

Radiflow

Cybersecurity Solutions for the Industrial IoT

A COMPLETE SECURITY SOLUTION FOR SCADA INSTALLATIONS

VISIBILITY

Radiflow's iSID Intrusion Detection System (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.



Comprehensive yet simple security solutions to protect your critical assets

Supervisory Control and Data Acquisition (SCADA) systems, used for controlling and monitoring remote operations in critical infrastructures such as power utilities, oil & gas, water and more, 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.

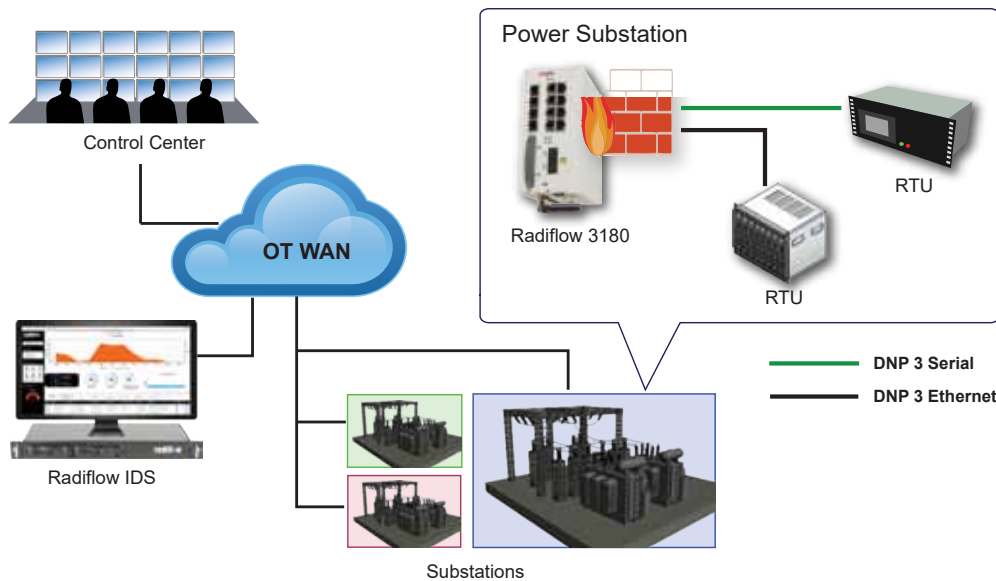
iSID Intrusion Detection System (IDS)

- ▶ Network visibility: highlight new entities based on self-learning of the SCADA network through passive scanning.
- ▶ Asset Management: automatic mapping of all industrial assets and their inventory information, and alerts on parameter change attempts.
- ▶ Signature-based detection: detection of known attacks, PLC vulnerabilities and known protocol vulnerabilities.
- ▶ Policy Monitoring: unique DPI firewall rules on every link, as well as dynamic firewall rules that apply to specific times.
- ▶ Anomaly detection: detect abnormal activity on the network compared to the normal device fingerprint.
- ▶ Event notifications via multiple reporting methods (GUI, Syslog and DNP3) to fit into various security and operational organizations.
- ▶ Smart probe: optimize the monitoring of distributed sites by a central iSID server using unique smart-probes at remote sites.

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.

Typical deployment on a distributed OT network



About Radiflow

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.

Your local Radiflow contact:

RASTER PRODUCTS

Raster Products BV
 Oude Maasdijk 30, 6621 AC Dreumel
 PO Box 3, 6620 AA Dreumel

tel +31 (0)487 - 57 27 19
 e-mail info@raster-products.com
 web www.raster-products.com