# CONVERGED INDUSTRIAL EDGE SOLUTION ARCHITECTURE

*Create a context-aware network from control center to the industrial edge*

***Challenges***

*Critical infrastructure like utilities face multiple challenges. They must evolve their IT-OT and business practices to improve cybersecurity, lower the cost of operations, and increase business agility without impacting critical services—the equivalent of upgrading the engines of a plane while in flight.*

***Solution***

*The Converged Industrial Edge is a best-in-class, open, multivendor solution architecture for a converged IT-OT edge. It is designed to simplify the life-cycle orchestration of IT-OT and OT-OT communications while maintaining the predictable requirements of critical infrastructure and providing comprehensive cyber visibility, threat detection, and mitigation.*

***Benefits***

- *Build a zero-trust, deny-by-default network from control centers to substations*
- *Create professionally engineered circuits to meet the needs of OT systems without compromise*
- *Reduce risk of human error by automating network service creation and ongoing service assurance*
- *Detect and prevent cyberthreats to protect against service disruptions*
- *Simplify audit reporting and reduce risk of noncompliance*

*Utilities and critical infrastructure providers need reliable, resilient, cybersecure communications that address the needs of critical infrastructure.*

## The Challenge

The energy industry transition demands grid communications modernization. Moving to a more diverse and sustainable energy mix is an opportunity for utilities to reimagine their communication networks in ways that provide maximum flexibility, coverage, and intelligence. Integrating distributed energy resources (DERs) like solar, wind turbines, and storage can provide energy where and when it's needed as the load shifts in time, duration, and intensity. Grid communication modernization is critical in an unpredictable world, as a smart, active grid can enhance power reliability while lowering costs.

With a greater reliance on digital infrastructure, power utilities have become major targets for criminal syndicates and malicious nation-states. The US Federal government has called for immediate action to protect electric grid distribution systems, which it has identified as vulnerable to cyberattack. With the flow of energy to homes and businesses at risk, utilities must strengthen their cybersecurity.

Utilities must also work to strengthen disaster readiness. Extreme weather events such as wildfires and hurricanes have become more frequent. Climate events resulting in more than $1 billion in losses increased 5X over the past decade, according to NOAA.

## The Converged Industrial Edge Solution

Critical infrastructure sectors like utilities, water and wastewater, transportation, manufacturing, and smart cities are all migrating to architectures like the Converged Industrial Edge to increase service reliability and flexibility, protect against cyberattacks, and lower operational costs.

Juniper Networks and its technology partners SEL Inc. and Dragos have developed the Converged Industrial Edge solution architecture to help utilities and critical infrastructure sectors meet these new market dynamics. The Converged Industrial Edge solution is a professionally engineered architecture that provides a best-in-class, integrated, secure, and automated network to meet the stringent needs of utilities and other critical infrastructure providers.

