

Full-Stack Software-Defined Manufacturing – Software-Defined Networking for Manufacturing

Accelerating AI-powered autonomous operations – Smarter, simpler network management



Value statement

The Cisco and Rockwell Automation Full-Stack Software-Defined Manufacturing solution enhances production quality, efficiency, and plant resilience by offering operational visibility and preparing for future AI insights and autonomous operations, helping businesses stay competitive as they evolve.

Software-Defined Networking (SDN) is a critical component of the Full-Stack Software-Defined Manufacturing reference design. SDN is an architectural approach that decouples the network control plane from the data plane, allowing for centralized management and dynamic configuration of network resources through software applications. This separation enables more flexible and efficient network management compared to traditional networking approaches.

In manufacturing, SDN supports the virtualization of Industrial Automation and Control Systems (IACS), enabling manufacturers to optimize production processes, improve security, and increase sustainability. By using SDN, manufacturers can achieve greater programmability and agility in IT and OT wired and wireless network configuration and management, which is essential for adapting to diverse operational requirements and scaling networks efficiently.

Key to the support of a software-defined network is Cisco Catalyst™ Center, a powerful network management system that leverages AI to connect, secure, and automate network operations. It optimizes resources, reduces spending, and enhances your organization's digital agility.

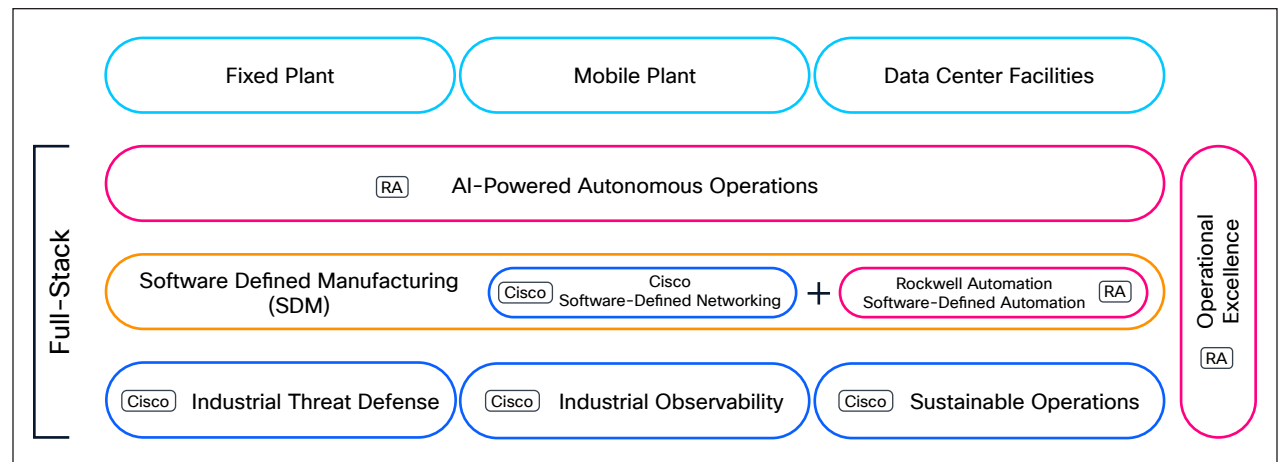


Figure 1. Components of the Full-Stack Software Defined Manufacturing solution

Overview

Businesses in today's industrial landscape must adapt to be more agile, scalable, and resilient due to competitive and geopolitical pressures, yet traditional network and traditional automation systems are often inflexible, limiting future capabilities like AI-powered autonomous operations.

The Full-Stack Software-Defined Manufacturing reference design brings together SDN with software-defined automation and the critical foundations of Cisco® Industrial Threat Defense, industrial observability, and sustainable operations.

Cisco's Software-Defined Network solution is managed with Cisco Catalyst Center, a powerful network controller and management dashboard that empowers you to take charge of your network, optimize your network and automation

investment, and lower your network spending. Catalyst Center provides a single dashboard for every fundamental management task to simplify running your network. With this platform, network operators can respond to changes and challenges faster and more intelligently.

The SDN architecture in manufacturing and OT environments delivers several key capabilities:

- **Centralized management:** SDN provides a centralized controller that manages both IT and OT networks, allowing for unified policy enforcement and automation across diverse network environments.
- **Programmability:** The architecture supports programmability through APIs, enabling dynamic network configuration and management tailored to manufacturing processes.

