

Full-Stack Software-Defined Manufacturing – Cloud-Based Engineering with Design Studio

Accelerating AI-powered autonomous operations – Streamline industrial automation system design and reduce time to market for customers



Value statement

The Full-Stack Software-Defined Manufacturing solution from Cisco and Rockwell Automation 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.

It provides a regulatory-compliant cybersecurity strategy from edge to cloud, crucial for plant availability and the manufacturing ecosystem's trustworthiness to support innovation and growth.

Cloud-based engineering is a modern approach to designing, building, and managing systems using cloud computing technologies. It's not just about hosting software in the cloud—it's about reimagining the entire engineering process to fully leverage the flexibility, scalability, and power of cloud platforms.

Cloud-based engineering refers to the strategic and technical discipline of creating systems that are optimized for cloud environments.

This includes:

- Designing cloud-native architectures.
- Automating infrastructure using tools.
- Ensuring scalability, security, and cost-efficiency from the ground up.

Unlike simply migrating existing systems to the cloud, this approach builds systems specifically for cloud dynamics, making them more resilient and adaptable.

Cloud-based engineering in Industrial Automation and Control System (IACS) networks is reshaping how industrial operations manage, monitor, and optimize their systems. It blends traditional Operational Technology (OT) with modern cloud-based IT solutions to enable smarter, more connected industrial environments. Bringing cloud to IACS is about carefully extending visibility, analytics, and collaboration beyond the plant—without compromising deterministic control, safety, or uptime. The core idea is to keep time critical control local, move data hungry and compute intensive work to the cloud, and stitch them together with a secure, segmented network and least privilege access.

Network segmentation and data paths

- **Zones and conduits:** Partition by function and risk; route all cross zone traffic through inspected conduits with policy controls. Apply the Purdue/Converged Plantwide Ethernet (CPwE) principles to separate enterprise, industrial Demilitarized Zone (DMZ), industrial zone, and cell/area networks.
- **Restricted outbound pattern:** Favor strictly controlled, outbound only connections from plant applications to cloud endpoints (brokered via DMZ), minimizing inbound exposure. This is a core CPwE cloud connectivity design stance.
- **Data flow pattern:** Edge → DMZ broker (buffer/normalize) → Cloud ingestion (IoT hub/Kafka) → Storage/analytics. Keep control loops and safety interlocks local; never depend on cloud latency for essential functions.

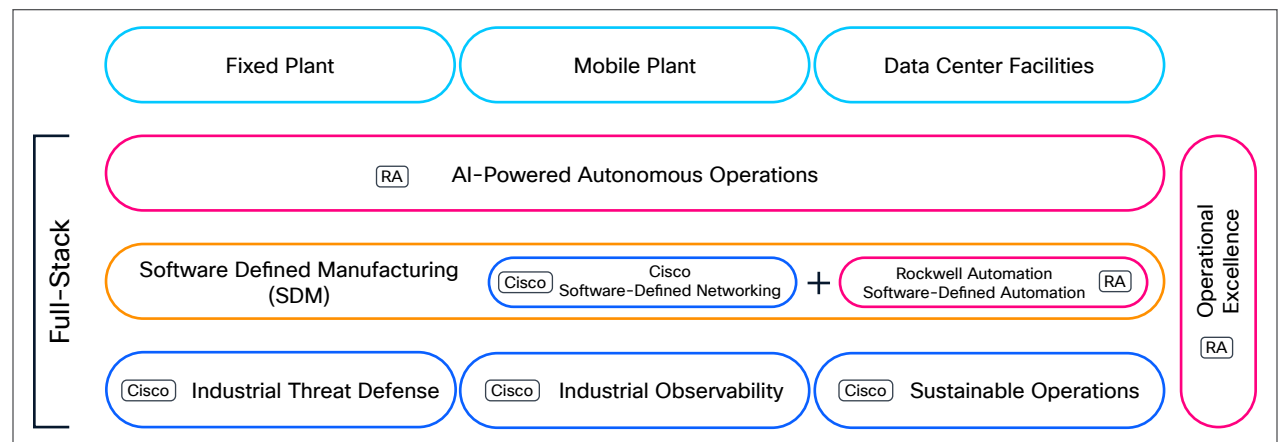


Figure 1. Components of the Full-Stack Software Defined Manufacturing solution

Overview

Before a cloud-based engineering approach was introduced into IACS networks, customers faced a range of persistent challenges that limited agility, visibility, and operational efficiency.

Here's a breakdown of the most common issues:

Limited data visibility

- Real-time insights across multiple sites were difficult to achieve.
- Remote monitoring was either impossible or required complex VPN setups.

