

# Project Ambassador

## Schweitzer Engineering Laboratories

Dennis Gammel  
Cybersecurity for Energy  
Delivery Systems (CEDDS)  
Peer Review

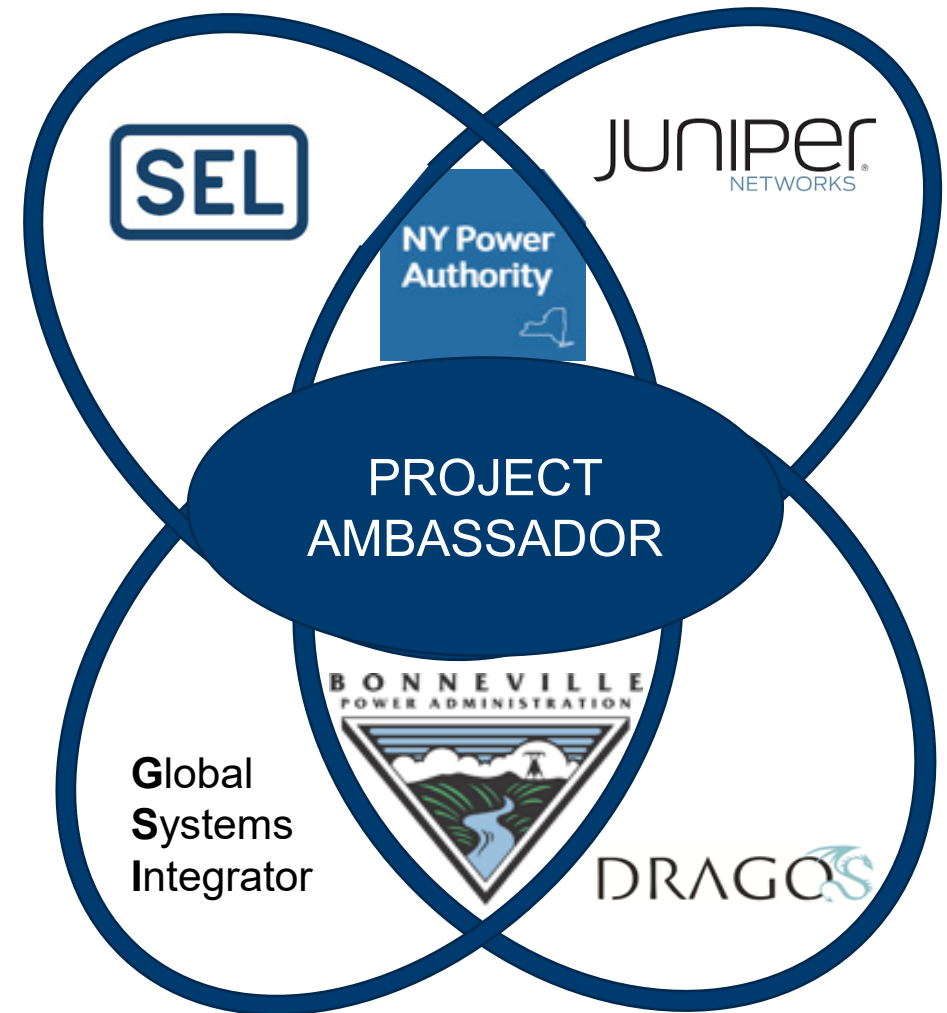
October 6-7, 2020



# Ambassador Project Overview

## Objective

- In order to strengthen the cybersecurity for energy delivery systems using the proven DOE OT SDN technology, the Ambassador project shall research, develop, demonstrate, and productize a joint manufacturing solution capable of managed trust and data sharing between multiple software applications for improving awareness and visualization of utilities' enterprise and OT systems.
- Ambassador intends to address CEDS Topic Area 4: Cybersecure Cloud-based Technologies in the Operational Technology (OT) Environment