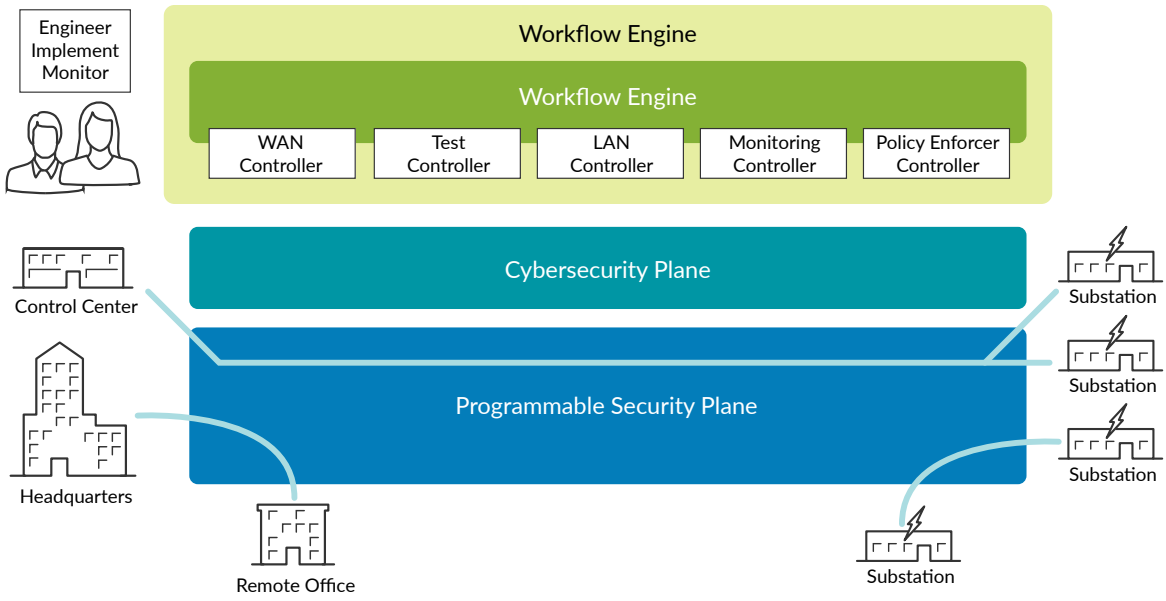


*Figure 1. Converged Industrial Edge solution architecture*

The Converged Industrial Edge solution architecture is optimized for on-premises private networks and is designed to be integrated with existing operational support systems and business support systems (OSS/BSS), work order, or management systems. The Converged Industrial Edge solution architecture simplifies the orchestration of IT-OT and OT-OT communications from the control center to the substations. Network service creation is automated and continuously assured, increasing network reliability and reducing the risk of regulatory noncompliance. Strong cybersecurity proactively detects and prevents threats at the OT/ICS edge.

## Features and Benefits

Utilities and other critical infrastructure sectors can safely put their trust in the Converged Industrial Edge solution architecture from Juniper, SEL Inc., and Dragos as they modernize and simplify their IT and OT infrastructure at the edge.

### Create a Programmable Network Fabric from Control Center to Substation

The foundation of the Converged Industrial Edge solution architecture is a programmable forwarding plane. The forwarding plane is comprised of Juniper Networks® MX Series Universal Routing Platforms for the IP/MPLS WAN transport and SEL OT-SDN switches for inter- and intra-LAN communications in substations. The individual routers and switches are abstracted into a programmable fabric that is centrally managed through SDN controllers.

The programmable forwarding fabric is designed as a deny-by-default, zero-trust environment. All IT and OT communications circuits from the control center to the substations are professionally engineered for a specific purpose, with detailed knowledge of who or what is allowed to communicate across the circuit and the exact set of communications that are permitted. Each circuit is engineered for the precise characteristics needed to support the connected devices, the communications, and applications. All other humans and devices are denied access to the network fabric by default.

The first set of circuits established are for the internal management network between the technology partners and are referred to as the Multisite Event Bus. This standards-based management network is present at each and every endpoint and allows for the free flow of information among vendor-specific devices, systems, and domains. The internal management network simplifies integration and the number of steps needed to coalesce control and telemetry data and turn it into actionable information. The Multisite Event Bus is encrypted and authenticated for strong cybersecurity.

### Automate Network Service Creation and Monitoring

The Converged Industrial Edge solution architecture is designed to drive down risk through automation, reducing human error, which is the leading cause of misconfiguration of grid assets. Automation drives down cost, due to a significant reduction in the amount of time it takes to create a SCADA communications circuit. Instead of spending dozens or even hundreds of hours, a circuit can be created in minutes. Automation reduces the number of truck rolls needed for network assessment, implementation, and troubleshooting.

The prescriptive nature of the Converged Industrial Edge automation plane allows electrical operations systems to drive the network requirements, instead of the other way around. Network engineers and architects use the Converged Industrial Edge automation plane software to express their intent to engineer, implement, and monitor communication circuits for IT-to-IT, IT-to-OT, and OT-to-OT uses.