Inflexible legacy infrastructure

- Many plants relied on proprietary or outdated control systems.
- Scaling or integrating new technologies was slow and expensive.
- Lack of interoperability between OT and IT systems created bottlenecks.

Security concerns

- OT networks were often air-gapped but lacked modern cybersecurity practices.
- Systems had no centralized identity or access management.
- OT networks were vulnerable to insider threats and unpatched systems.

High maintenance costs

- Manual updates and troubleshooting required on-site visits.
- Networks had no centralized patch management or remote diagnostics.
- Downtime during maintenance impacted production and revenue.

Slow innovation cycles

- Engineering changes required physical access and lengthy validation.
- Collaboration between teams (design, operations, vendors) was fragmented.
- There was no support for agile development or digital twin simulations.

Poor scalability

- Adding new sensors, controllers, or analytics tools required major rework.
- There was no elastic compute or storage; everything was fixed and local.
- Multisite coordination was inefficient and error-prone.



Key benefits of cloud-based engineering in IACS

Real-time data visibility across sites

- Centralized dashboards give operators and managers instant access to live metrics from multiple plants.
- Enables remote monitoring, diagnostics, and decision-making without physical presence.

Predictive maintenance and analytics

- Cloud platforms can analyze historical and real-time data to predict equipment failures.
- Reduces unplanned downtime and extends asset life through smarter maintenance scheduling.

Scalability and flexibility

- Easily scale compute and storage resources as operations grow.
- Add new sensors, controllers, or analytics tools without major infrastructure changes.

Enhanced collaboration

- Engineers, vendors, and stakeholders can co-develop, simulate, and troubleshoot systems remotely.
- Supports digital twin models and agile workflows for faster innovation.

Cost-efficiency

- Reduces capital expenditures for local servers and hardware.
- Pay-as-you-go cloud models optimize resource usage and lower operational costs.

Improved security posture

- Cloud providers offer advanced security protocols, identity management, and disaster recovery.
- When paired with ISA/IEC 62443-compliant architectures, cloud connectivity can be secure and compliant.

Faster deployment and updates

- Software updates, patches, and new features can be rolled out remotely and efficiently.
- Minimizes downtime and accelerates time to value for new capabilities.



Trends and challenges

Cloud-based engineering is increasingly **required** in IACS networks because it addresses long-standing limitations in visibility, scalability, and collaboration while enabling modern industrial use cases like predictive maintenance, remote diagnostics, and digital twins.

Here's why it's not just beneficial but **strategically necessary**:

Unlocks real-time data and visibility

Traditional IACS networks are often siloed, making it hard to access or analyze data across systems or sites. Cloud-based engineering enables:

- Centralized dashboards for multisite monitoring.
- Live data streaming for analytics and decision-making.
- Remote access for operators, OEMs, and integrators.

This visibility is essential for Industry 4.0 and IIoT initiatives.

Enables predictive maintenance and optimization

With cloud-based analytics, companies can:

- Detect anomalies before failures occur.
- Optimize energy usage and production schedules.
- Benchmark performance across assets and locations.

This leads to higher **Overall Equipment Effectiveness (OEE)** and reduced downtime.

Supports OT-IT convergence

Modern IACS architectures (like CPwE) are built on **EtherNet/IP and standard protocols**, making it easier to integrate cloud services with operational technology:

- Secure data flows from plant to cloud via DMZs and brokers.
- Share identity and access management across IT and OT.
- Unify security policies and monitoring tools.

This convergence is key to scalable, secure industrial operations.

Strengthens security and compliance

Cloud-based engineering supports a **defense-in-depth** approach:

- Multilayered security across physical, network, and application layers.
- Centralized logging and threat detection.
- Compliance with ISA/IEC 62443 and other industrial standards.

This approach helps protect critical assets while enabling innovation.

Accelerates innovation and collaboration

Cloud platforms allow engineers to:

- Simulate and test control logic remotely.
- Collaborate across geographies in real time.
- Deploy updates and patches faster and more safely.

This agility is crucial for competitive industrial environments.

How it works

This solution seamlessly integrates Rockwell Automation's cloud-native engineering and secure remote access tools with Cisco's Software-Defined Networking (SDN) and industrial observability platforms to deliver a secure, scalable, and intelligent infrastructure tailored for modern manufacturing environments.

By combining these technologies, manufacturers gain a unified ecosystem that supports remote collaboration, real-time monitoring, and automated network control, enabling faster innovation, reduced downtime, and enhanced operational resilience.

