Application Brief

SCADA Substation Automation

Challenge: Ensuring secure & reliable substation monitoring and control

Supervisory Control and Data Acquisition (SCADA) systems play a crucial role in substation automation, as they enable operators to remotely monitor and control protection relays, circuit breakers, voltage regulators, and other substation equipment. They provide functions like fault detection, alarm management, and automated switching to enhance system reliability and reduce outage durations.

SCADA systems employ communication infrastructure such as wired or wireless networks to establish connections between the control center and remote field devices, enabling real-time data exchange. IEC 104 and DNP3 are two communication protocols commonly used in the field of power systems automation and control.

As power grids become more interconnected and reliant on digital communication systems, ensuring cybersecurity becomes critical. Power utilities need robust communication networks with built-in security features to protect against cyber threats and unauthorized access. This includes encryption mechanisms, authentication protocols, intrusion detection systems, and secure remote access mechanisms to safeguard critical infrastructure and prevent potential disruptions.

Solution: RAD's Secure SCADA communications

RAD provides encrypted end-to-end SCADA communications over fiber and cellular infrastructure:

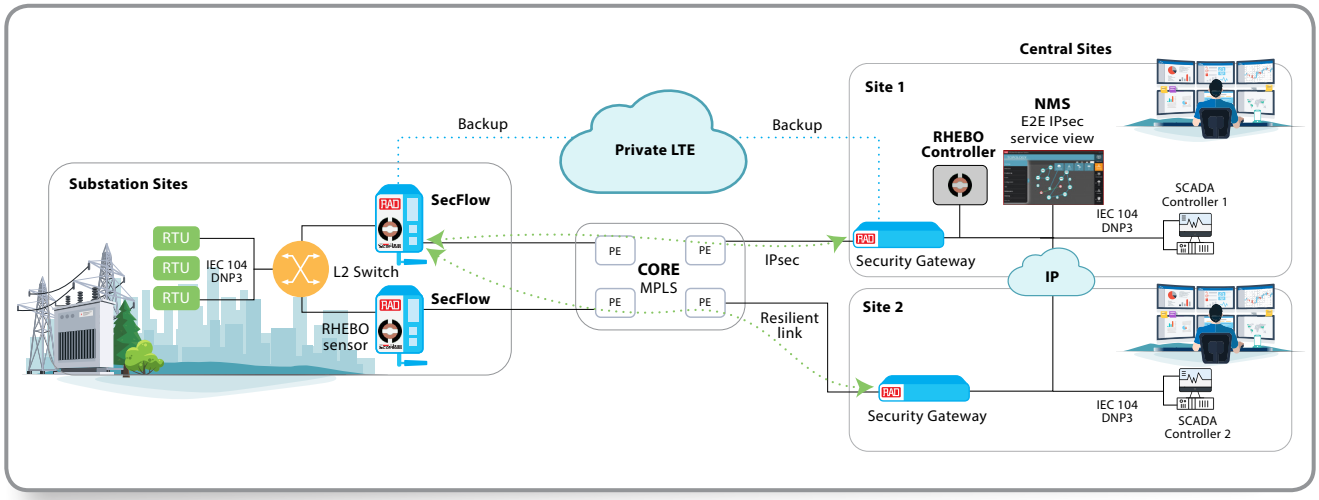
- The SecFlow IIoT gateway is deployed in each substation to provide communications to the central SCADA site via an MPLS network and/or LTE. The LTE/Private LTE can also serve as a backup in case of a failure of the optical link.
- A security gateway is deployed at the SCADA central site to terminate IPsec tunnels and forward the IEC 104 and DNP3 traffic to the SCADA controller.

Resiliency: Robustness and resiliency is achieved by deploying redundant SecFlow units in each substation, as well as two security gateways in each SCADA central sites. Even higher reliability can be achieved by using two cellular modems.

RAD

Your Network's Edge®

Application Brief
SCADA Substation Automation



Security: The SecFlow features a built-on firewall and security protocols such 802.1x, providing protection against unauthorized access. Hosted Docker container technology allows the installation of dedicated OT (operational technology) security applications for holistic security monitoring.

In addition, two IPsec tunnels are configured on each SecFlow unit for communications over the fixed MPLS network, where each tunnel is terminated on a security gateway that is located on a different SCADA central location. To ensure always-on secure communications in case of a failure in the fixed network, two IPsec tunnels are configured over the cellular link as well.

The SecFlow's operating system is based on secure Linux. Services and application run with minimal privileges, and the SecFlow and security gateways feature built-in firewalls. These can be configured to block specific IP and/or MAC addresses, as well as limit communications to allow only certain protocols, such as IEC 104 or DNP3.

Edge computing: The SecFlow features Docker containers that host third-party security applications, such as Rhebo's OT security application. It performs threat detection and network monitoring specifically designed for industrial control networks, as well as records and analyzes data traffic to automatically detect and report any anomalies.

End-to-end management: The SecFlow is managed by RADview, which includes a network element manager, an end-to-end service manager for IPsec and L2 tunnel services, performance monitoring, and fault management. RADview provides intuitive graphic representation of network clouds, links, nodes, end-to-end services, and network status indication. It also provides zero-touch functionality with auto-discovery capabilities, if needed. Fully ITU-T FCAPS compliant, RADview offers security management supporting user access profiles.

Highlights:

- Extensive security for end-to-end protection
- Full redundancy and resiliency for always-on operation
- Multi-protocol and multi-network support
- End-to-end management for automation and control

Learn more about RAD's SecFlow here»

To discuss your Remote monitoring needs for power transmission towers, contact us at market@rad.com.

RAD
Your Network's Edge®