The automation plane of the Converged Industrial Edge solution controls the programmable forwarding plane. The automation plane is on-premises software that presents a human-friendly abstraction of modular software components, including the Juniper® Paragon™ Automation Portfolio and the SEL OT-SDN Controller—the software-defined WAN and LAN controllers that maintain perfect, real-time knowledge of all network resources in use or ready for use as well as all transactions that are allowed and active on the network.

For example, a network engineer can create a SCADA circuit in software and express the intent through an electronic work order to have the circuit created. From there, a preprogrammed workflow uses standardized network configuration templates and circuit models to create the requested SCADA communications circuit. The configuration detail is decomposed into work orders that are specific to the configuration of the routers and switches in the WAN and substation LAN. These work orders are distributed to the SDN controllers to reserve the network resources for the instantiation of the SCADA circuit.

The actual creation of the SCADA circuit typically occurs after authorizations have been obtained from the stakeholders. Once scheduled and approved, network or security operations engineers can implement these work orders. Preprogrammed workflows instruct the SDN controllers for the WAN and LAN to push their configurations to the previously reserved network resources and the end-to-end circuit is instantiated in minutes.

To verify success, a preprogrammed workflow generates a circuit-specific test using the test controller module of the automation plane. The test controller dynamically creates a series of tests that document specifics like network throughput and latency. The test results are presented to a monitoring controller module. A preprogrammed workflow then copies the test results to the WAN controller, providing a digital fingerprint of the circuit's known capabilities and behavior.

The same information is used by the monitoring controller module for the ongoing surveillance of the circuit. From this point forward, nothing about the circuit should change—and if something does change, the anomaly will be flagged for further monitoring or action.

Because every communications circuit is professionally engineered, a new paradigm for compliance auditing is created. Audit reporting now becomes exception reporting. Because all network communications are known and documented, an unauthorized flow is immediately detected and remediated.

### Actively Detect and Prevent Threats at the Edge

Criminal syndicates and malicious nation-state actors continue to disrupt critical infrastructure. Whether a cybersecurity incident results from a successful phishing attack or a supply chain breach, the network must be able to detect threat behavior and respond before a compromise occurs.

The Converged Industrial Edge solution architecture is inherently secure with extensive security controls that reduce the attack surface. A threat-aware communications infrastructure extends from the control center, across the WAN, and into substations. The programmable forwarding plane is a deny-by-default, zero-trust environment. The Converged Industrial Edge automation plane authenticates, fingerprints, and surveils every packet, process, and port that's been engineered for use. Comprehensive network visibility allows for rapid investigation and response to fast-moving cyberattacks.

Beyond these advanced security measures, the Converged Industrial Edge solution adds the Dragos Platform for ICS threat detection and prevention capabilities to the substation operations environment. The Dragos Platform uses sensors and behavioral analytics to identify anomalous or malicious behavior. In an extreme case where Dragos matches observed behavior to a known set of malicious tactics and procedures, it can signal a policy enforcement capability in the automation plane and provide recommendations to quarantine or block network access to stop a fast-moving attack.

Additionally, utilities can choose to participate in Dragos' Neighborhood Keeper, a collective defense and communitywide visibility program, which shares threat intelligence across industries and geographic regions.

The Converged Industrial Edge cybersecurity plane improves uptime and ensures availability by detecting and remediating attacks before they affect service. The cybersecurity plane also reduces the risk of reputational damage due to a cyber incident as well as the hard cost of remediation and recovery.