Strategic benefits

- **Accelerated engineering cycles:** Cloud-native tools and AI support reduce development time and improve quality.
- **Secure remote operations:** VPN-based access and zero-trust architecture protect critical assets and data.

- **Intelligent network control:** SDN enables automated provisioning and policy enforcement across distributed environments.
- **Proactive maintenance:** Observability tools empower teams to detect issues early and optimize performance.

Product capabilities

- **FactoryTalk® Design Studio:** A cloud-based engineering platform that enables multiuser collaboration, AI-assisted programming, and virtual emulation of control systems.
- **FactoryTalk® Remote Access:** Provides secure, encrypted connectivity to industrial assets, allowing remote diagnostics, configuration, and support from anywhere.
- **Software-defined networking:** Offers centralized control, dynamic traffic routing, and secure segmentation of IT and OT networks, improving scalability and security.

- **Industrial observability:** Delivers real-time insights into device, application, and network performance using MELT data (metrics, events, logs, traces), supporting predictive maintenance and root-cause analysis.

How they work together

- **Design Studio** creates and tests automation logic.
- **Remote Access** allows secure deployment and support from anywhere.
- **SDN** helps ensure that the network is agile, secure, and segmented for industrial traffic.
- **Observability** provides deep insights into system health, enabling proactive maintenance and optimization.

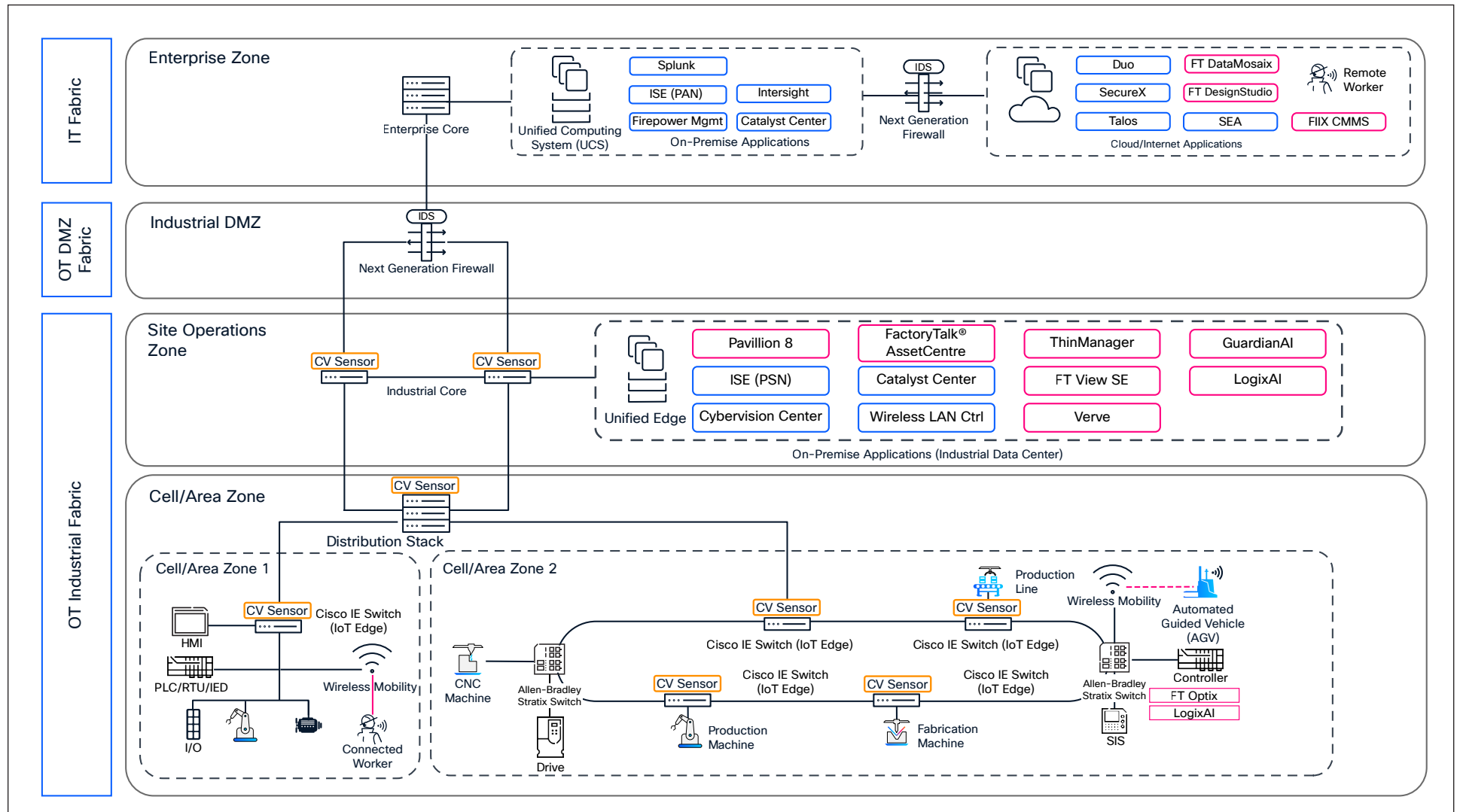


Figure 2. Full-Stack Software-Defined Manufacturing reference design

A better design experience using FactoryTalk® Design Studio over Remote Access using SDN.

