Cybersecurity Services

Improve substation cybersecurity

- Use certified SEL cybersecurity professionals for assessments, solution design, and implementation.
- Understand current security vulnerabilities and steps to achieve NERC CIP compliance.
- Design and implement solutions to secure access, authenticate users, manage passwords, and log security events.
- Test the capabilities of new systems with load simulation.

SEL

Services Overview

Security Assessments

Our general and customizable two-day assessments analyze existing security measures and review security plans, policies, and procedures.

A general cyber assessment provides a snapshot of your cybersecurity posture using ten of the most important security facets, such as assets, controls, and risk management.

A custom cyber assessment offers more detail with a specific focus. For example, a custom assessment might include system audits, compliance reviews (including NERC CIP), system scans, or a review of any of the following:

- **Cyber and physical security programs—**the security of people, property, and policies, including procedures, social engineering, risk awareness, and compliance.
- **Cyber and physical vulnerability—**patching, updates, good practices, gates, guards, and surveillance.
- **Network security—**firewalls, intrusion detection systems (IDSs)/intrusion prevention systems (IPSs), perimeters, and entry points.
- **Information technology (IT), operational technology (OT), and network considerations—**design, efficiency, resilience, and components.

SEL experts certified in compliance, security, IT, and networking provide a report detailing the results of the assessment and actionable areas for improvement.

Solution Design and Implementation

SEL cybersecurity professionals are experts in integrating increased security into existing substations while minimizing the impact to operations. Our solutions portfolio includes:

- Deny-by-default firewall configuration.
- Internet Protocol Security (IPsec) VPNs for site-to-site security.
- Automated password management for SEL devices.
- Event logging via syslog or acSELerator Team® SEL-5045 Software.
- Secure serial and Ethernet designs.
- Proxied command line interface to intelligent electronic devices (IEDs).
- Software-defined networking (SDN) for whitelisting network flows in substation LANs.
- Testing capabilities with load simulations.

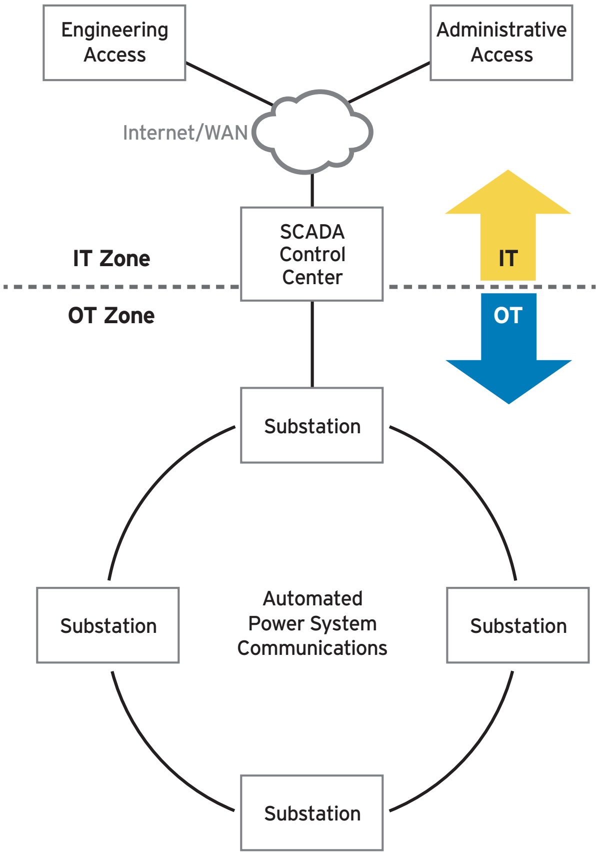
SEL Is the Right Choice for Cybersecurity

Cybersecurity is more vital than ever for the protection of critical infrastructure. Preventing attacks takes knowledge, technology, and skill. SEL helps you develop the skills and knowledge you need to keep your system secure, and we can help you identify and deploy appropriate technology to stop attacks before they even start.

Our extensive understanding of power system protection, automation, integration, control, information security, and compliance is the basis of SEL cybersecurity services. With that foundation, our certified security professionals support your development of sustainable security plans, policies, and procedures with comprehensive security testing and design services, including vulnerability assessments and scanning. Our experts in NERC CIP compliance provide services, including audit testing, that help your system comply with the latest standards.

From substation control systems to corporate security and compliance, our IT/OT approach to cybersecurity provides a unique balance of security and performance to meet the needs of critical, automated systems, including:

- Data priority
- Timing
- Latency
- Dependability
- Determinism
- Resilience/healing



The boundary between IT and OT zones requires an integrated comprehensive approach to cybersecurity.

SEL SCHWEITZER ENGINEERING LABORATORIES

SEL Engineering Services
Tel: +1.509.332.1890 | esinfo@selinc.com | selinc.com

PF00301 • 20181008