## Solution Components

| Converged Industrial Edge Solution Architecture | Products |
|---|---|
| Programmable Forwarding Plane | **Juniper Networks MX Series Universal Routing Platforms** provide industry-leading system capacity, density, security, and performance with unparalleled longevity.<br><br>**SEL Inc.'s Software-Defined Networking for OT** solution is Ethernet-based with better security, control, and performance than traditional networking. SEL-2740S and SEL-2742S are field-hardened SDN-enabled switches, and work in conjunction with the SEL-5056 Software-Defined Network Flow Controller to provide path- and packet-level control of communications flows, which eliminates common cybersecurity vulnerabilities and improves failover performance. |
| Automation Plane | **Juniper Paragon Pathfinder** (formerly NorthStar Controller) is a cloud-native controller that simplifies traffic engineering, making it easier to leverage benefits of MPLS/RSVP, segment routing, and network slicing. Operations teams can more efficiently manage strict transport service-level agreements (SLAs) through automated planning, provisioning, proactive monitoring, and optimization of large traffic loads dynamically based on user-defined constraints.<br><br>**Juniper Paragon Active Assurance** is a programmable, active test, and monitoring solution for physical, hybrid, and virtual networks. Paragon Active Assurance uses active, synthetic traffic to verify application and service performance at the time of service delivery and through the life of the service. Operations teams can use Paragon Active Assurance to verify that services are configured correctly the first time and validate that service changes don't impact service quality.<br><br>**Juniper Paragon Insights** (formerly HealthBot) is a cloud-native, network health and diagnostic solution that provides operational intelligence across all network domains from network access to the data center. Paragon Insights supports open-source data collection formats. Built-in advanced algorithms and machine learning correlate data sources, establish operational benchmarks, determine anomalies, and perform proactive corrective actions—all critical to intent-based networking.<br><br>**Converged Industrial Edge Workflow Orchestration** is a graphical user interface (GUI) that abstracts the interaction of the software modules using standards-based templates and service models to instantiate end-to-end circuits in minutes. Converged Industrial Edge comes standard with workflows for Layer 2 and Layer 3 VPN circuit for IT-to-IT, IT-to-OT, and OT-to-OT use cases. |
| Cybersecurity Plane | **The Dragos Platform** provides comprehensive visibility of ICS/OT assets, vulnerability management, threat detection, and threat investigation.<br><br>**Neighborhood Keeper** is a collective defense and communitywide visibility solution that provides a more effective industrial cyber defense by sharing threat intelligence at machine-speed across industries and geographic regions. |

## Summary—Drive Business Value and Meet Stringent Critical Infrastructure Requirements with a Converged Industrial Edge

The energy industry must evolve to improve cybersecurity, lower the cost of operations, and increase business agility without impacting critical services. This transition creates an opportunity to drive more business value while building a better, safer, and more reliable grid, but it relies on a modern industrial edge that is able to meet the unique requirements of OT and IT systems. Juniper, SEL Inc., and Dragos have partnered to create an integrated, proven solution for the converged industrial edge that enables utilities and industrial enterprises to break through to the next level as they meet evolving requirements at higher levels of reliability and with greater operational efficiency.

## Next Steps

To learn more about this joint solution, contact your Juniper account representative at Converged-Industrial-Edge-Juniper-Info@juniper.net or visit www.juniper.net/convergedindustrialedge.

## About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

## About Dragos Inc.

Dragos is an industrial cybersecurity company on a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. We offer industrial cybersecurity technology and services purpose-built for industrial control systems (ICS) and operational technology (OT) environments and continually informed by our globally sourced threat intelligence and industry expertise. Built by practitioners for practitioners, our solutions deliver the actionable insights and detailed guidance required to effectively and efficiently manage growing industrial cyber risk to increasingly connected industrial assets.

## About SEL Inc.

SEL specializes in creating digital products and systems that protect, control, and automate power systems around the world. This technology prevents blackouts and improves power system reliability and safety at a reduced cost. A 100-percent employee-owned company headquartered in Pullman, Washington, SEL has manufactured products in the United States since 1984 and serves customers worldwide.

**Corporate and Sales Headquarters**
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
**Phone: 888.JUNIPER (888.586.4737)**
**or +1.408.745.2000**
**Fax: +1.408.745.2100**
**www.juniper.net**

**APAC and EMEA Headquarters**
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
**Phone: +31.207.125.700**

Driven by Experience™