JUNIPER NETWORKS | Driven by Experience™

White Paper

CONVERGED INDUSTRIAL EDGE FOR UTILITIES ARCHITECTURE FOR COMMUNICATIONS MODERNIZATION

Adopt cloud-native technologies to create a private operational cloud with native support for IT-OT use cases

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Electric utilities rely on Operational Technologies (OT) networks to support Industrial Control Systems (ICS) essential to their businesses. Historically, OT/ICS systems have been developed, implemented, and managed independent of IT networks. Differences in modes of operation, duration of refresh cycles, and physical and cybersecurity considerations are common justifications for separate IT and OT domains. But as pressure on budgets mounts and business cases for modernizing the grid edge multiply, the benefits of reducing costs and streamlining operations are compelling utilities to reevaluate options for converging communications infrastructure.

A reframing of the existing IT-OT grid communications paradigm is vital to realizing the economic advantages of grid modernization. A critical step in this reframing is the safe application of cloud-native technologies in data centers and control centers, in the WAN, and within substations—all to create a common model with inherent support for IT and OT/ICS applications.

Note: While this paper does not promote the use of public cloud services for utility OT/ICS uses cases, it does promote the adoption of cloud technologies that simplify and improve orchestration, control, management, automation, cybersecurity, and predictive analytics in private, autonomous, packet-based networks. This paper encourages the creation of a private operations cloud, which provides a common communication platform pre-instrumented to natively support IT and OT use cases. It's a reframing of IT-OT convergence, from hostile and dangerous to resilient and purpose engineered. It's engineering simplified.

Introduction

Electric power systems, and the information and communications systems they rely on, are rapidly becoming more distributed, digitized, and dynamic, challenging the traditional models and reliability expectations of OT experts at utilities. Macroeconomic factors, like the ones in the sidebar, are animating the business use cases that OT/ICS edge modernization addresses. But to fully realize the value of OT/ICS investments, communications must act as an enabler, representing as little friction as possible in the implementation and ongoing operation of applications for both IT and OT. This paper will describe a high-level reference architecture that has been developed from the OT professional's perspective on reliability and availability, and built with secure, standards-based infrastructure for known scale and resiliency.

The architecture described in this paper was designed with cloud-native technologies specified from its inception. As such, it is open, standards-based, and multivendor by nature. The architecture development is premised on the need of a future-state communications network that largely monitors and troubleshoots itself through the collection and correlation of streaming telemetry and control information. This information is delivered into repositories and fed to predictive analytics controllers while utilizing machine learning (ML) and artificial intelligence (AI) to detect trends, proactively alert operators, and, if necessary, mitigate problems.

The network is specified to employ software-defined controllers such that the full life cycle of a circuit, whether it be for Supervisory Control and Data Acquisition (SCADA), teleprotection, or engineering access, be prescriptively designed, tested, and monitored either ad infinitum or for a prescribed duration. Given the architecture's centralized and prescriptive nature, any change to the engineered state of the circuit would be immediately known, ensuring compliance and cybersecurity. The network is specified to secure (that is, to encrypt, authorize, account, and attribute) every packet of every transaction based on policy. It can also enforce policy on any port of any device in the IT domain, as well as the IP address closest to an indication of compromise (IOC) in the OT domain.

The architecture's orchestration, control, and management is based on a cloud-native microservices platform, with each application exposing its functionality only through a standardized application programming interface (API) to ensure resilience, continuous software optimization, and feature velocity without affecting other applications. The software architecture is decomposable such that layers of orchestration management functionality can be deployed by domain (i.e., within the substation) with increasing resiliency.

Thus instrumented, this architecture is optimized to provide OT and IT experts with network situational awareness, robust configuration management, change detection, policy management, and enforcement capabilities, such as:

- On demand, real-time asset management—a comprehensive inventory of devices at a given substation
- Detailed reporting of physical ports in use, the protocols being spoken, the application(s) being supported, and how much bandwidth they're consuming
- The ability to model the addition of new circuits and applications without physically querying or inventorying equipment in production
- The ability to deploy circuits, individually or in bulk, on demand with a software-defined circuit turn-up capacity, without manually defining flows in any switches and without truck rolls
- Full life-cycle circuit support, including the safe teardown of ephemeral use cases like engineering access
- The creation and maintenance of corporate networking security policy-aware circuits that know what conversations are allowed and which are not

Macro Drivers of Grid Modernization

- Accelerating integration of Distributed Energy Resources (DERs) and grid-level battery storage
- Increasing malicious cybersecurity activity and risk; coordinated or standalone physical attacks on grid infrastructure
- Increasing need for improved situational awareness to predict and mitigate risk from climate-related natural disasters (wildfires, 100-year storms, hurricanes)
- Retiring operational personnel; 50% of the operations workforce is expected to retire in the next three years
- Revision of utility business model; edge modernization in an age of downward budget pressures
- Increasing natural or man-made disaster scenarios

The following sections will provide a brief background and history of the development of the Converged Industrial Edge for Utilities architecture, along with descriptions of the contextual application of cloud-native technologies in each of the technology domains the architecture addresses:

- The end-to-end packet forwarding plane
- The management control plane
- The cybersecurity plane

History

In 2018, the United States Department of Energy (DOE) Cyber Security for Energy Delivery Systems (CEDS) program issued a challenge to the industry: enhance the reliability and resilience of the nation's energy infrastructure through innovative solutions developed with *"cloud-based technologies for the operational environment."* Juniper Networks and SEL Inc., a leader in the protection and control infrastructure for electrical utilities, were already working on developing such a network technology solution. After deciding to pursue the research and development funding opportunity, SEL Inc. recruited a third technology partner, Dragos, Inc., an industrial control systems threat protection provider, and a long-time customer and research partner, Bonneville Power Administration (BPA), a federally owned generation and transmission utility, to complete the project team[1].

