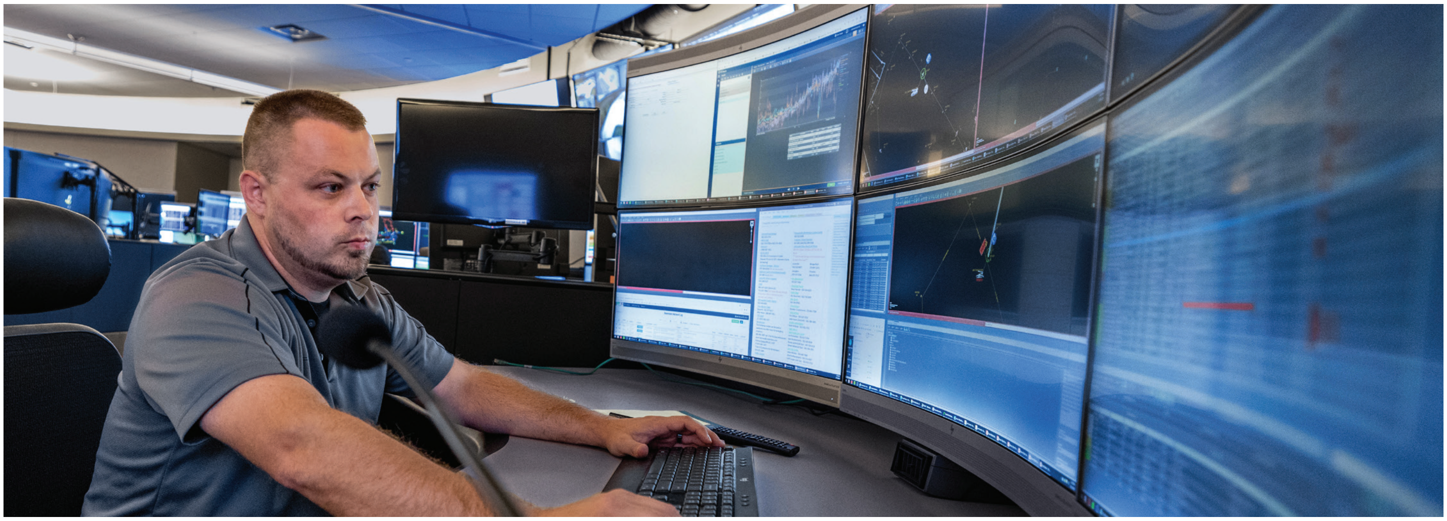


A NETWORK ARCHITECTURE SOLUTION

Converged Industrial Edge

The Converged Industrial Edge (CIE) is a network architecture solution developed by Schweitzer Engineering Laboratories, Inc. (SEL), Juniper Networks, and Dragos as the best approach for securely sharing information between operational technology (OT) networked assets and between OT and IT systems. CIE enables the secure and simplified information exchange across disparate parts of a network in a manner that strengthens the system's cybersecurity posture, reduces maintenance costs, adds greater situational awareness, improves grid reliability, and preserves the integrity of each domain's performance requirements.

Key Features/Benefits

CIE provides technical, operational, and business benefits, including:

- Complete end-to-end, Ethernet-based communications for data centers, WAN, and the edge.
- Standardized digital infrastructure layer for frictionless information exchange between vendors, systems, devices, and domains.
- Native cybersecurity through the combination of deny-by-default, zero-trust networking and threat detection and prevention at every port, packet, and process.
- Extensible design that allows flexible cloud-native technologies to automate repeatable tasks, reducing errors and the strain on human capital.
- Modular and pluggable format that integrates with existing operations support systems (OSSs) and business support systems (BSSs), work order and ticketing systems, IP address management (IPAM), and certificate authorities.
- Simplified cross-domain information exchange and trust management between domains.
- Detection and tracking of known malicious behaviors and tactics as well as automatic response for fast-moving, east-west attacks—before compromise and exfiltration occur.

SEL SCHWEITZER ENGINEERING LABORATORIES

JUNIPER NETWORKS

DRAGOS

Improve and Simplify the IT and OT Information Exchange

CIE was developed in response to the ever-growing connectivity and cybersecurity demands placed on critical infrastructure. These demands resulted in overly complex network architectures that are prone to misconfigurations due to repetitive manual tasks; limit system visibility; increase maintenance and operational costs; and increase the cyber-attack surface. Additionally, it can take months to engineer, test, and deploy any desired network changes based on changing business needs.

