Integrating CC-Link IE IACS into the Connected Factory Architecture

A Cisco Reference Design

First Published: April 2017

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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

Integrating CC-Link IE IACS into the Connected Factory Architecture

Executive Summary

A traditional factory network is composed of multiple siloed networks operated and maintained by different teams with different requirements, which drives up cost and complexity. Cisco Connected Factory provides a converged, factory-wide, secure network with fully integrated WiFi and Mitsubishi Electric's automation controllers. This document gives an overview of how Cisco's industrial networking products can help integrate existing plant floor networks with demanding industrial applications, such as the CC-Link Industrial Ethernet (CC-Link IE). CC-Link IE is supported on many of the Industrial Automation and Control System (IACS) devices in Mitsubishi Electric's vast portfolio. The CC-Link IE protocol evolved from the widely used CC-Link protocol, which provides general distributed control, synchronous motion control, and safety control together with comprehensive diagnostics functions and high communications integrity, thereby realizing higher reliability on an integrated Ethernet-based network.

Using a converged network architecture based on the industry-standard Purdue Model for Control Hierarchy, Cisco addresses connectivity, security, and resiliency based on a layered approach. Cisco's industrial Ethernet (IE) switches provide plant-floor level access to IACS devices running CC-Link IE, while Wireless Access Points (WAPs) and Wireless LAN Controllers (WLCs) provide mobile connectivity for other devices where a hardwired connection is not feasible or required. Multiple levels of redundancy are implemented using multiple physical links and aggregation switches, as well as protocols like Media Redundancy Protocol (MRP) designed especially for use in CC-Link IE networks. Security is also critical for industrial networks because a malicious or accidental change to an industrial device can cause considerable damage or downtime. The Cisco Identity Services Engine (ISE) and Cisco Adaptive Security Appliance (ASA) provide great flexibility and granularity to restrict network access based on a variety of criteria.

The document guides the reader through the high-level technology and architecture and includes:

- Architecture Overview, page 2—Describes the product portfolios from Cisco and CC-Link IE networked products from Mitsubishi Electric and how they fit together to form a converged CC-Link IE-based industrial network.
- Wired Access in Cell/Area Zone, page 11—Discusses the use of MRP within wired CC-Link IE networks for maximum resiliency.
- Wireless Access in the Cell/Area Zone, page 13—Discusses the options available for deploying Cisco wireless within CC-Link IE industrial environments and some key considerations and best practices.
- Security Overview, page 15—Discusses key considerations for using Cisco technology to secure CC-Link IE industrial networks based on device and user attributes.
- Hardware and Software Matrix, page 17—Provides a summary of recommended hardware models and software versions.
- References, page 17 are included for additional information.

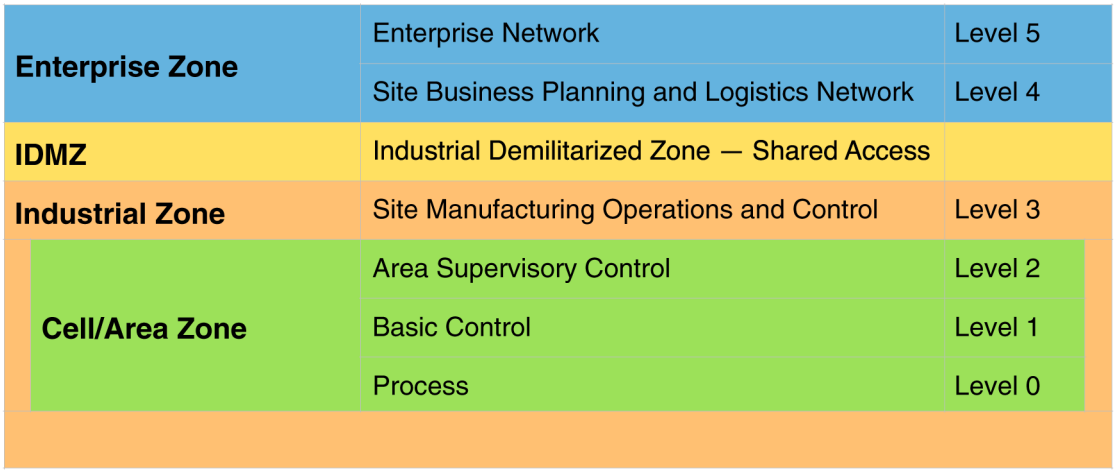
Architecture Overview

The Cisco Connected Factory architecture is designed from the ground up to leverage Cisco's industry-leading networking expertise and extend it to the factory floor, where industrial machines, controls, and other devices require maximum resiliency, extremely low latency, compliance with industry standards, and ease of use for operations personnel. The architecture converges the plant-floor network with the existing enterprise network, while layers of security protect mission critical data and machinery. This section outlines how Cisco's converged network portfolio works together with Mitsubishi Electric's industrial control devices that utilize CC-Link IE.

Purdue Model for Control Hierarchy

The Cisco Connected Factory solution employs the commonly used industry-standard Purdue Model for Control Hierarchy to divide the plant into a logical framework, as shown in Figure 1.

Figure 1 Purdue Model for Control Hierarchy



Starting at the bottom of the model, the Cell/Area Zone contains three levels of equipment:

- Level 0 - Process—Industrial sensors, drives, actuators, and similar devices that interact with the physical environment by taking measurements or performing actions like starting a motor or moving a robot arm.
- Level 1 - Basic Control—Controllers, such as programmable logic controllers, distributed control system, and generically programmable automation controller, that communicate directly with the Level 0 devices, other controllers, and higher level control systems.
- Level 2 - Area Supervisory Control—Operator interfaces including Human Machine Interface (HMI), alarm systems, and control room workstations.

The Industrial Zone contains (Level 0-3) systems that maintain site level control of the lower level IACS systems and include reporting, scheduling, file and patch servers, and network services such as NTP, DNS, DHCP, AD, etc. One or more of the Cell/Area Zones (described above) actually reside within the Industrial Zone, as depicted in Figure 1.

Sitting between the Industrial and Enterprise Zones is the Industrial Demilitarized Zone (IDMZ) which provides a layer of separation between the traditional Information Technology (IT) and Operational Technology (OT) operated areas of the network, allowing only the absolutely required traffic to traverse the zone.

The Enterprise Zone, containing Level 4 and Level 5, provides access to the Internet and higher-order network applications including email, database, Business-to-Business (B2B) and Business-to-Consumer (B2C) applications, and other non-critical resources. This area is often seen as a source of security threats to the lower level resources and is typically managed by the IT department.

