



AI-Ready Industrial Network for Manufacturing

Solution Brief

June 2025

AI-Ready Network and Security Industrial Infrastructure for Manufacturing

Cisco has been engaged in bringing standard networking and cybersecurity capabilities into manufacturing production environments for over 20 years. As with other industries, when internet technologies arrive drastic innovation comes along with it. And that is exactly what is occurring, especially with the introduction of Artificial Intelligence (AI) and Machine Learning (ML) technologies into production systems. These technologies are driving improvements in product quality, increased efficiency, cost reductions and enabling more automation. The use cases are astounding and abundant, - AI is driving improvements in machine vision, adaptive and coordinated robotic operations, manufacturing processes, enabling cloud-based Digital Twins and making personnel more effective and efficient. All of this is driving Software Defined Industrial Automation (SDIA) – where the key logic of the production system is moving away from HW-based to software driven.

Critical to enabling these use cases is the ability to give the AI applications secure, high-speed/low-latency, resilient access to the production assets and the data they produce. The ability to deploy these applications at the edge – next to the asset - in the plant data center to take advantage of hyper-converged computing or in the cloud to access compute intense LLM AI capabilities is critical. The network needs to provide resilient, flexible, deterministic, high-bandwidth connectivity to connect AI applications to the data and devices in the production systems. This expanded network access requires a more in-depth industrial cyber security approach to protect the assets, data and the new applications.

Benefits

Accelerate AI deployments in production facilities

- Improve quality and safety with AI/ML-driven Machine Vision
- Reduce costs and maintenance effort by virtualizing plant assets such as HMIs, Workstations and PLCs
- Maximize efficiency by quickly delivering data to AI/ML applications
- Improve security of critical applications and data

This solution takes Cisco Industrial Automation solution to the next level – making the customer production systems network and security AI ready. It provides not only a reference architecture blueprint, but tested and validated design and implementation guidance so IT and OT teams can confidently drive convergence and digitization of production environments. The guidance is based on extensive testing with operational IACS systems and in collaboration with many of those vendors. It is used by IT/OT partners and system integrators to accelerate deployments.

Cisco is the leader in industrial networking and cybersecurity. We are leveraging the Cisco extensive portfolio of products and technology to easily deploy, manage, and secure these AI-ready Industrial Automation infrastructure for Manufacturing.

Cisco Validated Designs (CVDs) provide the core network foundation that meets the needs of operations and IT. This solution brief is a high-level overview of the reference architecture described in the [“Networking and Security in Industrial Automation Environments” CVD](#).

AI Use Cases

There are many AI use cases in manufacturing production systems. AI technology can be used to enhance worker productivity, improve product and process quality, reduce waste and energy consumption, and optimize supply & demand forecasting.

Our solutions enable a host of AI use cases to be quickly deployed and provided secure access to data and systems in the production environment. The key use cases this solution incorporates include:

- Improve the speed, quality and adaptability of machine vision applications to increase product quality, decrease “false-fails” where discrepancies are mis-identified and increase automation when combined with robotic operations
- Drive SDIA with virtualization of key production compute and control assets to improve security, reduce costs, and improve flexibility by operating the workloads on more efficient hyper-converged compute platforms
- Enhance worker productivity and safety through AI-driven co-pilots and problem identification/resolution
- AI-driven adaptive robotics can be used to automate more challenging tasks such as product inspection, valve manipulation or tactile insertion tasks that have been difficult to automate in the past
- Make data available from AI/ML technology that analyzes machines and process telemetry, to identify far in-advance when parts and machines need replacement or maintenance
- Analyze product and process data to improve product quality, reduce waste and decrease energy utilization
- Monitor network traffic to identify patterns to create security policy and detect anomalies that may represent cyber-security risks and threats

In this solution, we will focus specifically on three key use cases:

