CYBER SERVICES

SEL Cyber Services Approach to System Security

Charles Carroll
Schweitzer Engineering Laboratories, Inc.

This executive overview is provided by SEL Infrastructure Defense Cyber Services (CS) to describe the high-level philosophy, methodology, and security controls that SEL incorporates into the overall architecture of industrial control systems (ICSs). This approach follows the principles of defense in depth and zero trust to align with common security standards, such as those provided by the National Institute of Standards and Technology (NIST), NIST Cybersecurity Framework (CSF), and International Electrotechnical Commission (IEC) (IEC 62443, specifically).

The controls mentioned in this overview are not all-inclusive in terms of the technology available, nor is the implementation meant to be prescriptive. Many additional security controls exist that can help meet your desired risk profile; this overview describes a basic tool set and how it may be implemented in a typical control system.

No one solution is effective or logical for all system owners; SEL CS designs each system to uniquely support the mission of the customer company in terms of both effectiveness and affordability. Therefore, our intent with this overview is to provide a general understanding of how SEL uses technology to support its mission of making electric power safer, more reliable, and more economical. The following sections describe how defined processes, purposeful architecture, and continuous monitoring can improve the security posture and system visibility of an organization.

Overview

The true cybersecurity posture of an organization is best illustrated by the maturity of its cybersecurity program. Maturity, in terms of security, begins with having a clear vision and plan of which controls should be implemented (a baseline knowledge of the system and what needs to be protected) and ends with a cycle of constant metric-based improvements and optimization, as shown in Figure 1.1.

LEVEL 0	Incomplete ▪ Operates ad hoc and without structure ▪ Lacks network visibility and cybersecurity governance strategy ▪ Completes projects inconsistently
LEVEL 1	Initial ▪ Reacts unpredictably ▪ Considers assessments and strategy development ▪ Completes projects, but often late and over budget
LEVEL 2	Managed ▪ Plans and tracks work ▪ Develops governance strategy, gains network visibility, and expands controls ▪ Executes, measures, and controls projects
LEVEL 3	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
LEVEL 4	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
LEVEL 5	Optimizing ▪ Adapts and improves continuously ▪ Plans for future regulatory compliance ▪ Builds ongoing resiliency into network strategy ▪ Responds to change and pursues opportunities with agility

Figure 1.1: Cybersecurity Maturity Model

Security Philosophy

Governance is fundamental to the overall approach of securing a system. Governance refers to the policies, procedures, and standards that inform security decisions in the context of the controls and architecture chosen to secure a system. Often, governance is implemented using published standards along with organization-specific modifications or additions to ensure that cybersecurity exposure is aligned with risk tolerance.

SEL Infrastructure Defense promotes adherence to the NIST CSF. This framework is not prescriptive in requiring the use of specific technology or controls. Instead, it seeks to implement a defense-in-depth approach by using a systematic philosophy to identify areas where existing controls or processes can be improved or new controls or processes should be implemented. Additionally, the framework is not a one-time solution; rather, it is a process of continuous improvement. System architecture should be designed with security in mind, and because new threats are always emerging, it should incorporate a process of continuous improvement.

The Economics of Security

When designing security into a system, the first questions to ask are: Where will controls be implemented? How will they work? And who will manage them? Answering these questions requires balancing cost against the benefits to the overall security posture of the system.

Among security measures, system architecture provides the greatest security value at the least ongoing cost. At the opposite end of the spectrum, offensive measures offer minimal value, incur high costs, and raise ethical and legal concerns. Between these extremes lie passive defense, active defense, and intelligence, each offering progressively less value and higher costs as they shift from proactive to reactive. See Figure 1.2.

This overview focuses on the first two security measures above—architecture and passive defense—as they involve technical components. The other security measures, such as active defense, intelligence, and offense, are part of ongoing security operations after the system is commissioned.