Cisco Industrial Network Portfolio

Cisco's portfolio of network equipment includes ruggedized hardware designed to operate in the harsh environments present in manufacturing, transportation, utility, mining, and other demanding industries. Specially designed switches, routers, firewalls, etc. provide the connectivity, resiliency, and ease-of-use required in today's converged industrial networks, all while meeting strict industry standards for operating in less than ideal environments. Support for various industrial protocols, Power over Ethernet (PoE), zero-touch deployment, etc. provide a targeted solution for common OT requirements. This section provides a brief overview of several products in Cisco's Internet of Things (IoT) portfolio, many of which are featured in the solution described in this document.

Cisco Industrial Ethernet Switches

Cisco IE switches include:

- Cisco IE 1000 Series Switches—Very compact, fixed, lightly-managed switching platform available in various models providing up to 10 Ethernet interfaces including GE fiber uplinks options and multiple PoE/PoE+ ports.
- Cisco IE 2000 Series Switches—Compact, fixed switching platform available in two form factors: DIN rail mounting and wall or pole mounting qualified for Ingress Protection 67 (Cisco IE 2000 IP67 model). The Cisco IE 2000 models offer up to 16 10/100Base-T (Fast Ethernet) interfaces and two Gigabit Ethernet interfaces. The Cisco IE 2000 IP67 model supports up to 24 Ethernet interfaces. The Cisco IE 2000U is designed for specific electrical utility applications.
- Cisco IE 3000 Series Switches—Multilayer switching modular platform that includes a main module and expansion modules so you can scale the configuration up to 26 Ethernet interfaces. A fixed 19-inch, one- rack unit model is also available, the Cisco IE 3010 Series Switches.
- Cisco 2500 Series Connected Grid Switches—A series of 19-inch, one-rack unit fixed-configuration switches designed for electrical utility applications.
- Cisco IE 4000 Series Switches—The industry's first DIN rail-mounted 40 Gigabit Ethernet switch platform that offers high bandwidth and low latency. The Cisco IE 4000 is available in various models with up to 20 Gigabit Ethernet interfaces.
- Cisco IE 4010 Series Switches—19-inch, one-rack unit switches with 28 GE interfaces and up to 24 PoE/PoE+ enabled ports.
- Cisco IE 5000 Series Switches—A 19-inch, one-rack unit multi-10 Gbps aggregation switch equipped with 24 Gigabit Ethernet ports plus four 10-Gigabit or four 1-Gigabit ports, making it ideal for the aggregation layer or backbone in large-scale industrial networks.

One key feature of the Cisco IE 2000, Cisco IE 4000, and Cisco IE 5000 switches is support for Media Redundancy Protocol. This provides extremely quick reconvergence times in the event that a link or switch fails. This feature is discussed in detail in Wired Access in Cell/Area Zone, page 11.

Cisco Wireless

Cisco offers a wide range of Wireless Access Points (WAPs) to meet the demanding requirements of enterprise and industrial deployments. Within the Connected Factory solution, there are a wide variety of available WAPs which include support for up to the latest 802.11ac wireless standards, as well as various internal and external antenna options to meet the tough requirements for industrial environments, all while providing high speed and reliable connectivity. The WAPs typically rely on a single cable to a Cisco switch that provides both data and power (PoE) over a single Ethernet cable.

In addition to WAPs, Cisco's Unified Wireless portfolio includes the Cisco Wireless LAN Controller (WLC), available in multiple form factors depending on scalability requirements. Cisco's WLCs provide centralized control, management, and troubleshooting. The Cisco WLC is able to provide RF management to improve signal quality by proactively identifying potential interference, thereby improving wireless performance. Depending on which Cisco WLC is chosen, the system can scale to thousands of access points and tens of thousands of clients.

Wireless Access in the Cell/Area Zone, page 13 provides a detailed look at how wireless is used in the solution and some technical considerations that are valuable to know when planning a converged industrial and enterprise network.

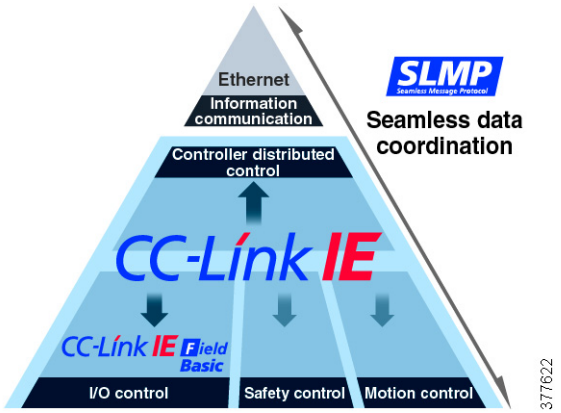
Cisco Identity Services Engine

Cisco's Identity Services Engine (ISE) plays a key role in securing the converged plant and enterprise network. Cisco ISE is a powerful software application that gathers detailed information about the devices and users that are trying to access the network, whether it be through a wired, wireless, or Virtual Private Network (VPN) connection. With this information, Cisco ISE can apply custom policies to allow or deny access to any network resources based on any criteria. For example, Cisco ISE can communicate with Microsoft Active Directory (AD) to authenticate users that are trying to connect to specific switches in the network. Based on their AD group membership, dynamic access control lists can be programmed on the switch to restrict access to only the necessary network resources. Additional sample use cases are covered later in this document to further describe the versatility and flexibility that the Cisco ISE can provide.

CC-Link IE Protocol Introduction

CC-Link IE leverages connectivity between the plant floor and IT systems with both horizontal and vertical integration between networked devices. Extensive visualization with advanced data connectivity is realized by deterministic data collection incorporating SeamLess Message Protocol (SLMP), which enables seamless connectivity and a high-speed 1 Gbps communications network. The network incorporates general distributed control, synchronous motion control, and safety control in one network. The topology is versatile which enables flexibility in system configuration. In addition, comprehensive diagnostic functions can yield higher reliability and enhanced communication integrity, thereby minimizing disruptions to the IACS.

Figure 2 CC-Link IE Reference Model



- Extensive visualization with advanced data connectivity.

  Big Data analytics require deterministic data collection, which can be realized by incorporating two key features:

  - SLMP enables seamless connectivity between devices in the IT layer and on the shop floor.
  - A high-speed, large-capacity 1 Gbps communications network that enables the handling of large data, such as production, quality, and control data between different production processes.

- General, motion, and safety control integrated into one network.

CC-Link IE incorporates generic distributed control, synchronous motion control, and safety control enabling secure communications across multiple safety devices, all on the same network. The topology is quite versatile, based on twisted-pair cables, which enables flexibility in system configuration while helping to keep installation cost low.

- Comprehensive diagnosis yields higher reliability.