- **Enhanced security:** By integrating IT and OT systems, SDN enhances security measures, for robust protection against cyberthreats.
- **Operational efficiency:** SDN enables and facilitates the virtualization of IACS, optimizing production processes and improving operational efficiency.
- **Scalability:** The architecture is designed to scale efficiently, accommodating the evolving needs of manufacturing environments.

When combined with AI-powered autonomous operations and operational excellence, the full-stack solution enables customers to support their evolutionary shift from automation to autonomy.

Benefits

- **Minimized downtime and enhanced reliability:** SDN supports network redundancy, failover mechanisms, and predictive maintenance, helping ensure continuous operation of critical manufacturing processes and reducing unexpected outages.
- **Enhanced security and compliance:** SDN enables micro-segmentation and policy-based security, isolating critical assets, enforcing consistent security measures, and helping ensure compliance with industry standards.
- **Scalability and adaptability:** The centralized control and programmability of SDN allow for a scalable network architecture, quick addition of new devices, and adaptability to changing production requirements, helping ensure flexibility in modern manufacturing environments.
- **Operational efficiency and cost savings:** SDN simplifies network management through centralized control and automation, reducing complexity, freeing up IT/OT staff, and enabling cost-effective upgrades with vendor-agnostic solutions.
- **Accelerated digital transformation:** SDN facilitates rapid deployment of new services and applications, enhances real-time monitoring and centralized management, and supports initiatives to accelerate time to market and improve cost efficiency.

Provision, manage, and program networks more rapidly

According to the recent [Cisco 2024 Global Networking Trends Report](#), the emergence of the network platform to help customers simplify operations and drive digital resilience is becoming more prevalent.

A survey conducted for the report found that, while one in five organizations (21%) surveyed are currently using multiple, separate management systems when managing their campus, branch, WAN, data center, and multicloud domains, 39% are currently leveraging a platform architecture across networking domains. Survey respondents were strongly supportive of network platform adoption, given the alignment of benefits from that approach with the IT and business outcomes they are trying to achieve. Those outcomes include faster IT and business innovation (43%), improved network performance and security posture (40%), and cost savings (37%).

Seventy-two percent of IT leaders and professionals expect to have a platform architecture in place across one or more networking domains in the next two years.

Traditional enterprise networks are complex systems. Managing this complexity in a fast-changing digital landscape can be challenging. When network policy is tied to hardware, provisioning can be a time-consuming process. And with a focus on individual components, network administration can slow down the deployment of new applications. To save time, modern enterprises must find a more simplified and agile solution.

OT customers are facing the following challenges with their plant networks:

- Addressing network complexity
- Ensuring end-to-end resilience
- Enhancing scalability and agility

- Optimizing production and maintainability
- Covering needed tasks despite a skills shortage

By decoupling network functions from hardware, SDN creates a virtual overlay on top of the underlying physical networking infrastructure. SDN provides zero-trust security and secures access—by all users, by all devices, and from all locations—across your applications and network environment.

SDN, enabled by Cisco Catalyst Center, helps ensure policy consistency by defining and enforcing policies, preventing unauthorized access, and containing breaches, enabling faster launches of new business services and significantly improving issue-resolution times while being open, extensible, and reducing operational expenses.

Provision, manage, and program networks more rapidly

According to the recent [Cisco 2024 Global Networking Trends Report](#), the emergence of the network platform to help customers simplify operations and drive digital resilience is becoming more prevalent.

A survey conducted for the report found that, while one in five organizations (21%) surveyed are currently using multiple, separate management systems when managing their campus, branch, WAN, data center, and multicloud domains, 39% are currently leveraging a platform architecture across networking domains. Survey respondents were strongly supportive of network platform adoption, given the alignment of benefits from that approach with the IT and business outcomes they are trying to achieve. Those outcomes include faster IT and business innovation (43%), improved network performance and security posture (40%), and cost savings (37%).

Seventy-two percent of IT leaders and professionals expect to have a platform architecture in place across one or more networking domains in the next two years.

Traditional enterprise networks are complex systems. Managing this complexity in a fast-changing digital landscape can be challenging. When network policy is tied to hardware, provisioning can be a time-consuming process. And with a focus on individual components,

network administration can slow down the deployment of new applications. To save time, modern enterprises must find a more simplified and agile solution.

