Solution brief
Cisco confidential

The bridge to possible

Making Industrial IoT Simpler

The power of Cisco DNA Center in industrial automation networks

Industrial automation systems have fully adopted standard networking technologies and rely on them for the bulk of their communications. These networks must have the scale, flexibility, performance, and resiliency needed for these critical systems. This connectivity is the foundation for the industrial IoT and Industry 4.0 evolution – connecting sensors, actuators, and control systems to the machine-learning, digitization innovations in the cloud. IT/OT convergence in networking and security technology is not just established but critical to a wave of optimizations and improvements in the ecosystem.

Oddly, the network management and tools are still far from converged. Operational Technology (OT) personnel do not have the same access to, and benefit of the network and security management tools used by IT. Yet they still need to rely on the network to operate the production environment, often without tools that tell them how the network is performing and the ability to maintain that network. If a link fails or a device connects improperly, it takes a sleuth to identify and resolve the problem. Key challenges facing OT personnel include:

- Lack of visibility into network status and events that impact production
- Difficulty of applying consistent network configurations
- No effective means to update network infrastructure after initial deployment

Benefits

Cisco DNA Center improves industrial operations by:

- Increasing overall equipment effectiveness and uptime
- Lowering operational costs
- Simplifying network management for IT and OT
- Enhancing security
- Helping ensure network performance
- Transforms network operations

Meanwhile, in the IT ecosystem, network management is going through a “software-defined” evolution to help IT organizations operate and maintain networks with less operational effort, more automation, and the benefit of machine learning to give assurance that the network is doing its job. Cisco DNA Center is a software-defined network controller for enterprise networks. The solution described here applies Cisco DNA Center to industrial automation networks and, alongside IT, gives OT a curated view and set of functions to perform key network maintenance tasks, consistently and scalably. It’s a first step in the evolution to a fully software-defined network such as Cisco Software-Defined Access. Key benefits of integrating Cisco DNA Center into production networks include:

- Increased production uptime: Identify and resolve issues that impact production more quickly to avoid and reduce downtime
- Lowered costs: Automate and scale time-consuming activities such as configuration and updates to network infrastructure
- Optimized network performance for critical industrial automation applications and devices
- Increased security: Enhance the visibility of assets and interactions; segment the network by defining and applying access policies
- Simplified management: Operate the industrial network (wired and wireless) with views and functions for both IT and OT roles
- Transformed network: Benefit from cloud-based AI/ML to optimize network operations and as a platform for extensibility

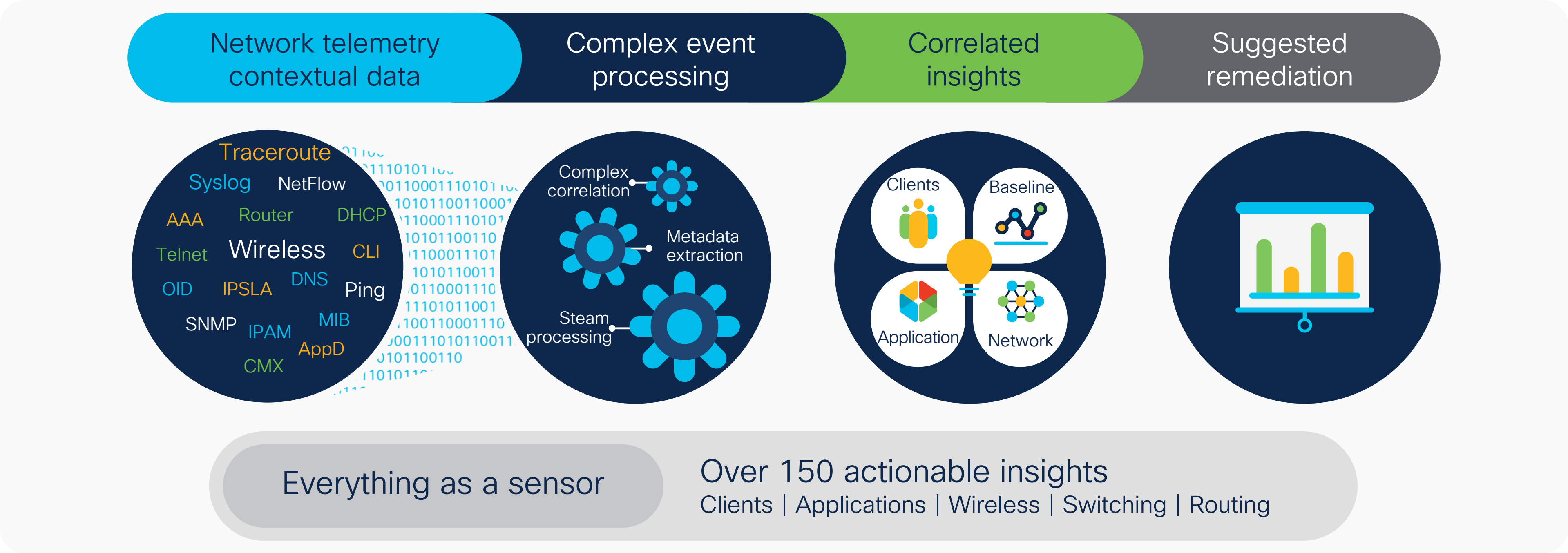
The following sections provide an overview of the key Cisco DNA Center features–Assurance and Automation–and review an Industrial Automation Reference Architecture, concluding with a summary of the solution benefits for customers, system implementers, and partners in the industrial automation ecosystem.

