VISION, EXPERIENCE, ANSWERS FOR INDUSTRY, ENERGY, & INFRASTRUCTURE

ARC Advisory Group

ARC View

# Why Modern Networks Are Critical for AI-Ready Manufacturing Operations

By Chantal Polsonetti, Vice President

**KEYWORDS:** Manufacturing Resilience, AI-Powered Processes, Shop Floor Virtualization, IT/OT Collaboration, Converged Cybersecurity

## Executive Summary

Driven by the need for increased productivity, efficiency, and competitiveness, the manufacturing industry is undergoing a significant digital transformation. Integration of AI, software-defined industrial automation, digital twinning, and virtualization into existing manufacturing systems is essential for building future-ready manufacturing operations. However, these advancements require a modern, robust, and secure network infrastructure.

***This report outlines the critical role of modern networks in enabling AI-ready manufacturing, the challenges involved, and the solutions that can help organizations successfully navigate the transition. It highlights the necessity of a high-performing enterprise-grade OT network that is secure by design and provides recommendations for manufacturers embarking on their network modernization journey.***

## The Need for Future-Ready Manufacturing Operations

To remain competitive in a rapidly evolving global market and respond to relentless demand for continuous improvement across all aspects of production, manufacturers must embrace a new generation of technologies to better address several key challenges. These challenges include escalating requirements for ongoing enhancements in operational productivity, efficiency, flexibility, resiliency, and overall product quality to meet ever-increasing consumer expectations and cost pressures.

Emerging technologies such as software-defined industrial automation, shop-floor virtualization, AI-powered processes, mobile and autonomous robotics, digital twins for simulation, and production-related cloud applications are reshaping the industry. These are no longer theoretical concepts but practical tools for optimization and improvement. These innovations promise to unlock unprecedented levels of optimization and agility.

At the same time, as manufacturing becomes increasingly powered by software and connected to cloud resources, it also becomes a more attractive target for cyber threats. This creates an imperative to strengthen cybersecurity to protect against evolving threats and minimize risk. The potential for production downtime, intellectual property theft, regulatory violations, or safety incidents due to a cyber-attack makes a proactive security posture non-negotiable.

This technological shift is further driven by the need to accelerate innovation and significantly reduce the time-to-market for new products and processes. In a competitive landscape, the ability to quickly adapt and

launch new offerings is a critical advantage. This is compounded by persistent operational challenges, such as minimizing supply chain disruptions, addressing critical workforce skill gaps, and the ongoing need to upgrade outdated or obsolete infrastructure.

***Primary implementation hurdles to adoption of advanced technologies often revolve around the limitations of existing network infrastructure. Issues with network performance, flexibility, scalability, reliability, resilience, security, manageability, and observability can stall or derail critical modernization initiatives.***

## Future-Ready Operations Demand a Modern Future-Ready Network

A modern network is the bedrock upon which future-ready manufacturing operations are built. The advanced technologies reshaping the factory floor have stringent network requirements that legacy networks simply cannot meet. Factory floors require a robust networking foundation that is scalable, secure, and resilient, capable of handling the massive data volumes and low-latency communication that technologies like AI-powered processes, digital twins, and cloud applications demand.

The operational technology (OT) network itself must be upgraded to become an enterprise-grade OT network. Such a network must also support new capabilities, including high-wattage Power over Ethernet (PoE) to power modern devices like high-resolution cameras and sensors, as well as the edge compute necessary to process data locally.

***Evolution to a future-ready network requires delivering the determinism and resilience required for industrial environments while also incorporating enterprise-class security, scalability, and high bandwidth.***

Intelligent management systems are essential to managing this complex environment. By leveraging automation and centralized, intelligent network management, organizations can reduce manual tasks, boost performance, and maximize network availability. This allows IT and OT teams to move collaboratively from a reactive to a proactive stance, responding to business challenges more quickly and preventing downtime before it occurs.

Given the scale of modern industrial networks, "bolt-on" cybersecurity solutions are often complex, costly, and ineffective. A modern approach requires a "cyber-native" network with OT security features embedded directly into the infrastructure. Capabilities such as asset visibility, micro-segmentation to prevent lateral threat movement, and zero-trust remote access become integral parts of the network itself, providing security that can scale effectively.

Virtualization is a key enabler of future-ready operations. By decoupling industrial applications from specific physical hardware, manufacturers can address more use cases and significantly reduce both capital expenditure (capex) and operational expenditure (opex). Consolidating the hardware footprint reduces maintenance costs while simultaneously enhancing security, safety, and overall product quality.

This convergence of technologies fosters a necessary IT/OT partnership on a cultural and technical level. Integrated solutions and a unified network architecture encourage collaboration between IT and OT teams, bridging the gap between their traditionally separate domains. This allows the organization to leverage best practices from both worlds to support a cohesive digital transformation strategy.