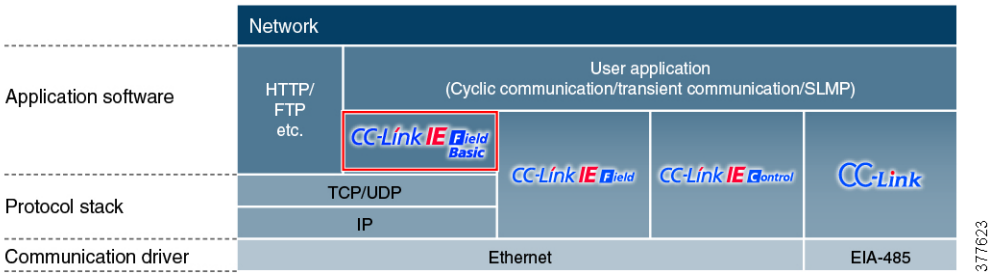
  Disruptions to the control system are kept to a minimum through:

  - Comprehensive diagnostics functions
  - High communications integrity owing to the noise-resistant characteristics of the optical cable
  - Communication re-routing capabilities made possible with a ring topology

  In addition, network errors can be rectified quickly by visualizing the network system image using the engineering software and remotely from a HMI such as a GOT (Graphic Operation Terminal) directly on the machine or production line.

CC-Link IE Field Network Basic, which is part of CC-Link IE, is a software-based protocol (not requiring ASIC) operating on a standard Ethernet protocol stack that can be used together with TCP/IP communications. This allows CC-Link IE Field Network Basic compatible products and Ethernet compatible products to be connected on the same Ethernet communications line, enabling a highly-flexible and low-cost system.

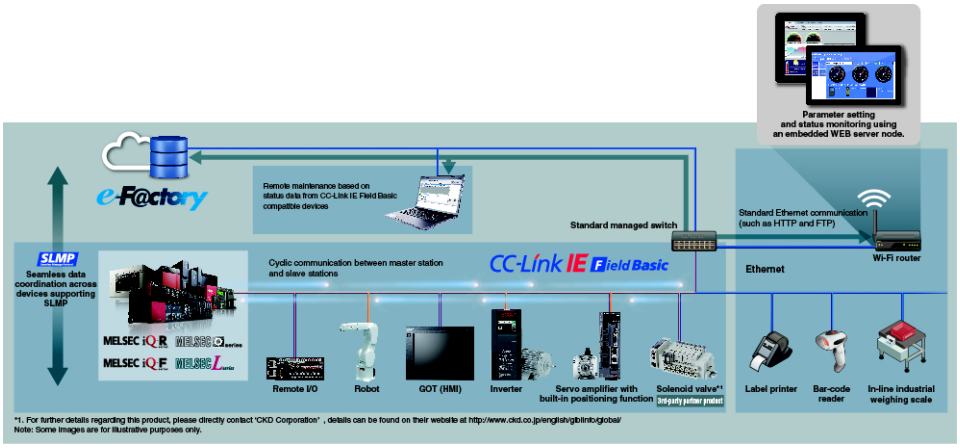
Figure 3 CC-Link IE Communication Profile



CC-Link IE communications are realized using general-purpose Ethernet technology which is highly scalable for compact control systems that do not require ultra high-speed control performance while realizing simpler implementation.

- Cyclic communications realized on the software protocol stack realizes simpler system implementation for network-compatible devices
- Simultaneous communications with standard Ethernet TCP/IP (HTTP, FTP, etc.) reduces wiring as communications can be done on the same network topology
- Easy realization of network master on an IPC (Industrial PC) or personal computer without requiring a dedicated interface board

Figure 4 CC-Link IE Field Basic System Overview



377624

SLMP is a simple client-server common protocol that enables communication between Ethernet products and CC-Link IE-compatible products regardless of network hierarchy. SLMP can be implemented on a network hierarchy, such as TCP/IP and CC-Link IE, with only software development required for TCP/IP devices (no additional hardware modifications are required), which enables communications between Ethernet- and CC-Link IE-compatible products. SLMP supports seamless communication across multiple network layers, which enables the setting of parameters and maintenance from a computer, for example.

Mitsubishi Electric CC-Link IE Portfolio

The Mitsubishi ELectric SEquence Control (MELSEC) brand is well known in the automation industry for robust quality and excellent performance that realizes a reduction in total cost of ownership (TCO). The MELSEC lineup consists of various products, the flagship products being the MELSEC-Q Series and MELSEC iQ-R Series. These high-end programmable controllers, mainly used for controlling processes in manufacturing lines and advanced machines, are complimented by small- to medium-sized controllers like the MELSEC-L Series and the MELSEC iQ-F Series, which are commonly utilized for cell manufacturing and stand-alone applications. The MELSEC Series controllers include network modules that enable connection to various different networks, such as CC-Link IE, depending on the module used. All MELSEC controllers are standardly equipped with an Ethernet communications port which enables connection to a CC-Link IE Field Basic network.

