

Comprehensive yet simple security solutions to protect your critical assets

Supervisory Control and Data Acquisition (SCADA) systems are used for controlling and monitoring remote operations in a variety of critical infrastructures, such as power utilities, oil & gas, water and others. SCADA networks often extend across multiple remote sites, allowing automation devices to be controlled from the control center.

Cyber threats to SCADA systems have in recent years been on the rise. Terrorists and criminals have set their sights on critical infrastructures that utilize SCADA systems due to these systems' inherent vulnerabilities and the huge potential to disrupt civilian life and may cause high financial losses to the utilities.

Radiflow's security tool-set validates the behavior of both M2M applications and H2M (Human to Machine) sessions in distributed operational networks. Radiflow's security solutions are available both as in-line gateways for remote sites and as a non-intrusive IDS (Intrusion Detection System) that can be deployed per site or centrally.

Visibility



Radiflow's IDS automatically learns the network topology (links, protocol and devices) using passive scanning. Any new activity is highlighted on the GUI.

Protection



Radiflow's IDS and Secure Gateways protect the SCADA networks from a variety of cyber threats such as network scanning, infected RTU and technician activity.

Compliance



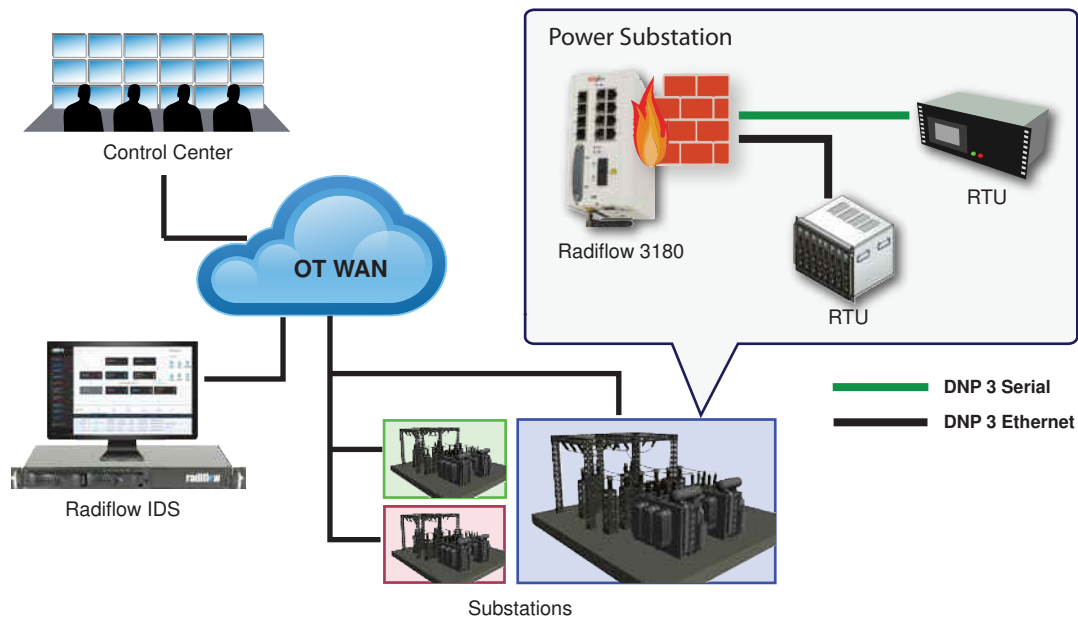
Radiflow's security products help make your network compliant with major security standards: NERC CIP version 5, NIST SP 800-82 V2, ISA 99 and IEC 62443.

Intrusion Detection System (IDS)

- Network visibility: highlight new entities based on self-learning of the SCADA network through passive scanning.
- Maintenance management: plan and audit maintenance sessions at remote sites from a central location.
- Signature-based detection: detection of known attacks, PLC vulnerabilities and known protocol vulnerabilities.
- Virtual firewall: unique DPI firewall rules on every link, as well as dynamic firewall rules that apply to specific times.
- Anomaly detection: detection of abnormal activity in comparison with the normal base line.
- Operational behavior: monitor network health, detect abnormal network load delays in links and more.

Secure Gateway

- Authentication Proxy Access (APA) authenticates users and provides them with preconfigured task-based access.
- Detailed log of all user activity within each remote access session for compliance and audit.
- Validation of each user's SCADA behavior using a per-port Deep Packet Inspection (DPI) firewall.
- IPsec VPN for secure inter-site connectivity between substations and EMS/DMS control centers.
- Ethernet and Serial interfaces for connecting modern and legacy devices over wire and cellular.
- Ruggedized appliances compliant to IEC 61850-3/IEEE 1613 requirements for operation in harsh environments.



Radiflow was founded in 2009 as part of the RAD group, a family of ICT vendors with over \$1Bn in annual revenues.

Radiflow's security solutions, introduced in late 2011, have been successfully deployed by major utilities world-wide, and validated by leading security research labs.

Radiflow's security solutions are sold both as components within global automation vendors' integrated end-to-end solutions, and as standalone security solutions by local channel partners.