Ultimately, an enterprise-grade OT network facilitates a unified data flow from the shop floor to the data center and the cloud. This seamless integration enables comprehensive operational visibility, allowing for more informed decision-making based on real-time data from every part of the operation. To support this, AI-powered troubleshooting tools empower OT technicians, who may not have deep networking expertise, to troubleshoot network issues using conversational language, thereby maximizing uptime and freeing up specialized IT resources. This all contributes to enhanced resilience, as upgraded networks provide superior backup and failover capabilities, including advanced disaster recovery and redundancy to ensure business continuity in the face of any disruption.

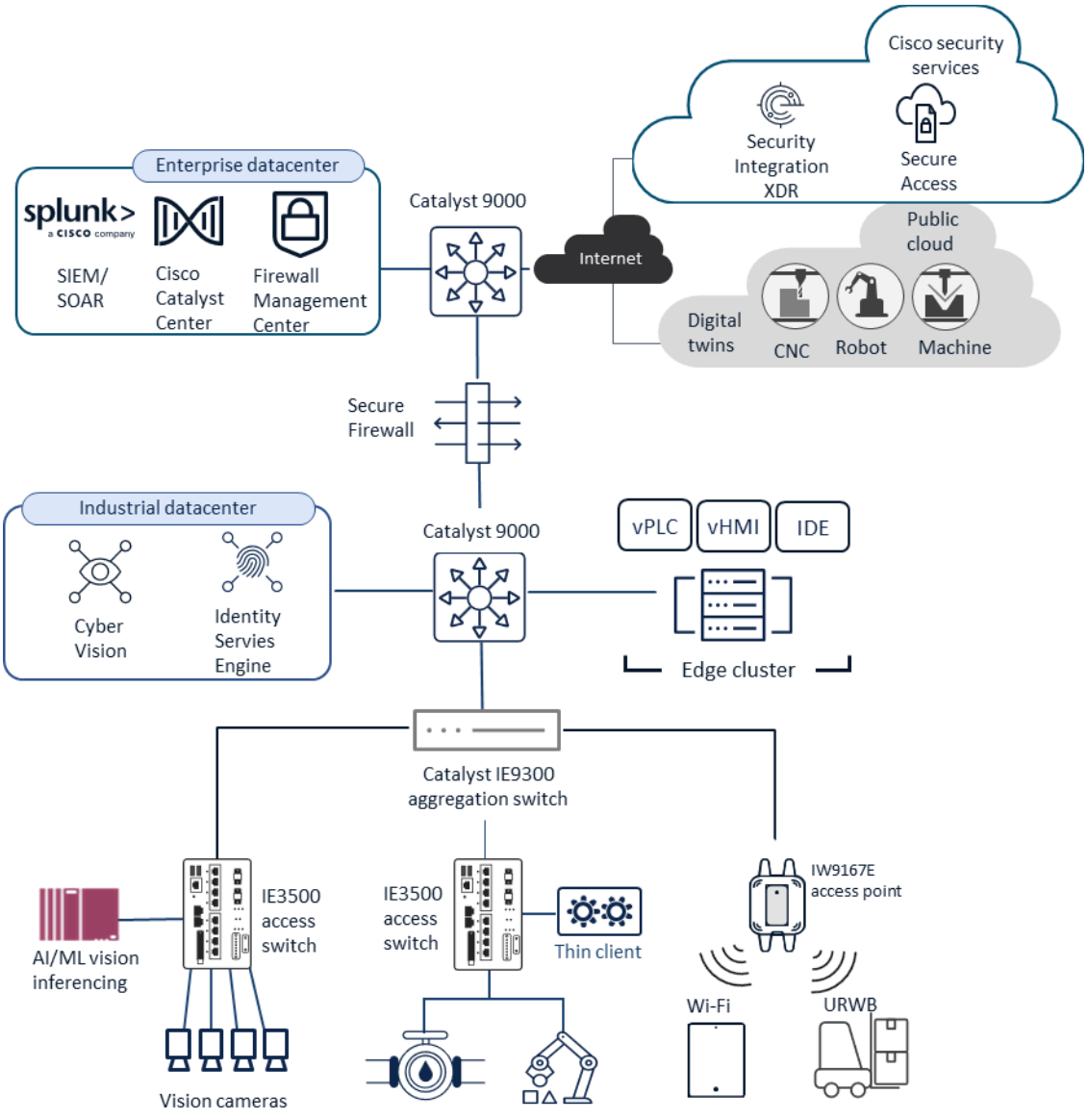
## Audi's EC4P Integrates Virtualization, Cloud, and Edge in Future-Ready Manufacturing Platform

Audi, part of Volkswagen AG, the world's second largest carmaker, has embarked on a groundbreaking project known as the Edge Cloud 4 Production (EC4P). In Audi's view, the traditional model of delivering production equipment to the plant floor is outdated, and the future is software-driven production. By virtualizing essential shop floor assets such as HMIs, industrial PCs, and PLCs, EC4P streamlines operations, reduces hardware complexity and costs, and ensures security, while enabling easy and timely upgrades. This new architecture empowers Audi to deploy advanced AI solutions for predictive maintenance and quality control, paving the way for software-defined factories and data-driven decision making. Ultimately, EC4P establishes a scalable, AI-ready infrastructure that supports Audi's vision for efficient, adaptable, and future-proof production. Market leading supplier Cisco provides the critical EC4P networking infrastructure that ensures high availability of production and compute resources from the shop floor to the data center. See the section on Further Information below for a link to an ARC report on Audi's EC4P initiative.