[1] DOE SEDS Ambassador DE-0E0000900

The project team agreed on a vision to create an open, multivendor network architecture composed of a) a single packet-based forwarding plane stretching from the data/control center to the electrical substation; b) a single management-control plane for end-to-end provisioning, monitoring, and testing; and c) a single cybersecurity plane for NERC-CIP compliance and industrial control systems threat detection. The name of this architecture is the Converged Industrial Edge for Utilities.

The objectives of the Converged Industrial Edge for Utilities architecture are:

1. Enhance the reliability and resilience of energy infrastructure using cloud-native technologies.
2. Centralize what you can, distribute what you must.
3. Reduce complexity, security gaps, and expense.

The objectives guided the development of the architecture and the technology domains that form its scope: the data/control center, the WAN, and the distributed control system substation.

Solution Requirements

The effort to document solution requirements began with a survey of utility employees, from BPA and other utilities, with responsibilities ranging from NOC/SOC engineer to control, protection, and field engineer, among others. The aggregated solution requirements document (SRD) served as the primary source for framing the desired technical solution outcomes. This white paper focuses on the functional architectural specifications needed to satisfy the requirements captured in the SRD, with a particular emphasis on the following primary use cases:

- Automated, end-to-end circuit provisioning
- Telemetry aggregation and visualization
- End-to-end testing
- System security monitoring, intrusion detection, and threat hunting

The project methodology called for Juniper's development team, SEL's R&D team, and Dragos' development team to employ an Agile approach to the project. Developments were broken down into iterations, or sprints, which were roughly two weeks long. At the end of each sprint, the result was presented to the team members and stakeholders. A formal feedback session was established to improve the process and contribute to the next sprint.

The project proof-of-concept is maintained in Juniper's POC lab in Herndon, VA. The POC lab, which emulates a data/control center and multiple substations, is built on the following constituent technologies:

- Juniper Networks Ethernet VPN (EVPN)/Virtual Extensible LAN (VXLAN) Ethernet fabric
- A multi-node Kubernetes cluster for deployment of microservices
- A Juniper MPLS mesh WAN, made up of Juniper Networks® MX Series 5G Universal Routing Platforms configured as MPLS provider (P) and provider edge (PE) routers to emulate grid communications requirements for SCADA, teleprotection, distribution, and transmission substations
- SEL Inc. Ethernet LAN infrastructure for Operations Technology Software Defined Networking (OTSDN) and IEC61850 substation communications, precise timing, hardened compute and remote terminal units (RTUs), intelligent electronic devices (IEDs), and other equipment necessary to emulate electrical power substations
- Dragos Inc. sensors and Site Store for ICS threat detection and adversary hunting

Having established and reinforced the objectives with solution requirements, defined the use cases, and established the lab environment and developmental methodologies, the project team began working on producing a private operations cloud solution (see Figure 1).