Cisco and Mitsubishi Electric Integrated Industrial Network

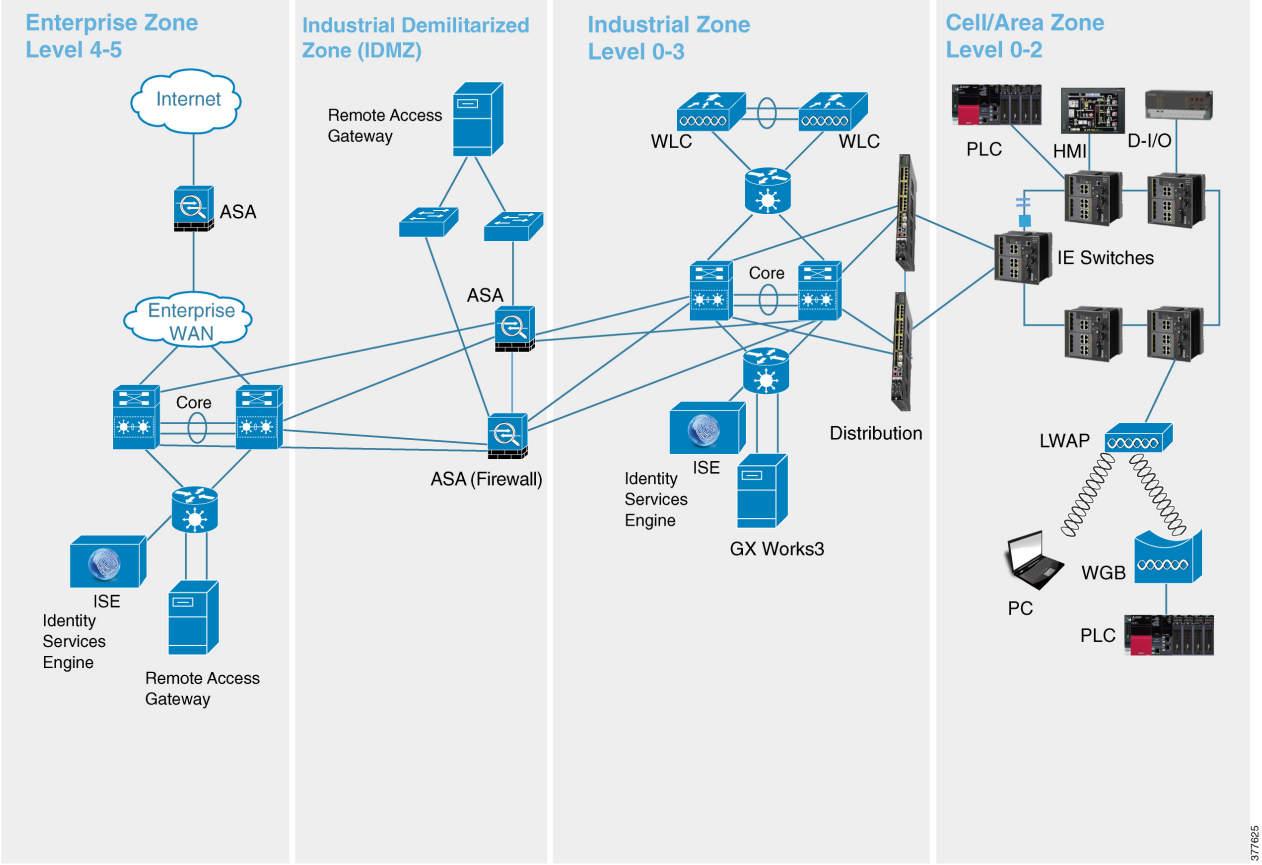
At a high level, the Connected Factory network looks similar to a traditional enterprise campus network which uses a layered design to provide low latency, high resilience, high throughput, and secure connectivity to wired and wireless clients. However, some aspects of the Connected Factory network diverge from the typical enterprise-only campus network due to the physical requirements of an industrial setting, as well as the specific characteristics and protocols used by the connected devices. The network is divided into several layers:

- Access—The access layer provides Layer 2 (in the OSI model) connectivity to end devices, such as computers, industrial controllers, sensors, etc. This physical connectivity can be wired (with copper- or fiber-based Ethernet) or wireless (IEEE 802.11 WiFi). The network infrastructure physically comprises Cisco IE switches (2000, 3000, 4000) and WAPs. The access layer of the network architecture roughly maps to Levels 0-1 of the Purdue Model.
- Distribution—The distribution layer aggregates all of the access layer switches and acts as the Layer 3 (OSI model) boundary, providing a highly-redundant, high throughput connection to the rest of the network. The network infrastructure at this layer typically includes more powerful switches, including the Cisco IE 5000 and Cisco Catalyst series switches (3800, 4500, 6800). The distribution layer of the network architecture roughly maps to Levels 2-3 of the Purdue Model. Sitting between the distribution and core layers is the IDMZ, which separates and secures the industrial network from the enterprise.

- Core—The core layer is the backbone of the network. This layer is often combined with the distribution layer functions in smaller networks and provides routing, load balancing, and interconnections to other networks, as well as the IDMZ. The network infrastructure at this layer is made up of Cisco's enterprise switching portfolio including the Catalyst 4500 and 6800 series. The core layer of the network architecture roughly maps to Levels 4–5 of the Purdue Model.

As shown in Figure 5, the Cell/Area Zone is at the access layer of the network. In an industrial environment it is typical to use a ring topology to connect a series of access switches together due to the physical layout of the plant floor. A ring topology allows every point in the ring to have multiple potential paths out of the ring, which is critical in case there is a cable or device failure. If a failure in the ring occurs, the network must be able to detect the problem and start forwarding traffic around the failure as quickly as possible (this is called reconvergence). In a CC-Link IE deployment, Cisco's IE switches use the MRP protocol to intelligently and rapidly reconverge after a failure significantly faster than Spanning Tree deployments that are often used in standard enterprise campus networks. MRP is discussed in detail in Wired Access in Cell/Area Zone, page 11.

Figure 5 Connected Factory Architecture



In addition to wired connectivity directly to an access switch, wireless is becoming an increasingly appealing access method for devices where a wired connection is not feasible. Cisco's wireless solutions consist of two main pieces. Wireless Access Points (WAPs) are the physical radios that form the edge of the wireless network. The WAPs can be deployed as root WAPs that can serve multiple wireless clients connecting simultaneously or they can be used as a workgroup bridge to provide a wireless connection to a wired network behind the WAP. Cisco WAPs can also be configured in two different basic architectures, autonomous and unified. When Cisco WAPs are operating autonomously, their configuration and operation is managed locally on the WAP with no centralized management application. In a Unified model, the Cisco WAPs connect back to a central Wireless LAN Controller (WLC) that is responsible for configuration, firmware management, and potentially switching traffic. Within the Unified model, there are two main options:

- Local mode—All management and control traffic, as well as all data traffic to and from the WAP is encapsulated in Control and Provisioning of Wireless Access Points (CAPWAP) protocol packets and processed by the WLC.
- Flexconnect local switching mode—All management and control traffic is still encapsulated in CAPWAP packets and processed by the WLC, but all data traffic is able to be locally switched out of the WAP Ethernet interface and does not need to be processed by the WLC.

It is recommended to deploy the Cisco wireless solution in a Unified model with Flexconect enabled in order to reap the maximum benefits. Wireless Access in the Cell/Area Zone, page 13 discusses in detail the options and recommendations for Cisco wireless.

Cisco's proven history of securing enterprise networks applies directly to newly converged industrial networks. As mentioned previously, Cisco ISE sits at the center of the security story, providing device and user level authentication and authorization. Highly customizable policies are used to restrict access to network resources based on a wide variety of criteria and dynamically push security policies (in the form of dynamic access control lists) to the edge of the network. Cisco's popular ASA firewall also provides high performance network segmentation to restrict communication between the enterprise and plant floor to only essential services and applications, as well as providing a secure, encrypted means of remote access for workers as required. Both wired and wireless clients are authenticated with 802.1X and ISE and WPA2 ensures wireless connections are encrypted and secured.