Assurance of network performance

Outages and downtime in production environments result in significant loss, whether caused by network failures, human error, or equipment failure. Bringing production back online quickly reduces the impact. The Cisco DNA Center Assurance suite of features and functions helps IT and OT quickly identify network outages or performance issues and resolve them rapidly. The key use cases this solution incorporates include:

- Discovering the network infrastructure and network topology and visualizing them in easy-to-configure views
- Collecting and analyzing network telemetry information, including Simple Network Management Protocol (SNMP), syslog, and IP Flow Information Export (IPFIX) and NetFlow1 data
- Identifying and profiling end devices connected to the network and their connectivity status, including Industrial Automated Control System (IACS) devices such as sensors, actuators, and controllers, as identified by Cisco® Cyber Vision and communicated via Cisco Identity Services Engine (ISE)
- Having visibility into applications operating on the industrial networks1
- Proactively identifying issues in the network that impact production systems
- Collecting contextual information for accurate root-cause analysis without the need to re-create the issue
- Helping step through remediation options to speed issue resolution
- Examining VLAN settings to solve reachability issues
- Providing network and device health monitoring status and history
- Using the Machine Reasoning Engine (MRE) to accelerate remediation of issues
- Providing security compliance views to indicate potential risks
- Using tools such as path trace and packet capture to aid in problem resolution
- Identifying VLAN and inter-switch link configuration mismatches (e.g., VLAN, speed, duplex)
- Customizing to allow OT- and IT-specific roles based on feature-set and location/site

Figure 1. Overview of key Cisco DNA Center Assurance processes



Network automation

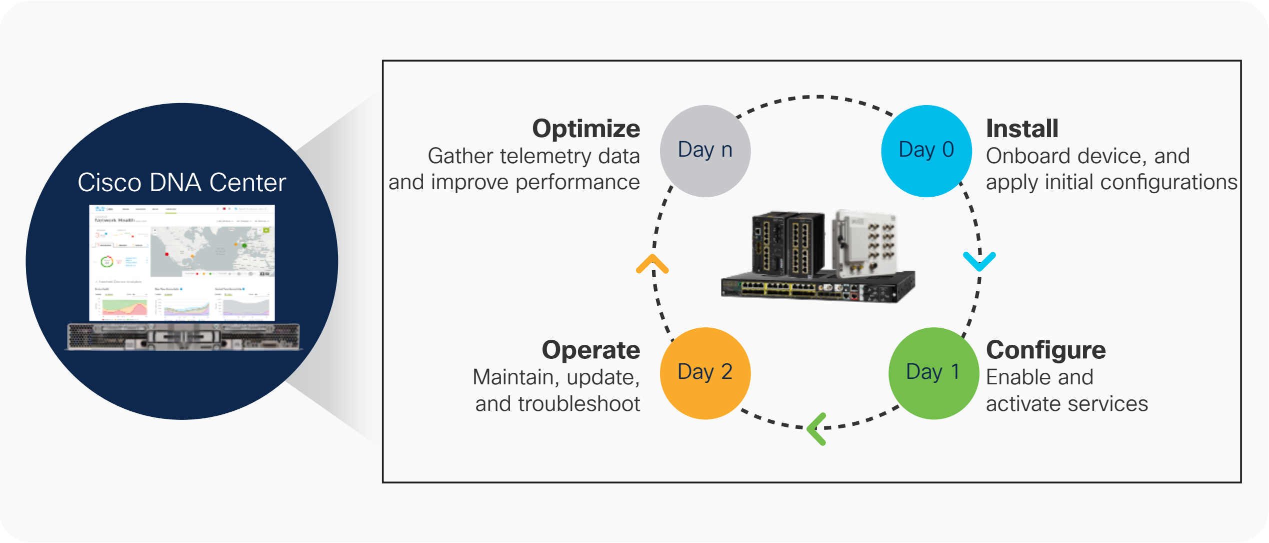
From the start of this transition to standard networking for industrial networks, the operational teams have lacked the skills and expertise typically found in IT networking organizations. The Industrial Ethernet infrastructure is often installed and maintained by personnel with minimal networking background. The result is often network configurations that are consistent when first brought into operational mode but that drift with time, as network infrastructure is rarely if ever maintained or improved. This results in inconsistent configurations, uneven network device software images, and erratic security settings, all of which affect system performance.