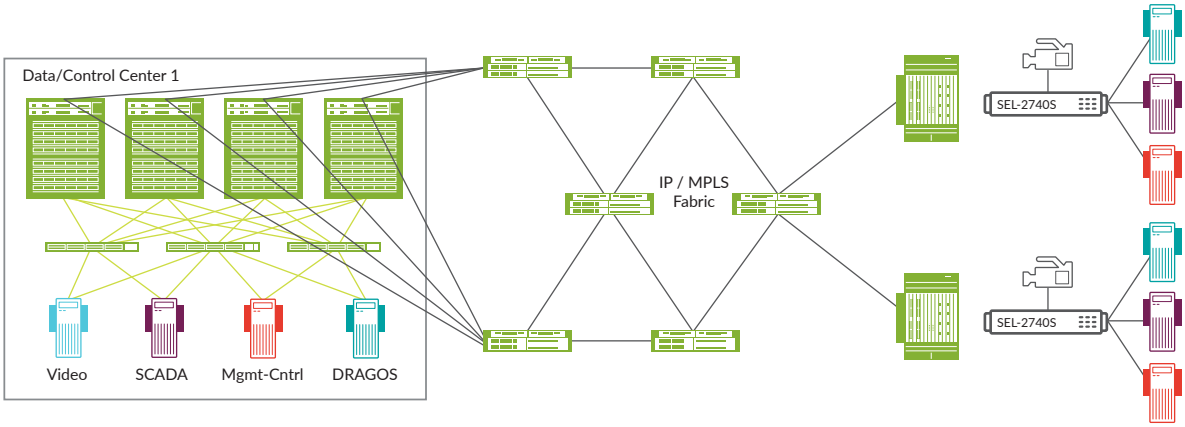

Figure 1: Private operations cloud solution

The project team was working to reduce or eliminate the friction caused by competing communication networks that hinders the adoption of economically justified IT and OT/ICS use cases. The decision to create the Converged Industrial Edge for Utilities architecture, and to use cloud-native technologies as its foundation, was informed by the solution requirements collected from utilities. Creating a single, secure architecture with inherent support for IT and OT applications reduces the lag in addressing challenges represented by increased cyber attack activity, pressure on CapEx and OpEx budgets, and the need for enhanced situational awareness in the face of climate-related risks and the retirement of valued OT personnel. Although there are significant "future-proofing" benefits to the solution, the true value is in increasing the resilience and intelligence of the systems that support the safety and reliability of the grid.

The following sections describe the contextual application of cloud-native technologies in each of the technology domains that the Converged Industrial Edge for Utilities architecture addresses: end-to-end packet-based forwarding plane, the management control plane, and the cybersecurity plane.

Private Operations Cloud

Packet-Based Forwarding Plane

The packet-based forwarding plane of the Converged Industrial Edge for Utilities architecture is composed of Juniper Networks routers, switches, and firewalls, architecturally optimized for two use cases: secure, cloud-ready data/control center and WAN transport core, aggregation, and edge. The packet-based forwarding plane is extended to the electrical substation using SEL Inc.'s OT-SDN Ethernet solution. Interoperability between the control center, WAN, and the substation is achieved using standard protocols; end-to-end LSPs, L2/L3 VPNs, and logical flows can be created, tested, monitored, and torn down across this infrastructure using the management and control plane described below.

The packet forwarding plane is fundamental to delivering end-to-end circuit provisioning, as well as telemetry aggregation and visualization. It provides the class of service, timing, and synch and control plane flexibility to solve for deterministic applications demanding millisecond resolution. It also solves for traffic engineering and network resiliency with application service-level agreement (SLA) guarantees maintained in real time with node-level streaming telemetry.

The packet forwarding plane provides a common platform that enables the use of OT-SDN, a software-defined solution with broad support for applications using DNP3, Modbus, SSH, and IEC61850 protocols, as well as MPLS, VPLS, MPLS-TP, and Segment Routing in the WAN. When required, the packet forwarding plane supports brownfield environments containing serially attached RTUs and IEDs by encapsulating serial data streams in Ethernet frames for transport while maintaining latency, asymmetry, and network healing attributes for synchronous applications like line current differential teleprotection[1].

[1]For more information, please see "LINE CURRENT DIFFERENTIAL PROTECTION OVER MPLS" www.juniper.net/assets/us/en/local/pdf/whitepapers/2000733-en.pdf

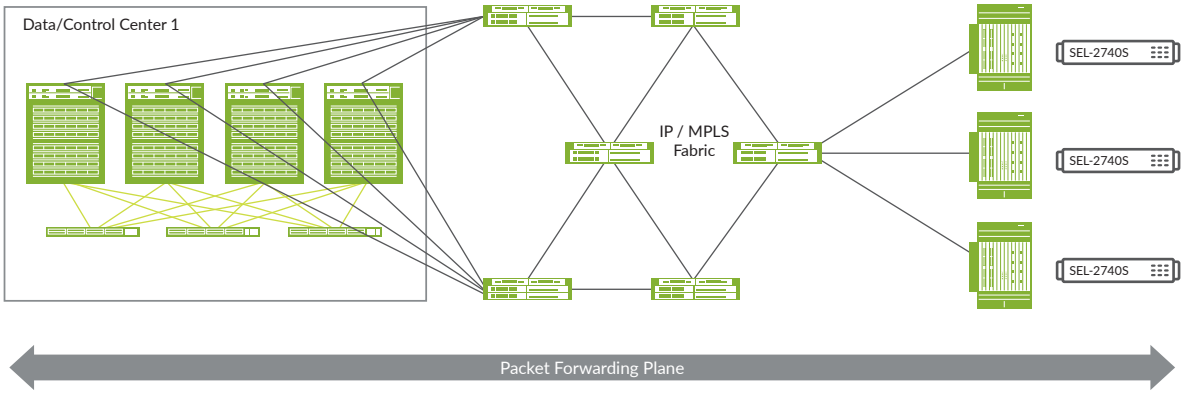

Figure 2: Solution requirements components for the packet-based forwarding plane

The Converged Industrial Edge for Utilities packet-based forwarding plane architecture calls for a data center-compliant Ethernet fabric to simplify and automate many of the tasks associated with managing a data center and extending its connectivity to other data centers or cloud offerings. As such, the Ethernet fabric provides the following functionality:

- A Layer 3 IP-based underlay, also known as a Clos network. Ideally, the IP fabric utilizes a spine-and-leaf architecture that provides low-latency, nonblocking, high-bandwidth connectivity from any physical device (server, storage device, router, or switch) to any other physical device.
- An EVPN-VXLAN overlay for network virtualization. With overlays, endpoints such as servers or virtual machines (VMs) can be placed anywhere in the network and remain connected to the same logical L2 network, decoupling the virtual topology from the physical topology. Overlays enable multitenancy (IT-OT) within a network and for sharing the same physical network while isolating one tenant's traffic from everyone else's.
- A multiprotocol IBGP protocol to exchange reachability information across an IP network, enabling flexible overlay services like bridged, routed, and edge-routed services.
- A fabric control function used to create a single fabric backplane for primary and backup control centers, enabling geo-redundant Data Center Interconnect (DCI).

