Industrial Automation Networking

Solution Brief

August 2024

Improve Operational Efficiency

Introduction to the Cisco Industrial Automation Networking Solution

For over a decade, manufacturers seeking operational improvements from their production systems and assets have used the Cisco® Industrial Automation Networking solution to drive IT/OT convergence and digitization.

Artificial Intelligence, Digitization, Industry 4.0 and Industrial Internet of Things (IIoT) initiatives are making improvements in manufacturers' production processes and supply chains and enhancing their products' value. These initiatives require visibility and access to the data of the industrial automation and control systems (IACS) in production environments.

This solution 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.

Benefits

Reduce downtime, improve operational efficiency and product quality with:

- Connectivity for demanding industrial automation and control systems
- Highly available, industrial network infrastructure and architecture
- Reduced risk to the production environment through industry-leading industrial cybersecurity
- Securely integrated to IoT, enterprise, and cloud services

389035

Cisco is the leader in industrial networking and cybersecurity. We are leveraging the Cisco extensive portfolios of products and technology to easily deploy, manage, and secure these ever larger and critical production networks and the data that flows through the IIoT.

Cisco Validated Designs (CVDs) provide the core network foundation that meet 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.

Converged networks providing secure connectivity throughout the plant

Production environments have been adopting standard networking for more than 20 years, transitioning from proprietary, niche networking technologies of the past. This solution provides a reference architecture and new networking approaches to help with the transition to standardized networks and realize the promise of ubiquitous connectivity. The key use cases this solution incorporates include:

- Connectivity for IACS devices and applications, including sensors, actuators, and controllers' and assets such as robots, machines, tools, and process skids
- Support for plant-wide applications such as manufacturing execution systems, supervisory control and data acquisition (SCADA), historians, and asset managers

- Network access for on-premises personnel to manage the plant and access remote resources as needed
- Visibility and continuous monitoring by IT and OT personnel of the network and security status of the IACS devices and communication
- Macro- and micro-segmentation of critical plant zones and assets
- Integration into corporate security threat detection and response services including Security Incident and Event Management (SIEM)
- Secure remote access for employees, vendors and contractors to configure, manage, and troubleshoot production assets without time-consuming and costly site visits
- Enable IoT applications with edge computing such as predictive analytics and maintenance, digital twin, and machine learning and optimization
- Secure access to IACS for data acquisition and integration with enterprise or cloud-based predictive maintenance, optimization applications, and data warehouses
- Automated network deployment and configuration with built-in compliance management of network infrastructure, operating systems and configurations
- Quick identification of network outages or performance issues and their rapid resolution with AI-driven assurance of network operations
- Mobility and wireless connectivity for nomadic or mobile equipment and backhaul services

Key requirements

The solution supports systems and environments that are critical to companies where downtime and network issues quickly have significant impact on revenue, reputation, and product quality. Therefore, key requirements the solution delivers include:

- High availability for all key industrial automation systems and services
- Real-time, deterministic application support with low network latency and jitter for the most challenging applications, such as motion control
- Converged network to support communication from sensor to cloud
- Support for a range of IACS vendors and protocols
- Ease of use as IACS networks are often deployed, configured, and managed by non-IT personnel with limited Ethernet and IP networking skill
- Reliance on open standards to ensure vendor choice and protection from proprietary constraints
- 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
- Availability of precise time across the site to support motion applications and schedule-of-events data collection
- Scalable from small (tens to hundreds of IACS devices) to very large (thousands to 10,000s) deployments
- Support for long operational lifecycles—often production environments and assets are not upgradeable for years or decades, therefore equipment and software updates may be very limited and newer network deployments must account for older devices with limited networking capability

Target audience

To successfully connect and secure the industrial environment, all stakeholders must work together; OT understands the industrial environment—the devices, the protocols, and the processes, IT understands the IP network, and the security team understands threats and vulnerabilities. By working together, they can leverage existing networking and security technologies, tools, and expertise to protect the industrial network without disrupting production safety and uptime. This solution is intended to be used by IT, OT, security teams, and their relevant partners and system integrators.

Operations will appreciate the ease of use and simple deployment, as well as the broad support of various IACS vendors and protocols with OT-designed tools. IT network managers will appreciate the ability to apply skills, technology, and applications already deployed in the enterprise when integrating production environments. Security teams will have visibility into industrial assets and security events with context enriched by control engineers.

Industrial ecosystem integration

Most industrial environments are supported by a wide range of vendors and suppliers. It is not atypical to see hundreds if not thousands of suppliers for companies' operational environments. The solution not only supports a large range of vendor equipment and the industrial protocols they support, but the design and implementation guidance has been developed with key vendors over more than 15 years and is deployed at thousands of facilities around the world. The solution integrates expertise from Cisco, the market leader in industrial networking and cybersecurity technologies, with that from the OT ecosystem. The solution is used in environments that support all the major IACS platform vendors including Rockwell Automation, Schneider Electric, Siemens, Emerson, Honeywell, Mitsubishi, and Omron, among many others.

This solution provides both IT and OT teams with the foundation to confidently collaborate and deploy secure, converged industrial automation networks and cybersecurity.