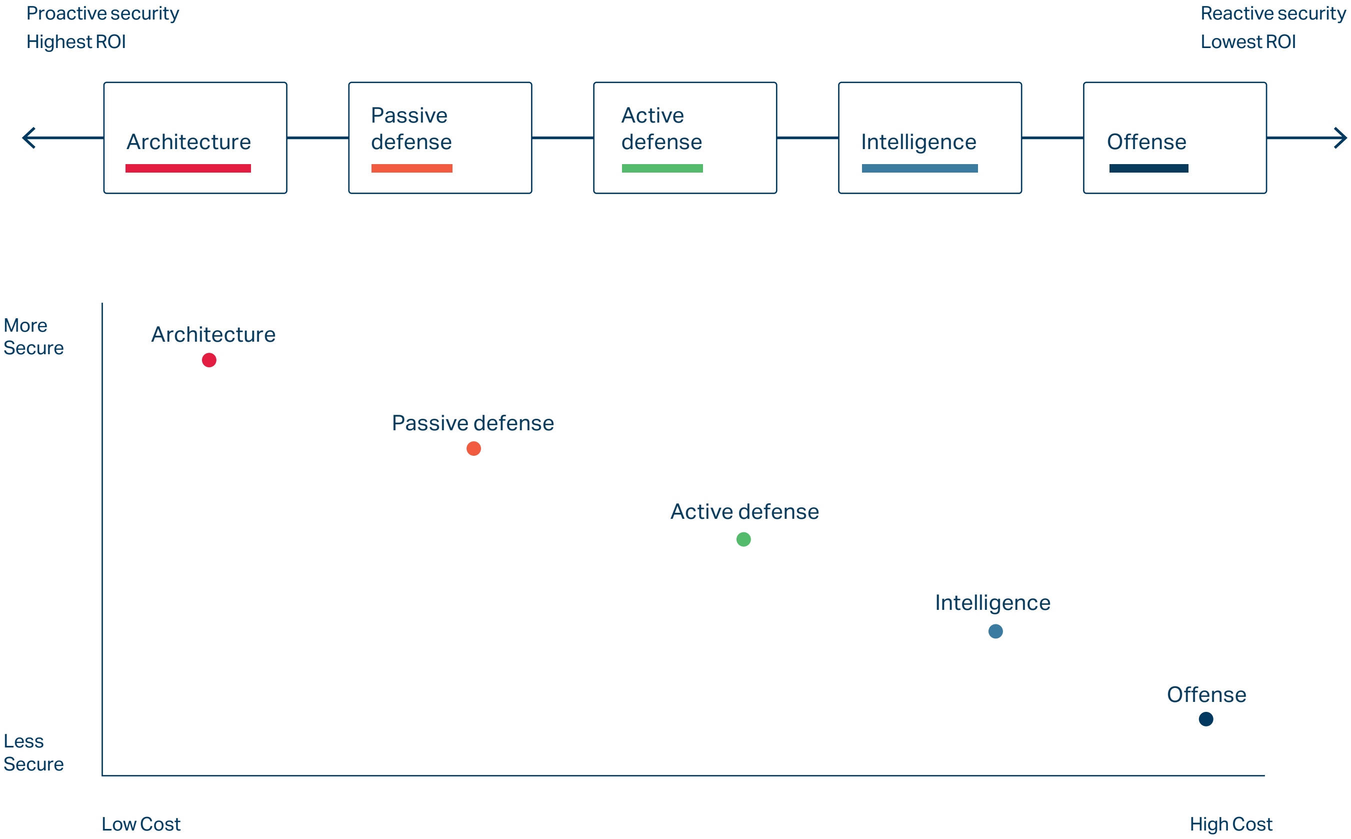

Figure 1.2: The Economics of Cybersecurity

Design Principles and Standard Services

Risk Assessment

Before designing a network, it is essential to understand the security needs of a system in context. This context includes the business goals of an organization, potential threats pertinent to the nature of its business and the data it handles, regulatory requirements, and best practices of network security. These factors should inform the design of the network and ensure that it aligns with the specific needs and security considerations of the business.

With the initial understanding of the business context established, the design phase incorporates this information to plan for appropriate security measures. During the design phase, the risk assessment is more specific and evaluates the proposed network architectures, potential vulnerabilities associated with various design choices, and mitigation of these risks through design strategies and security technologies. Once the design is complete, a detailed risk assessment is performed to validate the design decisions. This involves a thorough evaluation of the planned network infrastructure, ensuring that all identified risks are adequately addressed with the chosen security controls and that the design aligns with cybersecurity best practices.