Juniper Networks data center-compliant fabric is marketed as our data center portfolio. Please visit www.juniper.net/us/en/products-services/switching/qfx-series/ for more information about Juniper's complete data center switching portfolio.

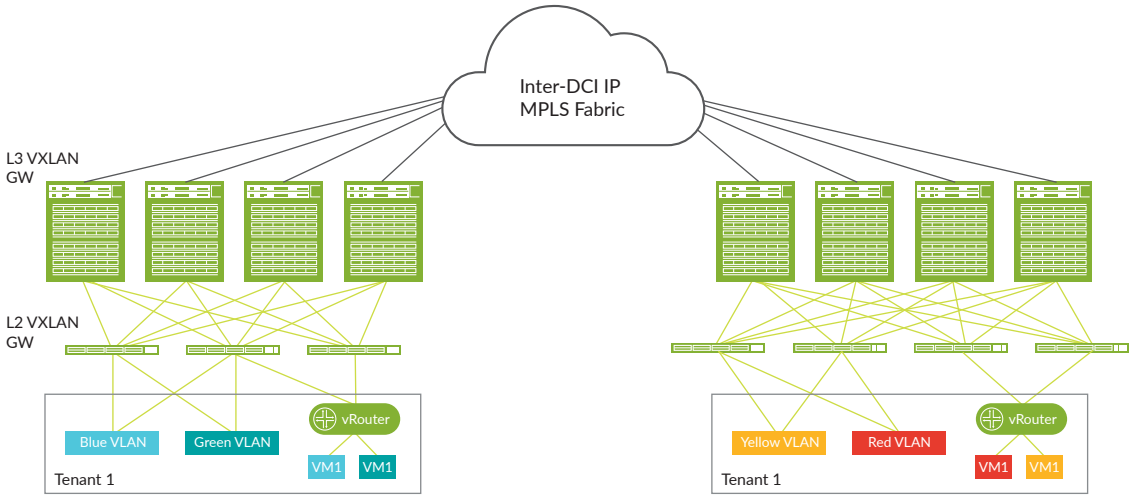

Figure 3: Single fabric, geo-redundant data center

The Converged Industrial Edge for Utilities packet-based forwarding plane architecture calls for a feature-rich MPLS WAN capable of supporting all manner of utility IT and OT/ICS use cases, be they deterministic, best effort, permanent, or ephemeral, between control centers and substations, and between substations and substations. As such, the MPLS WAN provides the following functionality:

- Separate control and forwarding planes for network scalability and security
- Common software and user interfaces across all devices to create "golden" configurations and reduce provisioning errors by streamlining training for engineering staff
- Modular operating system to enable better resource utilization and isolation of network functions
- Purpose-built systems designed for service provider applications with 99.999% or greater reliability
- Scalable and programmable silicon that eliminates "rip and replace" upgrades to support new software functions
- Standards-based, nonproprietary protocols and functions to ensure interoperability, allowing best-of-breed networks without vendor lock-in
- Support for legacy services in conjunction with new technologies like EVPN and Segment Routing for a phased migration when adding new services alongside existing applications
- Full MPLS-based design with advanced traffic engineering based on RSVP and/or Segment Routing
- A rich set of APIs for complete SDN control as well as on-box automation capabilities to support operations teams
- Support of advanced timing for phase, frequency, and time of day from IEEE 1588v2 primary or reference clock using G.8265.1 and G.8275.1 profiles
- Support of NEBS Level 3 and IEEE 1613 hardening compliance

Juniper's MPLS WAN is marketed as our routing portfolio. Please visit www.juniper.net/us/en/products-services/routing/ for more information about Juniper's complete MPLS WAN portfolio.

The Converged Industrial Edge for Utilities packet-based forwarding plane architecture calls for an OT-SDN and IEC 61850-compliant Ethernet fabric, capable of supporting all manner of utility IT and OT/ICS use cases within the distributed control system substation. As such, the OT-SDN and IEC 61850-compliant Ethernet fabric must provide the ability to:

- Traffic-engineer each communications flow with a deny-by-default architecture, per application
- Support proactive configuration of predetermined primary and failover communication flows
- Provide network convergence times of less than 100 microseconds for critical applications
- Utilize every port and link on a given Ethernet node (no blocking ports)
- Test and validate configurations without affecting existing service or applications
- Commission new services on demand or on a scheduled basis
- Provide C37.238 Precise Time Protocol (PTP) transparent clock, ensuring sub-microsecond time synchronization of end devices
- Utilize open, standards-based protocols and APIs for integration into higher level automation platforms
- Allowlist network flows with matching rules on fields in Layers 2 through 4

SEL Inc.'s OT-SDN and IEC 61850-compliant Ethernet fabric is marketed as the SEL-2740S Software-Defined Network Switch. For more information, please visit https://selinc.com/products/2740S/.