Realize Improved Communications Performance

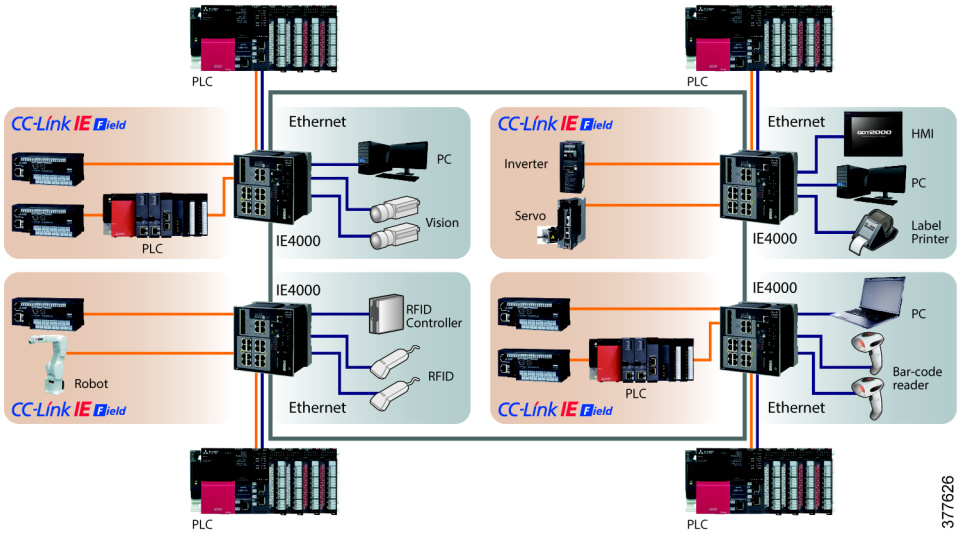
When configuring an IACS which includes a mixture of CC-Link IE Field and standard Ethernet devices, it is usually necessary to separate the network cable topology between these two architectures. In addition, if a communications fault develops between Ethernet switches, communications will stop on the network at this point.

Alternatively, by combining with the Cisco IE 4000 Ethernet switch it is possible to integrate CC-Link IE and standard Ethernet devices utilizing the same communications line, which reduces cabling. In addition, this network architecture is robust during network failures because if a fault develops between switches, the failure is detected and rerouted, improving network reliability.

Integration of Network and Redundancy

Figure 6 highlights the integration of CC-Link IE Field network and Ethernet by VLAN using Cisco IE 4000 Series switches. System communication between factory automation products and Ethernet-compatible devices is realized across the same Ethernet communication line, reducing overall cable installation costs. System integrity is also enhanced by utilizing MRP technology between Ethernet switches, which ensures the communication of system operating and information data when a failure occurs, improving productivity and quality.

Figure 6 System Example Showing Integration of CC-Link IE Field Network and Ethernet Across VLAN



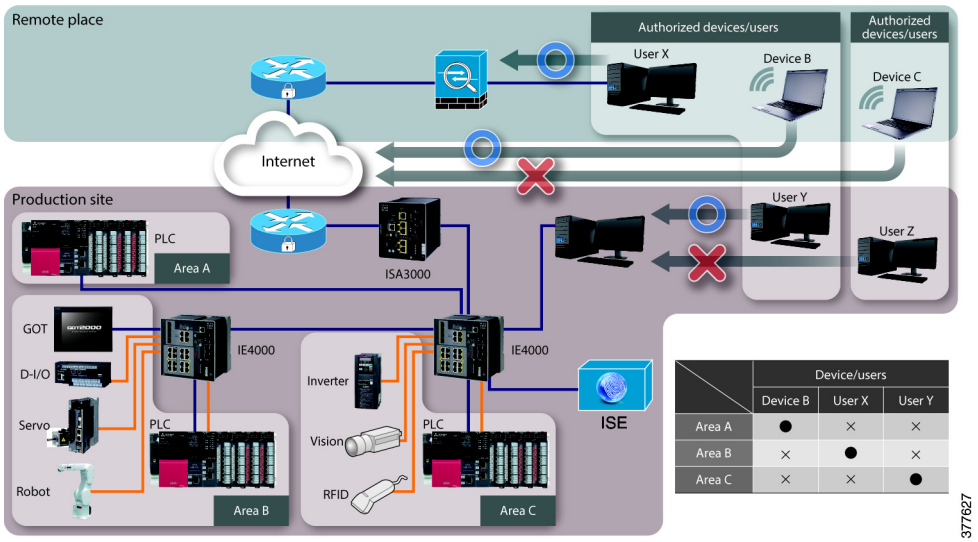
Robust Security Across the Plant Floor

As technology becomes more complex and the distribution of manufacturing systems more global and interconnected to the Internet, it is imperative to protect intellectual property and prevent unauthorized access into the control network. With manufacturing information being held directly in programmable automation controllers and HMI, security must be enhanced.

This enhancement can be realized by utilizing enhanced security features in Cisco network products in two key areas, hardware and user authentication. Hardware security is enhanced by MAC address blocking, preventing unauthorized access to the control system. User security is enhanced by implanting user authentication by multi-level login ID.

Figure 7 highlights how security can be implemented across the plant floor. In this example, authorization of devices can be done using either MAC address blocking or by user authentication through login ID and password. MAC address blocking, which is more robust compared to IP address blocking, enables only registered MAC addresses to gain access and cannot be modified as the addresses are set at the hardware. User IDs can be registered, preventing unauthorized users from gaining access when multiple personnel use the same computer. Information-level access can also be set, ensuring that relevant information is shared only with authorized personnel.

Figure 7 System Example Showing How Security is Implemented Across the Plant Floor



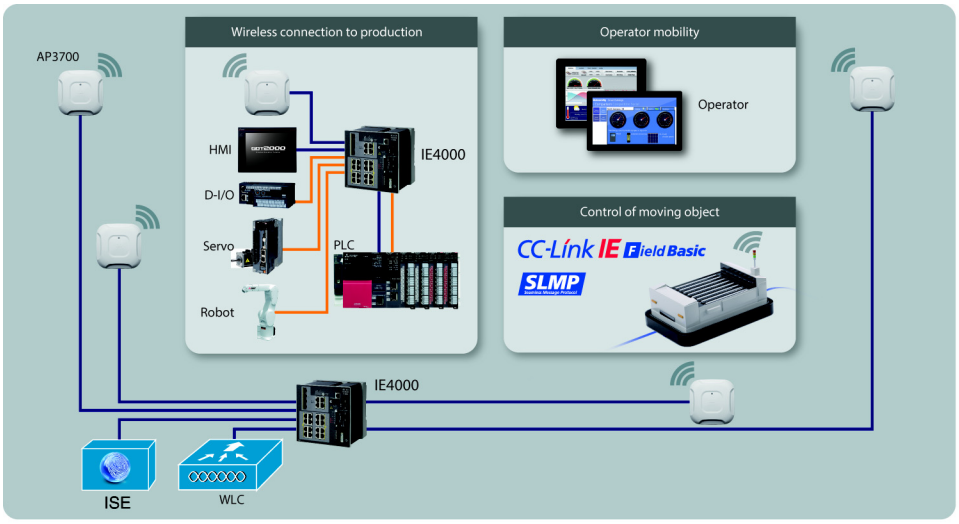
Implement Reliable Wireless Communications

Modern manufacturing is experiencing an increase in the use of wireless communications mainly driven by the need to reduce physical network cabling on the plant floor and the increasing use of mobile information terminals such as tablets for maintenance activities. In addition, mobile production devices such as automated guided vehicles (AGV) require wireless communications as they move further from the main control system. However, you must consider various factors when implementing wireless communications in manufacturing, such as robust shielding of equipment that may cause interference to the propagated radio waves by correctly arranging wireless LAN access points.