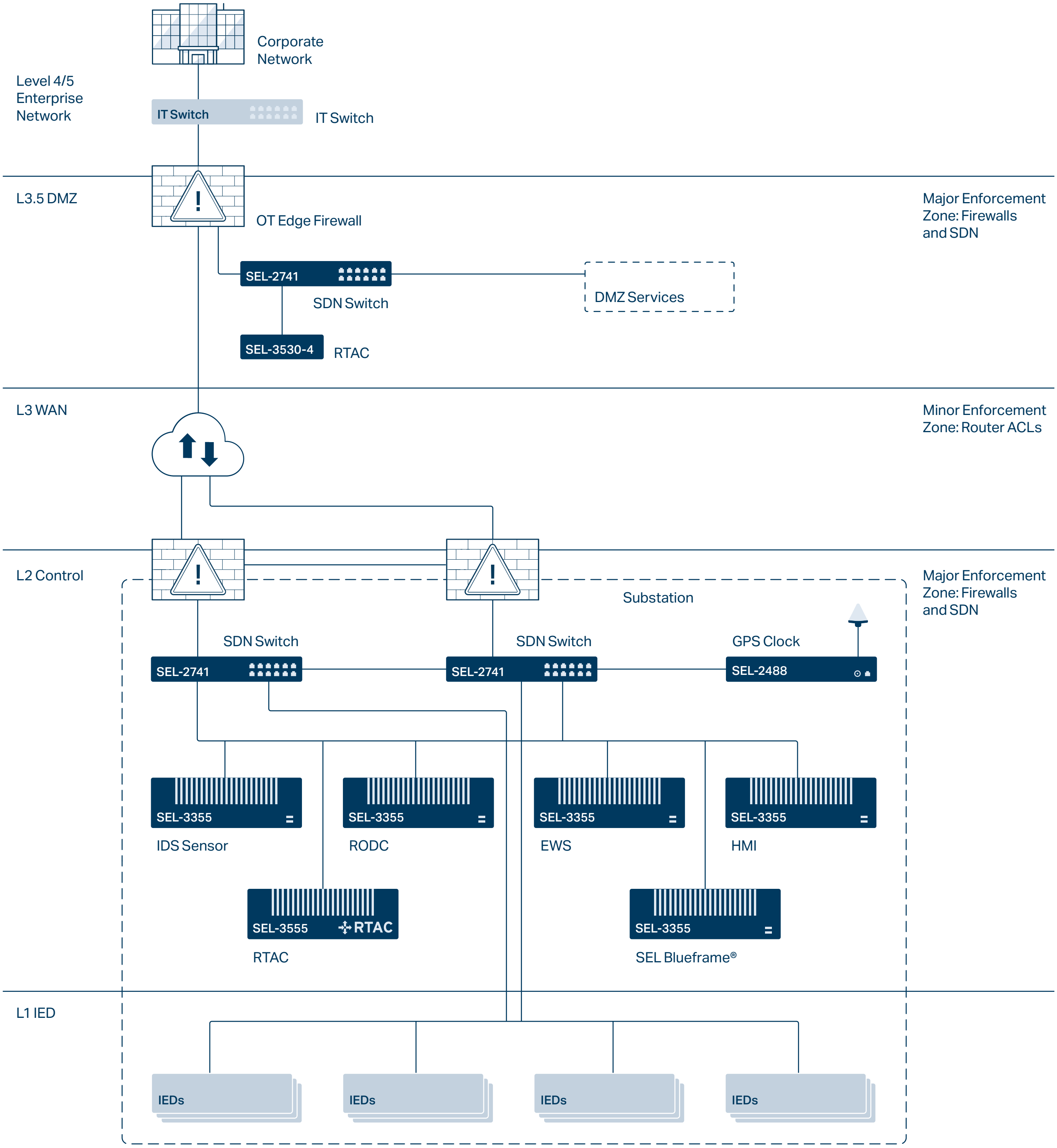

Figure 1.3: Purdue Enterprise Reference Architecture

Architecture

System architecture is fundamental to a secure ICS design. Architecture can be influenced by existing corporate security requirements or by leveraging a published framework. In Figure 1.3, the Purdue Enterprise Reference Architecture (PERA) is used to classify assets in levels and then apply the appropriate amount of security between and within levels based on risk tolerance. This high-level architecture can vary widely among organizations, but PERA is a good starting point in designing which data will flow between zones and which controls are needed to govern how those data move between zones.

In this example, the operational technology (OT) system is segregated from the business network and a demilitarized zone (DMZ) that filters data that need to be exchanged between networks. Controls between networks are specified using firewalls and software-defined networking (SDN) between Level 4 (L4) and L3.5 as well as the access control lists (ACLs) on L3. Additional firewalls exist between L3 and L2 as well as L2 and L1, with OT SDN also present between L2 and L1.

DMZ services are included to provide centralized authentication services, antivirus (AV), public key infrastructure, multifactor authentication (MFA), and backup and recovery as well as view-only information from a Dragos or Nozomi Networks intrusion detection system (IDS) or SEL Blueframe® platform. These components are described in greater detail later in this overview.

The diagram in Figure 1.3 is not meant to be prescriptive, since every organization has a different architecture and risk tolerance. However, it is an example of a purposeful approach to securing and supporting the safe and reliable operation of a system.

SEL Project Life Cycle

SEL CS has an established, well-tested project life cycle procedure. This procedure is referred to internally as PROC-0206 and governs how an SEL Engineering Services (ES) project is executed. For each SEL ES project phase, the required documentation and/or deliverables must be completed before that phase can be exited and the next phase can begin. See Table 1.1 for the SEL phase gate approach to project execution.

