Cybersecurity Services

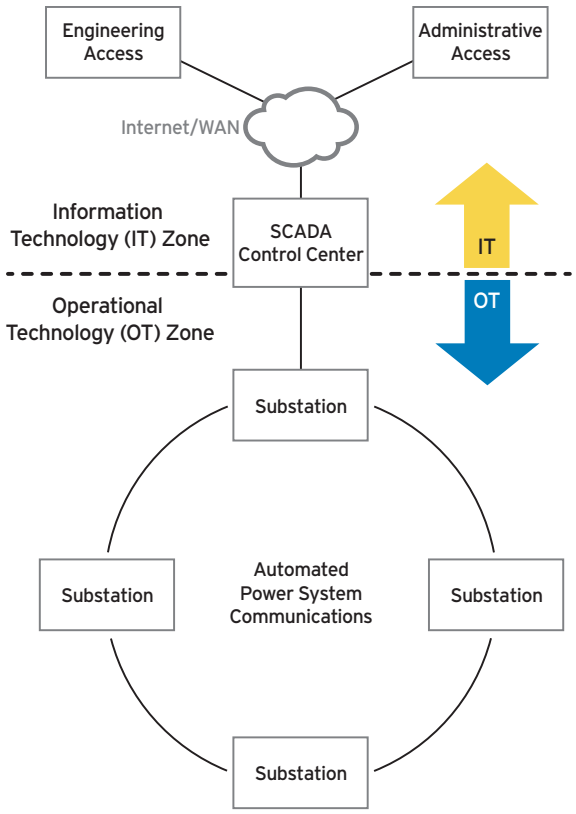
Comprehensive engineering services to secure and protect your assets

- Minimize costs by leveraging the capabilities of security experts and proven technologies.
- Secure critical infrastructure with comprehensive defense-in-depth solutions.
- Mitigate risks with effective assessments that go beyond compliance requirements.
- Comply with regulatory security requirements, including NERC CIP, with the help of accredited industry experts.

Cybersecurity Services From SEL

Now more than ever, cybersecurity is recognized as a vital necessity for the protection of critical infrastructure. Preventing attacks before they happen takes a combination of knowledge, technology, and skill. SEL cybersecurity services are enhanced by our extensive understanding of power system protection, automation, integration, control, information security, and compliance. We provide security testing and design services, including penetration testing, vulnerability assessments/scanning, and experts in compliance including NERC CIP services including audit testing. From substations control systems to corporate security and compliance, our operational technology (OT)/information technology (IT) approach to cybersecurity meets the specific performance 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 Solutions

Today's power systems face a growing number of potential risks varying in scope and complexity. We constantly look for ways to ensure our products and solutions stay ahead of the threat environment. Our solutions portfolio includes:

- Automated password management with SEL and other control system devices.
- Deny-by-default firewall configuration.
- Internet Protocol Security (IPsec) virtual private networks (VPNs) for site-to-site security.
- Risk and vulnerability assessments.
- Co-op- and municipality-focused security/compliance services.
- NERC CIP and FERC Order No. 693 compliance services.
- 10,000 intelligent electronic device (IED) connection directory in ACSELERATOR TEAM® SEL-5045 Software.
- Secure serial and Ethernet designs.
- Proxied command line interface to IED.
- Serial security solutions for SCADA and real-time protection.

Security Assessments

We offer general and customizable two-day assessments that provide an analysis of existing security measures and reviews of security plans, policies, and procedures.

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

- Cyber/Physical Security Program: Security of people, property, and policies, including policies/procedures, social engineering, penetration tests, risk awareness, and compliance.
- Cyber/Physical Vulnerability: Patching, updates, good practices, gates, guards, and surveillance.
- Network Security: Firewalls, intrusion detection system (IDS)/intrusion prevention system (IPS), perimeters, and entry points.
- IT, OT, and Network Considerations: Design, efficiency, resilience, and components.

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

	The OT Zone	The IT Zone
	Environments associated with critical processes or applications typically require OT. OT Zone technologies are often characterized by highly deterministic data paths and data propagation. The robust hardware used with these technologies reliably operates in extreme environmental conditions.	Enterprise or corporate networks typically use IT. IT Zone technologies are often characterized by nondeterministic data paths and propagation and hardware requiring environmental conditioning.
Feature	**OT Typical Performance**	**IT Typical Performance**
Healing	5 to 15 ms	50 to 150+ ms
Asymmetry	0.5 ms or less	30 ms or less (VoIP)
Dependability	Mean time between failures (MTBF) >100 years	MTBF <5 years
Latency	4 to 10 ms	150+ ms
Precise Timing*	Precision Time Protocol/IRIG-B (µs)	Simple Network Time Protocol (ms)
Security Approach	Availability > Integrity > Confidentiality	Confidentiality > Integrity > Availability
Environment	−40° to +85°C (−40° to +185°F)	0° to +40.5°C (+32° to +105°F)

*Note: Precise timing devices used by SEL include antispoofing features not typically available in IT-based solutions.

OT and IT systems are designed for different purposes and therefore have different performance characteristics.

A Unique Approach Using a Proven Strategy

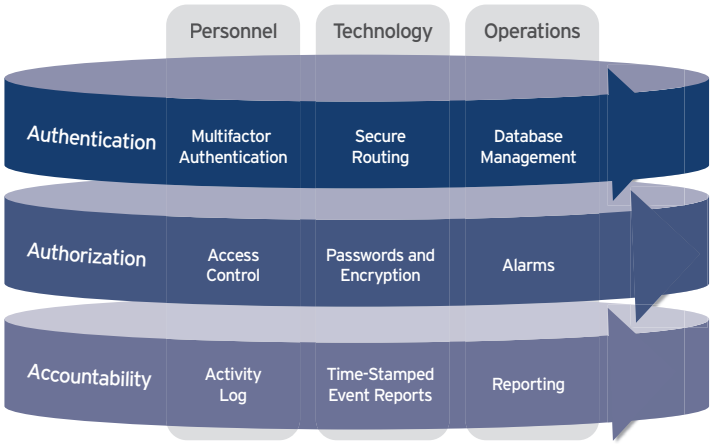
An IT approach to cybersecurity is typical of enterprise or corporate networks, which are designed from the user interface down to the IEDs.

At SEL, we design security. Substations and control systems have different security requirements than typical corporate assets. Our approach integrates layered security throughout the system, addressing the specific communications and security needs of critical systems.

We have certified security professionals support your efforts in developing sustainable security plans, policies, and procedures.

CISSP is a registered mark of the International Information Systems Security Certification Consortium in the United States and other countries.

The SEL Engineering Services team applies a mature cybersecurity strategy based on experience designing and building devices and solutions for mission-critical power systems. This strategy includes a repetitive process of planning, implementation, measurement, and documentation.



Layered cybersecurity addresses multiple factors across an organization.

SCHWEITZER ENGINEERING LABORATORIES

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

© 2013—2017 by Schweitzer Engineering Laboratories, Inc.
PF00301 • 20170227