# SEL Secure Solutions for Water and Wastewater

## SEL experts and solutions help you secure critical infrastructure

- Create a baseline of your current operational technology (OT) system, and identify potential vulnerabilities.
- Address gaps with secure network solutions, and meet the highest security standards and controls with minimal disruption to operations.
- Streamline cybersecurity monitoring efforts with centralized asset management, software and firmware updates, event logs, and password rotations.
- Detect cyber events, and ensure an effective response and prompt system restoration.

# Consider these questions to identify and address cybersecurity gaps

RESOURCES

### How is your cybersecurity team structured?

IT and OT systems have different performance requirements. We can help you implement cybersecurity strategies that minimize disruption to OT environments.

### Who manages your OT communications systems?

Day-to-day operations require specialized skills. We offer knowledgeable staff and resources to assist you with each aspect of OT system ownership.

### Who monitors the security of your system?

Proper design of event notification systems is crucial to situational awareness. We help design and implement turnkey security monitoring solutions, and we offer 24/7/365 monitoring services via our Security Operations Center.

FRAMEWORK

### Do you have an OT cybersecurity framework?

SEL secure solutions are designed around the National Institute of Standards and Technology (NIST) cybersecurity framework, which enables assessment adherence with other security frameworks, such as the American Water Infrastructure Act (AWIA). We can help develop the necessary risk management and emergency response plans. We can also help you prioritize a road map for implementing the NIST SP 800-82 and ANSI/AWWA G430 security standards along with constant system monitoring.

### Are you required to comply with cybersecurity standards?

We offer assessment services that confirm adherence with cybersecurity requirements, and we can provide hardening guides for your systems' computers, IEDs, and controllers.

### Is physical security integrated into your cybersecurity framework?

Physical security is part of the defense-in-depth approach to cybersecurity. SEL solutions consider physical security, along with natural and environmental disasters, to provide a holistic view of cybersecurity and address AWIA physical security requirements.

### Is vendor supply chain security one of your current considerations?

At SEL, we understand the importance of securing our supply chain and follow rigorous internal and external processes to qualify our products and applications. We own every line of our software and firmware code. This code is digitally signed, never shared outside of SEL, and continuously monitored for new threats. When you choose an SEL solution, you can be sure it is secure.

## CYBERSECURITY ARCHITECTURE AND NETWORK DESIGN

### When was the last time you had a third-party network assessment?

SEL experts stay abreast of the latest critical infrastructure threats, security controls, and indicators of compromise, especially those for the electric utility and water utility sectors. Employing a third-party assessor contributes to cost-effective and impartial analysis of the cybersecurity capabilities and security posture of your control systems. We offer onsite assessment, security control reviews, and compliance audits to support your needs.

### How do you secure network links for remote access?

We provide network design, consulting, and implementation of secure, encrypted remote access solutions.

### Have your OT devices been hardened?

We can ensure computing and control system device settings are locked down according to each device's application. We can also provide documentation about open ports, policies, and services that require additional system mitigation. In addition, we offer networking solutions that use software-defined networking (SDN) to whitelist approved network flows, disable unused ports and services, and eliminate several attack vectors of traditional LANs.

## PROCESSES TO MAINTAIN AND MONITOR OT SYSTEM SECURITY

### What is the process and strategy for managing your OT system assets?

Asset management for large OT systems can be a challenging task. SEL experts can identify asset management solutions, including continuous monitoring for patch and maintenance processes, and can provide complete OT system deployment.

### How do you manage version control of system settings?

Creating and maintaining a baseline of system settings is a crucial component of system ownership. We can provide OT asset management software that simplifies system baselining and version control.

### How do you approach patch management?

Understanding which patches are applicable and how to securely deploy updates can be challenging. We offer patch management services that monitor vulnerability notices, and we deliver a tested mitigation plan.

### How are user accounts managed for your OT devices?

OT networks have many devices with several permission levels. Passwords must be securely rotated, and user permissions must be assigned appropriately. We offer centralized user account management to simplify operations and user account maintenance.

### Are you prepared to detect cyber events on your system?

There are many indicators of compromise that point to potentially malicious activity and known tactics that attackers use. SEL secure solutions detect intrusions, and we provide playbooks for response procedures.

### Do you review recovery processes via tabletop exercises?

Policies and procedures are most beneficial when personnel are properly trained. We offer tabletop exercises to test personnel knowledge and the effectiveness of response procedures. Services like automatic settings backup can aid in the recovery process.

## Why SEL?

With extensive OT and cybersecurity expertise, we build effective turnkey solutions that improve cybersecurity and streamline asset management and ongoing maintenance. SEL understands the U.S. Environmental Protection Agency's direction, requirements, and tools and can help with system assessments, security control plans, risk management, and technology deployment. An SEL secure solution will be ready to defend against and prevent vulnerabilities and will not negatively impact other OT system requirements. SEL has certified engineers to help you develop and train for business continuity, risk management, and emergency response plans. SEL offers a broad portfolio of solutions and experts to do the work, as needed.

## Next steps

Contact SEL at **secure@selinc.com** to connect with our team of OT cybersecurity experts.

SEL SCHWEITZER ENGINEERING LABORATORIES

SEL Engineering Services
+1.509.332.1890 | secure@selinc.com | selinc.com


PF00661 • 20200622