PHASE 0 Opportunity	**PHASE 1** Planning	**PHASE 2** Definition	**PHASE 3** Development	**PHASE 4** Testing/ Validation	**PHASE 5** Commissioning	**PHASE 6** Close Out
Proposal development	Project planning and kickoff	Functional design specification creation	Security control and architecture design	Functional and staged factory acceptance test (FAT)	Installation and site acceptance test (SAT)	Project evaluation and life cycle support
Request for proposal (RFP) evaluation by solution architect	Stakeholder identification and secure workspace development	Identification of specific compliance or customer requirements		Security configuration and specifications verified	Oversight by qualified Cyber Services experts in compliance with onsite security protocols	Initiation of services for ongoing needs for cyber maintenance, monitoring, and readiness and response

Table 1.1: SEL Project Phase Gate Overview

Each group within SEL ES (protection, automation, and cybersecurity) has additional processes that are mandated when executing their individual project functions. Each group performs various activities to successfully complete a project. The following sections describe how these phases fit into the execution of the security-focused portion of a project.

Opportunity

During this phase, SEL evaluates the customer's request for proposal and their requirements to determine which SEL solution fulfills the customer's needs. Security and/or network requirements of the project are examined by an SEL security solution architect, and the basic solution architecture is defined and reviewed by an SEL security engineer for technical feasibility.

Planning

The planning phase is when the project is initialized. In the planning phase, the personnel who will be part of the project are identified. This includes identifying critical areas of expertise and any specific clearances, certifications, and/or specialized knowledge required to successfully complete the project. After the project personnel are defined, a secure workspace is created in the SEL internal network for storage of project documents, communications, and schedules. Access to this workspace is restricted according to the principle of least privilege.

Project stakeholders from all involved organizations attend the kickoff meeting. During this meeting, all project stakeholders are introduced to the overall project team, which is an important step to combat phishing and masquerading attempts to obtain sensitive project information.

As part of the project communications plan, a secure method of transferring documentation, schematics, and sensitive information outside of standard communications channels, such as email, is established, with access restricted to a limited number of necessary personnel. This prevents the accidental dissemination of information through email groups and provides an alternate channel for the transfer of information for processes, such as the exchange of hash values or digital media. The SEL Secure File Transfer Appliance (FTA) is often the agreed-on method for information exchange. The FTA is a secure internet-accessible appliance that allows granular control of read/write permissions for established users in a secured workspace. Workspaces in the FTA are temporary, and all data are securely erased upon expiration. Additionally, all files uploaded to the FTA are scanned for malware.

Definition

A functional design specification (FDS) is created during the definition phase. This document verifies the customer design requirements and describes how the system will be built to fulfill those requirements. Additionally, it addresses items such as specific security controls, additional controls as specified by customer policy, and steps to meet compliance goals.

Development

Upon approval of the FDS, the development phase begins. All system development takes place within SEL secured sites, project data is stored on SEL secured networks, and only SEL-approved devices are used. Individual project device security controls are implemented in the project development process and the device configurations.

Testing and Validation

The testing and validation phase begins during the development phase and includes factory acceptance testing. During testing, device configurations are reviewed to ensure they meet the security controls as specified in the FDS. At the end of factory acceptance testing, a report is provided detailing the test results, device audit reports, and any action items that need to be addressed.

Commissioning

Customer internal and system security controls govern onsite security activities during commissioning or site acceptance testing. SEL CS employees comply with security and safety policies while testing the final state of the delivered system. This ensures that all controls tested during factory acceptance testing have been validated, any remaining action items have been resolved, and the system is ready to be placed in production.

Life Cycle Services

SEL CS provides comprehensive support beyond final commissioning to maintain, monitor, and enhance security throughout the operational life of an ICS or OT system. These services are designed to maximize cybersecurity effectiveness with proactive planning and response and staff augmentation from experienced SEL CS personnel. See the following subsections outlining SEL CS life cycle services offerings.

Cyber Maintenance

Cyber maintenance services focus on preserving system reliability and security through routine updates and assessments. Key activities include:

- Applying software and firmware updates to maintain compliance and mitigate vulnerabilities.
- Reviewing security logs to identify optimization opportunities.
- Performing periodic system assessments to detect and address potential issues before they escalate.

Cyber Monitoring

Cyber monitoring services provide real-time visibility into network activity and threat indicators. SEL CS acts as an extension of your security team by:

- Monitoring network traffic for anomalies and alerting designated personnel when suspicious activity is detected.
- Generating regular reports on security events and trends.
- Reviewing access and system logs to identify unauthorized activity, effectively fulfilling the role of an internal security analyst.

