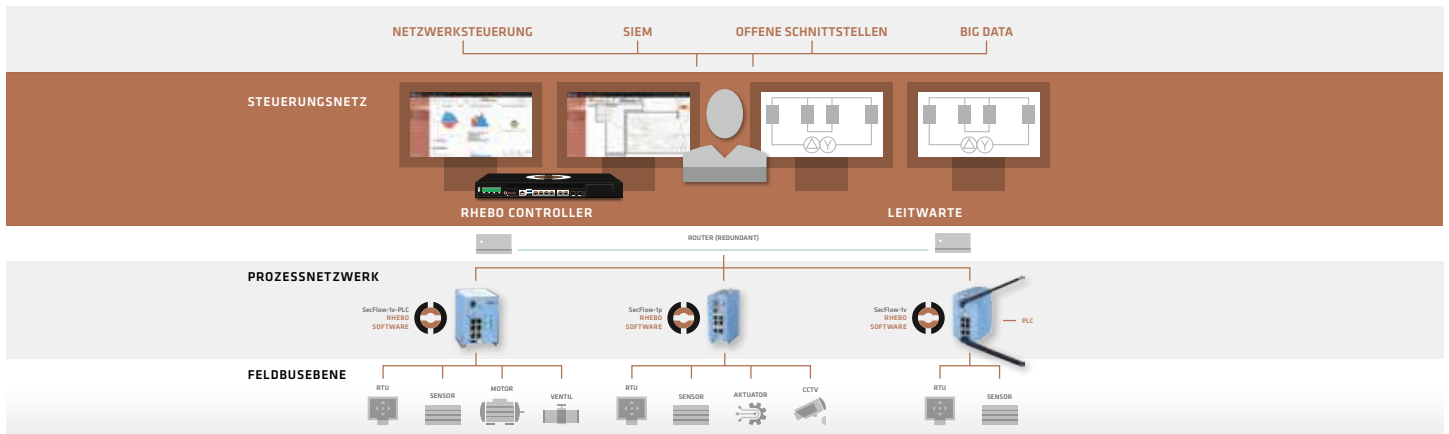
- ✓ **360°-SICHTBARKEIT** vom Netzwerk bis zu den Geräten, von der Leitwarte bis zum Umspannwerk und Kraftwerk
- ✓ **FORTSCHRITTLICHE ANGRIFFS-ERKENNUNG** mit kombinierter Stateful Firewall und Anomalieerkennung
- ✓ **ERHÖHTE HANDLUNGSFÄHIGKEIT** durch integrierte Risikobewertung und forensische Datenspeicherung
- ✓ **ÜBERWACHUNG AUF UNTER-STATIONSEBENE** für lokale Cybersicherheit und Erkennung von Angriffen, Sabotage und Schwachstellen
- ✓ **VERBESSERUNG DER ANLAGEN-VERFÜGBARKEIT** und Versorgungssicherheit durch frühzeitige Erkennung technischer Fehlerzustände
- ✓ **KOSTENEFFIZIENTE, CONTAINER-BASIERTE BEREITSTELLUNG** über zentrale RADview-Schnittstelle

Netzwerkzustandsüberwachung für erhöhte Verfügbarkeit

Der integrierte Rhebo Industrial Protector liefert detaillierte Informationen über schadhafte Kommunikation, Cyberattacken sowie Netzwerkqualität und -leistung. Alle Anomalien werden in Echtzeit gemeldet. Betreiber Kritischer Infrastrukturen können über alle Standorte hinweg gleichbleibend hohe Verfügbarkeit, Sicherheit und Effizienz sicherstellen. Der Einsatz von Rhebo Industrial Protector erfolgt über die zentrale Steuerungsoberfläche RADview. Dies ermöglicht die äußerst kosteneffiziente Umsetzung eines tiefgreifenden Cybersecurity- und Verfügbarkeitsmanagements für eine beliebige Anzahl von Unterstationen. Durch die Integration von Netzwerk- und Nicht-Netzwerk-Funktionen auf derselben Hardware reduziert der SecFlow die Anzahl der Geräte im Netzwerk. Neben

einem integrierten Router und LTE-Modem verfügt der SecFlow über Funktionen wie eine SPS, ein LoRaWAN-Gateway, ein Protokollkonverter, ein Videoüberwachungs-DVR und mehr. Es unterscheidet sich von anderer verfügbarer IIoT-Hardware durch:

- Handhabung verschiedener Funktionalitäten, die sonst verschiedene Geräte erfordern würden;
- Unterstützung für jeden Medienanschluss, der vor Ort verfügbar ist, im selben Gerät;
- Protokollkonvertierung damit sich Feldgeräte mit dem Netzwerk verbinden können, auch wenn sie keine neuen IIoT-»Sprachen« nutzen.



Zwei starke Partner für Sicherheit und Verfügbarkeit ferngesteuerter Energieanlagen



Rhebo

a Landis+Gyr company



Your Network's Edge®

Rhebo entwickelt und vermarktet innovative industrielle Monitoringlösungen und -services für Energieversorger, Industrieunternehmen und Kritische Infrastrukturen. Das Unternehmen ermöglicht ihren Kunden, sowohl die Cybersicherheit als auch die Verfügbarkeit ihrer OT- und IIoT-Infrastrukturen zu gewährleisten und somit die komplexen Herausforderungen bei der Absicherung industrieller Netze und Smart Infrastructures zu meistern. Rhebo ist seit 2021 eine 100%ige Tochter von Landis+Gyr AG, einem global führenden Anbieter integrierter Energiemanagement-Lösungen für die Energiewirtschaft mit weltweit rund 5.500 Mitarbeitern. Rhebo ist Partner der Allianz für Cyber-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI) und engagiert sich aktiv beim Teletrust – Bundesverband IT-Sicherheit e.V. und Bitkom Arbeitskreis Sicherheitsmanagement für die Erarbeitung von Sicherheitsstandards.

RAD Als globaler Anbieter von Telekom-Access-Lösungen setzt sich RAD dafür ein, dass Dienstleister und Betreiber kritischer Infrastrukturen jeden Service über jedes Netzwerk weiterentwickeln können. Durch unsere Vorreiterrolle bei bahnbrechenden Technologien und die Zusammenarbeit mit unseren Kunden sind wir bestrebt, Dienstleistern dabei zu helfen, die Wertschöpfungskette in einem für sie angemessenen Tempo voranzutreiben und gleichzeitig ihren Endkunden und Netzbetreibern einen Mehrwert zu bieten – sei es in den Bereichen Network Edge Virtualization und vCPE, Industrial IIoT oder 5G xHaul. Mit 40 Jahren Innovation und einer bedeutenden weltweiten Präsenz in über 150 Ländern verfügt RAD über eine installierte Basis von mehr als 16 Millionen Netzwerkkomponenten. RAD ist Teil der RAD-Unternehmensgruppe, einem weltweit führenden Anbieter von Telekommunikationslösungen mit einem jährlichen Umsatz von 1,5 Milliarden US-Dollar. www.rad.com

Kontaktieren Sie uns

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