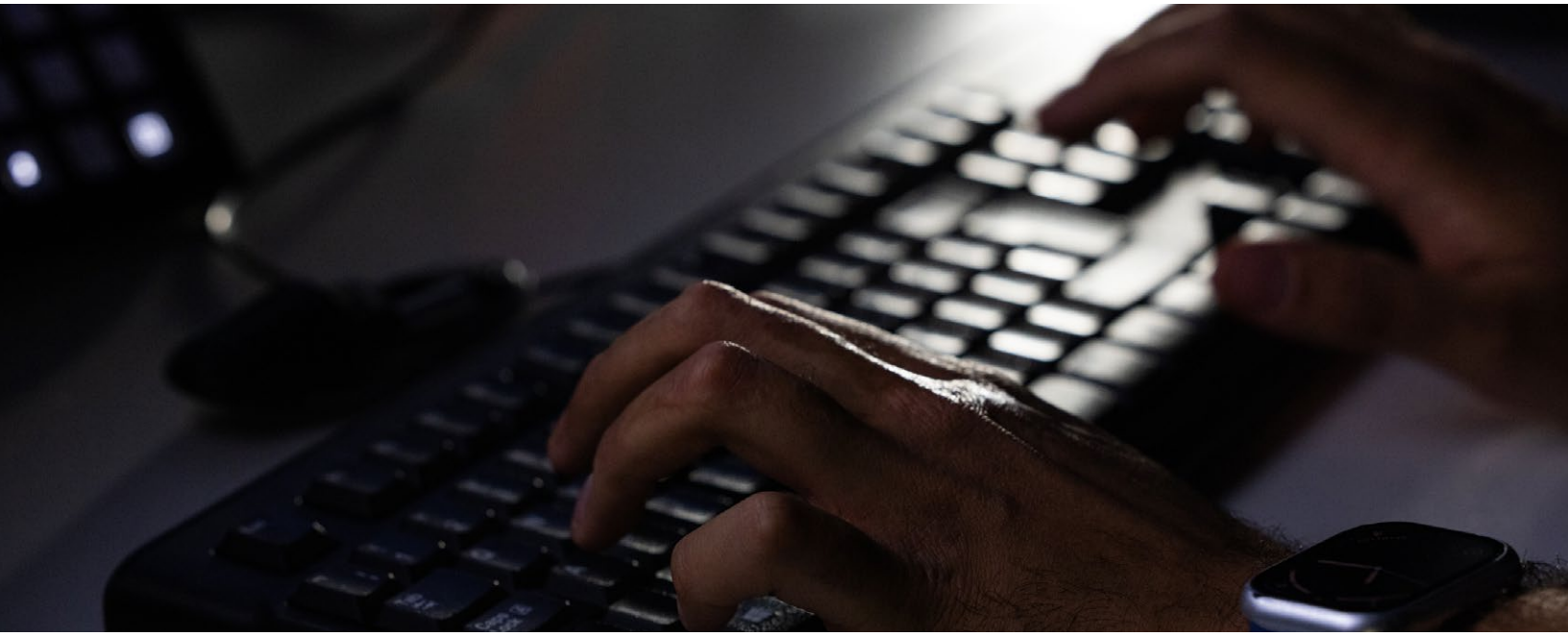
SEL Cyber Services Approach



Advance your security using SEL expertise and engineering rigor

- Strengthen operational technology (OT) security with an architecture-first approach built on defense in depth and zero trust.
- Align your security strategy with international frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and IEC 62443, while tailoring controls to meet operational goals and risk tolerance.
- Reduce risk through effective architecture, rigorous project execution, and adaptive management.
- Work with OT specialists who assess, design, deploy, monitor, and maintain secure industrial systems across the full system life cycle.

Our Philosophy

SEL Cyber Services helps organizations at every stage of the cyber-maturity journey improve system security. SEL achieves this through effective governance, purposeful architecture design, and adaptive security management. When you work with SEL, you gain a collaborator with decades of full-service OT engineering expertise and extensive experience applying defense-in-depth and zero-trust principles.

Governance as the Foundation of Security

Effective cybersecurity begins with governance. SEL helps organizations identify and create the policies and procedures needed to keep systems secure for the long term.

The Economics of Effective Security

When designing security into a system, not all controls provide equal value. SEL prioritizes security measures that provide the most protection with the least overhead, such as proactive network architecture and passive defense, to reduce risk while keeping long-term cost and complexity low.

Cyber Maturity as an Ongoing Journey

The pathway to cyber maturity requires continuous improvement. SEL Cyber Services assesses cyber maturity and provides tailored recommendations to strengthen security programs, whether new and ad hoc or mature and advanced. Clear governance, consistent execution, and data-driven improvement support progress at every maturity level.

Cyber-Maturity Model

LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Incomplete • Operates ad hoc and without structure • Lacks network visibility and cybersecurity governance strategy • Completes projects inconsistently	**Initial** • Reacts unpredictably • Considers assessments and strategy development • Completes projects, but often late and over budget	**Managed** • Plans and tracks work • Develops governance strategy, gains network visibility, and expands controls • Executes, measures, and controls projects	**Defined** • Acts proactively, not reactively • Codifies cybersecurity strategy and explores advanced network designs (defense in depth, layered networks, and zero-trust architecture) • Applies organization-wide standards across projects, programs, and portfolios	**Quantitatively Managed** • Is driven by data • Strengthens cybersecurity strategy with proactive network architecture, defense in depth, and clear parameters • Uses quantitative performance improvement objectives that are predictable and aligned to meet the needs of internal and external stakeholders	**Optimizing** • Adapts and improves continuously • Plans for future regulatory compliance • Builds ongoing resiliency into network strategy • Responds to change and pursues opportunities with agility

The SEL Design Process

SEL follows a structured process to design, validate, and implement security measures:

Opportunity and Planning

Understand mission requirements, risk context, and compliance needs.

Definition and Development

Design architecture, specify controls, and implement configurations within secure environments.

Testing and Validation

Verify security controls through documented reviews and factory acceptance testing in representative, real-world environments.

Commissioning and Closeout

Validate the final system state, and transition to operational support.

The Base Layer of Security

Effective network architecture is foundational to OT security. SEL designs networks with clear enforcement zones, strong segmentation, and deterministic communications. This base layer reduces the attack surface, enables fast recovery, and improves system visibility.

Key architectural elements include:

- Industrial firewalls engineered for OT environments.
- OT software-defined networking (SDN) for allowlisted, deterministic traffic flows.
- Segmentation aligned with Purdue Enterprise Reference Architecture principles.

Security and System Management Services

SEL complements architecture with integrated security and management services. These include:

- Asset management and configuration hardening.
- Access control and identity management.
- Centralized logging and monitoring.
- Patch management, backup, and recovery.

These capabilities facilitate secure, reliable operations while simplifying long-term system management.

Life Cycle Support

Whether cybersecurity systems are newly commissioned or well established, SEL Cyber Services helps organizations along every stage of cyber maturity. SEL provides support for:

- **Cyber Maintenance**—Updates, assessments, and configuration reviews.
- **Cyber Monitoring**—Continuous visibility into network activity and anomalies.
- **Cyber Readiness and Response**—Proactive planning and expert incident support.

Contact us today to learn more about our services.

selinc.com/services/cyber-services

SEL SCHWEITZER ENGINEERING LABORATORIES

Making Electric Power Safer, More Reliable, and More Economical
+1.509.332.1890 | info@selinc.com | selinc.com

LM00585-01 • 20260910

WORLDWIDE 10 years WARRANTY