OT customers are facing the following challenges with their plant networks:

- Addressing network complexity
- Ensuring end-to-end resilience
- Enhancing scalability and agility
- Optimizing production and maintainability
- Covering needed tasks despite a skills shortage

By decoupling network functions from hardware, SDN creates a virtual overlay on top of the underlying physical networking infrastructure. SDN provides zero-trust security and secures access—by all users, by all devices, and from all locations—across your applications and network environment.

SDN, enabled by Cisco Catalyst Center, helps ensure policy consistency by defining and enforcing policies, preventing unauthorized access, and containing breaches, enabling faster launches of new business services and significantly improving issue-resolution times while being open, extensible, and reducing operational expenses.

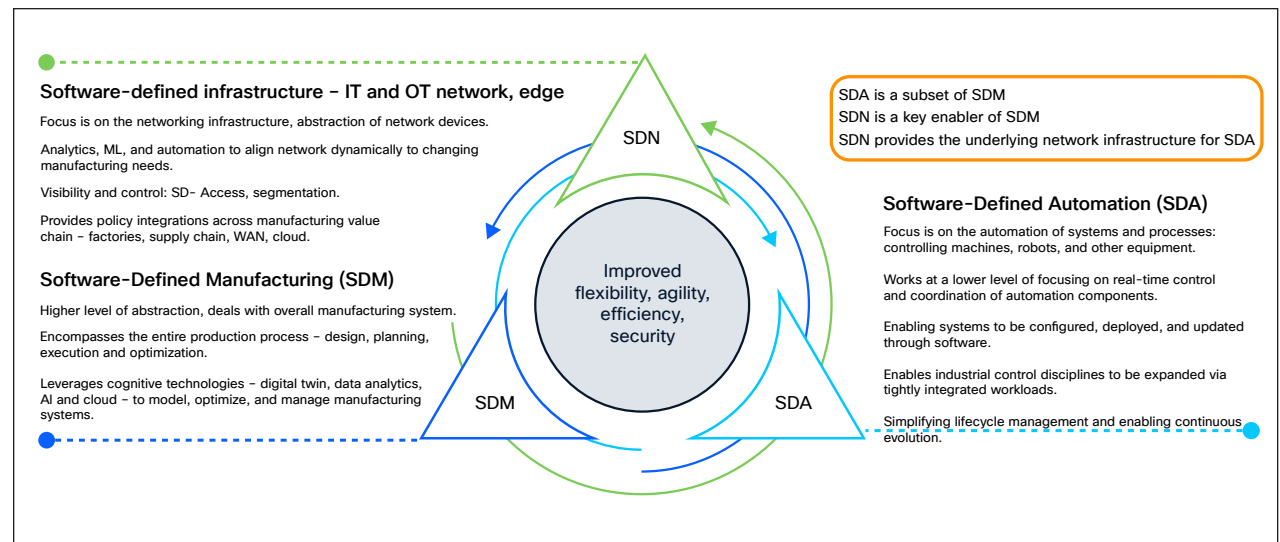


Figure 2. Benefits of software-defined manufacturing

How it works

In traditional networks, control and data planes are intertwined within each network device. SDN decouples these planes, centralizing network control in a controller (like Cisco Catalyst Center) while leaving the data forwarding to the network devices. This separation allows for:

- **Centralized control:** A central SDN controller has a holistic view of the network, enabling intelligent decision-making and policy enforcement.
- **Programmability:** The controller provides a programmable interface (APIs) that allows administrators to define network behavior through software, automating tasks and enabling dynamic adjustments based on real-time conditions.
- **Abstraction:** SDN abstracts the underlying network infrastructure, simplifying network management and allowing administrators to focus on business needs rather than low-level device configurations.

Cisco Catalyst Center offers centralized, intuitive management that makes designing, provisioning, and applying policies across your network environment fast and easy. The Catalyst Center GUI provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience.