With the increase in cybersecurity risks, the increased need to provide end-to-end connectivity while maintaining the highest levels of availability results in a critical need to consistently deploy more sophisticated configurations and maintain them throughout the network's useful life. Industrial automation systems rely on the consistent, repeatable, and maintainable deployment and operation of sensors, controllers, and other equipment. Why should this not apply to the network infrastructure?

Cisco DNA Center focuses on deploying and maintaining network infrastructure with automation, bringing consistency, reduced effort, and reliance on simplified workflows for both IT and OT personnel. In many ways, Cisco DNA Center can be viewed as the "controller" for the network infrastructure. Key use cases supported by Cisco DNA Center automation features include:

- Discovering existing network infrastructure, adding to the inventory, and establishing telemetry (e.g., SNMP, syslog, and end-device tracking)
- Providing a network topology view with key status information
- Using Network Plug and Play to automatically detect and provision new network infrastructure
- Backing up network configurations and replacing malfunctioning network infrastructure (RMA process)
- Checking for inconsistent configurations and deploying updates scalably and consistently
- Deploying Quality-of-Service (QoS) values based on templates
- Creating application policies for visibility of QoS[1]
- Deploying network software images and patches automatically and at scale
- Performing compliance checks for configurations and software images
- Providing OT with functions relevant to their responsibility
- Deploying applications onto the edge-capable network infrastructure[1]
- Preparing network infrastructure for Cyber Vision sensor deployment
- Maintaining an audit log for all network changes for accountability

Figure 2. Cisco DNA Center's network automation functions


Cisco DNA Center
Optimize
Gather telemetry data and improve performance
Day n
Day 0
Install
Onboard device, and apply initial configurations
Operate
Maintain, update, and troubleshoot
Day 2
Day 1
Configure
Enable and activate services

[1] This feature may require specific models or software versions in the portfolio.

Industrial cybersecurity

Features:

- Build a dynamic inventory of Industrial Control System (ICS) assets and their communication patterns
- Segment communications within the industrial zone and industrial DMZ
- Monitor and detect abnormal ICS behaviors
- Contain malware and other attacks
- Integrate operational and enterprise security