Cyber Readiness and Response

Cyber readiness and response services strengthen organizational resilience against cyber threats through strategic planning and rapid incident response. These services include:

- Conducting proactive assessments to identify and remediate vulnerabilities.
- Implementing preventive measures to reduce the likelihood of successful attacks.
- Providing expert guidance and technical support to minimize downtime and restore normal operations following an incident.

Standard Network Security Controls

Network security controls form the base layer of security on an ICS. As explained above, the security architecture must be designed to minimize risk to critical systems. The following sections describe some of the technologies that can be used to achieve the desired segmentation and inspection points between network zones. This is not an exhaustive list of controls that can be used; many additional network devices can either augment or replace those listed below. SEL CS can help determine how best to meet specific customer needs.

Firewall

SEL CS recognizes the critical importance of firewalls in safeguarding critical OT infrastructure from external connectivity threats. Our approach begins with an in-depth analysis of business needs, industry challenges, and system vulnerabilities. We carefully plan and execute our strategies in various stages, including design, configuration, testing, and implementation. The firewall solution does not solely focus on defense; it also seamlessly integrates with OT systems and processes. This integration ensures that it not only protects your network but also supports and enhances your operational environment.

Switching

The SEL OT SDN switch offers a transformative approach to network management and security, with cutting-edge technology engineered to deliver unparalleled security, situational awareness, reliability, and performance in OT environments.

The use of SDN switches enables granular control of ingress and egress traffic, providing a strong security posture as well as fast failover within each network. SDN does not depend on traditional loop prevention protocols, such as the Rapid Spanning Tree Protocol (RSTP), as found in standard Ethernet switches. In the event of a link or switch failure, network convergence with RSTP can take seconds. In the SEL SDN implementation, convergence times are typically under 100 ms. SDN differs from typical switched networks in that all flows are predefined, allowing for rapid recovery from typical network failures. Additionally, SDN switches deny all traffic by default.

An OT SDN network is secured with a rule set that allows only predefined, or allowlisted, traffic. Each rule within the rule set is referred to as a flow. Once the network has been baselined with a set of flows, all other new and unexpected traffic is blocked by default. Traffic flows are generally defined based on the IP address and User Datagram Protocol/Transmission Control Protocol (UDP/TCP) port of the intended hosts within each packet ingressing or egressing an SDN switch. In the case of GOOSE traffic, virtual local-area network tags and Ethernet type are matched to restrict broadcast messages to their intended recipients. The basic anatomy of a flow is shown in Figure 1.4.

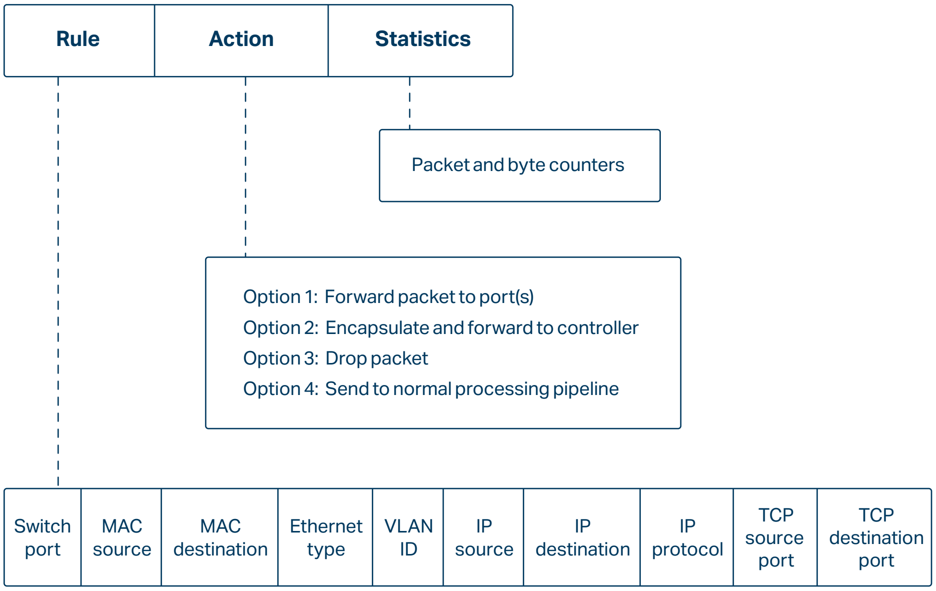

Figure 1.4: Anatomy of an SDN Flow

SEL SDN technology is officially certified and included on the U.S. Department of Defense (DoD) Information Network Approved Products List. This certification underscores the rigorous testing that SEL SDN switches have undergone, meeting stringent OT requirements and aligning with advanced cybersecurity frameworks and standards, such as U.S. DoD industrial control system tactics, the MITRE ATT&CK framework, and zero-trust architecture principles.