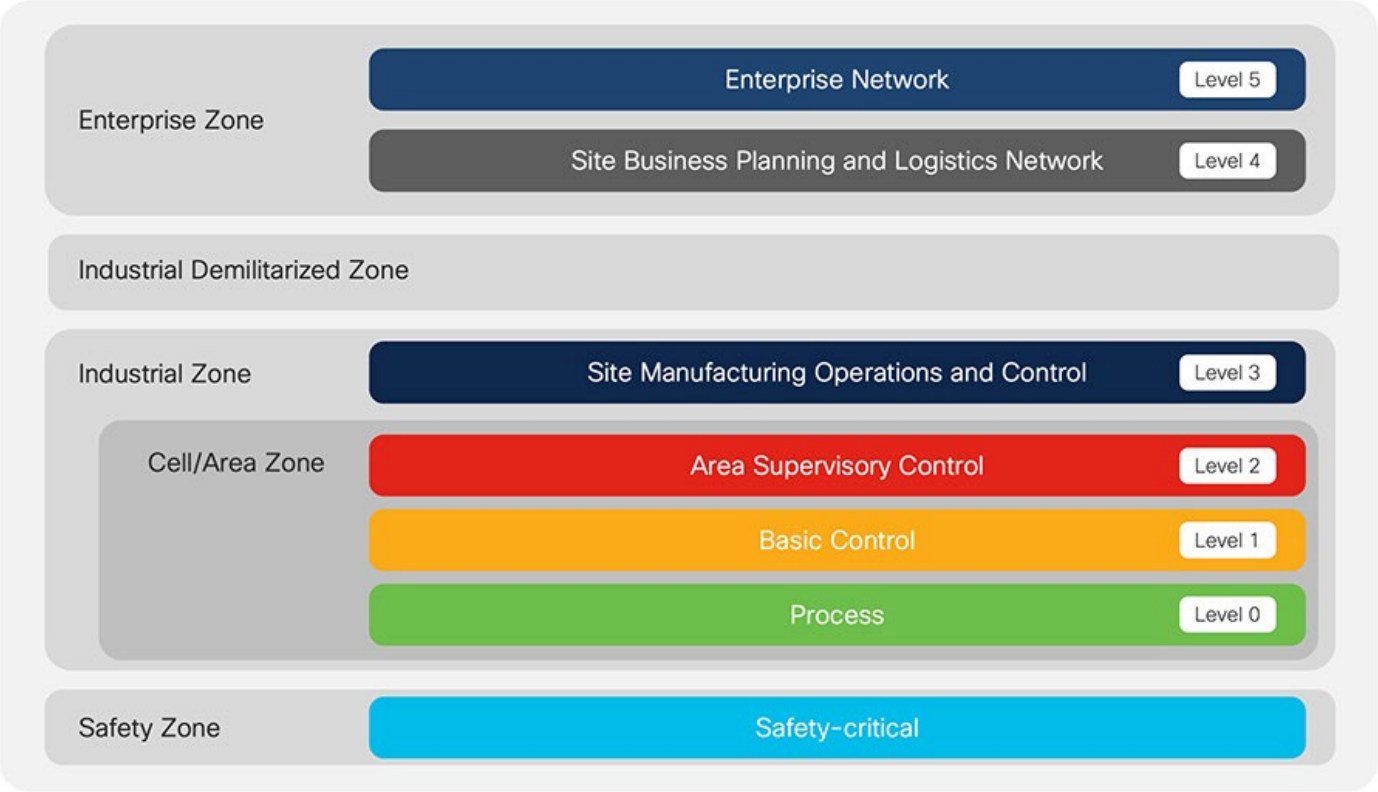
Industrial Automation reference architecture

The underpinning of the solution is the IA reference architecture, which depicts key functions of the manufacturing environment and relevant network security capabilities. The reference architecture is the core map to the design and implementation guidance provided by the solution.

Plant logical framework

This solution applies the Purdue model as a base framework for the architecture to help give context and align with industry concepts and standards. The Purdue model describes industrial, or production levels of control used to describe how automation and control technologies are applied. The Purdue model is shown in Figure 1.

