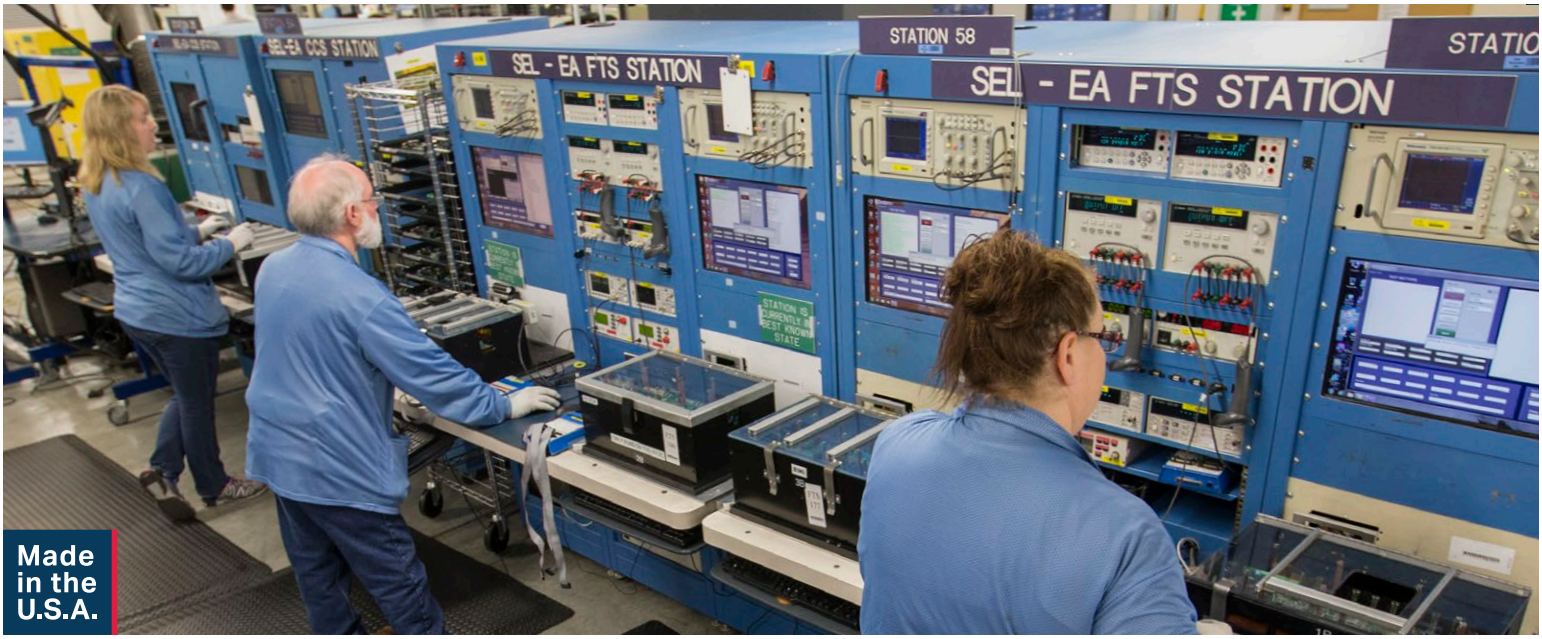
SEL SDN

Software-Defined Networking



Protect your critical infrastructure with SEL's made-in-America SDN switches

- Engineered to deliver improved security, situational awareness, reliability, and performance.
- Purpose-built using a deny-by-default approach that offers proactive traffic-engineered circuit provisioning for securing critical infrastructure networks.
- Certified on the U.S. Department of Defense (DoD) Information Network Approved Products List.
- Designed, tested, and manufactured in the United States in facilities SEL owns and operates—a critical step for ensuring our secure supply chain management.
- Transparently priced up front, with no annual support or maintenance fees.

SEL

Optimize Operational Technology (OT)

Traditional Ethernet switches generally behave similarly regardless of the environment (one size fits all). With SEL OT SDN, LAN switching can be optimized for the specific requirements of the environment. OT SDN allows you to purpose-engineer your networks like you purpose-engineer your critical control system.