When traditional switching is preferred over an OT SDN solution, it is critical that performance and security requirements are carefully considered. Many of the standard features of Level 2 switches inherently present easy attack vectors and unintended failure scenarios. Features that are required should be carefully engineered to support the safe reliable operation of the system, and features that are not required should be disabled or removed.

Standard Security Services

Asset Management

The first step in developing a cybersecurity framework is a thorough identification of the cyber assets in place. An asset management strategy provides detailed hardware and software information about a system. Furthermore, a system cannot be reliably audited and assessed without an exhaustive list of all cyber assets that are part of that system.

All SEL-designed systems are delivered with a full asset inventory and can be integrated with existing asset management-tracking technologies, policies, and procedures.

Data Protection and Personnel Controls

SEL maintains strict role-based access control on all internal data repositories and implements both protective and detective security controls on internal information systems. Physical access controls with 24/7 monitoring and alerting are implemented at all SEL facilities. Additionally, all SEL employees are subject to initial and ongoing background checks and drug screenings and are required to report any arrest or conviction.

Detailed system information must be transmitted during the detailed design and implementation stages of any project. Controlling system information during development is critical to prevent data exfiltration or manipulation before the system is fully operational. All project deliverables are securely transferred through the SEL secure transfer site. System information is not transmitted by email. Items such as settings and configuration files are accompanied by a SHA-256 cryptographic hash to validate the integrity of all system configurations.

Supply Chain Security

Supply chain risk management is an essential component of a complete cybersecurity program. The interconnectedness and complexity of supply chains makes it more important than ever to systematically assess risks. At SEL, we have made security, including supply chain security, a top priority for over 30 years, and we believe that managing supply chain risks is fundamental to ensuring the quality of our products. For more information on the SEL approach to supply chain security, please refer to **Secure Supply Chain Management** (selinc.com).

Software Allowlisting and Change Management

Application allowlisting is the single most effective control in prohibiting the execution of malware on a computing device. Unlike traditional antivirus solutions that monitor the system for malicious files and block them from running, allowlisting only permits the execution of files and libraries that have been preapproved in the list of allowed software. Allowlisting can be implemented using a standalone application, embedded operating system (OS) functionality, or as part of an Endpoint Detection and Response (EDR) package.

Devices running SEL embedded operating systems (including the SEL-3555 Real-Time Automation Controller and SEL Blueframe software platform) enable allowlisting. Software and executables not cryptographically signed by SEL are prevented from executing on these platforms.

Configuration Hardening

Device configuration hardening focuses on reducing the vulnerability of hardware and software by systematically reviewing and reinforcing the default configurations of computing devices, to eliminate unnecessary functions and close off potential attack vectors. This proactive measure is critical in establishing a strong security foundation, ensuring that devices are resilient against both common and sophisticated cyber threats. By disabling unused ports and services, removing unnecessary software, applying the latest security patches, and configuring appropriate access controls, the potential for unauthorized access or exploitation is significantly minimized. Such actions serve to limit the attack surface, making it more difficult for cyber threats to penetrate a device. Integrating device hardening into the security plan ensures that each device contributes to a robust and resilient security posture, capable of withstanding and responding to a variety of cyber threats while maintaining compliance with regulatory requirements.

SEL CS typically uses published benchmarks, such DoD secure technical implementation guides, DoD security requirements guides, or Center for Internet Security benchmarks, as the baseline hardening strategy for device hardening. Using recognized, published benchmarks provides an auditable, secure configuration from which evidence can be produced to prove and monitor the configuration of the system.

Access Control Management

A directory service is essential for implementing effective access control management, which is crucial to ensure security within network systems. It effectively manages user accounts and groups, controlling access to OT systems by allowing access only to authorized personnel. The access control management system facilitates identity verification and management, ensuring that only verified individuals can access critical systems and information. The ability of directory services to maintain logs and records of access control activities supports compliance with NERC CIP standards through detailed audit trails. By assigning users to specific groups, organizations can enforce role-based access controls. This ensures individuals have only the necessary access for their job functions, further minimizing the risk of security breaches.

Configuration Monitoring and Vulnerability Assessment

Processes and procedures for continuous configuration monitoring provide a clear overview of the current state of the system and allow for swift remediation of any unauthorized or unintended changes. Alongside configuration monitoring, a comprehensive approach to vulnerability assessments ensures that the system is safeguarded against known vulnerabilities. A comprehensive patch management process ensures that patches are applied in a timely manner, do not disrupt system operations, and effectively address identified security vulnerabilities.