Figure 1. Depiction of the Purdue model



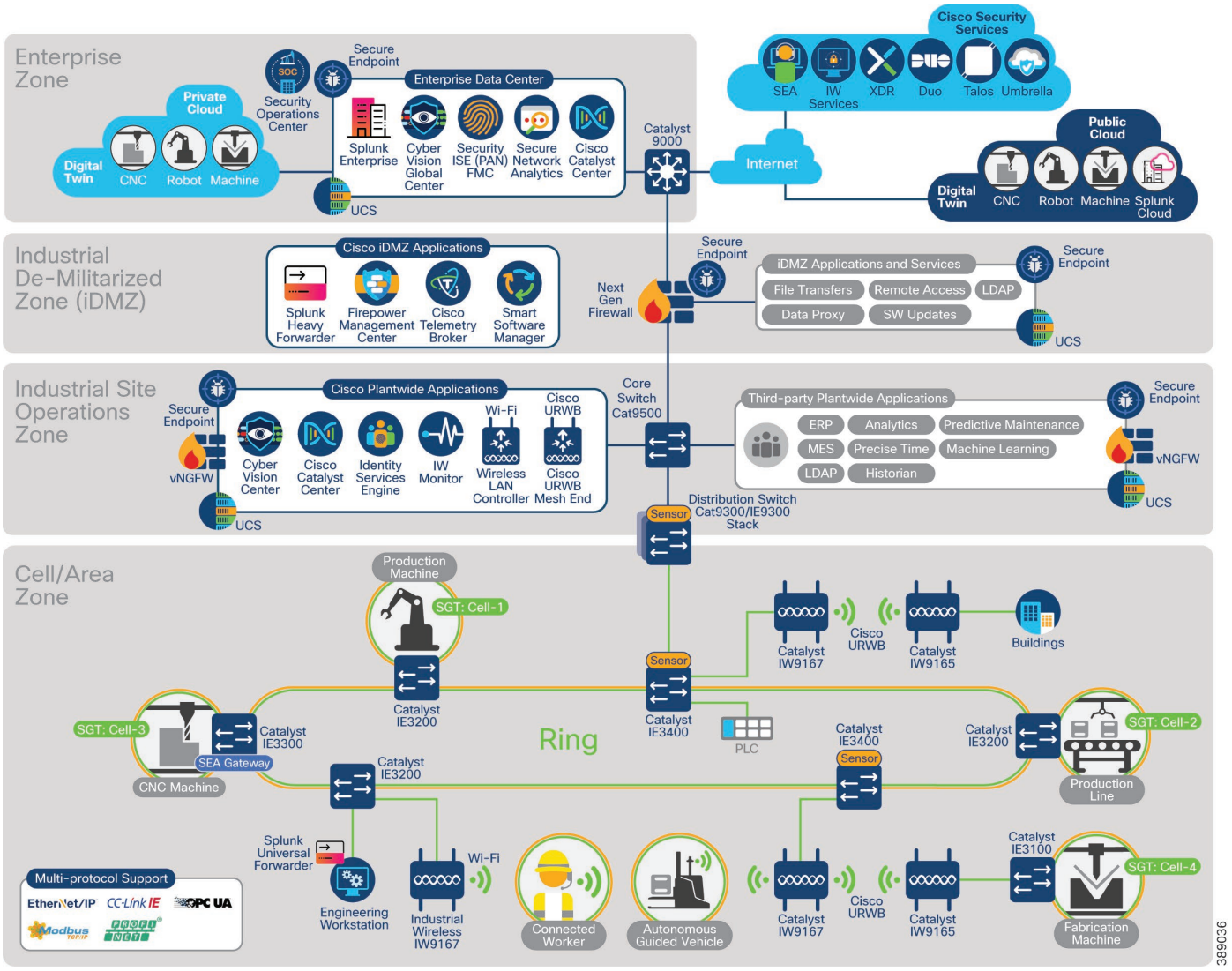
The Purdue model is useful in that it breaks down key functions of industrial applications. The network requirements for these applications drive key considerations and capabilities for the solution described later in this paper.

Industrial Automation reference architecture

The IA 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 Industrial Automation architecture map is shown in Figure 2.