Utilizing Cisco's wireless LAN technology with CC-Link IE, it is possible to monitor network level integrity and the operating health of access points to quickly diagnose network problems. You can quickly implement the wireless network through the simplified configuration of WLAN access points. Security can also be maintained as it utilizes security features similar to the hard-wired communications network.

Figure 8 highlights the implementation of wireless technology across the plant floor. Wireless technology can be useful when the installation of physical cables can be costly or due to technology restrictions of the application, such as an automated guided vehicle that moves across the plant. Implementing wireless technology can result in more flexible layout designs and can improve maintenance by enabling factory personnel to use tablet devices.

Figure 8 System Example Showing Implementation of Wireless Network



Wired Access in Cell/Area Zone

Functional Description

The cell/area zone contains all of the plant floor industrial equipment including access switches typically deployed in a ring or star topology. At this level of the Purdue model, resiliency and low latency communication are of paramount importance. The Cisco and Mitsubishi Electric connected factory solution cell/area zone utilizes the Media Redundancy Protocol (MRP) and Mitsubishi Electric's CC-Link IE. MRP defined within the International Electro technical Commission (IEC) 62439-2 standard provides fast convergence in a ring network topology for industrial automation networks. Media Redundancy Manager (MRM) defines its maximum recovery times for a ring in the followings range: 10ms, 30ms, 200ms, and 500ms, which are supported in the Cisco IE 2000, Cisco IE 4000, Cisco IE 5000 series. This solution is based on validation conducted on the Cisco IE 4000 only. The default maximum recovery time on the Cisco IE switches is 200ms for a ring composed of up to 50 nodes.

As illustrated in Figure 9, MRP ring enables rings of compliant Cisco IE switches to overcome a single segment failure with recovery times much faster than traditional Spanning-tree Protocol (STP) methods. Typical network convergence time of STP is 30ms with seven switch nodes and RSTP is 2s with seven nodes, while MRP can achieve 10-500ms with 50 nodes.

Within each MRP ring, there are two types of nodes: (Figure 10)

- Media Redundancy Manager (MRM) nodes:
  - Serve as the ring manager and initiate and control the ring topology to react to network faults.
  - Default state (Ring-Close state): One of the MRM ports is in a blocked state and the other ports in a forwarding state.
  - During network failure (also called Ring-Open state), MRM changes both its ports into a forwarding state.
- Media Redundancy Client (MRC) nodes:
  - Serve as member nodes of the ring, react to receive reconfiguration frames from the MRM, and detect and signal link changes on its ring ports.

- All MRC ports are in a default forwarding state (Ring-Close state).
- During network failure (also called Ring-Open state), MRC adjacent to the failure will be in a disabled/forwarded state and the other MRC will have both ports in a forwarding state.

Figure 9 Mitsubishi Electric CC-Link IE with Cisco MRP Ring

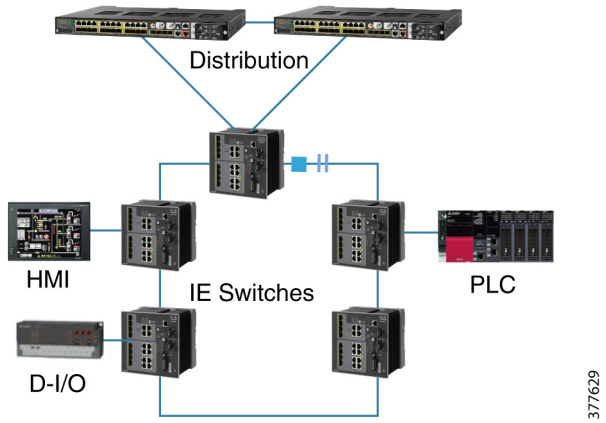
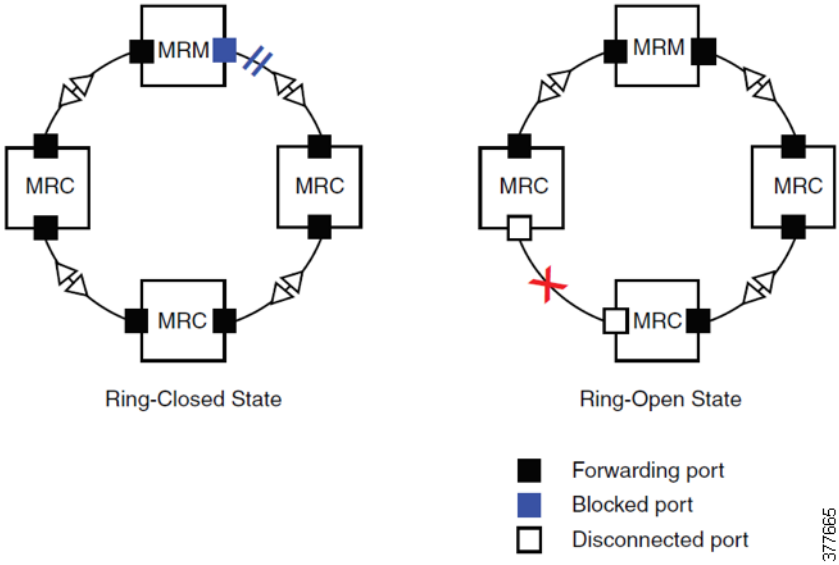


Figure 10 Media Redundancy Protocol Ring States



Mitsubishi Electric's CC-Link IE incorporates generic distributed control, I/O control, safety control, and synchronous motion control all in the same network. CC-Link IE, as shown in Figure 2, is a high speed, high bandwidth Ethernet-based open network which can use SLMP to integrate from device level to controller level. Figure 5 shows a typical Connected Factory solution which incorporates Cisco IE switches using the MRP protocol as the ring's state-aware protocol to satisfy the tight time constraint requirements for industrial network applications at the manufacturing plant floor.