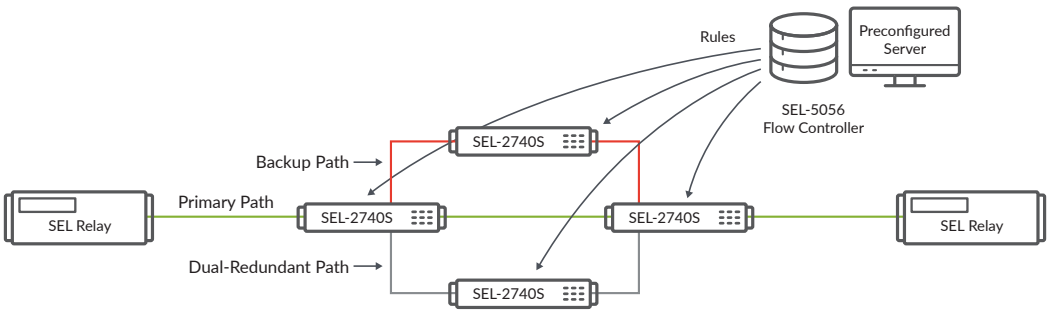

Figure 4: SEL Inc.'s OT-SDN Ethernet fabric

Management and Control Plane

"Centralize what you can, distribute what you must." Pradeep Sinhdu, Founder Juniper Networks

The Converged Industrial Edge for Utilities architecture's management and control plane is a set of discreet software applications like WAN and LAN controllers, telemetry aggregators, collators, and element managers, safely interoperating on a modern Kubernetes software platform to deploy use cases, services, and applications as workflows. The software components are integrated on physical servers optimized for on-premises, private, operational cloud (OC) deployments.

The Kubernetes cluster is a microservices architecture used to control and deploy multivendor applications as microservices that are small, messaging-enabled, bounded by contexts, autonomously developed, independently deployable, decentralized, and built and released using automated processes. Vendor software functionality is exposed only through standard APIs.

The architecture employs event-driven infrastructure (EDI) buses to support inter-application communication at the microservices level. An Argo workflow engine connects operator intent with corporate network security policy and inventory. Use cases are delivered as workflows, and workflows are triggered by sources such as event bus notices, form submissions, and alerts from distributed, intelligent LAN controllers in substations. Workflows trigger services that provision, monitor, and test circuits, processes, and state of the operations cloud network. An external identity management platform is integrated into the management control plane to ensure identity, encryption, and forensic accounting audit logging. This software architecture is a cloud-native, fault-tolerant, secure abstraction of containers, deployed in clusters and orchestrated and load-balanced for resilience.

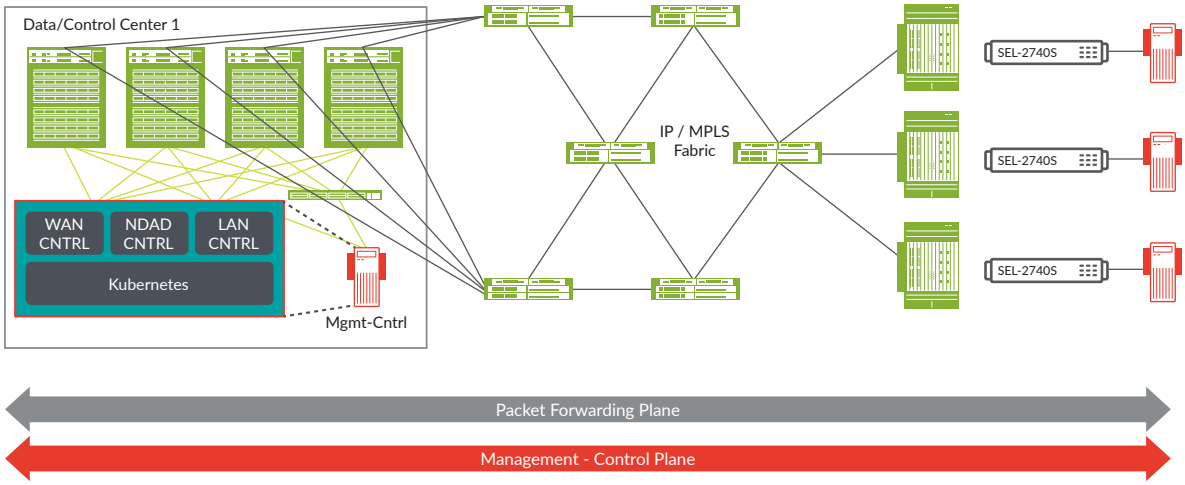

Figure 5: Solution requirements components for the management and control plane

The Converged Industrial Edge for Utilities architecture calls for an automation platform (described above) that resides in the data or control center. Other software integrated into the automation platform may include a virtual routing function used to create the networking plane of a Kubernetes cluster, enabling scalable routed services between virtual resources and network-based resources like storage.