As part of the security package, SEL performs both configuration scans and vulnerability scans on the in-scope system before commissioning. The detailed reports from the scans provide validation that the configuration and software components are delivered in a secure manner.

Additionally, SEL CS offers ongoing monitoring, maintenance, and reporting as an option available to augment customer resources. These services can assist in meeting both security and compliance requirements, thereby easing the overall burden of system maintenance.

Endpoint Detection and Response (EDR)

EDR provides enhanced visibility into endpoint activities, as well as efficient detection, investigation, and response to potential incidents. EDR uses advanced analysis, machine learning, and threat intelligence analysis to investigate system logs, network traffic, file changes, and user behavior to detect advanced threats that are missed by traditional antivirus applications, which rely on signatures for detection. EDR can detect suspicious activities, anomalies, malware, or indicators of compromise and comes with features to automatically contain and isolate infected devices to avoid infecting other computers; block unexpected, privileged access launch of applications; and roll back infected devices to a functional state. EDR also provides in-depth, post-incident investigation reports to analyze how and where the attack originated and propagated across the network and how it was contained. EDR is a valuable tool to improve endpoint security posture, providing real-time monitoring, advanced threat detection, incident response capabilities, and valuable insight into endpoint activities and behaviors.

Multifactor Authentication

Integrating multifactor authentication (MFA) into network security systems significantly enhances their overall security posture. MFA not only protects against external threats but also helps in safeguarding against internal threats by making unauthorized access by insiders more difficult. It adds an extra layer of defense, making it more challenging for unauthorized individuals to gain access to sensitive data and systems, mitigating the risk associated with compromised passwords. By requiring additional verification, MFA ensures that even if one security layer is breached, unauthorized users still face significant barriers to gaining access. Additionally, MFA plays a crucial role in regulatory compliance, as many data protection standards now mandate its use for enhanced security.

Log Management

Centralizing logs by consolidating all security-related logs into a single location establishes a unified log repository that serves as the definitive source for all security-related events across the network. This approach ensures streamlined and coherent aggregation of log data, which is crucial for efficient organization and storage.

Such centralization proves particularly beneficial in the context of incident response and forensic readiness because having all logs centralized simplifies the process of retrieving necessary data. When a security incident occurs, investigators can quickly access relevant logs from a single server, without needing to individually access multiple systems. This significantly reduces the time and effort required to gather information, enabling a faster response to security incidents. Moreover, centralized logging plays a critical role in the detection of suspicious activity. When an intruder gains unauthorized access to a system, they often attempt to cover their tracks to keep exploited vulnerabilities open, allowing them continued access to the network. However, with log forwarding enabled, the likelihood of an intruder successfully erasing all traces of their entry significantly diminishes. Even if they manipulate logs on individual systems, the footprints of their activities are preserved in the centralized log server.

SEL Blueframe

Blueframe is specifically designed to support automation and application needs in a secured environment. An embedded, modular, container-based design supports a customized selection of applications which help solve and support system concerns. Additionally, Blueframe is an SEL proprietary, embedded, Linux-based OS, which drastically reduces maintenance overhead compared to a Microsoft Windows computer.

Blueframe Data Management and Automation (DMA) applications are beneficial for both monitoring and managing substation devices (in PERA L1 and L2).

The Credential Management application provides a proxy that allows the integration of authentication mechanisms, such as the Lightweight Directory Access Protocol, to SEL devices that do not natively support directory services. This enables the use of unique credentials for access to IEDs and role-based access control. Additionally, local passwords on IEDs can be automatically changed and reported, thereby easing the compliance burden.

The base Blueframe OS includes a Syslog application that either forwards logs from the system to a centralized Security Information and Event Manager server or stores logs locally for analysis in the case of an incident.

IEDs do not typically support Syslog for alerting events within the system; rather, they use a Sequence of Events (SOE) log and event reports. The Disturbance Monitoring application automatically listens, or polls, for events and SOE logs, providing a centralized repository of system information to support both general operations and security needs. The Configuration Monitoring application allows users to monitor the configuration of an IED; it alerts if the settings or firmware are changed. This functionality provides a first line of defense when unauthorized changes are made and an automated method to report firmware versions for vulnerability management.

Direct Resource Access allows Blueframe to act as an intermediate, or jump, server for authenticated access to the IED.

Blueframe DMA also includes protocol services, which enable Blueframe to interact with non-SEL platforms using a wide range of standard protocols, such as Manufacturing Message Specification or HTTPS, to bring asset information into the platform.