Through context-aware automated information sharing between subsystems, CIE alleviates these burdens.

Now, circuits that span the IT-OT divide can be instantiated from control center to substation, tested, fingerprinted, and placed under surveillance in minutes. Automation controllers reduce repetitive tasks and the potential for misconfigurations as well as provide the means to proactively build and maintain context-aware networking. Context-aware networking is having situational awareness of the combined physical location and logical connections of each device and linking that to the association with system operations. This enables network owners to always know exactly what devices are allowed on the network, what conversations each device is allowed to have, and what purpose those devices and conversations are fulfilling.

CIE also uses a deny-by-default, zero-trust forwarding fabric, guaranteeing that only authorized messages traverse the network and eliminating many of the inherent vulnerabilities present in other network fabrics. Unauthorized packets that access the network are denied by default and immediately dropped. Sensors detect and track known malicious behaviors and tactics and trigger a response for fast-moving, east-west attacks—before compromise and exfiltration occur.

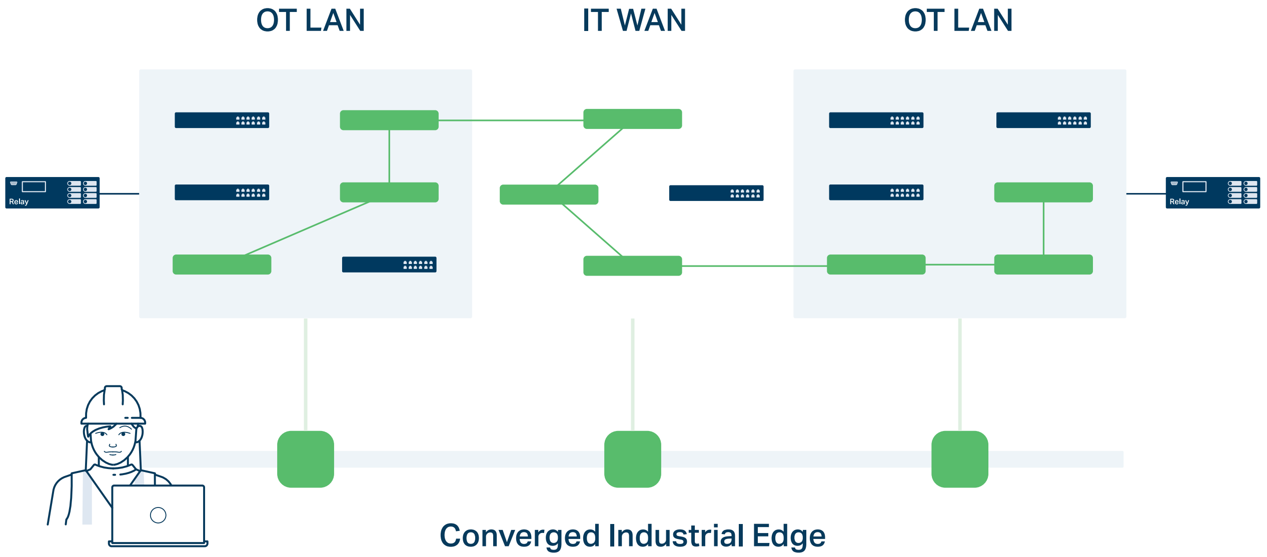
CIE answers the need for a purpose-engineered network architecture that is cybersecure, dynamic, and efficient.

For more information or to schedule a demonstration, please contact:

SEL
secure@selinc.com

Juniper Networks
converged-industrial-edge-juniper-info@juniper.net

Dragos
info@dragos.com



Previously, to add communications from one device to another meant traversing multiple networks, which meant involving multiple system owners from OT and IT teams. They all had to coordinate to provision the circuit and configure their respective devices along the way. This process could take months to complete, and it was prone to misconfigurations, fraught with engineering complexity, vulnerable to cyber attacks, and lacking system awareness.

With CIE, the WAN and LAN devices are incorporated into one deny-by-default, programmable forwarding fabric. Now, the task of provisioning that same circuit is reduced to one operator, who is essentially only working with one network. The engineer enters a work order, and because the controllers in the automation plane have total visibility of the devices throughout the network, it's possible to provision and test an end-to-end circuit in minutes.