WAN Controller

The Converged Industrial Edge for Utilities architecture calls for a network-aware WAN controller to serve as a single interface for managing the creation and deployment of WAN transport label-switched paths (LSPs) and L2/3 VPNs (IP). The WAN controller resides within the automation platform as a microservice; as such, the WAN controller provides the following functionality:

- Traffic engineering that provides visibility into and control over IP/MPLS flows in private enterprise networks. It must allow operators to optimize their network infrastructure through proactive monitoring, planning, and explicit routing of critical traffic loads, enabling a more efficient utilization of networks while ensuring predictability, resiliency, and SLAs.
- IETF and Web protocol standards to ensure integration with multivendor infrastructure and existing OSS/BSS systems. The WAN controller provides VPN/MPLS visualization and monitoring.
- Multilayer controller functionality that can dynamically interact with transport/optical controllers and reroute IP/MPLS flows, adapting to real-time changes in multiple layers of the architecture.
- Open standards like the Path Computation Element (PCE) architecture as defined in RFC 5440. It should leverage the "active stateful PCE" concept, which allows it to learn about the network and LSP path state via the Path Computation Element Protocol (PCEP) by communicating with a client-side component present in the network devices themselves. The client is referred to as a Path Computation Client (PCC).
- Dynamic topology discovery of the network by peering via IGP (ISIS-TE, OSPF-TE) and listening to BGP-LS updates. Modification of existing paths or provisioning of new paths through PCEP standard. Service mapping is performed using the Network Configuration Protocol (NETCONF) and YANG data modeling language.
- Identification and elimination of congestion scenarios in which traffic streams are inefficiently mapped onto available resources, causing overutilization of some subsets of network resources while other resources remain underutilized.
- Use of standard northbound APIs such as HTTP-based REST to ease integration with existing OSS/BSS systems, third-party traffic modeling/planning scripts, or custom applications.
- A testing microservice, implemented as a workflow, for testing VPNs between the WAN ingress/egress nodes and the end-to-end circuit, potentially spanning multiple substations. The testing service workflow includes settings for the configuration options for required testing, as well as for generating traffic for performing the test.
- Specific path ordering and synchronization, signaled across routed network elements and allowing a global view of network state for monitoring, management, and proactive planning.
- Predictable, deterministic state so as to minimize distributed state, increasing the efficiency of existing network elements via offloading of control plane processing.
- A foundation for additional centralized network infrastructure services—API for the network with NETCONF/Yang and RESTCONF. It also provides operational simplicity by enabling an SDN control point across disparate elements across the network.

The Juniper version of the WAN controller is marketed as the Juniper Networks NorthStar Controller. For more information, please visit www.juniper.net/us/en/products-services/sdn/northstar-network-controller/.

Analytics and Diagnostic Tool

The Converged Industrial Edge for Utilities architecture calls for intelligent network- and device-level analytics and diagnostics (NDAD) tools to provide actionable insights into the health of individual devices as well as the overall network. The NDAD resides within the automation platform as a microservice and securely exchanges telemetry, trigger, and other information with other microservices like the WAN controller. It can trigger workflows for automated responses to device- and network-level problems or indicators. As such, the NDAD provides the ability to:

- Integrate multiple data collection methods (such as Junos Telemetry Interface, NETCONF, system logging, OpenConfig, and SNMP); aggregate and correlate large volumes of time-sensitive telemetry data and analytics; and provide a multidimensional, predictive network view
- Translate troubleshooting, maintenance, and real-time analytics into actionable insights operators can use to determine the health of an individual device and the overall network
- Provide a framework for defining and customizing health profiles at the device and network levels
- Automate root-cause analysis and log file analysis, providing a framework to define and customize diagnostic workflows
- Provide multidimensional analytics across network elements and tools to establish operational benchmarks
- Provide a telemetry visualization function for monitoring and troubleshooting
- Define closed-loop automation and extend automation through open, standards-based interfaces to other automation assets with complementary capabilities (see closed-loop automation steps as shown in Figure 6)
- Interface with third-party provisioning network management systems (NMS), providing for multivendor network health monitoring

Figure 6: Closed-loop automation steps

The Juniper NDAD tool is called Contrail® Healthbot. For more information, please visit www.juniper.net/uk/en/products-services/sdn/contrail/contrail-healthbot/.

LAN Controller

The Converged Industrial Edge for Utilities architecture calls for a LAN controller to provide an orchestrated virtual environment, running on a ruggedized compute platform, for securing, managing, and isolating control system software applications within a substation.