# Ambassador Project Status

## Schedule

Project Start:	Oct 01, 2018
Project End:	Sep 30, 2021
✓ Concept Doc	Jun 28, 2019
✓ Network Test Bed	Apr 01, 2020
✓ Functional Design Spec	Apr 15, 2020
✓ Technical System Specs	Sep 15, 2020
❑ Message Bus Proto	Nov 15, 2020
❑ Code Complete	Mar 03, 2021
❑ Complete Integration	May 29, 2020
❑ Validation & Demo	Sep 01, 2021
❑ Final Deliverables	Sep 30, 2021

---

**Total Value of Award:** **\$ 5,114,520**

---

**Funds Expended to Date:** **37%**  
**\$ 1,893,188**

---

**Performer:** **Schweitzer Engineering Laboratories, Inc.**

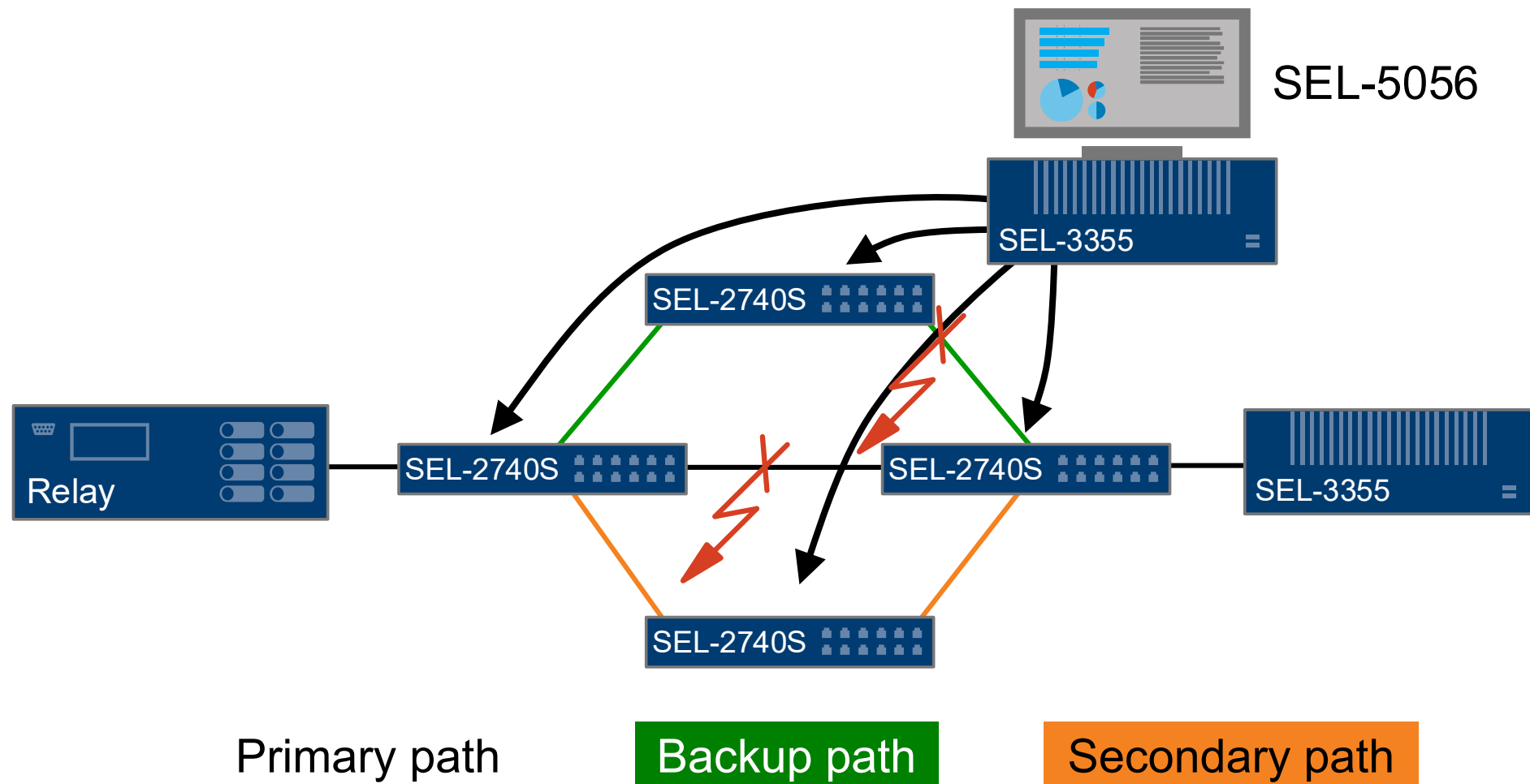
---

**Partners:** **Bonneville Power Administration**  
**Dragos Inc.**  
**Juniper Networks**

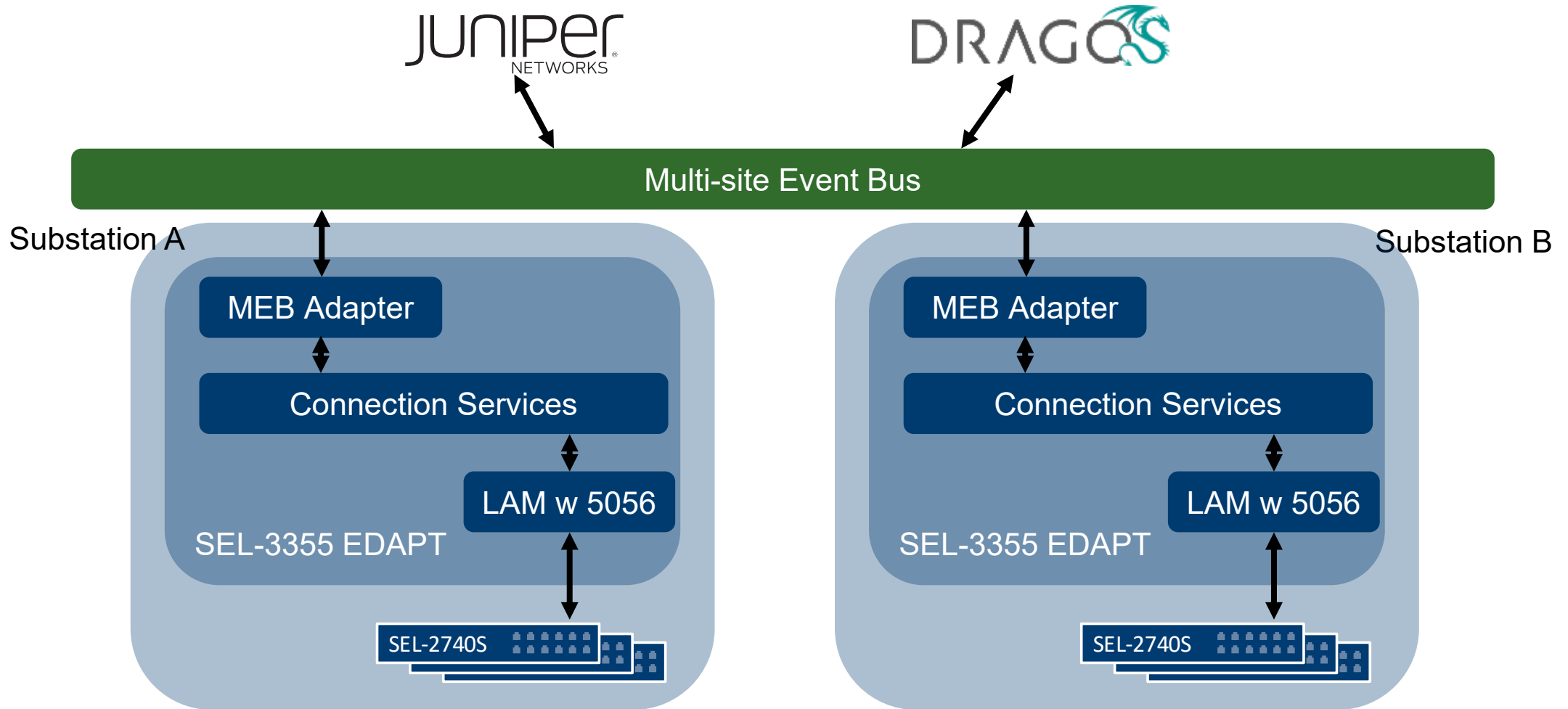
---

# Today's Present State of the Art (SOA)

## DOE's OT Software Defined Networking



# Advancing the State of the Art (SOA)



# Progress to Date

## Major Accomplishments

- Shared Development between 3 Manufacturers