Technical Considerations

The Cell/Area Zone is the primary region of the plant where Industrial Automation activities are performed; it is important to consider this zone as an isolated entity of the manufacturing environment. Network availability and performance are the most important considerations when designing an Industrial Automation network which supports the Cell/Area Zone.

The MELSEC iQ-R Series Ethernet module (RJ71EN71) is equipped with two ports that can be used as either a general Ethernet, CC-Link IE Field, or Control network module, providing flexibility when designing the network system as the module can be easily switched between networks.

The MRP protocol is a standard-based protocol. In order to use MRP with CC-Link IE, we need to first enable MRP CLI mode. The switch supports one MRP ring (one VLAN) with the mrp-manager license and up to three MRP rings in the same VLAN with the mrp-multi-manager license. Support for multiple MRP rings is available only through the CLI or Web Device Manager tool, not in Profinet mode. Cisco IE switches support 50 MRCs per ring. MRP cannot run on the same interface (port) as Resilience Ethernet Protocol (REP), Spanning Tree Protocol (STP), Flex Links, or Dot1X. STP does not run on MRP segments and MRP interfaces drop all STP BPDUs.

A recovery time profile, composed of various parameters, drives the MRP topology convergence performance. The 200 ms profile supports a maximum recovery time of 200 ms. The 500 ms profile supports a maximum recovery time of 500 ms. The default maximum recovery time on the Cisco IE switch is 200 ms for a ring composed of up to 50 nodes. You can configure the switches to use the 500 ms recovery time profile according to the size of ring.

Note: The 10ms and 50ms profile can also be supported on this platform.

Wireless Access in the Cell/Area Zone

Functional Description

An Industrial Wireless Local Area Network (WLAN) introduced into an industrial plant can provide many advantages including:

- A network topology that reduces cabling and hardware, which results in lower installation and operational costs
- Simplified connectivity to inaccessible areas, such as restricted and remote sites
- Productivity gains from increased employee and equipment mobility

WLAN for plant floor cell/area zone machine WiFi communications has two different architectures:

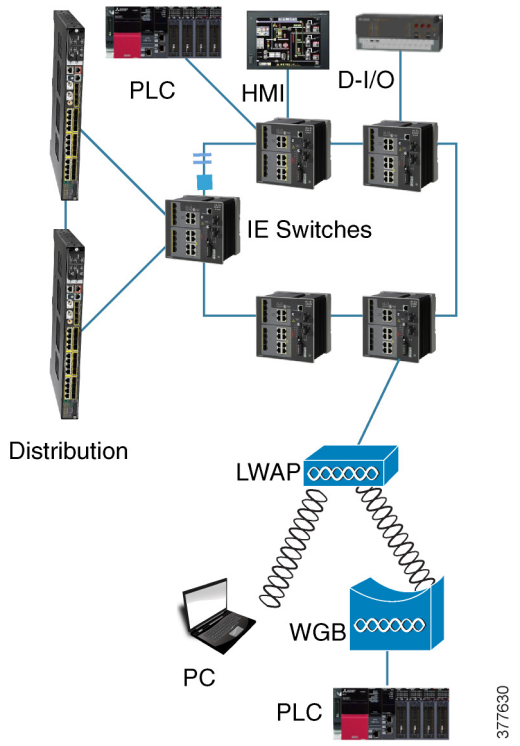
- Autonomous (Stand-alone) Access WLAN, whose benefits include:
  - Lower initial hardware cost and less technical expertise
  - Simplified setup
- Unified (Centralized) Access WLAN, whose benefits include:
  - Lower operational expenses
  - Dynamic and adaptive RF capabilities
  - Self-healing topology
  - Enhanced security
  - Support for plant-wide mobility

Unified WLAN architecture is compatible with both CC-Link IE Field network Basic and SLMP as they are based on standard Ethernet. The MELSEC iQ-R Series programmable CPU is standardly equipped with a CC-Link IE Field Network Basic communications port for communicating with the network. In addition, by using SLMP, communications are possible to other networked programmable controllers (MELSEC iQ-R Series, MELSEC-Q Series, and MELSEC-L Series) Ethernet ports.

These controllers can attach to Cisco wireless WGB as WGB's wired clients. MELSEC models can connect to Cisco IE switches on two separate ports with different VLANs, which requires WGB to enable the Downstream Broadcast on Multiple VLANS feature. Cisco Wireless Release 8.3 provides an enhancement to broadcast traffic support on multiple 802.1Q VLAN WGB deployments that traverse mesh networks in local mode; specifically, support for WGB downstream broadcasts over multiple VLANs (to differentiate and prioritize traffic) and bridging VLAN traffic to wired clients connected to the WGB. Applications for Cisco Wireless Release 8.3 are commonly found in the transportation and mining industries.

Figure 11 shows a typical Mitsubishi Electric CC-Link IE integrating with Cisco WLAN scenario, with Cisco Light Weighted Access Point (LWAP) and WGB attached to a Layer 2 MRP ring. Because a MRP ring is by default enabled on the trunk interface between interconnect switch links, it can seamlessly integrate with Mitsubishi Electric's CC-Link IE controllers for its operation. Unified WLAN wireless controller (WLC) is located outside of the cell/area zone for whole plant WLAN and LWAP management.

Figure 11 Mitsubishi Electric CC-Link IE with Cisco WLAN



Technical Considerations

Unified WLAN has local mode and flexconnect mode:

- Local mode—Most common default mode for LWAP creates two CAPWAP tunnels to WLC, one for management and the other for data traffic. Data traffic stops forwarding once it loses WLC connectivity.

- Flexconnect mode—Allow data traffic to be switched locally and not return to the WLC. Data traffic can be still forwarded locally and it does not always require a connection to the WLC.

The WLC flexconnect WAP authentication mechanism has different methods:

- Central authentication—Authentication through a central WLC
- Local authentication—Authentication through the WAP itself

The WLC flexconnect WAP switching mechanism can be central switching or local switching:

- Central switching—Data traffic forwarded through a CAPWAP tunnel to central WLC
- Local switching—Data traffic terminates locally at the WAP connected switch port

To satisfy industrial plant continuous operation requirements, it is recommended to use central authentication and local switching mechanism with flexconnect mode. Flexconnect mode VLAN mapping to local MRP ring VLAN is also required if LWAP directly-connected switchport is configured in trunk mode.

The Unified WLAN wireless RF spectrum allocation for channels, data rate, and transmit power is quite important for industrial plant controllers behind WAPs. The following are the general design considerations:

- Use only the 5 GHz frequency band for critical CC-Link IE applications such as I/O, peer-to-peer, and safety control.
- Use the 2.4 GHz band, if necessary, for personnel access and low throughput non-critical applications on the plant floor.
- Avoid using Dynamic Frequency Selection (DFS) channels in the 5 GHz band (channels 52-144) for CC-Link IE applications because of potential radar interference.