Figure 2. Industrial Automation architecture map

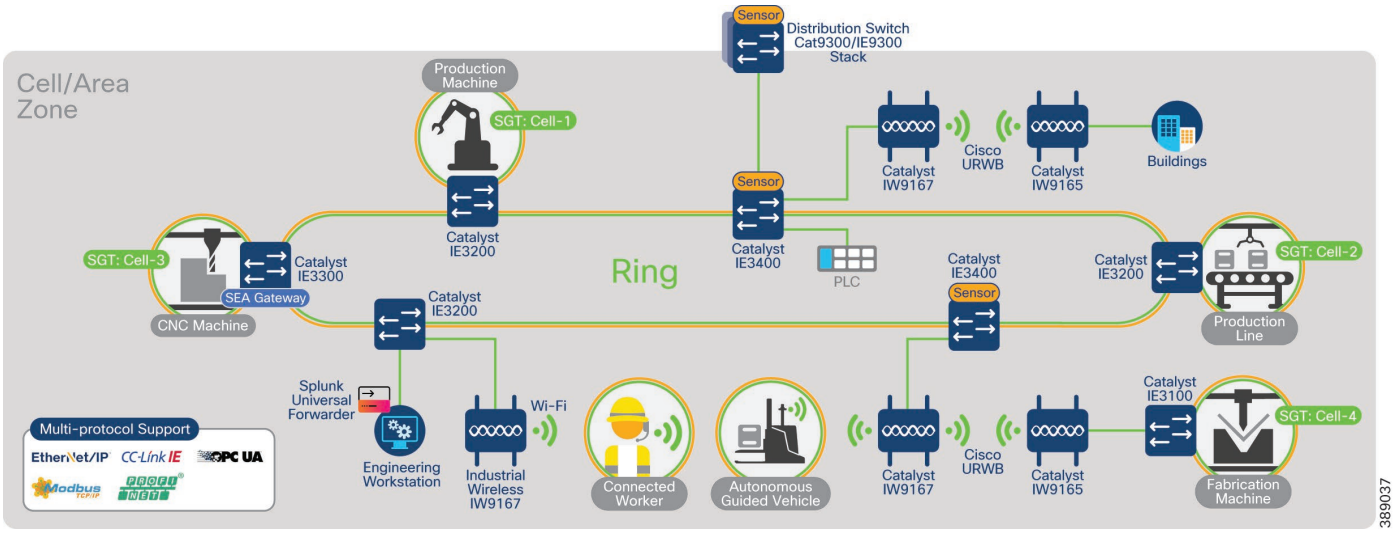


Cell/Area Zone

The Cell/Area Zone, a functional area within a plant or factory, is the foundation of the reference architecture. Most plants will have tens, if not hundreds or thousands, of functional areas. This is the network that connects sensors, actuators, drives, controllers, robots, machines, and any other IACS devices that need to communicate in real-time (I/O communication). It represents Levels 0-2 of the Purdue model. Most importantly, Cell/Area Zone networks support the critical automation and control functions that keep the plant operating and producing quality products, including nomadic and mobile equipment.

The Cell/Area Zone map is shown in Figure 3.

Figure 3. Cell/Area Zone Map



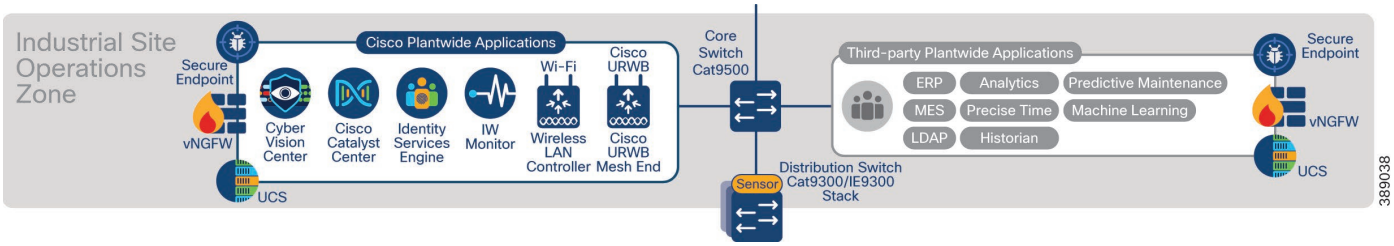
Fundamentally, the Cell/Area Zone is a Layer 2, access network; a subnet, a broadcast domain, a VLAN and/or an SSID. Programmable logic controllers (PLCs) communicate with their assigned sensors, actuators, and other IACS devices within a Cell/Area Zone. The solution outlines key design considerations and recommended implementations for these networks, both wired (Ethernet) and wireless (Wi-Fi and Cisco Ultra-Reliable Wireless Backhaul, URWB). The solution covers topics such as IACS traffic flows, topology, resiliency, industrial protocol support, multicast management, VLANs and trunking, IP addressing considerations, quality of service (QoS), time synchronization, visibility, security and segmentation, among many others. Often, Cell/Area Zone networks and equipment are deployed and managed by the operational (OT) organization.

Most importantly, the solution identifies how to seamlessly integrate these networks into a larger plant network design. This is critical to provide access to the rich data and information found in the IACS devices while maintaining their core operational requirements.

Industrial Zone

Along with the Cell/Area Zones, the Industrial Zone incorporates all the key applications and functions that support a production facility. The Industrial Zone supports site-wide applications and services required to maintain operational integrity of the production environment, including manufacturing execution systems, asset managers, historians, and SCADA systems, along with technical services such as time services, network management, security and identity services (for example, AAA), and wireless LAN control, among many others. To preserve smooth plant operations and functioning of the Cell/Area Zone IACS applications and the overall plant network, and in alignment with standards such as IEC 62443, the IDMZ provides clear, logical segmentation and protection from levels 4 and 5, or the enterprise and external networks, users, and applications. The Industrial Zone map is shown in Figure 4.

Figure 4. Industrial Zone Map



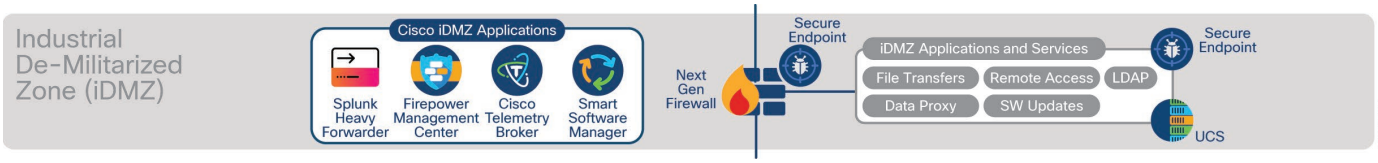
Besides supporting the site-wide applications, the Industrial Zone network also provides interconnectivity from these applications to the IDMZ, as well as between Cell/Area Zones for inter-zone traffic. Whereas the Cell/Area Zone can be thought of as Layer 2 access networks, the Industrial Zone network supports Layer 3 routing and includes distribution and core network infrastructure. Additionally, it supports access networks for site-wide applications that operate on plant micro-data center servers.