- Cloud based technology applied appropriately to OT systems
- Herndon, VA Lab containing integrated product and solutions
- Specification and Design complete on a Joint Capability between 3 manufacturers
- Development Complete on the Juniper Networks Solution

# Challenges to Success

## Shared Development Between 3 Manufacturers

- Understanding of each partner's goals and aligning those goals
- Understanding of shared capabilities between the partners
- Leveraging cloud technologies to realize new technology for OT systems

## Making Electric Power Safer, More Reliable and More Economical

- Listening to our utility partners
- Understanding the utilities' **needs**
- Aligning the manufacturers' joint capabilities and goals with the utilities' needs

# Collaboration/Sector Adoption

## **Plans to transfer technology/knowledge to end user**

- Utility end users include but are not limited to the following:
  - Enterprise and IT owners
  - Automation and substation communications engineers
  - IT and OT security engineers
- Steps to gain industry acceptance
  - Webinars and panels to teach the technology (Begin November 2020)
  - Demonstrate joint capability at utility partners' lab (Summer 2021)
  - White paper(s) on the technical aspects and technology benefits (November 2020)
  - Case studies on the pilot projects planned (Beginning Fall 2021)



# Next Steps for this Project

## **Approach for the next year or to the end of project**

- Dragos and SEL to complete development (March 2021)
- Functional testing of all 3 manufacturers' solutions (May 2021)
- Integration testing of solutions on the Herndon Lab test bed (July 2021)
- Demonstration of Joint Capabilities (August – September 2021)

