

ICS/SCADA Cybersecurity for Water and Wastewater Facilities

WHY RADIFLOW?

Radiflow is a recognized leader in industrial cybersecurity, offering dedicated solutions designed to meet the unique requirements of industrial infrastructures:

EXPERIENCE

Over 10 years' experience discovering and analyzing advanced persistent threats and targeted attacks, including attacks on critical and industrial infrastructure

UNIQUE METHODOLOGY

Radiflow offers a unique scan methodology to detect industrial attack vectors that can cause downtime.

EXPERTISE

Dedicated team of industrial cybersecurity experts who understand the colliding worlds of automation and security.

END-TO-END PORTFOLIO

Radiflow offers a holistic portfolio of services and technologies, including SCADA gateways, routers and firewalls, industrial network IDS and many more.



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 potential prime targets for cyber attacks aimed at damaging the basic infrastructure of modern life. Such attacks may originate from either on-site human activity or 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 remote access to the OT network.

Radiflow's IDS is able to detect anomalies, which may indicate an insider attack (e.g. a malware on one of the PLCs) in the operational network's behavior, based on its self-learned baseline behavior model. Alerts upon anomaly detection enable the operator to keep track of all operational changes done in the site.

The Secure Gateway is used to facilitate remote maintenance sessions, 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/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 Compliance

The Secure Gateway's hardware is compliant with the IEC 61850-3/IEEE 1613 requirements for operation in harsh environments.

Deployment