For many customers, the Industrial Zone network also represents the IT and OT demarcation of responsibility, where IT operates the data center servers and applications and the core/distribution network infrastructure. As the distribution network infrastructure straddles the two zones, Industrial and Cell/Area, deployment and management of this part of the network requires close collaboration between IT and OT. For example, resilient distribution network infrastructure and configuration is important for the site-wide applications as well as the IACS systems in the Cell/Area Zone. Therefore, distribution infrastructure is part of both Cell/Area and Industrial Zone design and implementation guidance to help ensure successful IT and OT collaboration.

Industrial Demilitarized Zone

Although not part of Purdue reference model, the industrial automation solution includes an IDMZ between the industrial and enterprise zones. The IDMZ is deployed within plant environments to separate the enterprise networks and the operational domain of the plant environment. Downtime in the IACS network can be costly and have a severe impact on revenue, so the operational zone cannot be impacted by any outside influences. The IDMZ helps ensure that. Network access is not permitted directly between the enterprise and the plant; however, data and services are required to be shared between the zones, thus the IDMZ provides architecture for the secure transport of data between the industrial and enterprise/cloud. The Industrial Demilitarized Zone map is shown in Figure 5.

Figure 5. Industrial Demilitarized Zone map



The main function of the IDMZ is to provide firewall-based segmentation and protection for the Industrial Zone. The firewall tightly controls and inspects the flow of data, files, and user access between the zones. In addition to the firewall, the IDMZ supports services such as file transfers, software upgrades, remote access servers, and proxied data services, such as the Cisco Telemetry Broker and the Splunk Heavy Forwarder. Due to the focus on cybersecurity and firewalls, the IDMZ is typically deployed and managed by IT (versus OT).

Capabilities required for industrial automation

Industrial applications at their core are focused on maintaining stability, continuity, and integrity of industrial processes. At the core is a loop of sensors, controllers, and actuators that must be maintained to safely operate the industrial automation and control processes. Additionally, several other applications need to gather information to display status, maintain history, and optimize the industrial process operations. These systems are often deployed by OT system integrators without the support of the IT organization and operated by OT personnel that lack IT capabilities and expertise. This solution outlines how to achieve a set of key requirements to support the installation and operations of the industrial systems.

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.

Industrial network topologies are often constrained by the layout of the facility and equipment and high cost of cabling. Therefore, the solution supports use of ring and redundant star network topologies that ensure network connectivity is maintained even if a key connection is lost. Additionally, considerations are also made for non-resilient topologies such as linear or star for customers choosing to forego this capability.

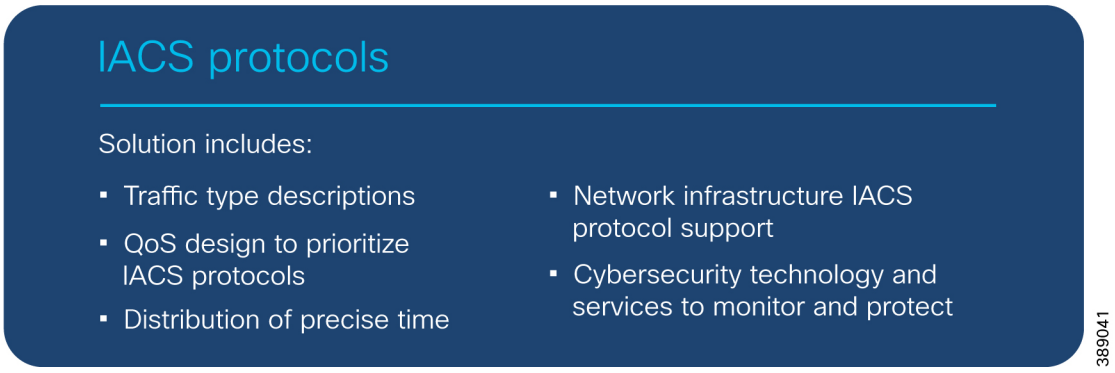
Network resiliency protocols are needed to take advantage of the redundant paths in the network topologies. The solution supports several protocols and outlines their capabilities as well as deployment challenges to help customers choose the right topology and resiliency protocol for their industrial applications. The list of protocols includes Spanning Tree Protocol (STP), Resilient Ethernet Protocol (REP), Media Redundancy Protocol (MRP), Parallel Redundancy Protocol (PRP), High-availability Seamless Redundancy (HSR), and EtherChannel.

A key consideration is redundancy at critical networking functions to decrease the impact of network equipment failure. The solution considers “stacking” of networking equipment as well as the Hot-Standby Resiliency Protocol to maintain routing capabilities.

In any industrial environment, equipment failures, including to the network infrastructure, must be dealt with quickly to reduce the amount of downtime. Fast replacement of failed network infrastructure is supported using replaceable flash-memory in the network infrastructure as well as via automated network management applications.

Support for a wide variety of industrial automation and control protocols

The IACS protocols used support the critical communications required to keep the plant operational. These protocols include the ODVA, Inc. Common Industrial Protocol (CIP™) and EtherNet/IP™, PROFINET®, Modbus® TCP, CC-Link™, and OPC UA™, among others. The solution specifically focuses on supporting these protocols.