Blueframe has a full-featured application programming interface (API), allowing users to move data sets to other Blueframe nodes in a granular fashion. For example, Blueframe devices in PERA L2 can interact directly with IEDs and can be programmed to publish read-only data to a virtual Blueframe instance in the enterprise. This enables users to control not only the access to critical data but the availability of data as well. This can support the overall security mandates of the organization and assist in compliance efforts. The Blueframe API also enables integration with existing asset management tools by providing an interface to move data into a desired platform.

Internal Network Security Monitoring (INSM)

INSM offers real-time monitoring and detection of cyber threats, vulnerabilities, and anomalies within industrial networks. As a critical part of an INSM program, an IDS leverages advanced algorithms and deep network visibility to effectively identify suspicious activities, ensuring timely alerts and actionable intelligence to mitigate risks. The components of asset visibility provide a deep understanding of network assets and their behavior, enabling precise monitoring and anomaly detection. Additionally, an IDS uses threat intelligence services that deliver actionable insights into emerging threats and vulnerabilities, tailored to the unique landscapes of OT and Internet of Things systems.

SEL CS has a well-established partnership with Dragos and Nozomi Networks. Through these collaborations, our team has received comprehensive training and enablement, ensuring we are fully equipped to leverage both platforms. We have successfully performed numerous deployments of INSM solutions across various industries, demonstrating our expertise and commitment to excellence. Post-deployment, our team continues to manage and support many installations, ensuring optimal performance and security for our clients.

Standard System Management Services

Jump Servers

Jump servers offer centralized and secure entry points to networks for accessing critical or sensitive systems. Jump servers can also enforce MFA to enhance security, alongside rigorous logging and monitoring, ensuring that access is granted only to authorized users and that all activities are recorded for auditing and compliance purposes.

This configuration effectively segregates the internal network from access attempts originating from less-secure networks, diminishing the attackable surface area and substantially lowering the risk of exposing internal systems to vulnerabilities.

Patch Management

Patch management plays a crucial component in network security by consistently monitoring, acquiring, testing, and deploying software updates to the components of the network. It provides defense against cyber threats and also ensures ongoing compliance with dynamic security standards, thus enhancing network resilience and operational integrity. At the commissioning of a system designed by SEL CS, all devices have up-to-date security and application patches.

SEL informs customers of security vulnerabilities in SEL products that are sold to the customer, and updated firmware is provided by customer sales representatives in a manner that is acceptable to each customer.

For non-SEL devices and software, SEL CS offers system maintenance services as part of the life cycle services program. This service provides vulnerability monitoring, remediation packages, and reporting.

Backup and Recovery

Incorporating a robust backup solution is pivotal in the landscape of network security, serving as a critical line of defense against data loss during system failures. The importance of a backup solution lies in its ability to preserve business continuity and mitigate the impacts of potential cyber incidents or hardware malfunctions.

A comprehensive backup strategy involves regularly creating secure and retrievable copies of essential data and system configurations. This ensures that in the event of a security breach, such as a ransomware attack or a catastrophic hardware failure, the organization can rapidly restore operations using the backed-up data, minimizing downtime and financial losses.

Security Awareness and Training

SEL CS can provide targeted cybersecurity training and awareness for personnel managing the cybersecurity aspects of their systems. This training is designed to impart essential knowledge of cybersecurity principles and practices relevant to system management and operations. The training program covers key cybersecurity concepts and the specific security features of the system, ensuring staff are aware of their roles and responsibilities in maintaining security. This focused approach ensures that the team managing the cybersecurity of the system has a solid foundation in the necessary security practices.

Conclusion

The SEL CS approach to ICS security provides a comprehensive methodology for securing critical systems through a combination of defense-in-depth and zero-trust principles. By adhering to established standards, such as NIST CSF and IEC 62443, SEL ensures that its security measures are both robust and adaptable to evolving threats.

Governance, risk assessment, and purposeful architecture are important in designing secure systems. Continuous improvement and the economic considerations of implementing security controls are needed. Key components, such as firewalls, SDN switches, access control management, EDR, device hardening, and MFA, contribute to a resilient security posture.

Monitoring and management solutions, including centralized logging, SEL Blueframe, and an IDS, maintain visibility and respond to threats. Additionally, management and recovery strategies, such as jump servers, patch management, and backup solutions, are essential for ensuring business continuity and mitigating the impacts of cyber incidents.

SEL CS focuses on supporting your organizational risk management strategy by following engineering design principles and integrating advanced technologies and best practices. Our designs are built to create secure, scalable, and efficient operational environments. By investing in these security measures, organizations can enhance their resilience against cyber threats and ensure the safe and reliable operation of their systems.

SEL SCHWEITZER ENGINEERING LABORATORIES

info@selinc.com | selinc.com | 20260312