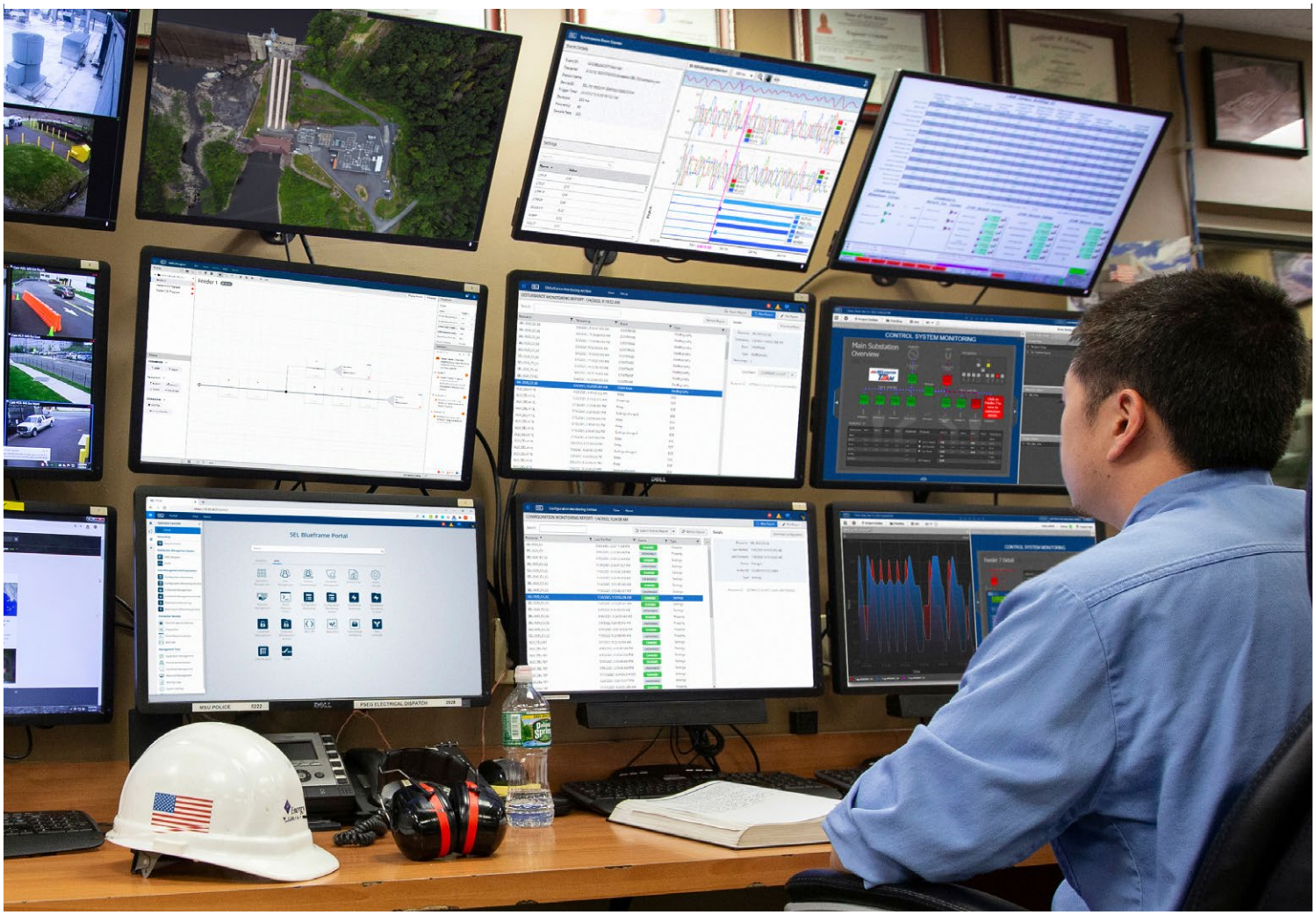
CYBERSECURITY SOLUTIONS

Zero Trust for Industrial Control System (ICS) and Operational Technology (OT) Cybersecurity



In both the public and private sectors, zero trust continues to gain popularity as a concept for securing systems and networks. Executive Order 14028, "Improving the Nation's Cybersecurity," issued on May 12, 2021, called upon the federal government to advance towards a zero-trust architecture. At the same time, private industry is pursuing zero trust as a cybersecurity best practice for today's threat landscape.