The support starts with detailed descriptions of the typical traffic flows including characteristics such as latency, jitter, and sensitivity to loss. This background is especially important for IT networking experts to understand the nature of the solution guidance and recommendations. For example, often these protocols use a mix of unicast, multicast, and broadcast traffic, all of which need to be reflected in network configuration. Therefore, the solution outlines how to deploy QoS in the network to prioritize critical traffic while also supporting other less-sensitive traffic.

In addition, more and more IACS systems require distribution of precise time. Precise time is used for sensitive applications, such as high-speed motion, but also for schedule-of-events to precisely track the order and timing of events in the system. As more applications consume precise time, sitewide distribution becomes important to maintain a single, synchronized sense of time across all the devices and systems.

Another key consideration is how the network infrastructure integrates into the IACS it supports. Therefore, much of the network infrastructure supports IACS protocols for monitoring and management purposes. The solution provides design and implementation guidance for these features.

Lastly, cybersecurity infrastructure and technology that understands, monitors, and protects IACS devices and communication is critical. This technology can analyze the IACS protocols in-line (in other words, without having to build an expensive out-of-band collection network to mirror the traffic to a central security platform) and thereby monitors for threats and anomalies as well as protects the systems. This is a significant enhancement of the cybersecurity stance for production environments.

Scalability

Production environments vary in size drastically, from small deployments (tens to hundreds of IACS devices) to very large deployments (thousands to tens of thousands of IACS devices) and the solution is designed to accommodate that variability. The solution reference architecture with Cell/Area Zones interconnected to distribution and core is the classic model for a scalable, repeatable network design. Key IA solution features include:

- Cell/Area Zones with support for Layer 2 VLANs to scale production environments and meet IACS application requirements
- Distribution and core network infrastructure supporting Layer 3 to interconnect Cell/Area Zones with each other and the Manufacturing Zone
- Support for plant-wide applications (for example, SCADA, historian, and MES) and network and security services (for example, DHCP, DNS, timing, and security)

Easy to configure, implement, and manage

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. The solution identifies and uses a number of key features and concepts to assist both IT and OT in this critical activity. Key IA solution features include:

- Templates and macros to ease configuration of network infrastructure with critical concepts such as segmentation (for example, VLANs and ACLs), QoS, and multicast management, among others
- Support plug-n-play for network infrastructure for easy and fast repair and installation
- Support for both IT and OT access to network management tools to give all relevant personnel access to tailored network monitoring and management features.

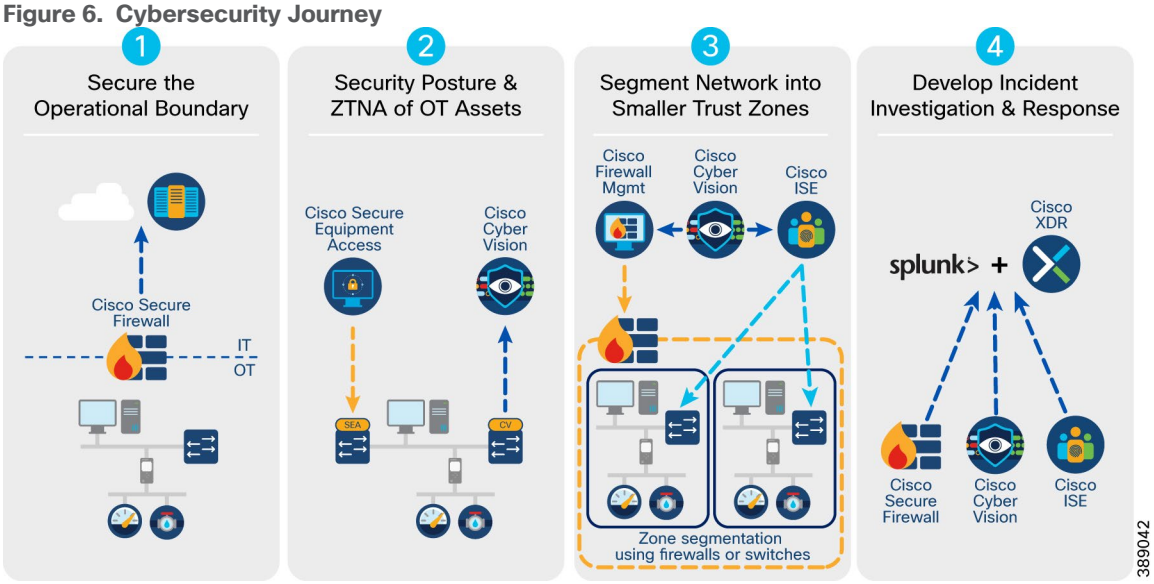
For more information on deploying network management, see the Cisco Catalyst Center for Industrial Automation Solution Brief.

Cybersecurity

Over the years, manufacturers around the world have been connecting their industrial environments to enterprise networks to automate production and gain operational advantages. Organizations are now deploying IoT technologies to migrate to Industry 4.0, optimize production, and build new generations of products and services. This deeper integration between IT, cloud, and industrial networks requires cybersecurity capabilities that can protect the production environment and assets and maintain operations.

