Converged Industrial Edge

Network Architecture Solution

Improve and simplify IT and OT information exchange

- Reduce operational expenses and simplify processes.
- Improve cybersecurity and situational awareness.
- Automate end-to-end circuit provisioning.
- Eliminate repetitive data entry and network configuration errors.
- Streamline intrusion and threat detection system integration.
- Simplify inventory management.

What is the Converged Industrial Edge (CIE)?

CIE is a network architecture developed by SEL, Juniper Networks, and Dragos as the best approach for securely sharing information between IT and operational technology (OT) networks. CIE enables 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.

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.

Key Features/Benefits

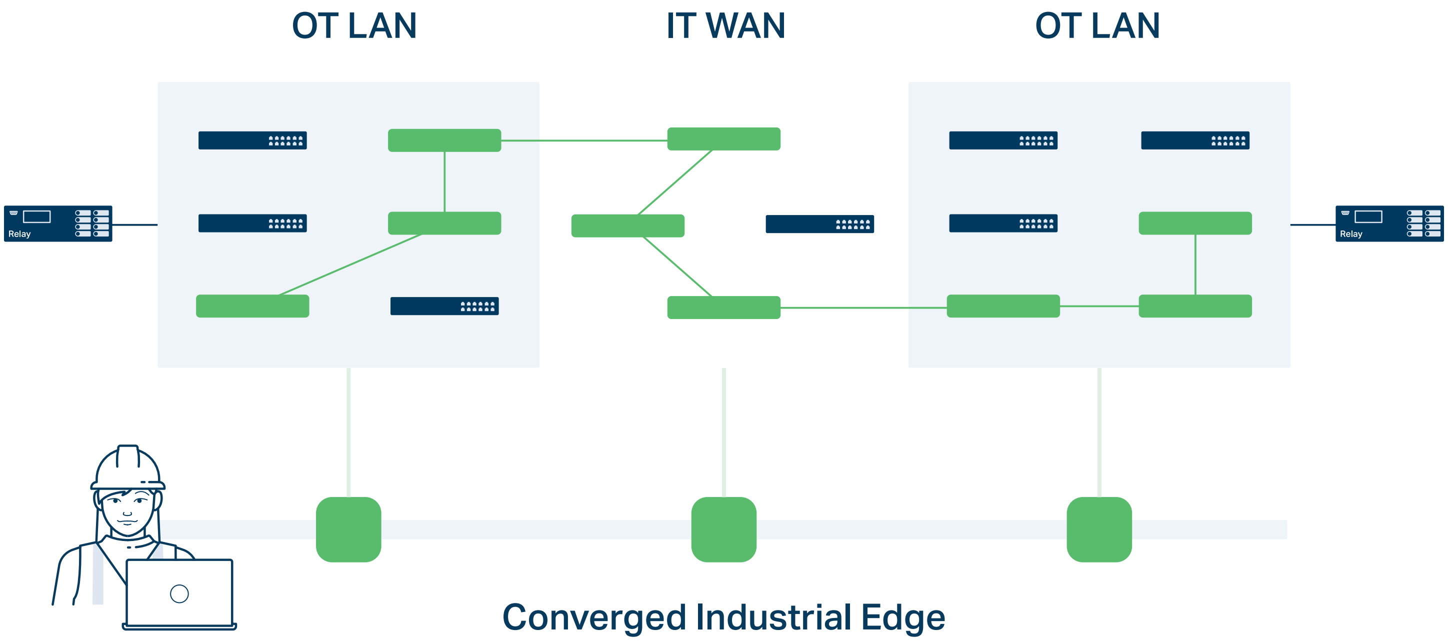
CIE provides technical, operational, and business benefits, including:

- 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.

By standardizing data structures and providing a secure, multisite communications medium, the CIE architecture simplifies cross-domain exchanges of information and manages the trust between the parties sharing information. Circuits that span the IT-OT divide can be instantiated from control center to substation, tested, fingerprinted, and placed under surveillance in minutes. Telemetry from the very edge of the control network can be presented to analytics engines to detect trends and, if necessary, take remedial action. Sensors can detect and track known practices and tactics of malicious actors and trigger a response to fast-moving cyber attacks before compromise and exfiltration occur, acting as a circuit breaker for fast-moving east-west attacks.

The CIE architecture embraces the existing requirements of critical infrastructure communications: it must be safe, reliable, predictable, secure, and ensure long life cycles. It brings the performance, security, automation, and situational awareness to your critical communications in much the same way remedial action schemes (RASs) or special protection schemes (SPSs) do for your electrical system. It enables accelerated detection of events and triggers predetermined corrective action, with or without human input, to keep critical communications up, reliable, and cyber-secure.

CIE provides automated orchestration of distributed networking, computation, and security resources, reducing human error and laying the foundation for novel joint capabilities between IT and OT systems without compromising the safety, reliability, availability, or security that critical infrastructure requires.



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.

SEL and CIE

SEL provides the LAN and information inventory management of the OT edge devices.

OT SDN

Software-defined networking (SDN) provides the deny-by-default, zero-trust cybersecurity foundation to proactively traffic-engineer all communications critical infrastructure needs to operate safely and securely. SEL's solution provides centralized visibility and distributed control for network management on all LANs for OT.

OT SDN allows for context-aware information sharing. Context-aware networking provides the situational awareness of combined physical location and logical connections of each device and links this to the association with the 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.

Blueframe™

SEL's Blueframe platform provides the secure, embedded operating system and application space to simplify administration and improve scalability and feature deployments. Blueframe allows information sharing between applications, reducing and eliminating repetitive data entry work and normalizing information across many applications.

Simplified Inventory Management

Simplify your inventory management and reduce repetitive data entry by using CIE to exchange information between controllers and automation layers. The centralized management provides the situational awareness of combined network topology and logical connections of each device, and links this to the association with the system operations. This enables network owners and threat detection systems 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.

Contact

For more information and to schedule a demonstration, contact **secure@selinc.com**.

SEL SCHWEITZER ENGINEERING LABORATORIES

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

© 2021 by Schweitzer Engineering Laboratories, Inc.

WORLDWIDE 10 years WARRANTY