ICS/SCADA-Cybersicherheit für Wasser- und Abwasseranlagen

ICS-BASIERTES ANGRIFFSERKENNUNGSSYSTEM (IDS)

Das für ICS/SCADA-Netzwerke entwickelte fortschrittliches IDS von Radiflow erkennt Anomalien und macht diese durch das selbstlernende SCADA-Netzwerks sichtbar.

SICHERES ROBUSTES GATEWAY

Authentication Proxy Access (APA) und Firewall Deep-Packet-Inspection (DPI) zur aufgabenbasierte Validierung der Zugangsdaten von Technikern und die Validierung aller SCADA-Sitzungen.

Umfassender Schutz der Wasser- und Abwasseranlagen vor möglichen Cyberangriffen

SCADA-Überwachungs- und Steuerungssysteme in Wasser- und Abwasseraufbereitungsanlagen sind heute vorrangige Ziele für Cyberangriffe zum Schaden hochentwickelter Infrastrukturen. Solche Angriffe sind meist auf menschliche Eingriffe vor Ort oder auf Eindringen in das Netzwerk zurückzuführen.

Radiflows umfassende Cybersecurity-Lösung enthält ein Angriffserkennungssystem zum Überwachen lokaler Vorgänge und einen sicheren Gateway mit hochentwickelter Firewall für den sicheren ferngesteuerten Zugriff auf das OT-Netzwerk (Operational Technology).

Das IDS von Radiflow kann durch sein selbstlernendes Standardmodell den Netz-zustand analysieren und Anomalien erkennen, die durch einen Insider-Angriff (z.B. Malware auf einer der SPS) verursacht sein können. Erkannte Anomalien alarmieren den Betreiber, alle am Standort erfolgten Zustandsänderungen nachzuverfolgen.

Für die sichere örtliche Wartung kann der Fernzugriff über das sichere Gateway durch einen sicheren VPN-Tunnel mit konfigurierbaren Zugriffsrechten aktiviert werden. Der Authentifizierungs-Proxy des Gateways überprüft alle externen Nutzer und beschränkt ihren Zugriff auf vordefinierte Aufgaben (Gerät, Zeitfenster, genehmigte Befehle usw.). Alle Remote-Sitzungen werden zum Nachweis aufgezeichnet.

radiflow

ICS/SCADA-Cybersicherheit für Wasser- und Abwasseranlagen

Schlüsselmerkmale

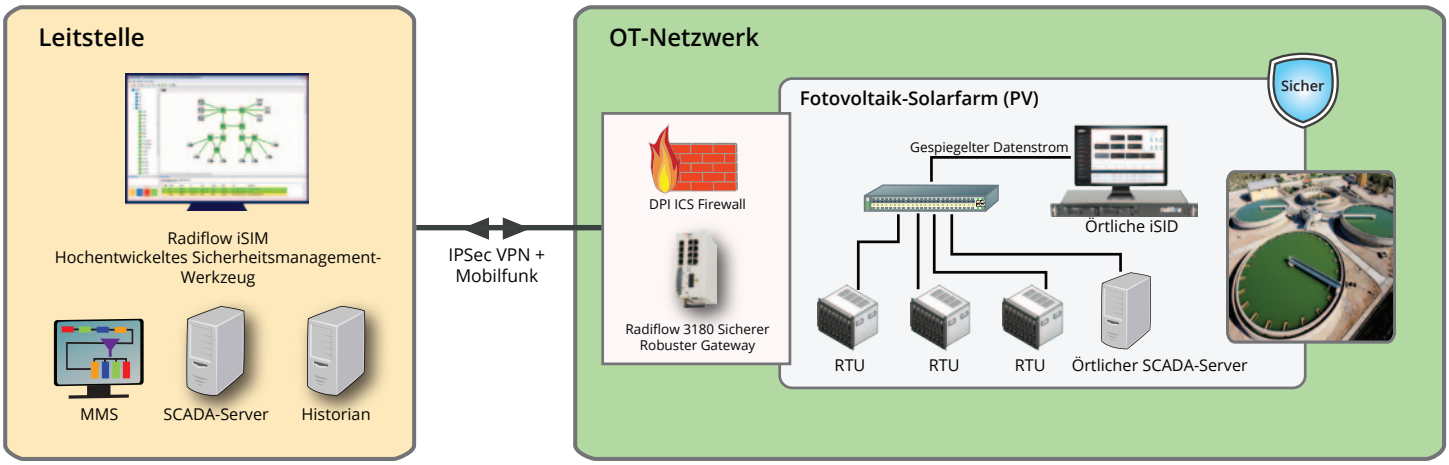
Angriffserkennungssystem (IDS)

- **Netzwerk-Sichtbarkeit**
  Anzeige aller Netzwerkressourcen und Änderungen der Konnektivität durch das selbstlernende SCADA-Netzwerk und passives Scannen aller Datenüber-tragungen.
- **Wartungs-Management**
  Überwachen und Protokollieren von Aktivitäten, die während Wartungssitzungen nach festge-legten Regeln ausgeführt werden.
- **Anomalie-Erkennung**
  Erkennen abnormaler Aktivitäten durch Vergleich mit dem vom IDS erstellten Standard-Verhaltensmuster, z. B. geänderte SCADA-Sequenzen, regelwidrige Speicherzugriffe und Firmwareänderungen.

Sicherer Gateway

- **Zugang durch Proxy-Authentifizierung (APA)**
  Prüft die Zugangsdaten für Techniker und erstellt einen festge¬legten aufgabenbasierten Zugang mit detailliertem Protokoll aller Benutzeraktivitäten bei Fernzugriffen.
- **DPI Firewall**
  Überprüft alle SCADA-Sitzungen mit der Deep-Packet-Inspection-Firewall.
- **Fernzugriff**
  Sichere Konnektivität zum Standort über einen direkten IPsec-VPN und ein 2G/3G/LTE-Dual-SIM-Mobilfunkmodem für den Notfallzugriff
- **Konformität zur Betriebssystemumgebung**
  Die Hardware des Sicheren Gateways entspricht den Anforde¬rungen von IEC 61850- 3/IEEE 1613 für den Betrieb in industriellen Umgebungen.

Einsatz



US und Kanada:
Tel.: +1 (302) 547-6839
sales_NA@radiflow.com

EMEA:
Tel.: +972 (77) 501-2702
sales@radiflow.com

UK:
Tel.: +44 (0) 800 246-1963
sales_UK@radiflow.com

Frankreich:
Tel.: +33 1 77 47 87 25
sales_FR@radiflow.com