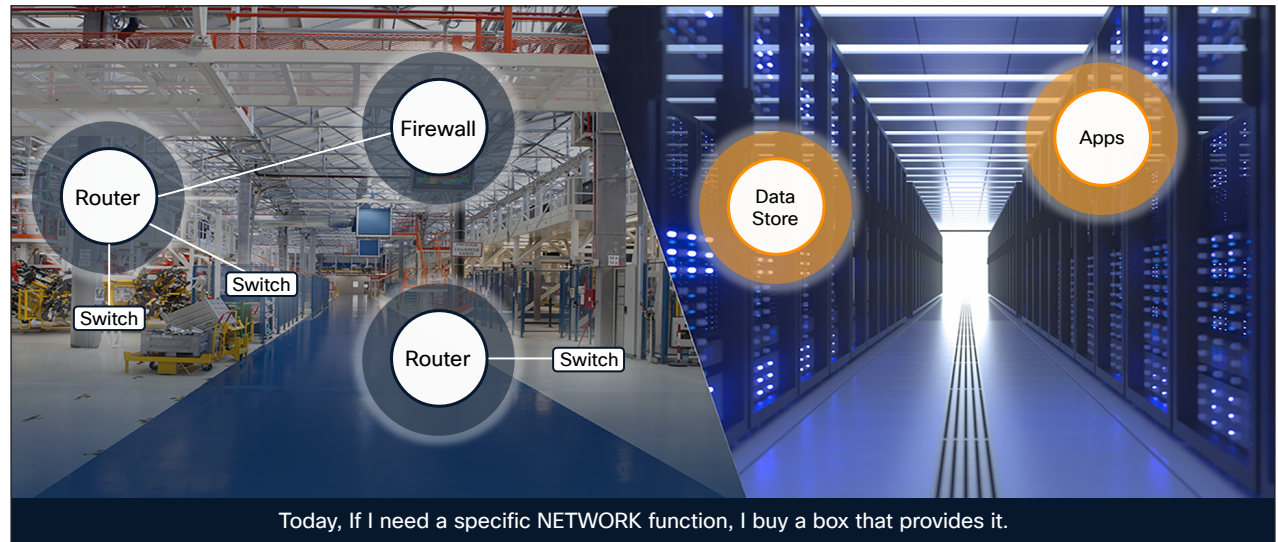


Figure 3. Traditional network, with control and data planes intertwined

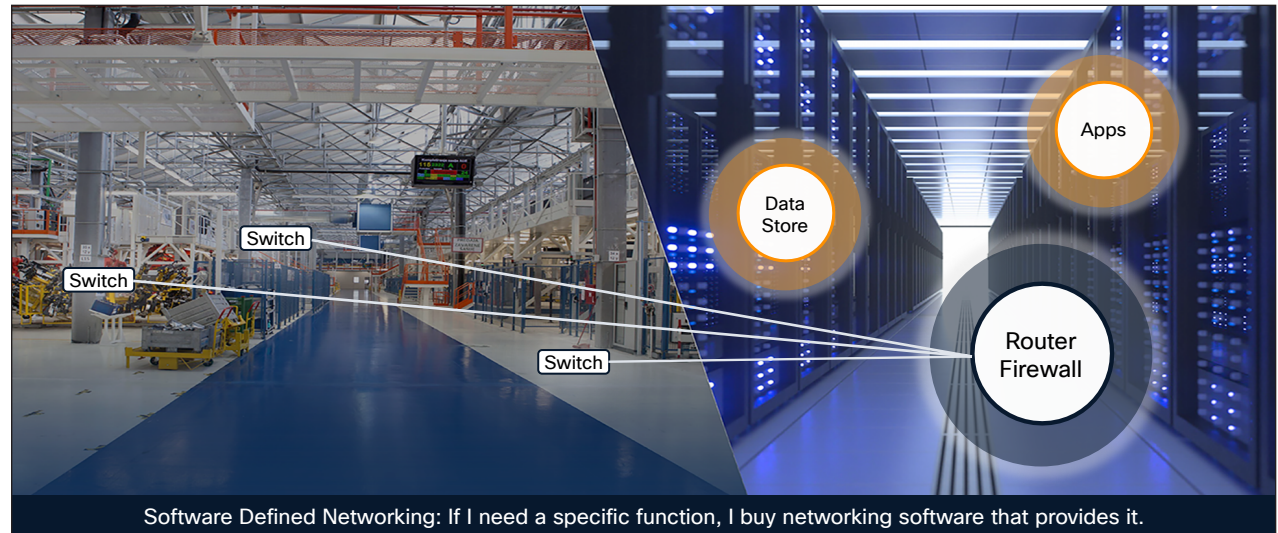


Figure 4. Software-defined networking



Catalyst Center simplifies the network experience to streamline complex network operations, resulting in a faster time to value. Leveraging AI/ML, Catalyst Center can increase business agility and operational efficiency by creating consistent orchestration across a wired and wireless network.

