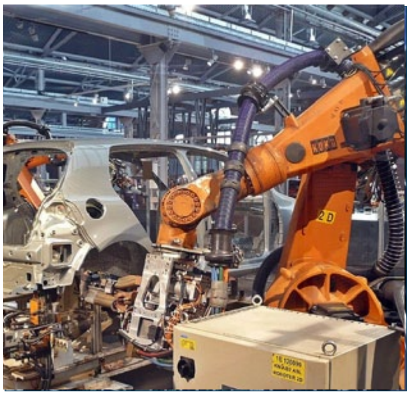
Application Note

Production Floor Security

Network Monitoring & Secure Access to the Production Floor



- ▶ Secure maintenance via Authentication Proxy Access (APA)
- ▶ Maintenance activity logging according to preconfigured policies.
- ▶ Unidirectional DPI firewall between the corporate network and the production floor
- ▶ Complete Network Modeling, including all assets, ports and Networked devices
- ▶ Policy management, per session on the ICS network
- ▶ Asset management, with alerting for changes in firmware, device configuration or critical commands

Industrial Control Systems (ICS), which run the production floor, are fundamentally different from IT networks; therefore, many attacks on the ICS network would not be detected by IT security solutions. What's needed is a solution designed specifically for ICS networks.

Radiflow's end-to-end solution combines its powerful Secure Gateway and its iSID Intrusion Detection System (IDS). Together they enable the detection of sophisticated cyber-attacks aimed at disrupting production processes.

The Radiflow 3180 Secure Gateway provides access to the production floor, with different access rights for each stakeholder.

The Gateway's authentication proxy authenticates each user and restricts the user's access based on role or predefined tasks (e.g., for a maintenance technician, the Gateway would restrict which PLC To access, during which time slot, the types of commands approved for use, etc.) Furthermore, all sessions are recorded for auditing purposes.

Radiflow's secure gateway enables manufacturers to maximize production line uptime by granting remote access to PLC vendors for monitoring their device's behavior and overall health.

Radiflow's iSID Industrial Intrusion Detection System (IDS) was designed to protect production floor operations by capturing and logging suspicious network traffic and detecting anomalies, such as unusual network scanning and changes in the production process model.

This is achieved through real-time analysis of all network traffic, which is validated against a dynamic baseline network behavior model created by the IDS (using passive network scanning).

The Radiflow iSID Industrial Threat Detection & Analysis Platform

The IDS will issue alerts for anomalies in the production floor that may indicate an insider attack (e.g. a malware on one of the PLCs.)

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.

EXPERTISE

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

END-TO-END PORTFOLIO

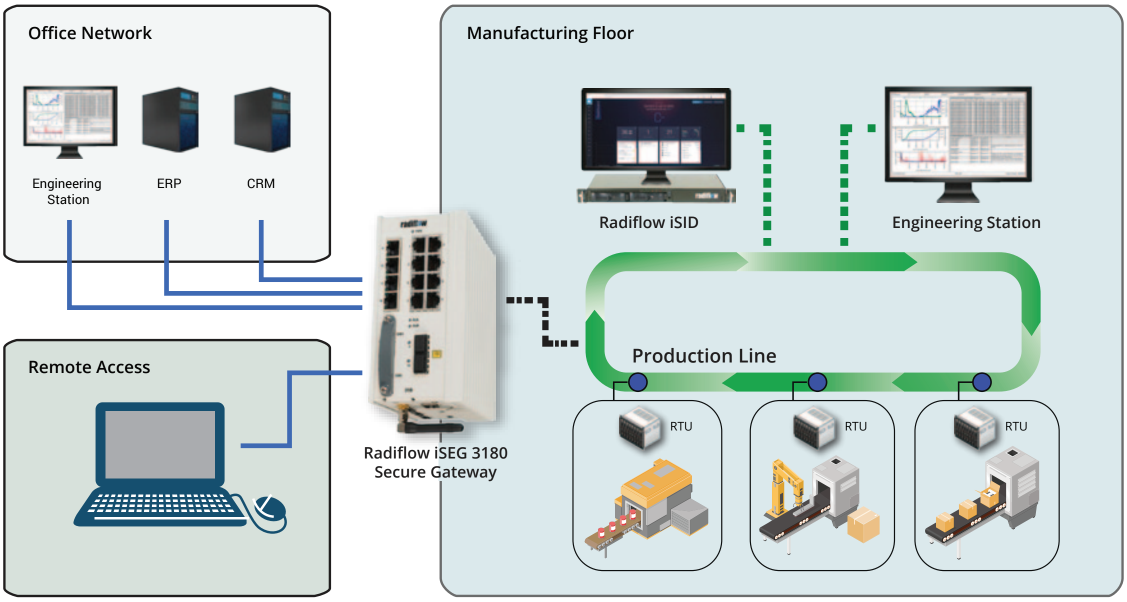
Radiflow offers a holistic portfolio of services and technologies, including secure gateways, Industrial IDS and many more.

Continued...

Key Features

- **Secure maintenance**: Authentication Proxy Access (APA) is used to validate technician credentials and provide preconfigured task-based access over an IPSec VPN tunnel.
- **Maintenance Logging**: Monitor and record all maintenance activities according to preconfigured policies.
- **Secure data collection from the production floor**: Unidirectional DPI firewall between the corporate network and the production floor.
- **Network Modeling:** Display of all network assets and any changes in connectivity, based on self-learning of the ICS network through passive scanning of all data transactions.
- **Anomaly detection:** Including changes in the production process sequence and abnormal memory access, based on the normal application behavior model created by iSID.
- **Policy management**: Definition of maintenance session policies. These rules, based on Deep Packet Inspection (DPI) for industrial protocols, allow the validation of specific commands and operational parameter ranges.
- **Asset management:** Managing, monitoring and auditing the PLCs in the factory. Any firmware changes, configuration or critical command (on/off) will trigger an alert.
- **PLC failures predictive analytics**: iSID's Anomaly Detection function constantly examines the behavior of the PLC. Once a behavioral change is detected the iSID will issue a request for inspecting the PLC.

Implementation



About Radiflow:

Radiflow is a leading provider of cyber security solutions for critical infrastructure networks. Radiflow's comprehensive portfolio of empowers critical infrastructure and industrial enterprises to maintain visibility, control and security of their operational environment. Our intelligent Threat Detection & Analysis Platform for Industrial cybersecurity minimizes potential business interruption and loss within your OT environment.

Radiflow's team consists of professionals from diverse backgrounds, from cyber-experts from elite military units and automation experts from global cybersecurity vendors. Founded in 2009, Radiflow' first solutions were launched at the end of 2011, validated by leading research labs and successfully deployed by major utilities worldwide. More at www.radiflow.com.