# Today's Utility Application State

## Software Environments

Platforms where Software Solutions are Deployed at the Customer Site

### Corporate OT Software

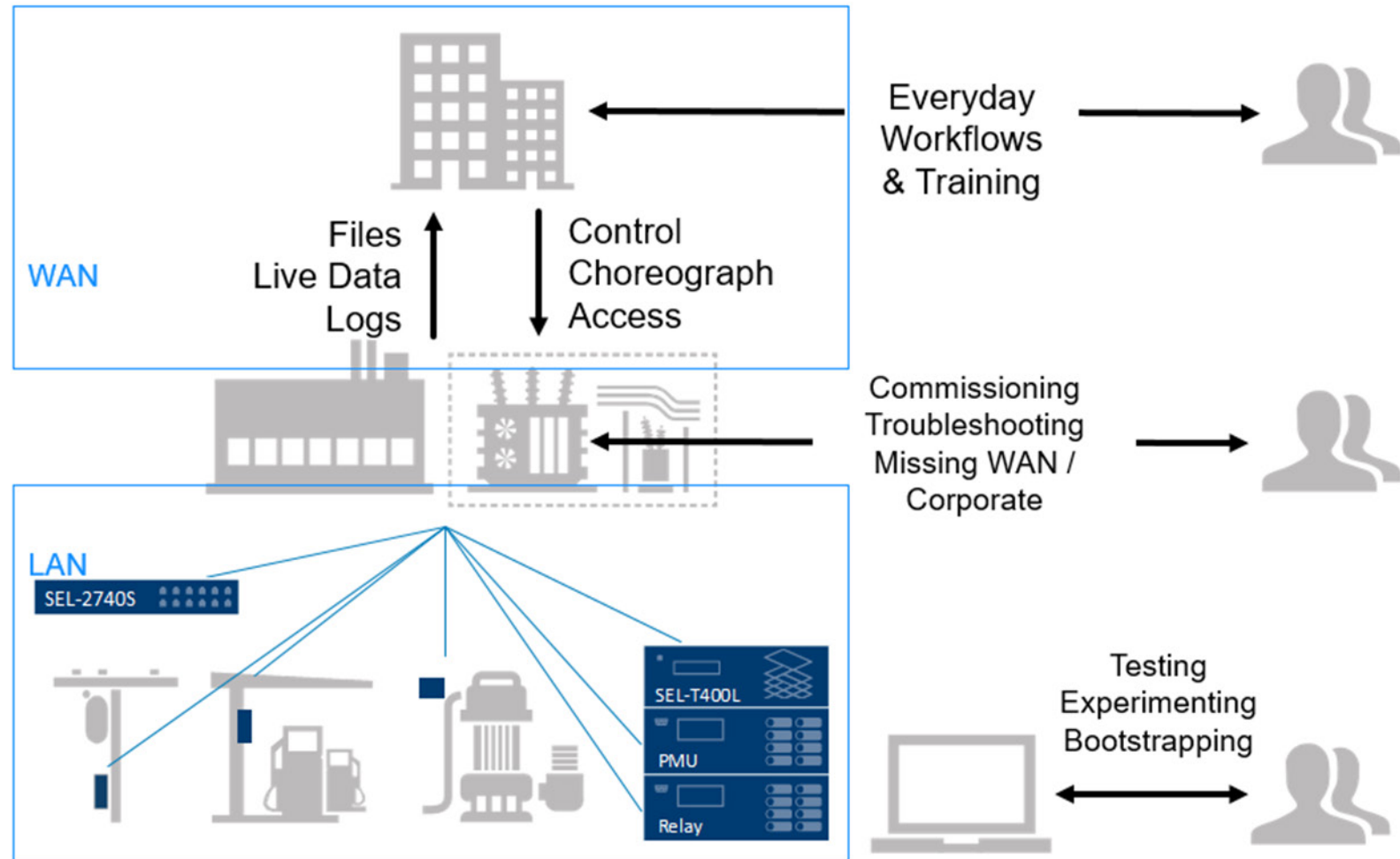
Multi-site Orchestration  
Audits / Reports / Analysis  
Historians / Mass storage  
Access Options

### Distributed Software

Tier 2 Control (FLISR / GCS / ADMS)  
Orchestration and Control Plane  
Data Aggregation  
LAN Device Management  
Access Point from Corporate to Local