A robust and agile SDN architecture consists of the following components:

Cisco Catalyst Center: A central management system that leverages AI to connect, secure, and automate network operations. It simplifies the management of the Cisco Catalyst network infrastructure and helps ensure a consistent user experience across wired and wireless networks.

Cisco Identity Services Engine (ISE): A secure network access platform that enables increased management awareness, control, and consistency for users and devices accessing an organization's network. Cisco ISE is an integral and mandatory part of Cisco Software-Defined Access (SD-Access) for implementing network access control policy.

SD-Access Fabric: An architecture that provides wired and wireless campus networks with programmable overlays and easy-to-deploy network virtualization, allowing a physical network to host one or more logical networks to meet the design intent.

Virtual Networks (VNs): VNs logically separate network topology into smaller virtual networks using a unique network identifier and separate forwarding tables. This is realized as a Virtual Routing and Forwarding (VRF) instance on

switches or routers, referred to as a virtual network in Catalyst Center.

Security Group Tags (SGTs): SGTs provide information about the devices, such as their role, the applications they use, and even the threat level they pose. This additional insight helps streamline the setup of firewall rules, web security policies, and access controls in various network devices.

Extended Nodes (ENs) and Policy Extended Nodes (PENs): ENs and PENs extend the enterprise network by providing connectivity to noncarpeted spaces of an enterprise, commonly called the extended enterprise. ENs offer a Layer 2 port extension to a fabric edge node while providing segmentation and group-based policies to the endpoints connected to these switches.

Cisco Cyber Vision: Addresses the visibility needs of industrial networks. It is built on an edge architecture comprising multiple sensor devices that perform deep packet inspection, protocol analysis, and intrusion detection within the industrial network.

Resilient Ethernet Protocol (REP): A Cisco proprietary protocol that offers an alternative to Spanning Tree Protocol (STP) for controlling network loops, handling link or node failures, and avoiding convergence time. It operates a single redundancy instance per segment or physical ring.

Parallel Redundancy Protocol (PRP): A protocol designed to provide hitless redundancy (zero recovery time after failures) in Ethernet networks. PRP uses a different scheme, where the end nodes (instead of network elements) implement

redundancy by connecting two network interfaces to two independent, disjointed, parallel networks (LAN-A and LAN-B).

Cisco Firepower® Threat Defense (FTD): Next-generation firewalls that establish an Industrial Demilitarized Zone (IDMZ) for protecting production systems.

Cisco Secure Network Analytics: Provides flow-based anomaly detection, with host-group information enriched from Cisco Cyber Vision.

SDN enabled by Cisco Catalyst Center helps you design, deploy, and manage large-scale OT networks at a fast pace, with features such as auto discovery, zero-touch provisioning, and configuration automation, enabling end-to-end network policy from edge to cloud.

Simplify operations: Build programmable networks that automatically discover and configure fabrics and switches.

Achieve faster troubleshooting: Improve the health of networks with network analytics, machine learning, and predictive insights.

Improve security: Deploy consistent zero-trust access across your network with policy-based segmentation.

Transform your infrastructure: Automate lifecycle management across access, WAN, and cloud network domains.

SDN offers a modern approach to network management, bringing agility, security, and automation to the increasingly complex environments of manufacturing, where IT and OT converge.