This solution represents the leading cybersecurity approach for production environments, encompassing a defense-in-depth model driven by the leading cybersecurity and networking technology provider conjoined with operational and IT expertise. Cybersecurity in industrial as well as enterprise areas relies upon solid process as much as on key technology. The IA solutions focus on helping customers through a key cybersecurity journey shown in Figure 6 to establish secure production systems and assets and integrate into enterprise cybersecurity operations, for example, incident detection and response.

Figure 6. Cybersecurity Journey



To support the cybersecurity journey, the solution starts with the reference architecture that describes critical segmentation concepts such as the IDMZ to secure the production boundary.

Rugged, access network infrastructure (switches and wireless access points) with industry leading cybersecurity capabilities is the foundation for further securing the industrial network. The access network is where IACS devices connect, and initial cybersecurity considerations are applied. The access network with Industrial Cybersecurity sensors identifies what is connected, understands the communication flows and the security posture of the connected devices and systems. This information is shared with Network Access Control applications designed to deploy macro- and micro-segmentation in the network (for example, VLANs and TrustSec) to protect the IACS devices. The connection processes (for example, DHCP for IP addresses) are secured and the IACS devices communicate with other allowed devices. This communication and its content are monitored. The network infrastructure can also act as a secure remote access gateway to allow Zero-Trust Network Access (ZTNA) to industrial devices and applications via the isco Secure Equipment Access (SEA). Cisco SEA and SEA-Plus services enable operations teams and their partners to easily connect to remote assets or machines for configuration, monitoring and troubleshooting. Key cybersecurity features in the network infrastructure include:

- Secure boot, secure memory, secure access (for example, TACACS AAA services) summarized as Cisco TrustAnchor, and secure software update features to protect the network infrastructure and ensure integrity of the hardware and software
- IEC 62443-4-1 and 4-2 industrial cybersecurity certifications for Cisco Industrial Ethernet (IE) 3x000 and 9300 switches
- Support for secure network access by end devices via IEEE 802.1x and MAC authentication bypass
- Support for protection of key network-based services and protocols, for example DHCP, DNS, resiliency protocols, LLDP, SNMP, and so on
- Support for advanced cybersecurity protocols such as access control lists (ACLs), NetFlow, TrustSec and MACsec
- Support for Cisco Cyber Vision OT-focused cybersecurity sensors (Cisco IE3400 and IE9300, Cisco Catalyst 9x00, Cisco IC3000 Industrial Compute Gateway, Cisco IR1101 Integrated Services Router, and Cisco Catalyst 9300)

- Support for Cisco Secure Equipment Access, SEA and SEA-Plus (Cisco IE3100, IE3300, IE3400 and IE9300, Cisco IC3000 Industrial Compute Gateway and Cisco IR1101 Integrated Services Router)

ISA/IEC 62443 recommends that systems be separated into groups called “zones” that will be able to communicate with each other through communication channels called “conduits,” whether they are physical, electronic, or process-based. Cell/area zones offer organizations a starting point for segmentation of the control network. The main goal for segmentation is to minimize the impact of any potential breach and can be applied with industrial switches or firewalls.

- Cisco Identity Services Engine (ISE) uses Cisco TrustSec technology to logically segment control system networks. Cisco TrustSec classification and policy enforcement functions are embedded into Cisco switching, routing, wireless LAN, and firewall products.
- Cisco Secure Firewalls can be deployed in both physical and virtual form factors. Cisco Secure Firewall provides full stateful traffic inspection including a range of IACS protocols.
- Regardless of the segmentation technology, Cisco Cyber Vision provides the first step of ‘virtually segmenting’ the network into the zones and conduits model and shares this context with both Cisco ISE and the Cisco Firewall Management Center (FMC) to turn visibility into enforcement.

The solution outlines key design and implementation of cybersecurity applications that play critical roles for both the IT and OT organizations to monitor and maintain the security of IACS and plant-wide applications. These include:

- Cisco Cyber Vision analyses application flows on the industrial network to build a detailed asset inventory and communication map. This helps security teams spot vulnerabilities to patch, identify malware and intrusions, and list all the assets to defend. Because Cisco Cyber Vision decodes IACS protocols, it gives OT engineers real-time insights on the actual industrial process status and raise alarms on unexpected process modifications such as variable changes or controller modifications.
- Cisco Secure Network Analytics uses NetFlow telemetry data from the network to provide visibility into communication flows and has many machine learning algorithms that can help an IT security professional detect possible malware propagation in the network. Cisco Secure Network Analytics does not have the specific IACS protocol analysis and support found in Cisco Cyber Vision.
- Cisco Identity Services Engine (ISE) is a network access controller (NAC) dedicated to creating and enforcing network security policies. It enables software-based device-level segmentation to manage network access control at scale. The solution describes design and deployment for industrial networks.

Network and security telemetry data are also collected and sent to various network and cybersecurity applications. Cyber vision and the industrial network infrastructure integrates with Security Operations (SecOps) by passing security events and information about OT assets to XDR and Splunk for Security Incident and Event management processes.