Refer to the local regulatory authority, product documentation, and the Cisco website for well-defined wireless deployment best practices in addition to those described above.

Unified WLAN utilizes a platinum QoS profile to satisfy the stringent industrial plant performance requirements for delay and jitter.

Security Overview

Functional Description

Figure 5 shows a plant-wide security infrastructure for Mitsubishi Electric/Cisco integration. Industrial plant security mechanisms include:

- Holistic defense-in-depth security—Cisco recommends a defense-in-depth approach to securing any network, including industrial networks. Defense-in-depth refers to not only utilizing traditional security mechanisms like firewalls, but also broadly monitoring the entire network to look for indicators of compromise. Cisco's extensive security product portfolio can not only attempt to block attacks at the network perimeter, but also look deep into the network to identify and eliminate attacks as they happen. When designing a secure network, one approach is to consider a model that addresses attacks on a continuum of before, during, and after. In each area of the continuum there are important measures to take to ensure that most attacks are prevented before they are started and any that do make it through the perimeter are quickly and properly identify and eliminated, all while recording critical details that can be used for analysis to prevent future incidents. While many details of this defense-in-depth strategy are beyond the scope of this document, Cisco.com contains a wealth of resources to describe the architecture, products, and features and how they work together.

- Identity Services Engine (ISE)—As described in Architecture Overview, page 2, the Cisco Identity Services Engine plays a critical role in the broader security of the industrial network. Cisco Identity Services Engine provides device and user level security policy enforcement functionality. Areas of the network or specific network resources can be protected by dynamic access control lists pushed down by the Identity Services Engine based on any number of criteria when, for example, a user attempts to login with a user name and password or a specific device type is plugged into a port on a switch. Strictly limiting network access in a flexible, dynamic manner provides maximum security for all resources connected to the network.
- Industrial Demilitarized Zone (IDMZ)—The industrial demilitarized zone acts as a kind of intermediate buffer zone between the enterprise and industrial (plant floor) networks. The industrial demilitarized zone includes several mechanisms to strictly limit the types of data flowing between the enterprise and industrial networks. Various proxy and gateway services reside in the industrial demilitarized zone that are used to broker IACS traffic between the networks such that it cannot flow directly between the networks. The industrial demilitarized zone also segments access to IACS network resources into sub-zones so that they can be accesses when required by IT or operations personnel or potentially trusted partners. The industrial demilitarized zone also contains Remote Desktop gateway services for secured access to industrial network resources from outside the industrial network.

Technical Considerations

IP Device Tracking

IACS devices tracking uses IP Device Tracking (IPDT) technology to keep track of connected hosts (association of MAC and IP address) by using ARP probes intermittently. IPDT facilitates the detection of the presence of new hosts and is extremely useful when its IP/MAC database of CC-Link IE association is used to populate the source IP of dynamic Access Control lists (ACLs) or to maintain a binding of an IP to a security group tag.

By enabling IPDT on trunk port, all hosts connected to the neighboring switch over the trunk port will be tracked, which results in a large device tracking table. Operation on a large table, such as searching a host, consumes more CPU time. A large number of tracked hosts will increase the network traffic and degrade switch performance due to periodic ARP probes sent to track the hosts. In addition, ARP probes may actually be sent by a remote switch connected to the local switch via trunk ports. This may increase the chance of duplicate IP addresses.

In order to achieve the optimal performance for IPDT working with CC-Link IE association:

- Set the non-zero source IP addresses in ARP requests to eliminate duplicate IP addresses.
- Delay the ARP probes that are dependent on IP Device Tracking and are triggered by a link-up.
- Disable IP Device Tracking on trunk ports.

802.1x Authentication

Plant personnel are granted onsite wired and wireless access by using IEEE 802.1X authentication. Use the 2.4 GHz band for plant personnel and the 5 GHz band for Cisco and Mitsubishi Electric IACS devices.

When the network has an interruption or the network is designed to intentionally segregate enterprise and industrial assets, to give secure access to the existing clients, ISE recommends to have a Policy Service Node in the Industrial Zone. AD Domain Services (AD DS) should be installed in accordance with Microsoft best practices. The synchronization of Domain Control (DC) between the Enterprise Zone and the Industrial Zone should be two-way accessible. An AD administrator should be able to create, delete, and update accounts in the Enterprise Zone and replicate the changes to the Industry Zone and the reverse must also be supported.

Unified WLAN recommends EAP-TLS, which is adoptable by Cisco and Mitsubishi Electric IACS devices, to provide security network service. Unified WLAN setup for EAP-TLS requires multiple services, such as DHCP, DNS, and AD, to be configured in the configuration. The certificate for the EAP-TLS security should be installed after the WAPs are converted into WGB mode.

Hardware and Software Matrix

Table 1 and Table 2 list the hardware and software versions used to validate this solution and hence are recommended.

Table 1 Mitsubishi Electric Product Matrix

Role	Product	Software Version	Notes
Network Unit	RJ71EN71	13	MELSEC iQ-R
Base Unit	R3nB	-	MELSEC iQ-R
CPU Unit	RnCPU	23	MELSEC iQ-R
Power Supply Unit	R6nP	-	MELSEC iQ-R
CPU Unit	LnCPU	1808	MELSEC L
Power Supply Unit	L6nP	-	MELSEC L

Table 2 Cisco Product Matrix

Role	Product	Software Version	Notes
Access Switch	IE 4000	15.2(5)E	MRP ring clients
Access Points	C3700	15.3(3)JD	
Gateway Switch	IE 4000	15.2(5)E	MRP ring manager
	C3850a	03.03.05SE	
Wireless Controller	WLC	8.3	
Firewall	ASA 5550	9.1(6)	
ASA ASDM	ASA	7.3(1)101	ASA GUI client

References

- Media Redundancy Protocol Configuration Guide for IE 2000, IE 4000, and IE 5000 Switches
  http://www.cisco.com/c/en/us/td/docs/switches/connectedgrid/cg-switch-sw-master/software/configuration/guide/mrp/mrp_switch.html
- Industrial Ethernet Switches
  http://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/index.html#~tab-products
- Cisco Wireless Controller Configuration Guide, Release 8.3
  http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-3/config-guide/b_cg83.html
- MELSEC iQ-R Series
  http://www.mitsubishielectric.com/fa/products/cnt/plcr/pmerit/concept/index.html
- CC-Link Partner Association
  https://www.cc-link.org/en/index.html