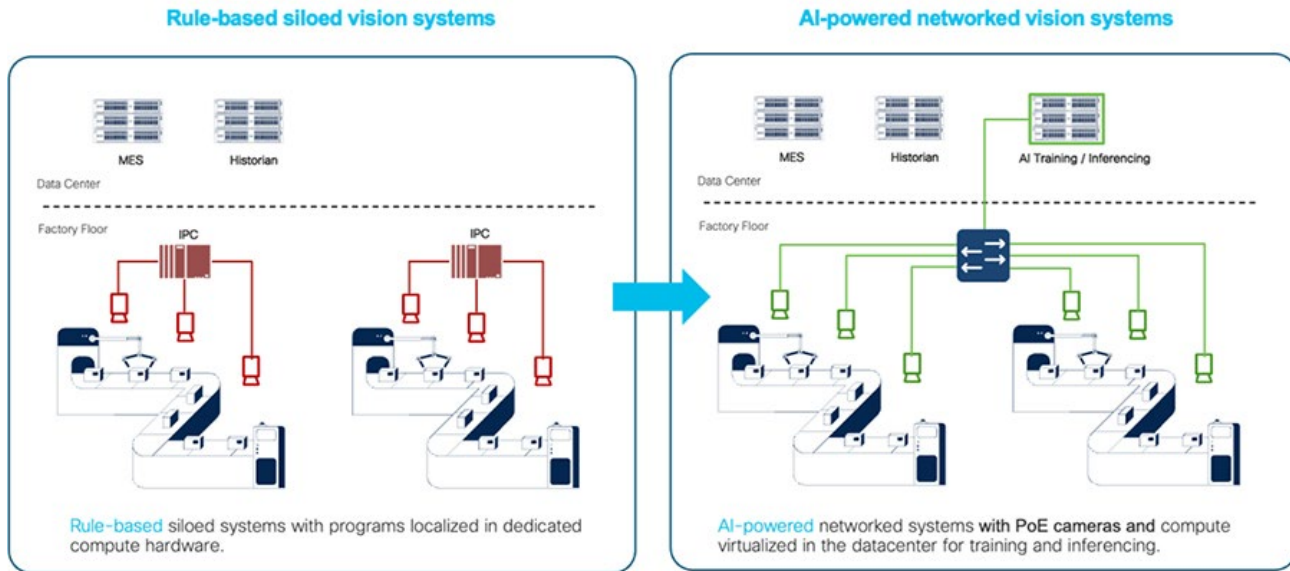
- AI/ML-driven machine visioning
- Virtualization of key production assets such as Human Machine Interfaces (HMIs), Industrial PCs (IPCs), and Programmable Logic Controllers (PLCs)
- Industrial Data Collection with secure, resilient and deterministic network from sensor to cloud connectivity to supply AI training and inferencing applications with data from the IACS systems

These cases are discussed in the following sections.

AI/ML-driven Machine Visioning

Machine Visioning (MV) in production systems is used for a host of applications – product quality assessment, coordinating robotic operations (for example, pick and place, tool/placement), scanning products or containers for text or barcodes, and safety for mobile assets. The camera sensors used in these applications are also rapidly improving – the granularity with which images are produced and the speed at which they are produced. AI/ML technologies are improving how quickly and effectively the vision data is processed, for example by adapting to changing conditions or processing the data in innovative ways (for example, area-scanning to line-scanning, or 2-D to 3-D scanning). AI/ML is significantly improving on the existing rules-based vision processing. See Figure 1.

Figure 1. Rule-based to AI-driven machine vision



The outcomes are impressive and include:

- Reduced number of false-fails, where a product or process was inappropriately identified as an anomaly, causing waste, output reduction and slowing production output
- Improved product quality by more precisely identifying anomalies, speeding up the time to check a product and adapting to changing lighting or other environmental conditions
- Reduced processing time of more granular images to increase speed of robotic operations, increasing output
- Increased success rate of identifying and reading bar-codes or character-based data on inventory and assets
- Reduced costs by optimizing the use of AI capable compute resources through flexible network connectivity

There are significant challenges to deploying the technology. These need to be overcome to accelerate adoption of improved technology. Key challenges include:

- Lack of bandwidth in production systems to handle the volume of data coming from MV cameras for processing or long-term storage
- Challenge to provide low-latency/jitter communications for other critical traffic applications with the presence of vision-driven jumbo frames
- Ability access quality data to train the new AI/ML applications due to lack of connectivity
- Support for MV creates jumbo frames to reduce network communication overhead
- Guidance on network configuration and set-up to provide confidence in deploying these applications