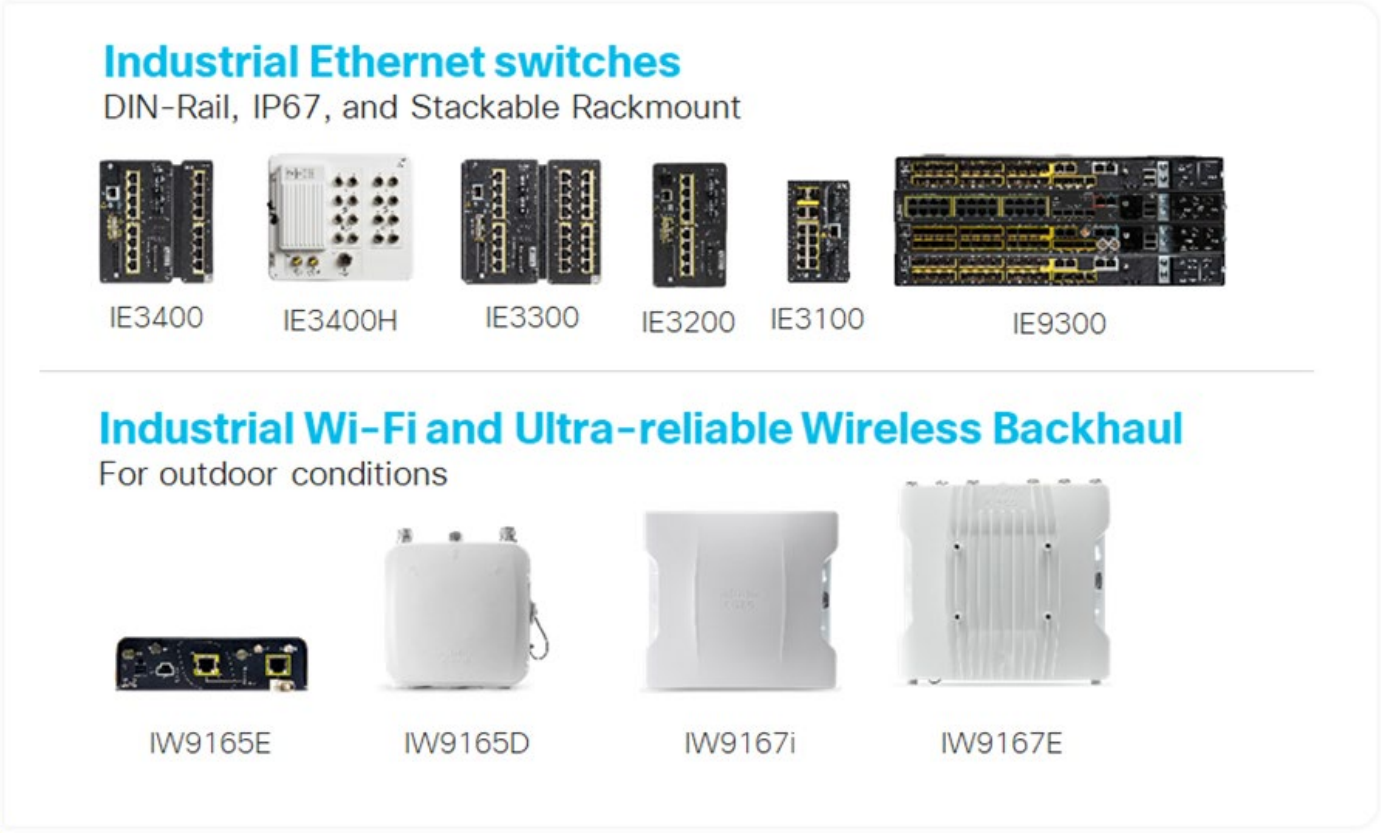
For more on our Industrial Cybersecurity design and implementation recommendations, see:

- Industrial Security Solution Overview,
- Industrial Automation Security Design Guide and
- Secure Remote Access for Industrial Networks

Ruggedization

The IACS end devices and network infrastructure may be in physically disparate locations and in non-controlled or even harsh environmental conditions such as extreme temperature, humidity, vibration, noise, explosiveness, or electronic interference. The solution relies upon Cisco Industrial Ethernet switches, firewalls, and edge computing designed to operate in these rugged conditions. All the Cisco equipment runs the operating system and software based on the commercial grade versions making them easier to deploy and manage for IT organizations. Ruggedized equipment is shown in Figure 7.

Figure 7. Industrial Ethernet Switches/Industrial Wi-Fi and Ultra-Reliable Wireless Backhaul



The solution not only includes a range of ruggedized equipment, but also includes guidance and recommendations for considerations such as connectivity (for example, cabling guidance).

Summary

The Cisco Industrial Automation solution and relevant product technologies are an essential foundation to securely connect and digitize industrial and production environments to achieve significantly improved business operation outcomes. The Cisco solution overcomes top customer barriers to digitization and Industry 4.0 including security concerns, inflexible legacy networks, and complexity. The solution provides a proven and validated blueprint for connecting 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**.

Printed in USA C78-xxxxxx-xx 08/24