The LAN controller physically resides within the substation, where it provides local orchestration, security, and management in a distributed microservices computing platform developed for control systems. The LAN controller functions as configured, even without communications to the automation platform, which is physically in the data or control center, providing laminar resilience to the overall solution. In normal operation, the LAN controller communicates with a "primary" microservice in the automation platform and securely exchanges telemetry, trigger, and other information with other microservices like the WAN controller and NDAD tool. The LAN controller can also initiate or respond to workflows from the local environment, or the automation platform. As such, the LAN controller provides the ability to:

- Participate on an event-driven infrastructure (EDI) "pub/sub" bus to manage individual LANs
- Describe the OT-SDN switches, existing dataflow rules, available communication service types (CSTs), flow groups, traffic meters, set queues, and additional switch information upon trusted query
- Support Layer 3 SCADA protocols like DNP3, Modbus, and others via OT-SDN infrastructure and services
- Provide the ability to create, deploy, and safely tear down VLANs within substations
- Continue functioning as configured during catastrophic situations wherein communications to the control center are cut off or severely diminished

- Maintain the identity of connected hosts and their connectivity information, as well as provide visual representations of state
- Process requests for logical connection configurations, which requires pushing CST configuration information to OT-SDN switches
- Maintain mapping of data between substation applications and devices
- Maintain separate, secured communication domains within the system
- Scale processing and storage requirements as systems grow
- Support redundant data flows and applications
- Ensure versioning applications adhere to security policies
- Process requests for safely rolling out application updates
- Manage complex settings that span multiple devices
- Secure the operating system with a secure boot loader and the communication interfaces

SEL Inc.'s LAN Controller is marketed as the SEL-5056 Software-Defined Flow Controller. For more information, please visit https://selinc.com/products/5056/.

Cybersecurity Plane

The Converged Industrial Edge for Utilities architecture's cybersecurity plane is composed of Juniper Networks SRX Series Services Gateways and vSRX Virtual Firewall, Policy Enforcer software, and threat-aware WAN networking equipment, as well as the Dragos Inc. threat protection and incidence response products and services for OT industrial control systems (ICS) environments. The technical interoperation between Juniper, SEL, and Dragos leverages open, standards-based protocols and APIs that provide the necessary connectivity to the higher level automation platform and the packet forwarding plane.

The Dragos Platform provides comprehensive visibility of ICS/OT assets. Based on its ability to identify assets, manage profile communications, and detect malicious threat behaviors, it can rapidly pinpoint malicious activity within the OT/ICS environment and provide security analysts or SOC personnel with context-rich insight into threats. Juniper's policy enforcement engine, integrated into the management control plane described above, can ingest indicators of compromise (IOCs) and other information from Dragos and take action based on threat levels. Actions may include threat intelligence gathering, redirection of a flow or VLAN, or, in extreme cases, the quarantining of traffic at the IP level.

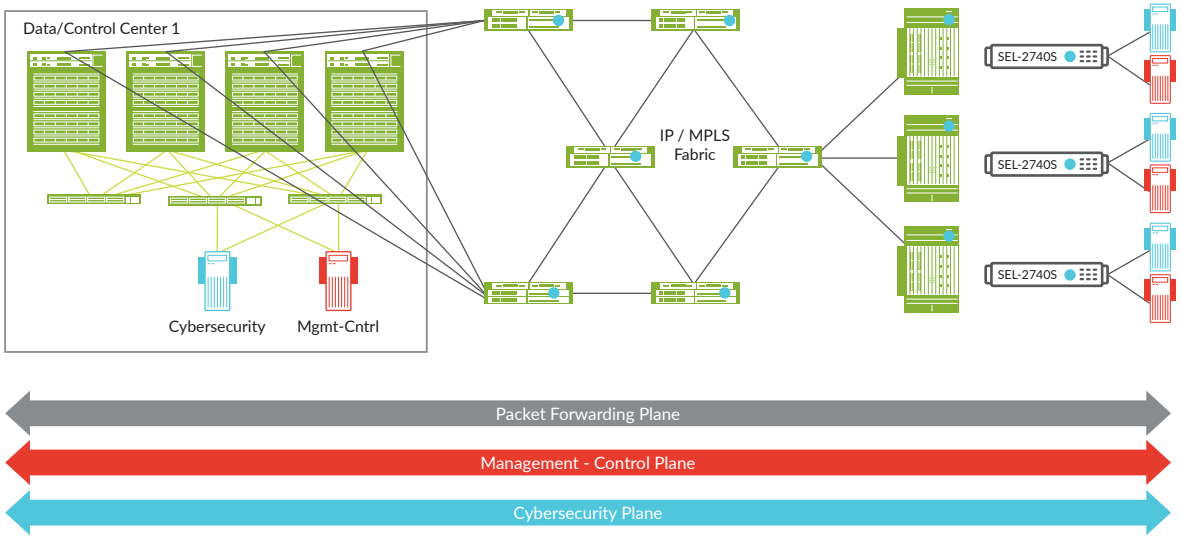

Figure 7: Solution requirements components for the cybersecurity plane

OT/ICS Threat Detection

The Converged Industrial Edge for Utilities architecture calls for an OT/ICS threat detection capability to passively discover assets and their communication profiles. The solution needs to include known malware threats and anomaly-based detection methods. Additionally, it will leverage advanced intelligence-driven analytics derived from known adversary tactics, techniques, and procedures to sufficiently identify and prioritize risks. As such, the ICS/OT threat detection capability must have the ability to:

- Passively identify OT/ICS device make, model, operating system, and firmware
- Provide in-depth analysis of network communications to baseline asset traffic profiles
- Dissect the traffic and identify configuration changes and behaviors that could be cyber threat-related
- Leverage threat behavior analytics to identify cybersecurity threats through intricate patterns of adversary techniques, tactics, and procedures
- Provide best-practice playbooks to investigate and efficiently respond to threats before they cause significant impacts against operations, processes, or people
- Provide context-rich alerts and notifications tied to investigation playbooks to help analysts respond to cyber threats

Dragos Inc.'s OT/ICS system is marketed as the Dragos Platform. For more information, please visit www.dragos.com/industries/?ind=114.