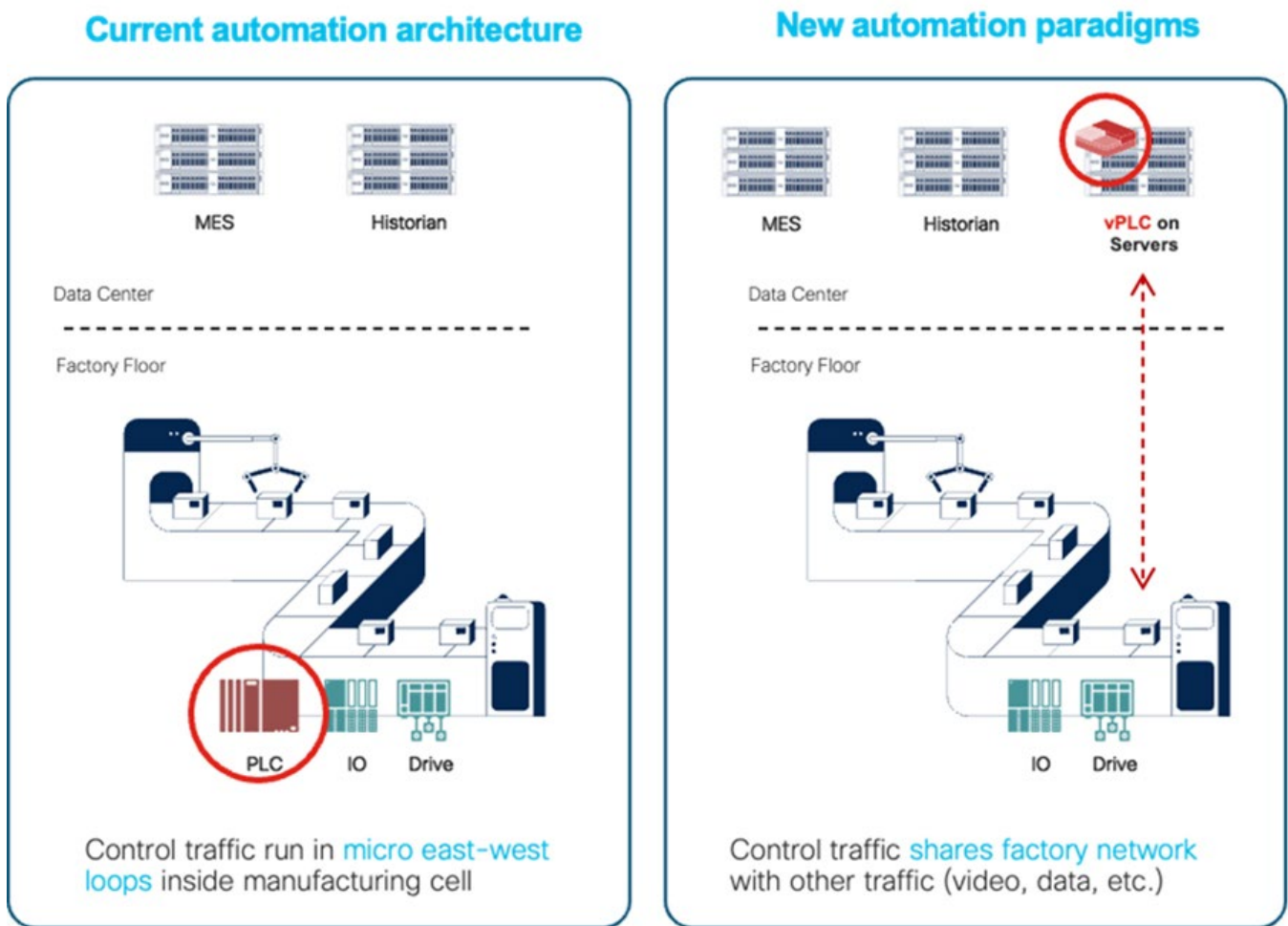
This solution will provide guidance based on testing and collaboration with a set of MV vendors on how to overcome these challenges and help manufacturers and the system implementers to accelerate the adoption of this exciting technology.

Production Asset Virtualization

For a long time, Production Managers and Engineers looking to add new functionality to production systems often entailed introducing new Industrial PC-based assets. That adds to the conflagration of compute systems for HMIs, workstations and data collectors. These IPCs can run into the 100s or 1000s in modern production environments. Maintaining and upgrading these, especially with the steady flow of security updates, is an overwhelming task that simply does not get done in most factories. Not only are these a management and security nightmare, they are expensive and often under-utilized assets as they are designed and deployed for single-purpose use.

Our customer and partner, Audi, has identified a need for a paradigm-shift “software, not hardware” for a new Software-Defined Factory. This shift is focused on virtualizing key production compute assets, such as HMIs, workstations and even Programmable Logic Controllers (PLCs) onto hyper-converged compute environments in factory-local data centers. All of this being done in brownfield production systems.

Figure 2. Paradigm-shift: Hardware to Software for new capabilities



A critical component of this virtualization is the ability to securely, resiliently and deterministically transport the Industrial Automation and Control System (IACS) traffic from the Cell/Area zone to local data center housing the virtualization platform. As most of the IACS traffic is designed to operate in LAN networks, that IACS traffic needs to be transported to the local data center with low-latency and high resiliency to operate the virtual workloads as they would if they remained local.

This solution will identify the requirements and propose a reference architecture to virtualize these critical assets. The result for manufacturing customers includes reduced costs, agility to deploy new applications quickly, and improved security by upgrading critical applications software with less effort and more frequently.

Industrial Data Collection

Manufacturers are constantly looking to optimize production processes and the quality of the products they create. As the famous quote from Peter Drucker states “if you cannot measure it, you can’t improve it”. Access to the data in the production systems is critical. Manufacturers are collecting information for optimization as well as regulatory and historical reasons. All of this requires access to the assets and devices and the ability to move that data to local, enterprise or cloud-based systems that store, sort, analyze and manage the data.

The Cisco AI-Ready Industrial Networking solution is a design that enables access and supports the secure movement of the production data to wherever it needs to go.