Eliminate Cyber Vulnerabilities

Traditional networks use features like MAC tables, the Rapid Spanning Tree Protocol (RSTP), and cast types for many conveniences, including plug-and-play functionality. However, these features also make traditional networking vulnerable to cybersecurity threats. With OT SDN, all network flows and backup paths are specifically defined in the controller, so there is no need for MAC tables or RSTP. In addition, OT SDN uses traffic engineering to process forwarding behavior, rather than relying on cast types.

Deny-by-Default Network Access Control

OT SDN provides deny-by-default, multilayer packet inspection at each hop, controlling what conversations each device is allowed to have on the network. Packets that do not match the rules do not get forwarded, providing protection against attacks which physically take place inside the firewalls or any unauthorized traffic that slips past the firewalls. This microsegmentation provides complete control over each conversation allowed on the network and is a foundation for zero trust.

Control Network Traffic With Great Precision

With OT SDN, it's easier to manage large amounts of network traffic than it is with traditional networking, because it eliminates unnecessary traffic on your network. Instead of having a node broadcast to all other nodes on the LAN, you can engineer specific paths and remove the extraneous ones. This ensures bandwidth availability and high performance in critical applications. And unlike RSTP switches, there are no blocked ports limiting bandwidth. SDN eliminates several problems inherent in traditional Ethernet switches.

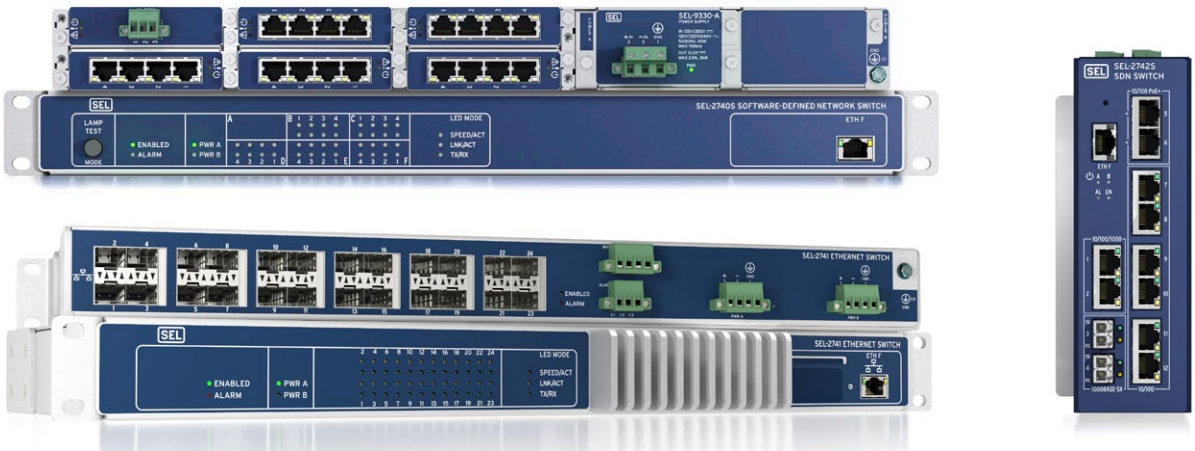
Rigorously Tested

SEL SDN switches are tested against challenging OT requirements, such as Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures for U.S. DoD industrial control systems, MITRE's ATT&CK framework, and the zero-trust architecture.

For a full list of certificates held by SEL, please visit **selinc.com/company/certifications**. To learn more about our approach to supply chain security, please visit **selinc.com/solutions/cybersecurity/secure-supply-chain**.

Ten-Year Warranty and Technical Support

All SEL products, including SDN switches, are warrantied for ten years and include free technical support.



SEL SDN switches feature flexible port options, wide-range and redundant power supplies, and clear activity and status indicators supporting simple onsite diagnostics.

SEL SCHWEITZER ENGINEERING LABORATORIES

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

LM00490-01 • 20230113