Physical and Virtual Firewall

The Converged Industrial Edge for Utilities architecture calls for a portfolio of security services gateways that range from an all-in-one, integrated physical device for use cases in home, office, and headquarters locations, to a highly scalable, chassis-based solution for the data center. It also includes virtual alternatives that can be deployed within the private operations cloud and the public cloud. The security services gateway should be able to ingest threat intelligence aggregated and delivered through a trusted, authenticated intelligence feed. As such, the security gateway must provide:

- Comprehensive threat protection against known and unknown threats
- Carrier grade reliability of 99.999%, with continuous uptime through in-service hardware and software upgrades
- Visibility and advanced security services for containerized and microservices environments
- Visibility into IT network threat behavior to maintain an effective security posture, including the ability to enforce policies through automated threat remediation capabilities on every port
- Advanced threat intelligence that can be maintained locally, with the ability to dynamically adapt to new threats
- Actions to stop the lateral propagation of security threats

Juniper Networks portfolio of security services gateways is marketed as the SRX Series Services Gateways. For more information, please visit www.juniper.net/us/en/products-services/security/srx-series/.

Threat-Aware Networking

The Converged Industrial Edge for Utilities architecture calls for the ability to aggregate and curate a threat data feed from multiple sources, along with the ability to deliver threat data to network infrastructure such as switches, routers, and firewalls for the purpose of distributing actionable intelligence and enforcement capabilities to all connection points in the network. As such, the threat data feed capability provides the following functionality:

- Actionable data sets including attacker IPs, Command and Control (C&C), GeoIP, infected hosts, and dynamic address groups
- Global as well as custom allowlists and blocklists of file hashes, domain names, IP addresses, malicious URLs, code signing certificates, signer organizations, and third-party threat data for policy enforcement
- Network infrastructure such as routers, switches, and firewalls capable of receiving and digesting a threat data feed such that identified blocklisted traffic like (but not limited to) C&C traffic can be automatically dropped

Juniper's threat data feed solution is marketed as Juniper Advanced Threat Prevention. For more information, please visit www.juniper.net/us/en/products-services/security/advanced-threat-prevention/.

The ability of Juniper's Networks to extend security intelligence to every connection point in the network is called Juniper Networks SecIntel. For more information, please visit www.juniper.net/us/en/products-services/security/sec-intel/.

Conclusion

OT/ICS personnel are justifiably suspicious of IT technology's lack of determinism and precision. The "best effort" nature of IT-based communications technologies fundamentally conflicts with the sub-millisecond demands of grid control and protection applications, putting expensive grid assets—and even personal safety—at risk. Even as the economics of OT/ICS systems modernization exposes the advantages of converging IT and OT networks, the lack of a common, trusted communications model impedes implementation and delays benefits.

The private operation cloud model is presented as a next-generation alternative. Carefully curated from the technologies that represent the leaders in the given domains, the operations cloud model accounts for all the precise timing and change controls required for grid operations, while introducing robust, cloud-native technology capabilities that improve cybersecurity, resilience, and situational awareness—all while driving costs down.

Juniper Networks has traditionally disrupted markets through innovation. From being the first router vendor to separate control and forwarding planes to leading standards committees in segment routing and EVPN, Juniper has always sought to solve the big problems. By partnering with SEL Inc. and Dragos Inc., Juniper both confirms its market leadership position and acknowledges the domain expertise of the best-of-breed partners it takes to exploit the power of open, standards-based communications platforms—along with creating business value by innovating with cloud-native technologies in the dynamic critical infrastructure market sectors.

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 SEL Inc.

SEL invents, designs, and builds digital products and systems that protect power grids around the world. This technology prevents blackouts and enables customers to improve 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 now serves customers worldwide. Our mission is simple: to make electric power safer, more reliable, and more economical. Learn more at www.selinc.com

About Dragos Inc.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The expert practitioners who founded Dragos were drawn to this mission through their decades of experience in the U.S. Military and Intelligence Community going head to head with cyber attackers who threaten the world's industrial infrastructure. Our solutions combine advanced technologies for asset identification, threat detection, and response with the battle-honed insights of our elite team of industrial control systems (ICS) cybersecurity experts. We arm enterprises with the tools to identify threats and respond to them before they become significant breaches. Dragos currently protects hundreds of organizations and provides the industrial control systems community with selected free technology products, research, and thought leadership. Dragos is privately held and headquartered in the Washington, DC area. Visit dragos.com for more information or follow us on Twitter or LinkedIn.

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