What makes an Industrial Network “AI Ready”?

Key requirements

AI-workloads are going to be deployed in various parts of the network dependent on the amount of data, real-time accessibility to data/assets and how much computing resources will be required to perform the task. They may be deployed in the industrial access network, in line with the assets, in the production data-center with other Plant-level applications or even in the private/public cloud. AI applications may require very large volumes of data, deliver with low-latency and with high-resiliency. That data may need to be processed quickly by local AI-inferencing engines or transferred to cloud-applications to help train AI models or stored for historical/auditing purposes. All the additional traffic must co-exist and not impact the existing control traffic and applications.

For example, with AI-driven machine-vision systems that have cameras support gigabit/second or faster connections and produce 10s-100s of Mb of data per frame where frames are often produced 10-100 times/second depending on the application supported. Depending on the underlying production cycle time, those images may need to be processed in single-digit milliseconds up to seconds. This will dictate if they are processed at the edge, nearby in a plant datacenter or in the enterprise/external cloud. The new sensors also have their own requirements – of power, of communications, and of synchronization to coordinate with the IACS. And the assets/sensors and the data they produce need to be secured.

In summary, the network and security requirements include:

- High-bandwidth throughout the network to support high-bandwidth devices and increasing amounts of data moving in and out of the industrial access networks
- Real-time, deterministic application support with low network latency and jitter to transfer data to AI applications,
- Agile, flexible and SW-defined network infrastructure to enable new or move existing workloads to optimal locations (for example, from the industrial edge in the Cell/Area zone to plant data center) depending on application requirements,
- Converged network to support communication from sensor to cloud to get the data to where it needs to be processed and our stored,
- New AI applications and traffic need to co-exist with Automation and Control and the range of protocols (for example, Profinet, CIP/EtherNet-IP, and others)
- Resilient connectivity to ensure the virtualized and AI-driven applications perform with the same or improved uptime
- Secure production environments with:
 - Visibility of devices and communication throughout the manufacturing zones
 - Protection from key threats by implementing the industrial demilitarized zone (IDMZ) and zone-based segmentation according to industrial security policies
 - Detection of threats including malware and malicious traffic

- Detection of abnormal process modifications such as unexpected variable changes or program uploads to automation devices
- Response to security risks through integration with security management applications
- Scalable from small (tens to hundreds of IACS devices) to very large (thousands to 10,000s) deployments

AI-Ready Industrial Automation reference architecture

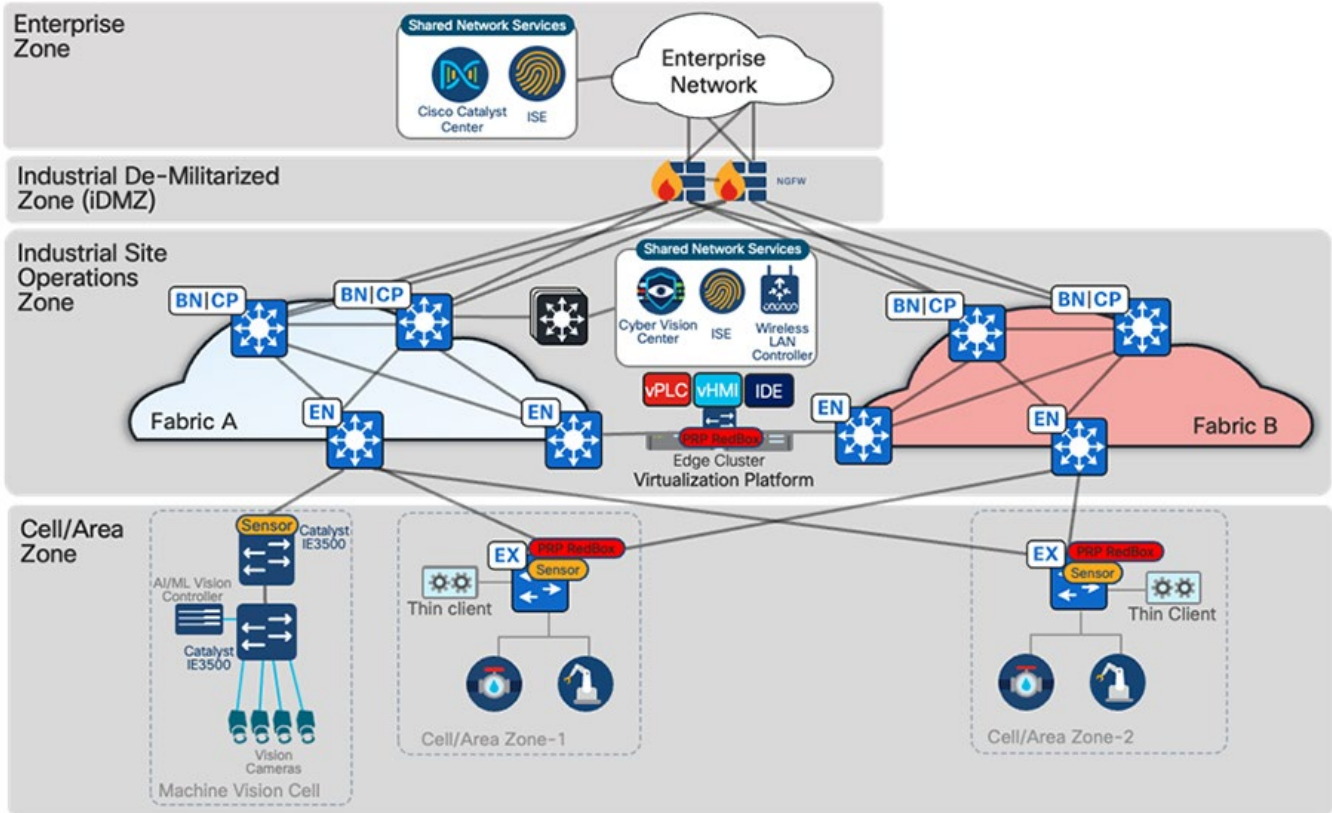
The AI-Ready Industrial Automation reference architecture is an evolution of our Industrial Automation solution. The reference architecture overlays the typical devices, applications, network infrastructure and security technology onto the Purdue framework to give context to the design and implementation guidance. The architecture is focused around three key networking areas: The Cell/Area Zone supporting the core IACS embedded in the production environment functional zones, the Industrial/Manufacturing Zone supporting plant-wide applications and services, and the Industrial De-Militarized Zone (IDMZ) providing key segmentation between production and enterprise systems.