***By leveraging a modern network infrastructure, Audi has been able to virtualize its production line controls, leading to major cost savings and significant gains in flexibility, efficiency, and scalability. This initiative serves as a powerful example of how a forward-thinking approach to network architecture can unlock the full potential of software-defined manufacturing and AI-driven processes.***

## Cisco Networking & Security Enables Future-Ready Manufacturing Operations

Cisco, a leading enterprise and industrial network infrastructure supplier, offers a comprehensive suite of networking and security solutions designed to help manufacturers build future-ready operations. The company's industrial IoT offerings form the basis of a future-ready architecture, empowering industrial organizations to respond quickly to evolving business and technology drivers without constraints posed by their underlying infrastructure. Implementing their portfolio allows manufacturers to directly address the challenges of modernization through integrated IT/OT solutions that promote seamless communication, collaboration, and unified management across these traditionally separate operational domains.




Cisco's Industrial IoT Portfolio and Validated Architecture Enables Future-Ready Manufacturing

Cisco's ruggedized hardware portfolio, including industrial ethernet switches, industrial cellular routers, and industrial wireless access points, specifically validated for operational use cases, delivers a resilient, secure,

and scalable networking infrastructure. Support for emerging, data-intensive use cases is enabled through high-bandwidth connectivity up to 10Gbps and advanced features like 90W PoE, which can power a new generation of industrial devices. Embedded OT security features such as asset visibility, zero-trust remote access, and segmentation enforcement are built directly into the network equipment, allowing manufacturers to secure operations at scale and enable seamless, policy-driven communication between IT, OT, and cloud resources.

Cisco solutions enable shop-floor virtualization, including the decoupling of virtual PLCs from physical cabling, allowing machines and their controllers to operate as a single, unified, and flexible system. Intelligent network management and AI-driven platforms accelerate decision-making and automate remediation. By providing actionable insights from real-time data analysis, these platforms improve overall network resiliency and performance. Cisco also equips front-line OT teams with an Agentic AI-powered tool that acts as a digital co-worker, enabling them to rapidly diagnose and resolve network issues using simple conversational language and drastically reducing mean time to repair.

## Recommendations

For manufacturers looking to modernize their industrial networks for AI, a structured approach is crucial. We advise utilizing proven, industry-validated architectures to mitigate deployment risks, maintain vendor interoperability, and expedite project timelines. Frameworks such as Cisco Validated Designs (CVDs) provide comprehensive blueprints and best practices that reduce project complexity and help ensure a successful outcome.

Implementation of shop-floor virtualization creates a virtualized control environment that greatly enhances operational flexibility and reduces dependence on specific hardware vendors. Cisco's Dual Fabric Architecture for Virtualized Industrial Applications offers a proven path for deploying this complex technology successfully.

To support the data-intensive requirements of AI-powered machine vision systems for quality control and inspection, a high-performance network capable of powering endpoints with 90 Watt PoE is essential. Cisco's machine vision design and implementation guide provides architectural guidance to ensure the network can handle the throughput and latency demands of these applications.

Industrial network security is paramount. The Cisco validated design for industrial security provides a robust framework for implementing network segmentation, asset visibility, zero-trust remote access, and threat detection to protect critical operational assets from cyber threats. By adopting these validated designs, manufacturers can ensure that their network modernization projects are built on a solid foundation of proven technologies and architectures, paving the way for a successful transition to AI-ready operations.

## For Further Information:

Cisco 2026 State of Industrial AI for Manufacturing Report

Cisco White Paper: AI-Ready Industrial Network for Manufacturing

Cisco blog on EC4P project: Software-defined Success: Audi's Production Lines Enter a New Era with Cisco

ARC Advisory White Paper on EC4P: Building Audi's EC4P Platform for Shop Floor Virtualization

Explore Cisco industrial IoT offerings: Industrial Internet of Things

Cisco Industrial Cybersecurity Solution Overview

Cisco Industry Validated Design Guides - Cisco

Global Intelligence in Industrial AI & Digital Transformation

*For further information or to provide feedback on this article, please contact your account manager or the author at cpolsonetti@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC, and no part may be reproduced without prior permission from ARC.*