Based on our in-depth understanding of ICS OT requirements, SEL works with you to implement a customized zero-trust architecture. Our solutions are precisely tailored to your priorities and the maturity level of your system, from pre-zero trust through advanced stages.

While the concepts are consistent, there is no one-size-fits-all zero-trust solution. Special considerations must also be made when applying zero trust to ICS OT environments.

A zero-trust architecture continually evaluates information access. There is no implicit access without explicit permission, which is only granted for a limited period.

Implementing an ICS OT Zero-Trust Architecture

The following steps outline the process for implementing a zero-trust architecture within ICS and OT networks:

1. Define the Protect Surface

Clearly identify and document the protect surface, which includes the critical data, assets, applications, and services an organization needs to fulfill its mission.

Critical components of the protect surface include:

- Information that serves the organization's mission and the systems maintaining that information.
- Assets that are critical to the organization's mission.
- Computing systems and software used to interact with the information and assets.
- Functions and services necessary to complete the mission, maintain assets, and generate deliverables.
- Set of personnel roles and skills necessary to maintain and deliver the mission.

2. Map the Information Exchange

Once the protect surface is defined, analyze the ingress and egress of information exchange between systems, applications, and users to fully understand who is accessing information and how it is being used. This determines where to place controls and least-privilege access.

Define the following to map the information exchange:

- Dataflow diagrams with directionality
- Devices that touch the data
- Users that touch the data
- Functions that touch the data
- Data flow paths

3. Network the Information Exchange

Where possible, define where to segment and isolate the information exchange between the organization's resources. This creates microperimeters between the assets and information resources and the subjects that need to interact with them.

4. Enforce a Trust Policy

Enforce a trust policy, which is the allowed function for execution and information exchange between an organization's resources over defined data paths. This is ideally under continuous evaluation with provisioning and deprovisioning of resources and access points.

5. Monitor and Maintain a Trust Service

Continuously monitor all information exchange on the network.

Steps to Begin Your Zero-Trust Journey with SEL

As noted earlier, there is no one-size-fits-all zero-trust solution. In addition to practices like multi-factor authentication and strong boundary segmentation, the following are available for consideration as we work together to create an optimal cybersecure solution.

OT SDN

Advance your organization's cybersecurity with an OT Ethernet networking solution that offers a zero-trust architecture by default. OT software-defined networking (SDN) from SEL is deny-by-default for all connected devices, which means that no communications happen on the network that the system owner has not authorized. Instead, all primary and backup communications paths are proactively programmed using the SEL-5056 Flow Controller.

In addition to its security benefits, OT SDN greatly reduces the complexity of integrating detection solutions and supports network visibility, metering, flow auditing, security alerts, improved reliability, and high-speed performance, all of which contribute to the network foundation of zero trust.

SEL Cybersecurity Services

Partner with SEL on cybersecurity solutions and services that help your organization meet its zero-trust goals. We support organizations from the pre-zero-trust stage through intermediate and advanced stages and customize projects according to specific priorities and goals. Services include:

- OT system baselining.
- Assessment services and risk remediation plans based on National Institute of Standards and Technology (NIST), North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), and IEC 62443 cybersecurity frameworks.
- Design and implementation of secure communications networks, access management, and remote access solutions.

Third-Party Technology Integration

SEL solutions complement third-party management and monitoring tools, including network intrusion detection systems and policy engines. Work with SEL to evaluate and integrate these tools into your zero-trust solution.

Our cybersecurity experts are ready to partner with you on implementing zero-trust solutions. For more information, contact SEL Infrastructure Defense at secure@selinc.com.

SEL SCHWEITZER ENGINEERING LABORATORIES

+1.509.332.1890 | secure@selinc.com | selinc.com

PF00692 | 20230104