The AI-Ready industrial network reference architecture supports secure, agile deployment of AI applications and the access to industrial automation and control devices, applications and data they demand. The architecture supports AI use cases at the edge: AI/ML-driven Machine Visioning, IACS asset virtualization, AI Robotics and industrial data collection. Key enhancements of the AI-Ready Industrial Automation network include:

- Support for AI/ML-Driven Machine Vision applications at the edge with the new IE3500 switches with
- Support for agile deployment of AI-applications and virtualization of key IACS assets with resilient Software-Define Access dual-fabric design relying on loss-less resiliency provided by the Parallel Redundancy Protocol to maintain production uptime

The Industrial Automation architecture map is shown in Figure 2.

Figure 2. Industrial Automation architecture map



Robust Connectivity

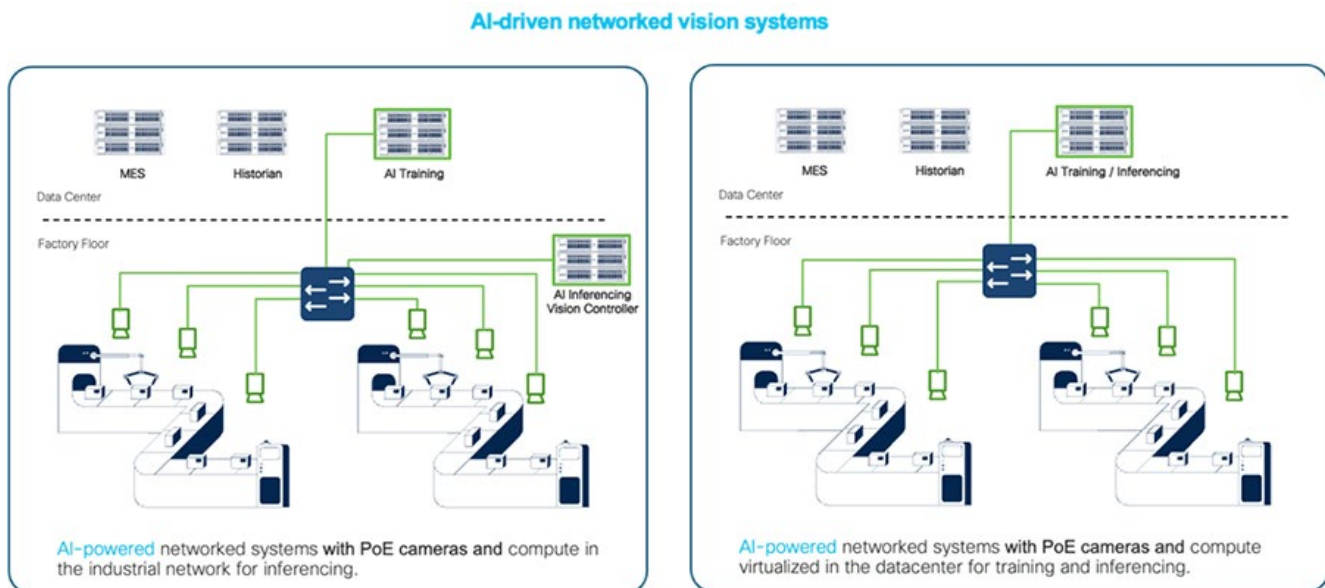
Industrial devices and sensors are constantly improving with more sensitivity, granularity and speed driven by improved compute built into sensors and actuators such as Machine Vision cameras, motion control, environmental sensors and much more. On top of this ability to produce more data, more quickly, there are more AI-driven applications that consume more of the data from these devices, well beyond just the IACS traffic such as Profinet and the ODVA Common Industrial Protocol (CIP) EtherNet/IP protocols. Machine Vision cameras are at the forefront of this initiative.