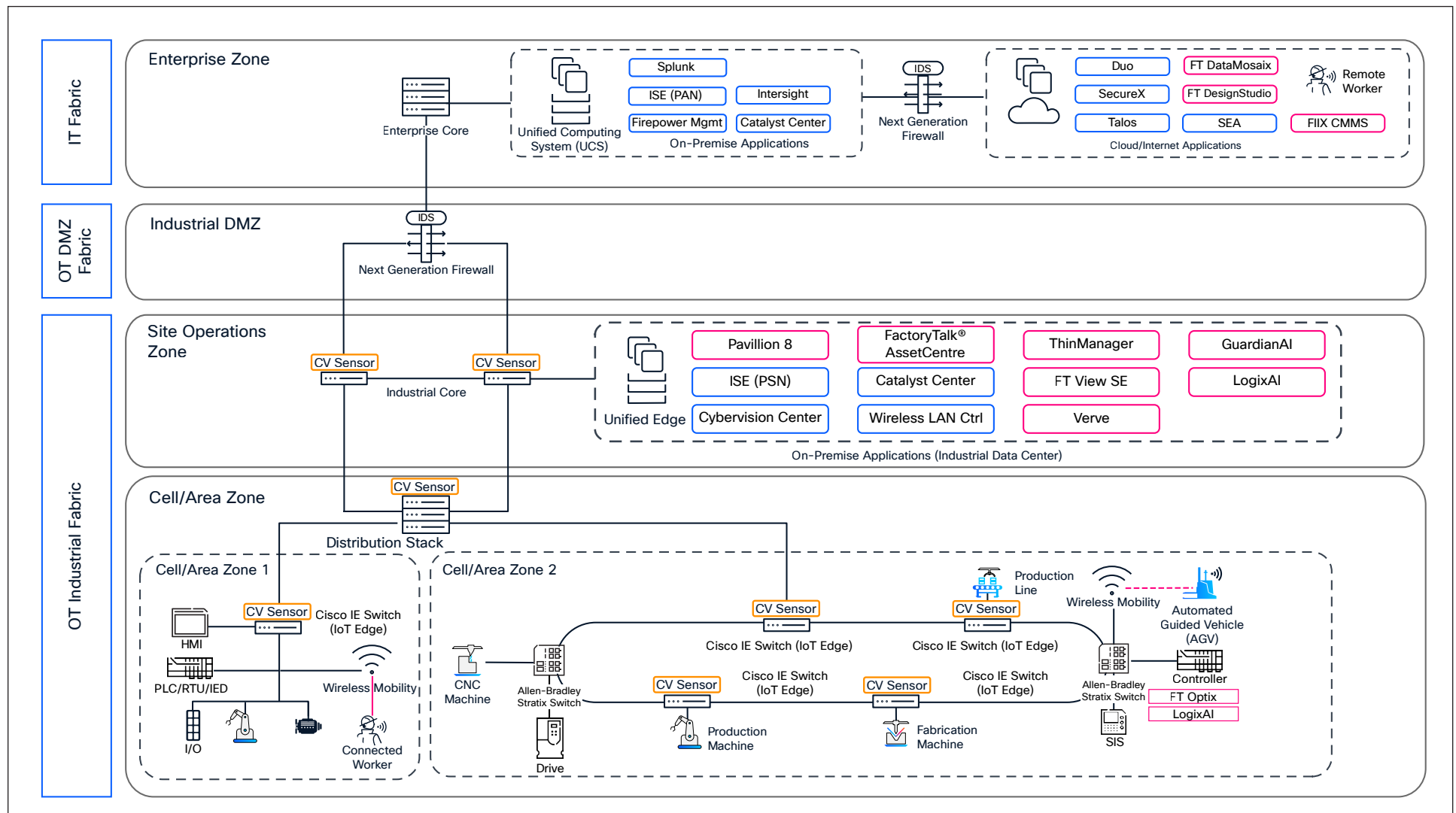


Figure 5. Full-Stack Software-Defined Manufacturing reference design

Implementing SDN in a manufacturing plant

SDN is revolutionizing the way networks are managed and operated, particularly in the realm of OT. In a manufacturing plant, where automation devices are integral to operations, SDN offers numerous benefits that enhance efficiency, security, and flexibility.

Key benefits of SDN in OT environments

- **Centralized control:** The SDN controller acts as the brain of the network, providing a centralized point for managing and configuring network devices. This centralization simplifies network management and enhances visibility across the entire network.
- **Programmability:** SDN allows network administrators to programmatically control the network using software applications. This programmability enables automation of network configurations and policies, reducing the need for manual interventions.
- **Dynamic configuration:** With SDN, network configurations can be dynamically adjusted based on real-time requirements. This flexibility is crucial in OT environments, where network demands can change rapidly.

