

SecFlow®

Secure IIoT Gateways with Edge Computing,
Ruggedized SCADA-Aware Gateway/Switches
and Routers



The SecFlow line of compact gateways/ruggedized switches and routers features a built-in security mechanism designed to control mission-critical operations. They are ideal for industrial IoT (IIoT) applications requiring edge computing, enabling fast, secure and economical deployment of new IoT sites. Allowing secure connectivity over wireless or fiber networks – either public (e.g., cellular) or private, they connect all types of industrial devices, including RTUs, smart meter aggregation devices, IoT base stations or concentrators, CCTV cameras, point of sale devices, Wi-Fi base stations, and more. RADview's security information and event management (SIEM) enables collection of all security events detected in the network. The system collects events from SecFlow devices and displays them visually on customizable dashboards.

SecFlow is also used for operational WANs, providing reliable secure Layer 2 and Layer 3 communication for power utilities, water and gas utilities, public safety and homeland security agencies, as well as intelligent transportation operators.



Part of
RAD's Service Assured
Networking Solutions



Your Network's Edge®

SecFlow

Secure IIoT Gateways with Edge Computing, Ruggedized SCADA-Aware Gateway/Switches and Routers

Key Takeaways:

- Provide next-generation communications for critical infrastructure with advanced routing, switching and security functionalities
- IIoT gateway functionality supports edge computing, trusted connectivity and security, protocol and data bridge, storage and analysis, device access control management and processing of virtual functions for IoT applications
- Comprehensive multiservice support for IEC 61850, IEC 60870-5-104, DNP 3.0, and their serial legacy protocol equivalents reduces the number of network elements and simplifies operations
- Secure and easy to deploy using RADview and zero-touch provisioning
- Certified to meet industrial grade requirements

Use SecFlow for:



- Cyber Shield Overlay for Operational WAN
- Secure Industrial IoT Backhaul



- Industrial IoT Backhaul for Distribution Automation and Smart Metering
- Oil and Gas Utility Communications
- Water Utility Communications