Cloud based engineering with secure remote access over a software-defined network.

Example 1	Example 2	Example 3
Faster development, improved collaboration and security	Reduced downtime, lower travel costs, faster issue resolution, and better visibility	Secure segmentation, centralized policy management, resiliency, and quick remote access
With FactoryTalk® Design Studio, AI assistance and cloud tools reduce engineering time and manual effort, and teams can work together in real time, regardless of location. In addition, role-based access and encrypted cloud infrastructure protect sensitive data.	With FactoryTalk® Remote Access, quick remote support minimizes production interruptions, eliminates the need for on-site visits for routine tasks, enables experts to respond instantly, even across time zones, and provides audit trails to help meet regulatory requirements and improve transparency.	• SDN enables logical separation of enterprise (IT) and industrial (OT) traffic. • Protects Rockwell IACS assets—such as Programmable Logic Controllers (PLCs), Human-Machine Interfaces (HMIs), and Supervisory Control and Data Acquisition (SCADA) systems—from lateral threats. • Supports zero-trust architecture, helping ensure that only authorized devices and users can access critical control systems. • Network policies (e.g., access control, Quality of Service [QoS], VLANs) are managed from a single SDN controller. • Simplifies enforcement across distributed Rockwell IACS environments. • Reduces configuration errors and accelerates deployment of new automation cells. • SDN can automatically reroute traffic during link failures or device outages. • Minimizes downtime for Rockwell-based control systems and production lines. • Supports high availability for mission-critical automation processes. • SDN can prioritize time-sensitive industrial protocols like EtherNet/IP used by Rockwell devices. • Helps ensure deterministic communication for I/O, motion control, and safety systems. • Adapts routing paths based on network health, latency, or congestion.



Use cases

Table 1. Use cases

Industry	Use cases
Automotive Industry	Remote commissioning: Deploy PLC logic to assembly lines, paint booths, and robotic stations without being on-site. Multicontroller management: Coordinate multiple controllers across production zones using cloud-based tools. Secure vendor support: OEMs and integrators can troubleshoot and update systems remotely via VPN-secured access.
Food and beverage	Batch process automation: Design modular control logic for mixing, cooking, and packaging lines. Compliance monitoring: Use remote access to validate system changes and maintain audit trails for food safety standards. Reduced downtime: Quickly diagnose and fix issues in temperature, flow, or conveyor systems from anywhere.
Energy and utilities	Grid automation: Remotely configure and monitor substations, transformers, and breakers. Disaster recovery: Restore or update control systems in remote or hazardous locations without physical access. Secure communication: FactoryTalk® Remote Access ensures encrypted connections to critical infrastructure.
Water treatment and infrastructure	Pump and valve control: Design and deploy logic for filtration, distribution, and waste management systems. Remote monitoring: Track system health and performance across distributed facilities. Collaborative design: Engineers and municipal teams can co-develop projects in FactoryTalk® Design Studio from different locations.

Key capabilities that enable these use cases

- **Cloud-to-edge workflow:** Build in the cloud, and deploy to physical controllers like ControlLogix or CompactLogix.
- **Multiuser collaboration:** Teams can work on shared projects with auto-merge and conflict resolution.
- **Generative AI copilot:** Speed up code creation, error explanation, and system modeling using natural language.
- **Secure VPN access:** FactoryTalk® Remote Access uses Stratix routers and runtime licenses for encrypted connectivity.



“To maximize AI’s productivity benefits in a manufacturing environment, connecting islands of automation is critical. Connecting multiple lines in a plant and then connecting multiple plants can generate petabytes of data. Some applications make sense to go back to the data center; that will continue to happen. But other decisions need to be made in real time at the edge—especially on a manufacturing floor. Edge computing requires an integrated platform approach where the compute, the networking, and of course, the security all come together. Performant, secure networking at the edge is absolutely essential.”

Blake Moret
Chairman and CEO of Rockwell Automation

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.