Use cases

Table 1. Use cases for software-defined networking

Industry	Use cases
Life sciences manufacturing	SDN enables a secure, compliant, and agile network infrastructure to support precision manufacturing, real-time monitoring of critical environments, and integration of lab systems with production lines. It enhances traceability and data integrity, and supports regulatory compliance (e.g., FDA, GxP).
Mining	SDN supports ruggedized industrial switches and wireless mesh networks for reliable connectivity in harsh, remote environments. It enables real-time equipment monitoring, autonomous vehicle communication, and predictive maintenance, enhancing safety and operational continuity.
Tire manufacturing	SDN supports high-speed, low-latency communication between production machines and quality control systems. It enables flexible reconfiguration of production lines, predictive analytics for equipment health, and improved traceability across the supply chain.
Data center	SDN integrates with the Cisco ACI® and Nexus platforms to deliver policy-driven automation, scalable fabric architecture, and secure segmentation. This enables dynamic workload mobility, hybrid cloud connectivity, and high-performance data center operations.
Food and beverage manufacturing	SDN helps ensure secure and resilient connectivity across processing, packaging, and distribution systems. It supports compliance with food safety standards, real-time quality monitoring, and agile response to changing consumer demands and supply chain disruptions.



Transforming network architecture

A network platform is an integrated system that combines software, policy, and open APIs with an intuitive user interface, advanced telemetry, and automation. It provides a centralized operator experience, end-to-end network management, and an API-driven ecosystem that simplifies operations and enables digital experiences across one or more networking domains.

The evolution to an AI-native network platform equips IT teams with the continuous intelligence and automated control required to consistently deliver quality digital experiences.

Forty-two percent of IT leaders and professionals say a network platform can better support cross-domain management to unlock better performance, innovation, and cost savings.

For additional information, visit [the Cisco 2024 Global Networking Trends Report](#).

How Rockwell Automation and Cisco provide expertise to customers

Rockwell Automation and Cisco bring together their respective strengths in OT and IT to offer comprehensive solutions for modern manufacturing challenges. Here's how they provide their expertise to customers:

Converged Plantwide Ethernet (CPwE):

Rockwell Automation and Cisco have developed the CPwE architecture, a set of tested and validated designs that help manufacturers build a secure, scalable, and resilient network infrastructure. This architecture integrates IT and OT systems, helping ensure seamless connectivity and robust security.

LifecycleIQ® Services: Rockwell Automation's LifecycleIQ® Services, enhanced by Cisco's Cyber Vision solution, offer advanced cybersecurity threat detection and response capabilities. These services help manufacturers protect their networks from cyberthreats and ensure business continuity.

Digital transformation solutions: Together, Rockwell Automation and Cisco provide solutions that support digital transformation initiatives. These solutions include industrial IoT, predictive analytics, and smart manufacturing technologies that enhance operational efficiency and agility.

Industry-specific expertise: The partnership offers tailored solutions for various industries, including water and wastewater, food and beverage, life sciences, mining, and oil and gas. This industry-specific expertise helps ensure that the solutions meet the unique challenges and regulatory requirements of each sector.

Training and support: Rockwell Automation and Cisco provide extensive training and support to help customers implement and manage their network infrastructure. This includes hands-on training, virtual labs, and access to a wealth of resources and documentation.



Learn more

For additional information, visit Cisco and Rockwell Automation - [Cisco](#)

For additional information on Cisco software-defined networking, visit Software-Defined Networking (SDN) Definition - [Cisco](#)

For additional information on Cisco Catalyst™ Center, visit Cisco Catalyst Center Network Management - [Cisco](#)

For additional information on Cisco Industrial Threat Defense, visit Products - Cisco Industrial Threat Defense At a Glance - [Cisco](#)

The Cisco and Rockwell Automation Advantage

Cisco and Rockwell Automation have been global strategic partners for over 18 years, leading the digital transformation for the connected enterprise by bringing industrial automation together with industrial networking and security solutions. Today, Cisco and Rockwell Automation are once again leading change in the industrial automation landscape as it evolves to embrace full-stack software-defined manufacturing and enabling the shift from automation to autonomy.

Cisco is a global leader in IT networking and cybersecurity, with decades of experience securing enterprise networks, bringing a deep understanding of IT security principles, technologies, and best practices.

Rockwell Automation is a global leader in industrial automation and control systems, with unparalleled expertise in OT environments, industrial protocols, and manufacturing processes.

Only Cisco and Rockwell Automation can deliver the full-stack combination of AI-enabled autonomous operations, software-defined manufacturing, Industrial Threat Defense, industrial observability, sustainable operations, and operational excellence.