Manufacturers are excited about the abilities the camera and the AI-Driven machine vision can support, but they are highly concerned with the bandwidth and connectivity these require.

Our launch of the IE3500 switch and this solution are specifically targeted for these types of applications. Specifically, the new switch and solution will help accelerate the deployment of AI-Driven MV by:

- Reducing the required cabling by combining:
 - High-bandwidth data transfer with Gigabit, multi-Gigabit and 10 Gb connectivity to interconnect cameras to AI-capable machine vision controllers
 - Ppoe and other PoE features to resiliently power the MV cameras
 - Synchronization with the IACS applications via Precision Time Protocol
 - Ability to connect via copper and fiber at significantly longer distances than other technologies (examples are USB, co-ax)
- Support for larger jumbo frames (9Kb) to lower vision traffic latency
- QoS and Frame-preemption options to limit the impact of vision traffic to IACS traffic
- Optimize using expensive AI/ML compute and controllers via scalable connectivity to connect multiple camera types
- Cybersecurity observability and segmentation with Cyber Vision and TrustSec support in the network

Figure 3. Machine Vision Connectivity Options



The AI-Ready solution will specify design and configuration considerations to support connectivity of Machine Vision cameras to AI-powered vision inferencing and control applications, in the plant data center or on the plant floor. The solution guidance will cover cameras and technology from a wide set of camera vendors and help manufacturers accelerate adoption and deployment of this important AI capability.

Software-Defined Access for Agility, Automation and Ease-of-Use

AI-Ready in Manufacturing is also tightly integrated with initiatives to create SW-Defined Factories. The ability to virtualize assets and operate them on hyper-converged compute environments is a key step to creating a SW-Defined Factory.

This pivot enables customers to deploy SW to gain access to new functions which AI technologies provides, rather than deploying new boxes and compute infrastructure in the industrial environment. For this to be successful, the industrial network must also be SW-defined and capable of dynamically, deterministically and securely providing these new SW capabilities with access to the existing, brownfield devices (robots, drives, sensors, machines, etc.). Cisco Software-Defined Access capability supported by Catalyst Center is designed to provide these features.

The reference architecture and solution design and implementation guidance will provide a blueprint and guidance for deploying SDA in production networks specifically to support the virtualization of key production assets as deployed by Cisco Catalyst Center network management and controller application. Key features required by AI applications that SDA support include:

Stretch industrial VLANs– Ability to quickly connect new AI and Virtualized applications with Layer-2 connectivity to IACS assets in the production network regardless of their location. A critical capability in SDA is to “stretch” industrial VLANs across larger routed networks (fabrics) to transport critical control protocols (for example, Profinet) deterministically, resiliently and with low-latency between brownfield devices and the virtualized assets, such as an HMIs, workstations or PLCs that control and manage them.

Segment – A key capability of SW-defined networks is the ability to easily segment network resources for security and operational priority considerations. With Cisco SDA, it is easy to apply macro and micro-segmentation to the network, enabling safe sharing of network resources, while protecting the production assets and enabling separate resource allocations for IT and OT applications and use cases

Minimize Spanning Tree impact – Spanning Tree is a key technology to protect the network from mis-cabling that can produce network impacting loops, an important consideration as OT personnel manage production network cabling. But Spanning Tree events can also cause disruptions for OT applications as it reacts to network topology changes. SDA helps minimize impact of STP events while maintaining its important benefit of loop detection and avoidance.

Intent-based configuration SDAs– Workflows and architecture allow IT and OT personnel to simply, quickly and at scale perform a range of tasks with simple user interactions – by applying Intent versus much more tedious and complex network Command-Line Interface (CLI) interactions.

APIs and interfaces for additional Automation – converged IT/OT environments probably benefit the most from the ability to programmatically perform updates, changes, compliance checks in the deployed network. Making critical tasks such as creating and deploying switch configurations, upgrading network operating systems or even management of security policy highly automated tasks saves time resources and requires less expertise (once design and tested). Programming and automating network management activities decrease error-rates, require fewer skills of the operators, and significantly reduces work effort.

These capabilities all combine to make the industrial network AI-ready; ready to dynamically and securely create connectivity between new AI applications and industrial assets.