Toward zero-trust security for industrial operations

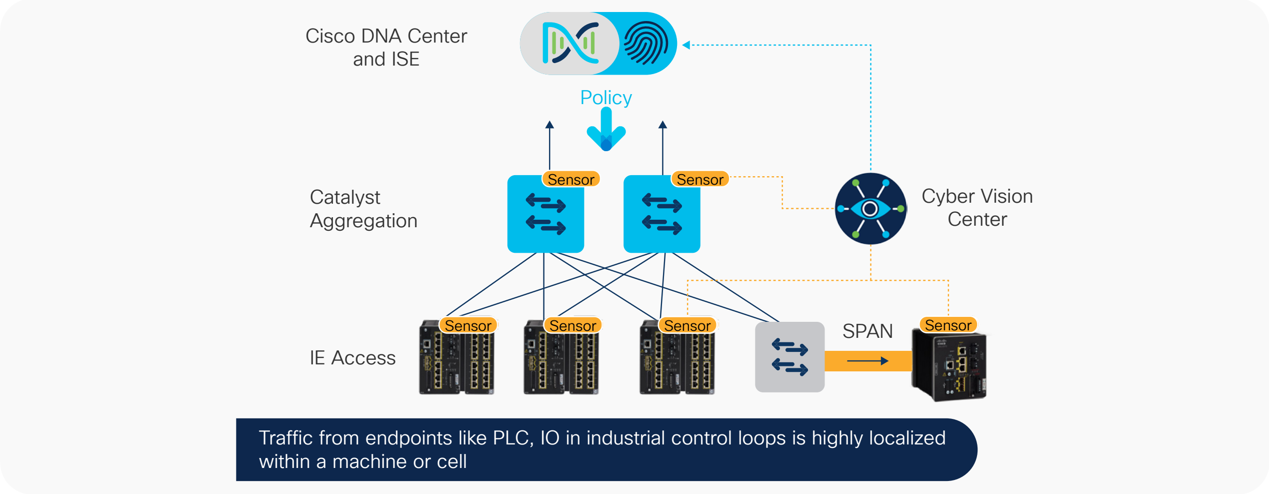
The rapid digitization of operations has resulted in connected control systems, growth in the use of IoT devices, and the need to collect operational data to derive insights. Operations can no longer be secured only by firewalls in the industrial DMZ that were primarily designed to keep IT and operational networks separate. Innovative approaches are needed that leverage security models developed by IT, such as zero trust, which relies on deeper visibility into connected endpoints, their role in operations, and their interaction with other endpoints, enabling access policies to be developed and the network segmented.

Cisco DNA Center, with integration with Cyber Vision and ISE, can help secure your operations in the following ways:

- Importing connected industrial assets as discovered and profiled by Cyber Vision and grouped in ISE
- Visualizing communication patterns between asset groups using NetFlow traffic and helping define and validate access policies
- Deploying policies with confidence using day-n templates and segmenting the network to restrict unnecessary access
- Allowing the use of other Cisco security applications such as Cisco Umbrella®, Secure Network Analytics (Stealthwatch), and Cisco SecureX™ for further enterprise security integrations

For details on how to secure your manufacturing operations, please refer to the Securing Industrial Networks Solution Brief.

