The Converged Industrial Edge was developed in response to the ever-growing demand for cybersecurity and converged connectivity for critical infrastructure. It solves for overly complex network architectures that limit visibility, increase operational costs, and expose cyberattack surfaces. Utilities and other critical infrastructure providers can reduce time-to-value by automating the engineering, deployment, testing, and surveillance of critical infrastructure communications.

Create an ultra-resilient, secure network from control centers to substations
Automate network service creation to reduce human error and truck rolls
Simplify audit reporting and reduce risk of noncompliance
Easily engineer communication circuits to meet precise OT requirements
Actively detect and prevent cyber threats protect against service disruptions

Overcoming Challenges, Both New and Old

Aging Infrastructure
40% of utility executives consider aging assets or technology to be a major challenge.

Improved Resilience Is a Priority
$1 billion 5X increase in losses due to extreme weather over the last decade.

Utilities rose to the #3 most-attacked industry in 2020 after financial services and manufacturing.

5 Reasons to Build a Converged Industrial Edge

1. Create an ultra-resilient, secure network from control centers to substations
2. Easily engineer communication circuits to meet precise OT requirements
3. Automate network service creation to reduce human error and truck rolls
4. Actively detect and prevent cyber threats protect against service disruptions
5. Simplify audit reporting and reduce risk of noncompliance

Modernize and Simplify IT and OT Infrastructure at the Edge

Industry leaders Juniper, SEL Inc., and Dragos have engineered the Converged Industrial Edge solution architecture to automate the orchestration of IT-OT communications and simplify information exchange to achieve business outcomes for critical infrastructure and industrial IoT without compromise.

Build Your Converged Industrial Edge Faster and with Less Risk

Programmable Forwarding Plane
Build a resilient, deny-by-default, Zero Trust network fabric from control centers to the industrial edge (such as substations)

Automation Plane
Automate network service creation, deployment, testing, monitoring and assurance

Cybersecurity Plane
Create a threat aware network, end-to-end. Actively detect and mitigate malicious threats within the OT industrial controls systems environment

To learn more about the Converged Industrial Edge solution architecture from Juniper, SEL, and Dragos, contact your Juniper account representative at Converged-Industrial-Edge-Juniper-Info@juniper.net or visit www.juniper.net/convergedindustrialledge.

---

1. “X-Force Threat Intelligence Index,” IBM, 2021
3. “Billion-Dollar Weather Events and Climate Disasters: Overview,” NOAA, 2021. There were five times more $1 billion weather events from 2018 to 2020 than during the 2000s.