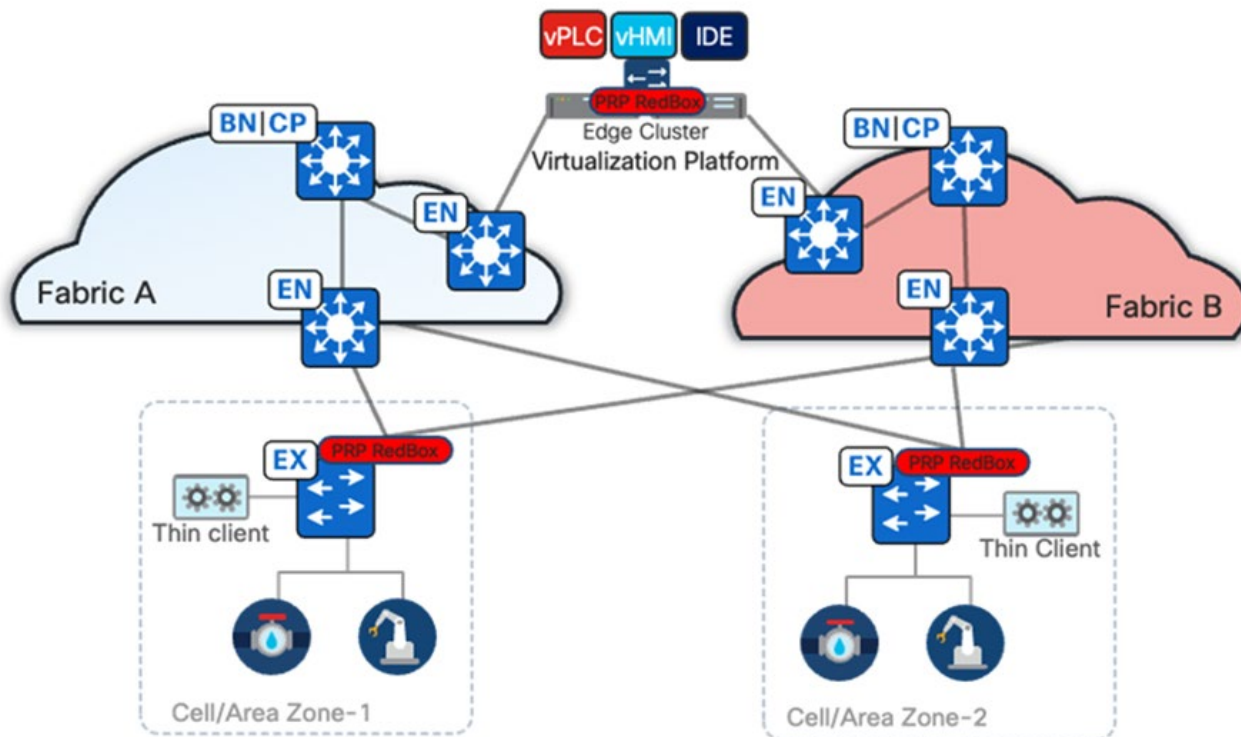
Resiliency and availability

Uptime is a key consideration for any production environment. Industrial applications often operate continuously for weeks, months, or years and any downtime, especially unplanned, results in significant loss of production output and costs, directly impacting the bottom line. The network infrastructure is critical to those industrial applications; therefore, several resiliency mechanisms are considered in this solution. And supporting the migration of critical assets; HMIs, workstations and PLCs, makes the network connectivity even more critical. For IT considerations, minor network disruptions measured in hundreds of milliseconds may seem minimal, but those disruptions in a manufacturing IACS application may result in significant outages of the critical Automation and Control systems, bringing production to a halt.

The solution architecture highlights a dual-fabric and the Parallel Redundancy Protocol at the industrial access layer to provide loss-less resiliency if network connections or infrastructure experiences outages. This level of resiliency is required to maintain critical IACS communications between the virtualized production assets and the automation and control devices in the brownfield industrial network.

The combination of the robust network connectivity, resiliency and SW-defined networking allow Manufacturers to migrate key workloads from the industrial edge to a local data center while maintaining low-latency, highly available and agile communications designed and validated for stringent Industrial Automation and Control. The solution design and implementation guidance will provide guidance on how to set up and configure these networks.