Figure 3. Cisco Cyber Vision integration with Cisco DNA Center and ISE



Industrial Automation CVD

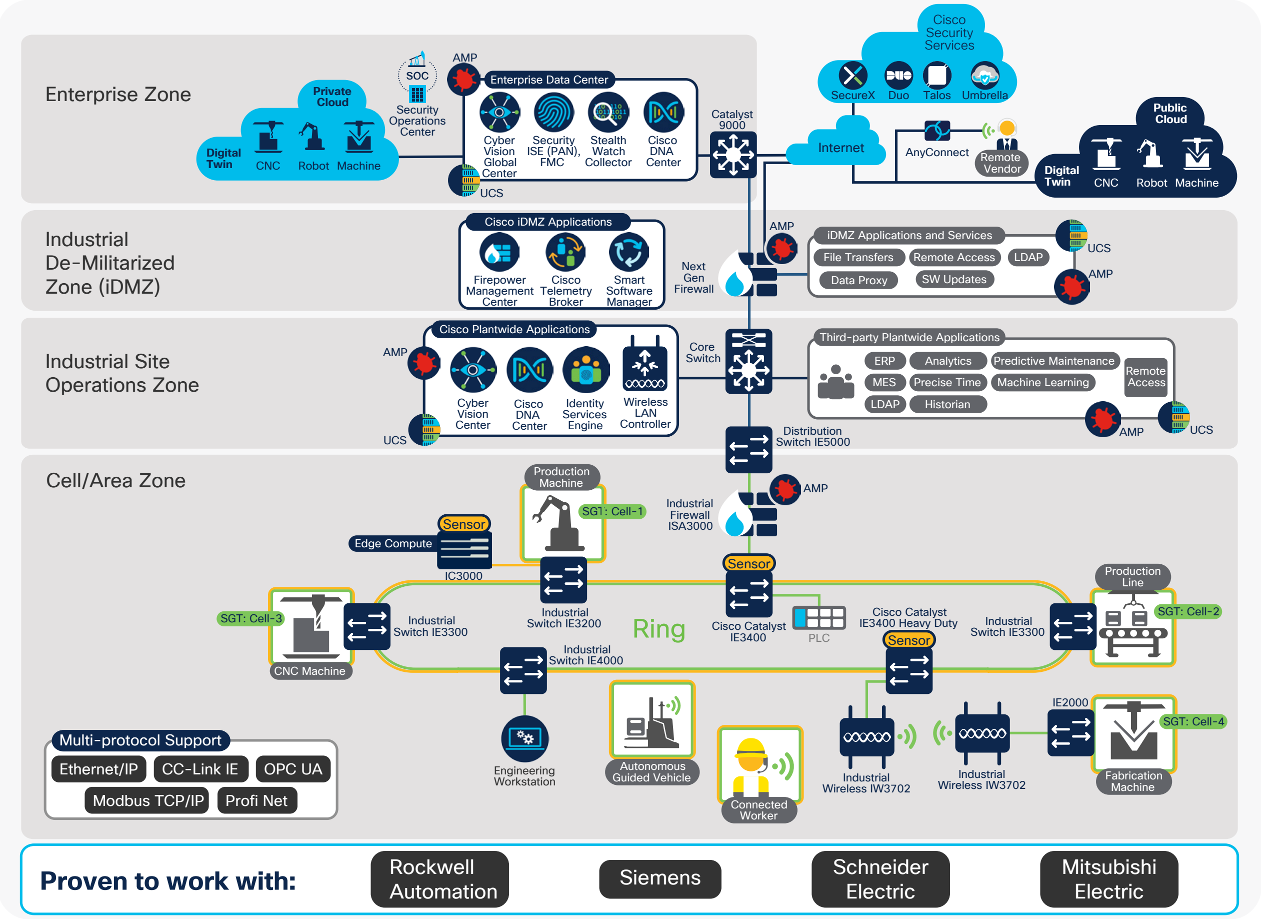
Key features:

- Resilient connectivity (wired and wireless) for IACS sensors, actuators, and controllers
- Visibility into IACS devices and communications
- Plant and Cell-area zone segmentation for protection of critical operations
- Secured remote access to production assets
- Availability of IACS devices and data for IoT applications

Industrial automation reference architecture with Cisco DNA Center

The Industrial Automation Reference Architecture describes the core network and security features and functions overlaid on an industry model for IACS. The integration of Cisco DNA Center into the industrial automation solution is depicted below. This is a key first step toward a fully software-defined network represented by Cisco’s Software-Defined Access model.

Figure 4. Industrial automation reference architecture



Key design and implementation considerations

Integrating Cisco DNA Center into the industrial automation solution includes these key considerations:

- Deploying a Cisco DNA Center on-premises appliance as part of the industrial zone
- Interfacing Cisco DNA Center with Cisco cloud services (MRE, software updates, etc.) via a data proxy service and on-premises smart software manager (license information)
- Interfacing Cisco DNA Center with an ISE deployment (management node and pxGrid)
- Monitoring and managing Cisco Industrial Ethernet (IE 2000 Series, Catalyst® IE3x00 Rugged Series, Catalyst IE3400 Heavy Duty Series, and IE 4000 and IE 5000 Series) and Catalyst 9300 and 9500 Series switches
- Integrating IACS device information discovered by Cyber Vision into ISE
- Deploying Cisco Telemetry Broker to scalably convey network and security telemetry data beyond the industrial zone
- Updating the industrial DMZ firewalls to the Cisco Firepower® 2110 Series supporting Cisco SecureX Threat Response and Secure Firewall Management Center (FMC)
- Monitoring and managing wireless networks and users

Summary

Providing automation and assurance to the industrial networks that form the basis of industry IoT initiatives greatly simplifies these initiatives, thereby accelerating the significant business benefits of digitization. On their own, these capabilities alleviate key problems associated with managing and operating these networks: a lack of visibility into network and end device connectivity status and a need for a consistent, scaled means to deploy and maintain these networks, reducing effort and making network management capabilities more widely available. Our solution helps customers and partners achieve these benefits by integrating Cisco DNA Center into our Industrial Automation CVDs.

For more on the industrial automation solution, please visit the Industry CVD page.