



Dual Fabric Architecture for Virtualized Industrial Applications

Modern manufacturing is undergoing a profound digital transformation. To improve scalability, accelerate time to market, and integrate advanced AI-driven analytics, manufacturers are increasingly adopting virtualization architectures. This shift involves moving compute-intensive workloads—such as engineering workstations, Human-Machine Interfaces (HMIs), and, most critically, the “brains” of industrial automation, the Programmable Logic Controller (PLC)—into virtualized environments.

While the benefits of virtualized PLCs (vPLCs) are clear—offering greater flexibility, reduced capital expenditure, and simplified lifecycle management—they introduce significant architectural challenges. Traditional PLC networks were designed under the assumption of a fixed physical location, direct connection to local industrial devices, and minimal network hops. Virtualization shatters these assumptions. When control logic is decoupled from physical hardware, it becomes dependent on the shared underlying compute, storage, and network infrastructure. In this new paradigm, latency, jitter, and network congestion are no longer just IT concerns; they are direct threats to the stability and safety of the industrial control process.



The challenge: Bridging the IT/OT divide

The primary challenge for manufacturing network architects is to provide an infrastructure that supports the agility of IT-managed virtualization while maintaining the deterministic, low-latency, and high-availability requirements of Operational Technology (OT).

Traditional enterprise and data center networks are built on Layer 3 boundaries and IP subnet isolation, which do not natively support the Layer 2 adjacency required by many industrial protocols like PROFINET.

Furthermore, standard network reconvergence times—which are acceptable for enterprise email or web traffic—are often too slow for real-time industrial control loops. If a network link fails, a standard fabric may experience a brief interruption during reconvergence; in industrial environments, even short disruptions can trigger safety systems that stop the process, cause PLC communication faults, or result in unplanned production downtime.

The dual fabric solution

Cisco's Dual Fabric Architecture for Virtualized Industrial Applications provides a robust, validated framework to address these challenges. By deploying two fully independent Cisco® [Software-Defined Access](#) (SD-Access) fabrics, this solution creates an environment where flexibility and determinism coexist.

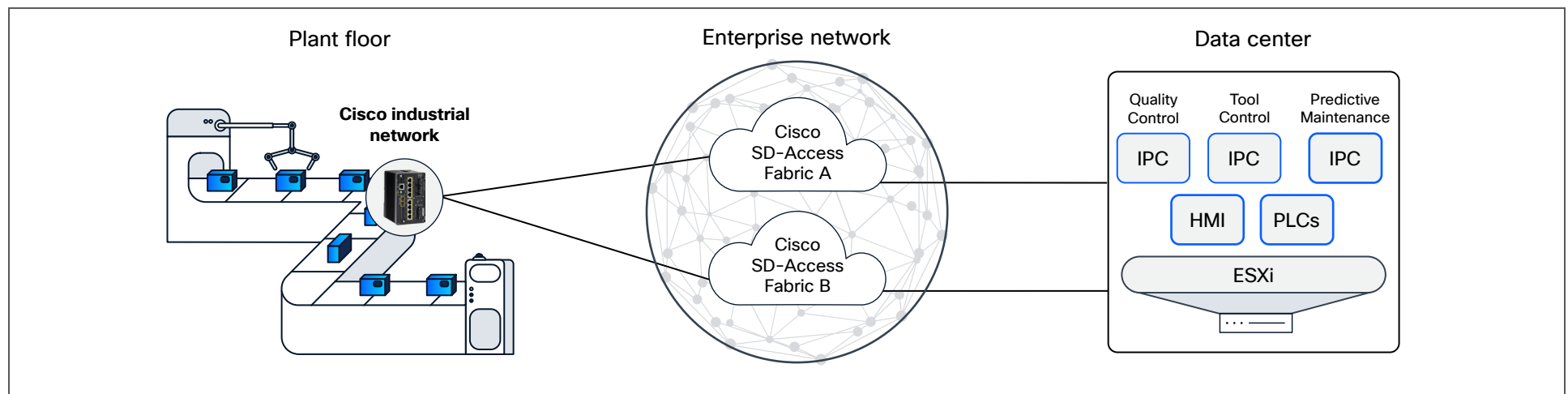


Figure 1. Dual fabric architecture

The architectural foundation

The architecture is built on three core pillars:

- **Dual independent SD-Access fabrics:** Instead of a single redundant network, this solution deploys two entirely separate SD-Access fabrics (Fabric A and Fabric B). Each fabric operates with its own control plane, forwarding plane, and failure domain. Because there are no shared forwarding states between them, a failure, misconfiguration, or maintenance event in one fabric has zero impact on the other.
- **Layer 2 traffic tunneling:** The solution enables PLCs to be located far from the machines they control while maintaining seamless communication as if they were on the same local network. This is achieved by encapsulating machine control traffic (operating at Layer 2) within the SD-Access Layer 3 fabrics using [VXLAN technology](#), preserving protocol information across the network and conforming to the strict time constraints for such traffic.
- **Parallel Redundancy Protocol (PRP):** To achieve hitless network resiliency, the architecture leverages the Parallel Redundancy Protocol. For time-critical traffic, frames are duplicated and transmitted simultaneously across both fabrics. The receiving endpoint (or redundancy box) accepts the first valid frame and discards the duplicate. If one fabric fails entirely, the other continues to deliver traffic without a single lost packet or interruption.

