Application Note

ICS/SCADA Cybersecurity for Water and Wastewater Facilities

Comprehensive protection for water and wastewater facilities against all types of potential cyber-attacks

Supervisory Control and Data Acquisition (SCADA) systems at water and wastewater treatment facilities have become in recent years prime targets for cyber attacks originating both from on-site human activity and remote network breaches.

Radiflow's comprehensive cybersecurity solution consists of an Intrusion Detection System for monitoring local operations, as well as a Secure Gateway that serves as an industrial firewall and provides secure access to the OT network, both on-site and remote. Together they enable detecting attacks on operational processes.

Radiflow's IDS is able to detect anomalies in the operational network's behavior and alert the operator, based on its self-learned baseline behavior model. Such anomalies may indicate an insider attack (e.g. a malware on one of the PLCs) that couldn't have been detected by the secure gateway.

In case of emergency, remote access can be enabled via the Secure Gateway by means of secure VPN tunnel, with configurable access rights. The Gateway's authentication proxy validates each remote user and restricts the user's access according to his predefined tasks (device, time slot, approved commands, etc.) All remote sessions are recorded for auditing purposes.

ICS-DEDICATED INTRUSION DETECTION SYSTEM (IDS)

Radiflow's advanced IDS, designed for ICS/SCADA networks, provides full network visibility and anomaly detection, based on self-learning of the SCADA network.

MAINTENANCE MANAGEMENT

Real-time monitoring and logging of actvities performed during maintenance sessions, according to pre-configured policies.

SECURE RUGGEDIZED GATEWAY

Authentication Proxy Access (APA) and DPI Firewall used for task-based validation of technician credentials and validation of each and every SCADA session.

ICS/SCADA Cybersecurity for Water and Wastewater Facilities

Key Features

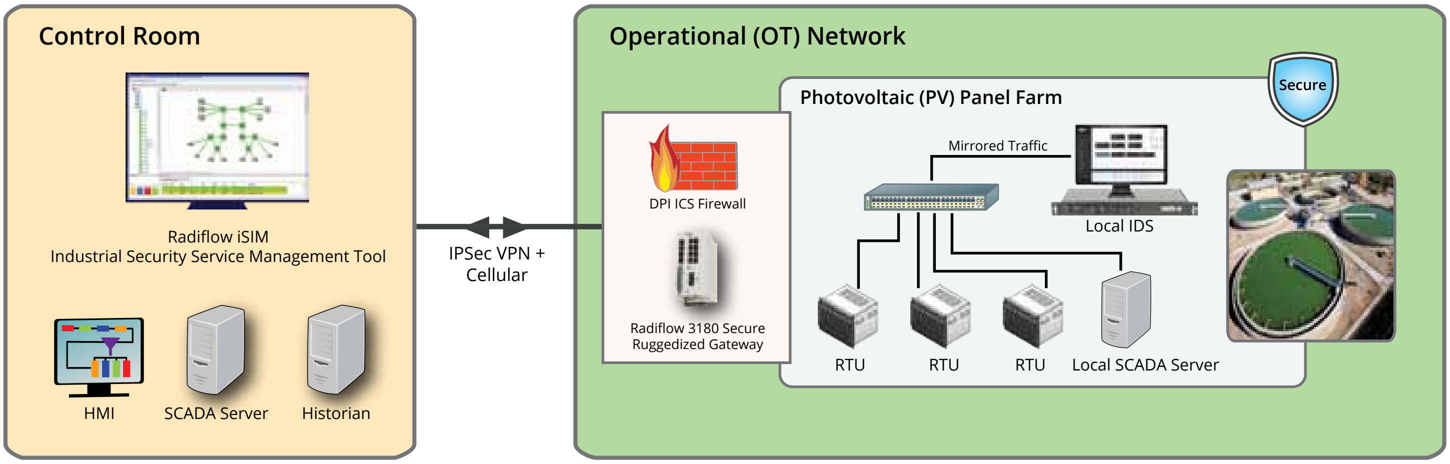
Intrusion Detection System (IDS)

- **Network Visibility**
  Display of all network assets and any changes in connectivity, based on self-learning of the SCADA network through passive scanning of all data transactions.
- **Maintenance Management**
  Monitoring and logging of activities performed during maintenance sessions according to pre-configured policies.
- **Anomaly Detection**
  Detection of abnormal activity such as changes in the SCADA process sequence, abnormal memory access and firmware changes, based on the normal application behavior model created by the IDS.

Secure Gateway

- **Authentication Proxy Access (APA)**
  Validate technician credentials and provide preconfigured task-based access, as well as a detailed log of all user activity during each remote access session.
- **DPI Firewall**
  Validates each SCADA session behavior using a Deep Packet Inspection firewall.
- **Remote Access**
  Secure connectivity to site via end-to-end IPsec VPN as well as 2G/3G/LTE dual-SIM cellular modem for emergency access
- **Operating Environment Complience**
  The Secure Gateway's hardware is compliant with the IEC 61850-3/IEEE 1613 requirements for operation in harsh environments.

Deployment


Control Room
Radiflow iSIM
Industrial Security Service Management Tool
HMI
SCADA Server
Historian
IPSec VPN +
Cellular
Operational (OT) Network
Photovoltaic (PV) Panel Farm
Secure
DPI ICS Firewall
Radiflow 3180 Secure
Ruggedized Gateway
Mirrored Traffic
Local IDS
RTU
RTU
RTU
Local SCADA Server