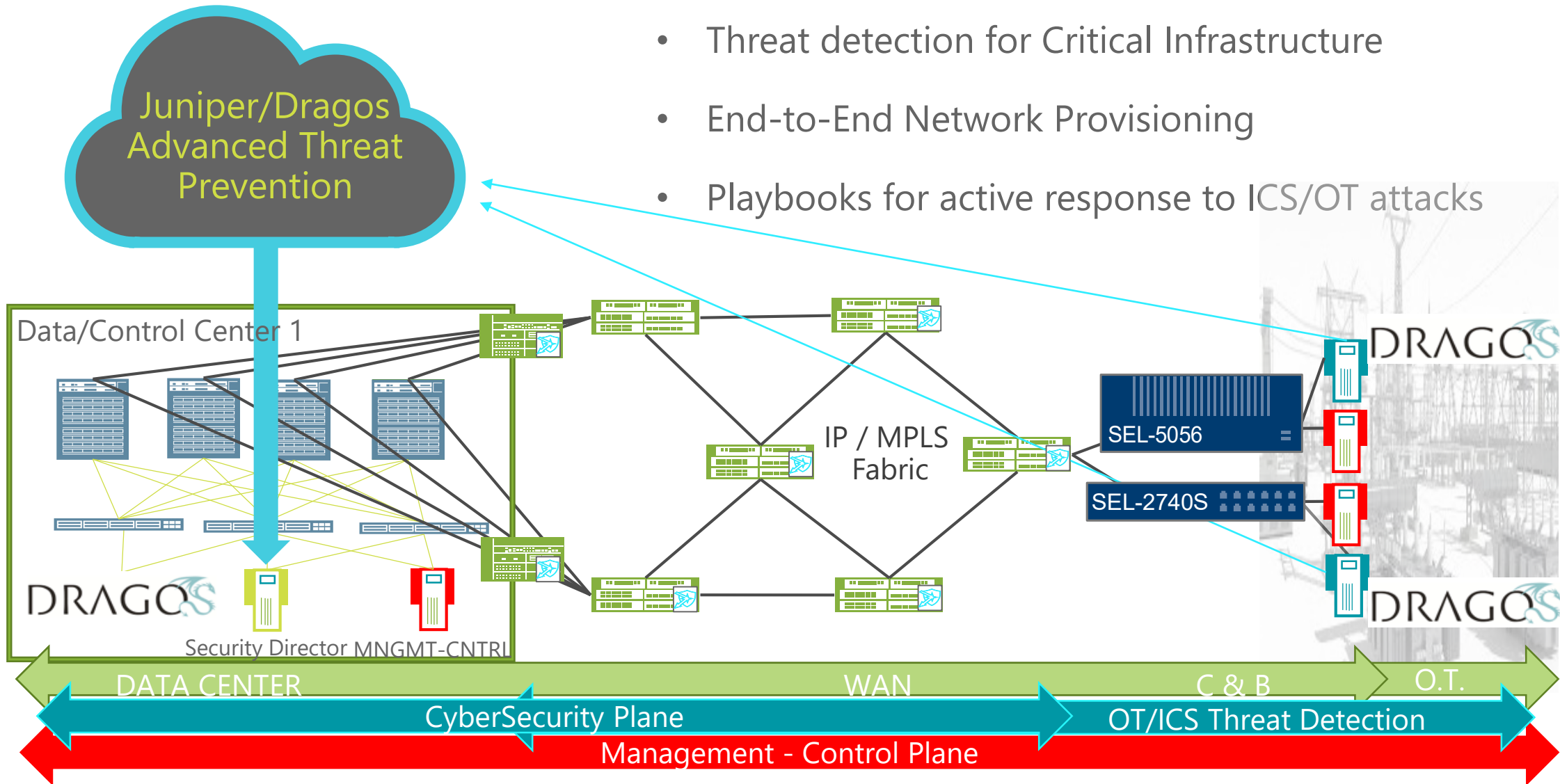
### Edge

Tier 1 Control (Protection etc..)  
Data Sensors  
Actuators

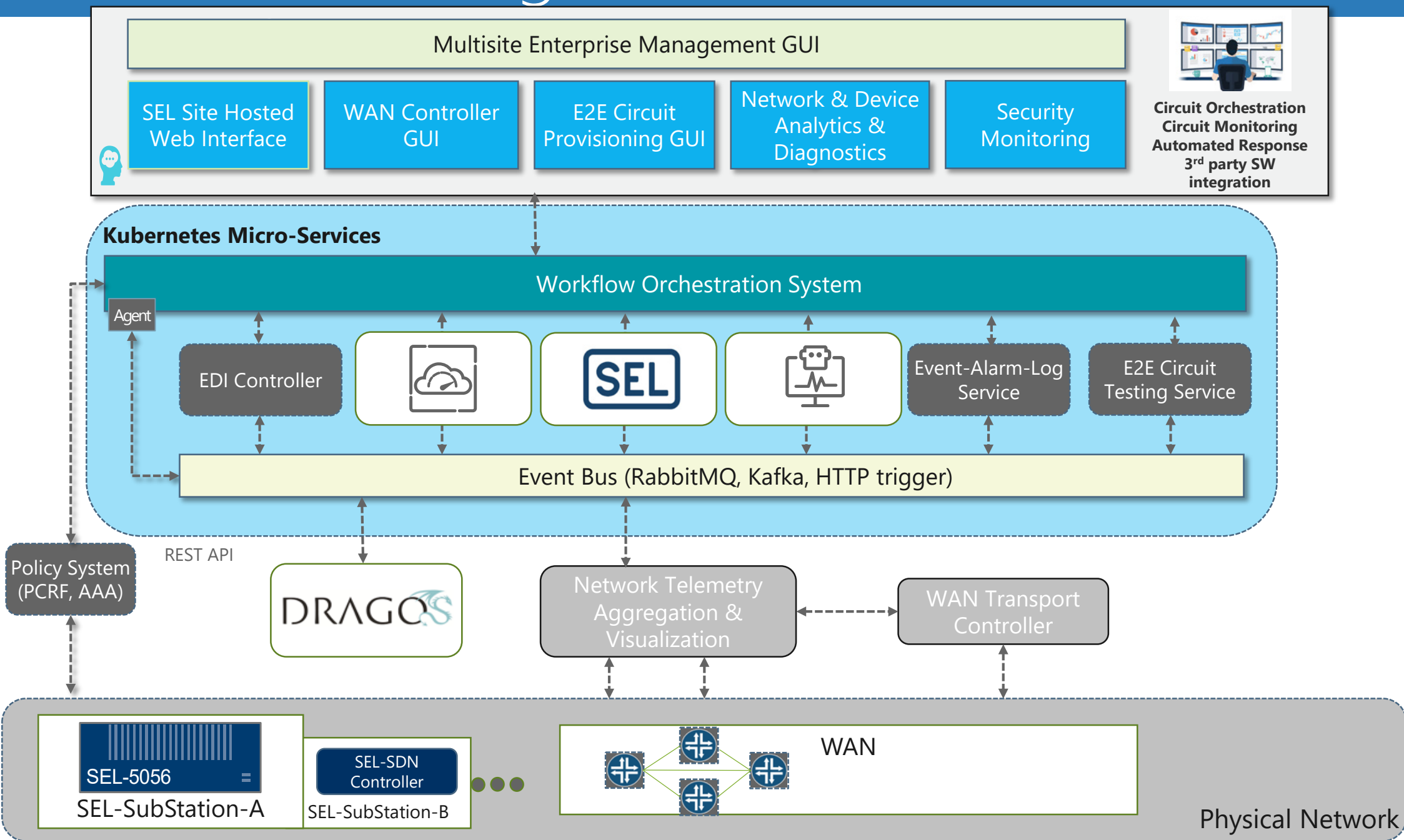


# Full-Stack Enterprise + OT Solution

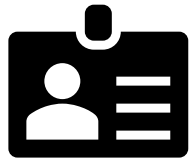
- Threat detection for Critical Infrastructure
- End-to-End Network Provisioning
- Playbooks for active response to ICS/OT attacks



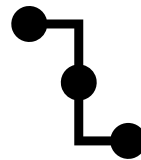
# IT - OT Convergence Solutions



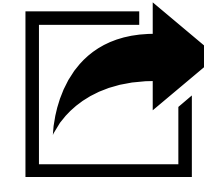
# Multi-Site Event Bus Adapter



**Authenticate**  
To MEB broker



**Translate**  
Provisioning and  
teardown requests  
from MEB  
To Connection Services model



**Publish**  
Configuration and  
Diagnostic  
information to MEB  
For enterprise monitoring and  
threat hunting context