Strategic benefits for manufacturers

By adopting this dual-fabric approach, manufacturers gain more than just a resilient network; they gain a foundation for long-term operational excellence:

- **Uninterrupted availability:** The combination of PRP and dual-fabric isolation eliminates single points of failure. Critical control loops remain active even during catastrophic network events, protecting safety and production uptime.
- **Workload mobility:** SD-Access uses VXLAN technology to decouple logical connectivity from physical topology. This allows vPLCs to be moved, recovered, or redeployed across the factory floor without requiring physical rewiring or complex VLAN reconfigurations.
- **Simplified lifecycle management:** Software-based PLCs can be managed using standardized IT workflows while adhering to OT change-control practices. Firmware updates, backups, and rollbacks become faster and less risky.
- **Enhanced security:** The architecture integrates Cisco TrustSec®, providing micro-segmentation that is independent of IP addressing. This allows manufacturers to enforce granular security policies—limiting communication between production cells or isolating engineering workstations—without the complexity of traditional firewall rules.
- **OT visibility:** Through the integration of Cisco Cyber Vision, manufacturers gain deep, passive visibility into industrial assets and communication patterns. This allows teams to identify potential threats, troubleshoot connectivity issues, and make informed decisions about segmentation without impacting production traffic.

“For Edge Cloud 4 Production (EC4P), Cisco provides the critical network infrastructure that ensures production and computing resources are available from the factory floor to the data center. Cisco is our partner in ensuring seamless and resilient communication for industrial applications. With the Cisco team at our side, we were able to implement the project within a very short period of time.”

~Sven Müller, EC4P project manager, Audi

Conclusion and references

The move to virtualized industrial control is inevitable, but it requires a network that is as agile as the software it supports. The dual-fabric SD-Access architecture provides the necessary bridge, enabling manufacturers to embrace the benefits of virtualization without compromising availability, determinism, and security that their operations demand. By choosing Cisco, manufacturers are not just installing switches; they are deploying a resilient, future-ready foundation that turns the network into a strategic asset for the modern digital factory.

Read also

- [Dual Fabric Architecture for Virtualized Industrial Applications: Design and Implementation Guide](#)
- [Building Audi's EC4P Platform for Shop Floor Virtualization](#)
- [Cisco Validated Designs for Manufacturing](#)

Why Cisco is the only choice

While other vendors offer networking components, Cisco is the only vendor capable of delivering this architecture as a **Cisco Validated Design (CVD)**. This distinction is vital for several reasons:

- **Integrated ecosystem:** The solution is not a collection of disparate parts; it is a holistic, tested system. It integrates Cisco's industrial-grade hardware (Cisco Catalyst® [Industrial Ethernet switches](#)), enterprise-class SD-Access fabric nodes, [Cisco Identity Services Engine \(ISE\)](#) for policy enforcement, and [Cisco Cyber Vision](#) for visibility.
- **Validated predictable performance:** Cisco has performed rigorous testing to ensure that the combination of SD-Access and PRP meets the strict requirements of industrial protocols like PROFINET. This validation removes the guesswork from deployment, helping ensure that the network behaves as expected under both normal and failure conditions.
- **OT-centric design philosophy:** Unlike approaches that try to force-fit enterprise IT solutions into the factory, Cisco's architecture is built around the realities of industrial operations. This includes native support for industrial protocols such as PROFINET on industrial switches, and capabilities like line-rate Network Address Translation (NAT) to handle common challenges such as duplicated IP addressing in machines, all while maintaining consistent network behavior.
- **Operational simplicity:** Through [Cisco Catalyst Center](#), IT and OT teams can automate the provisioning, monitoring, and lifecycle management of both fabrics. This shared management plane bridges the gap between IT and OT, fostering collaboration rather than friction.
- **Security fused-in:** Cisco uniquely integrates both IT and OT environments with embedded security technologies like [TrustSec](#), Cyber Vision, and [Secure Equipment Access](#) directly into the network fabric. This unified approach provides a resilient, automated, and visibility-rich foundation that uniquely addresses the complex requirements of virtualized industrial environments.