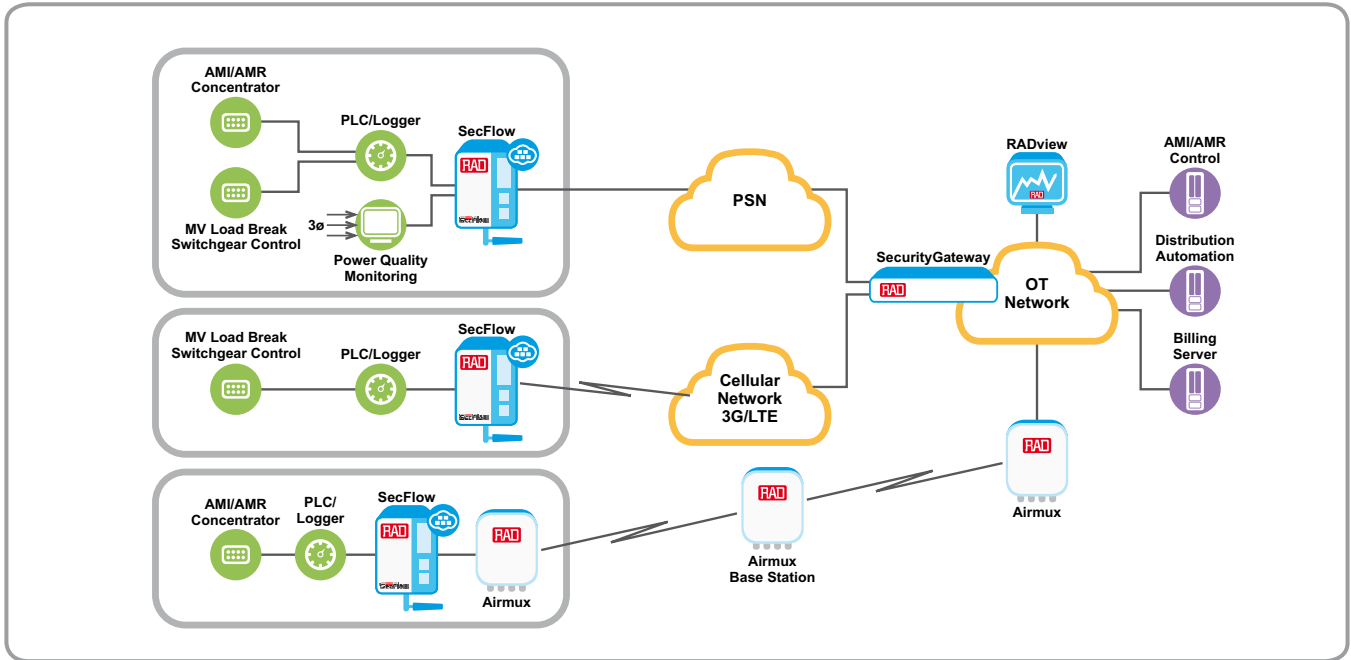


- Highway Communications
- Industrial IoT Backhaul for Remote Unmanned Sites

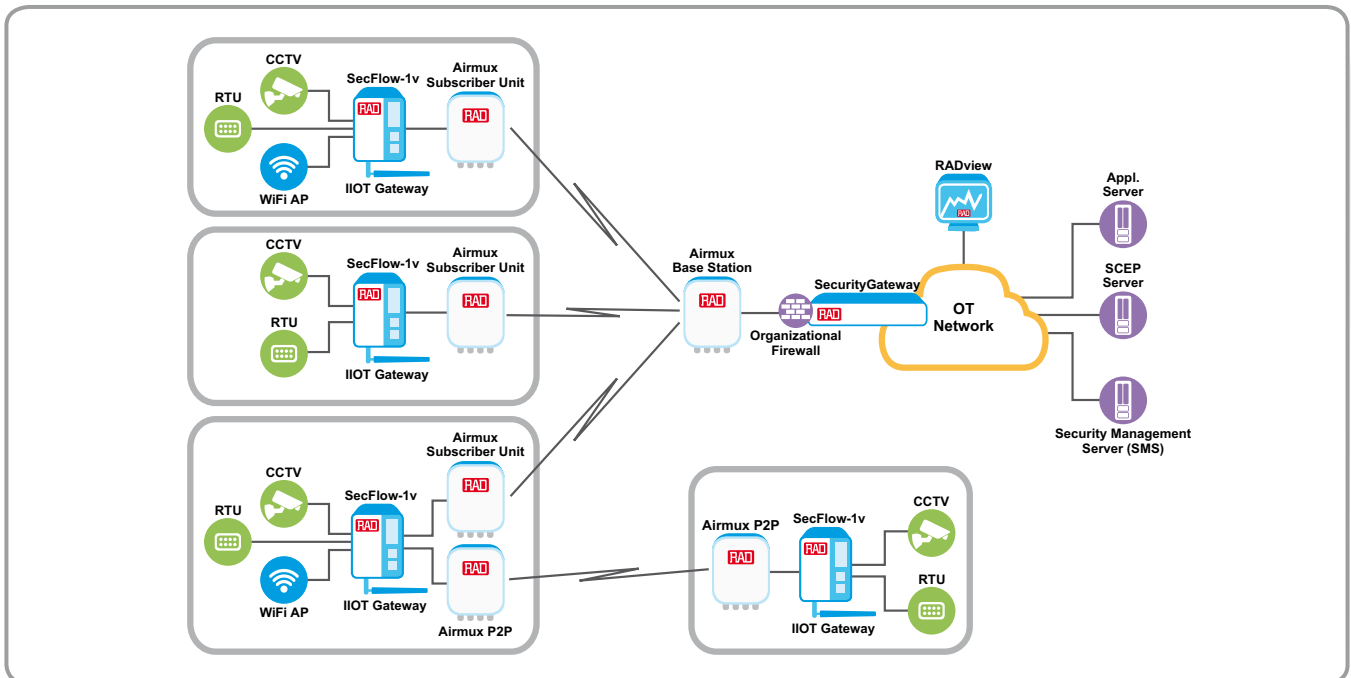


- Industrial IoT Backhaul for Smart Cities

Industrial IoT for Distribution Automation and Smart Metering



Secure Field Area network (FAN) for Power Utilities



Quick Specs:

- Hosting of third-party software using Linux LXD container technology (SecFlow-1v)
- Multiservice support: GbE copper and fiber, serial RS-232/485, Power over Ethernet (PoE)
- Connectivity to remote and isolated sites using a dual SIM
- Single or dual cellular modem for 2G/3G/HSPA+/HSDPA/LTE uplink
- WiFi connectivity as access point
- Dynamic routing with OSPF, BGP, VRF and secure VPN using IPsec, DMVPN and NAT for flexible connectivity
- Cyber security suite: 802.1X, IPsec encryption with automated PKI, ACL, stateful firewall
- Serial protocol handling with transparent tunneling/protocol conversion/terminal server feature set for IEC-60870-5-101, IEC60870-5-104, Modbus RTU to Modbus TCP and DNP3.0 RTU to TCP
- Comply with IEC61850-3 and IEEE 1613
- Zero-touch provisioning, firewall configuration, fault management and reporting, bulk software upgrade and database management using RADview



SecFlow-1v
Secure IIoT Gateway



SecFlow-1
Ruggedized SCADA-Aware
Gateway



SecFlow-2
Ruggedized SCADA-Aware
Ethernet Switch/Router