Figure 4. Dual-Fabric High Available design with Parallel Redundancy Protocol



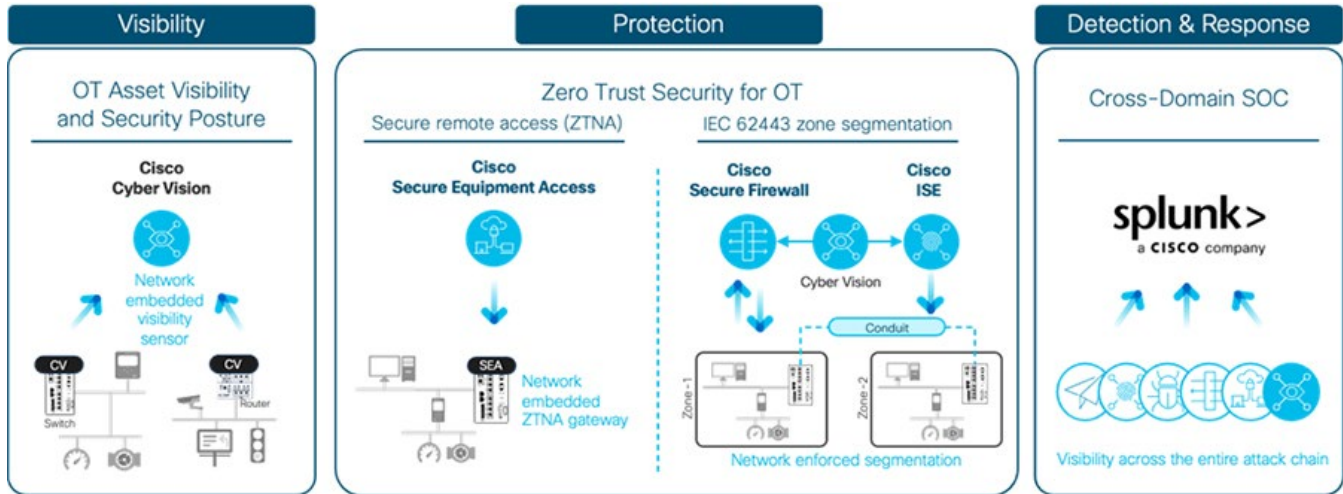
Industrial Cybersecurity

Historically, production environments and the IACS in them have been the sole responsibility of the operational organizations, such as plant managers and control engineers. But as Ethernet and IP networks have become the standard for IACS systems, IT departments are increasingly engaging with plant managers and control engineers to leverage the knowledge and expertise in standard networking technologies for the benefit of plant operations. Nonetheless, ease of configuration, implementation, and management are key considerations as often IT or OT personnel or partners may be involved in deploying the network and security infrastructure. Cisco has developed the Industrial Security 3.0 Design Guide

to help Manufacturers overcome key challenges and deploy robust security capabilities for production systems. Key Industrial Security steps include:

- Gaining Visibility and Understanding Security Posture of the production systems
- Applying Preventative Control in Plant networks
- Providing Secure Remote Access based on Zero-Trust Network Access
- Cross-domain Detection, Investigation, and Response to cyber security risks and events

Figure 5 Industrial Security Journey



This approach is critical for secure application of AI applications. The approach:

- Gives Manufacturers visibility to the data flows AI applications create
- Indicates the security posture of the Industrial Devices communicating with AI applications
- Allows secure transfer of data between the production systems and AI applications; at the industrial edge, in the plant data center or with Enterprise/Cloud deployments
- Provides micro-segmentation capabilities to manage what data AI applications can access and what AI-based inferencing results impact
- Enables Security Detection, Investigation and Response if risks arise to the industrial or AI applications.

For more information on industrial cyber security, see the Cisco [Industrial Security 3.0](#) Design Guide.

What's New

The AI-Ready Industrial Network builds upon the concepts, features and architecture developed in our Industrial Automation CVD. The key new features and capabilities include:

- Robust connectivity and security for AI/ML Driven Machine Visioning applications
- Inclusion of the new IE3500 industrial switch as an industrial access switch especially suited for AI/ML-driven Machine Visioning

- Cisco Software-Defined Access (SDA) architecture deployed by the Catalyst Center to drive automation and assurance of network deployment, configuration, and management to quickly connect AI applications to IACS devices and data
- Dual-fabric SDA design with PRP on the IE Cell/Area switch for highly-available network connectivity for critical IACS traffic between virtualized production assets (PLCs, HMIs, Workstations) and brownfield IACS devices

Figure 6. Industrial Ethernet IE3500 and IE3500H



Summary

The AI-Ready Industrial Network solution provides a network and security platform on which Manufacturers can quickly, resiliency and securely deploy AI/ML applications. The Cisco solution overcomes the customer barriers to AI/ML deployments: accessing critical data, security the production systems, and simple, scalable networking solutions. The solution provides a proven and validated blueprint for connecting AI/ML applications to IACS and production assets, improving industrial security, and improving plant data access and operating reliability. Following this best practice blueprint with Cisco market-leading technologies will help decrease deployment time, decrease risk, decrease complexity, and improve overall security and operating uptime.

Americas Headquarters
 Cisco Systems, Inc.
 San Jose, CA

Asia Pacific Headquarters
 Cisco Systems (USA) Pte. Ltd.
 Singapore

Europe Headquarters
 Cisco Systems International BV Amsterdam,
 The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)