Security

Sichere Prozessautomatisierung, jetzt!

Klarer Blick. Mehr Wert aus Daten.
Und alles Sicher?

Klaus Lussnig, Industrial Automation und
Jens Bußjäger, Acht-Werk/IRMA
www.scada.online
ww.acht-werk.de | www.irma-box.de

Prozessautomatisierung schafft Tempo und Sicherheit in Wasser, Chemie, Lebensmittel sowie Öl und Gas. Daten liegen in Echtzeit vor und führen durch den Tag. Betriebsteams sehen dieselben Bilder im Leitstand und mobil. Die Instrumentierung liefert verlässliche Werte. Historisierung macht Zusammenhänge sichtbar. Reporting liefert Nachweise auf Knopfdruck. Alarmmanagement lenkt Aufmerksamkeit auf das Wichtige. So entsteht Ruhe im Betrieb und ein klarer Fokus auf Qualität und Effizienz.

KPIs stehen jederzeit bereit und ermöglichen die kontinuierliche Verbesserung der Produktion und der Produkte. Sind hier auch die KPI des Security Managements mit enthalten? Gab es Fehlkonfigurationen, die zu Störungen führten? Wer hat versucht den Remote-Access unberechtigt zu nutzen und wurde abgewiesen?

So schafft man durchgängige Konnektivität

Was geht? Schützen Rollen und Zonen bereits den Betrieb. Standardisierte Schnittstellen verbinden IT und OT und sind abgesichert. Redundanz hält die Systeme verfügbar. Edge verarbeitet nah an der Anlage Eine gesicherte Cloud eröffnet zentrale Auswertungen und Vergleiche zwischen Standorten.

Offene Protokolle wie OPC UA und MQTT sorgen für durchgängige Konnektivität bis in die Feldebene. Single Pair Ethernet bringt Ethernet auf bestehende Zweidraht-Infrastruktur und öffnet die letzte Ebene der Anlage für Echtzeitdaten. Das schafft Tempo in der Integration und erhöht die Sicht aber auch neue Gefährdungen in die Ebene der Sensoren und Aktoren.

Hier zählt Security von Beginn an. Verfügbarkeit und Integrität sind das Ziel:

- Feldbus über Ethernet bräuchten Authentifizierung und Verschlüsselung. Gibt es kaum!
- Controller und Feldgeräte sind eindeutig identifizierbar. Stimmt das?
- Die Netzsegmente der Anlage sind sauber getrennt. Das ist kontinuierlich zu prüfen, oder?
- Protokollierungs- und Ereignisdaten laufen zentral zusammen werden korreliert. Werden alle Änderungen wirklich beachtet?
- Die Edge Gateways und der Datenaustausch in die Cloud ist vollumfänglich gesichert. Doch wer kontrolliert diese Verschlüsselungen und wo stehen die Server? Wer ist Eigentümer des Anbieters?
- Und wo es keine Protokollierungsdaten gibt, ist das Netzwerkmonitoring mit OT Protokoll Erkennung einzusetzen. Schon geplant?
- Letztendlich begleitet Risikomanagement jede Erweiterung fortlaufend mit Blick auf die Bedrohungen und in Abwägung des Nutzens. Gibt es immer diese Risikobetrachtung, wenn Erweiterungen geplant werden und in Betrieb gehen?

Oft wird nur der Nutzen gesehen ohne die Auswirkung auf Gefährdungen der Verfügbarkeit. Seien Sie wachsam. ☐