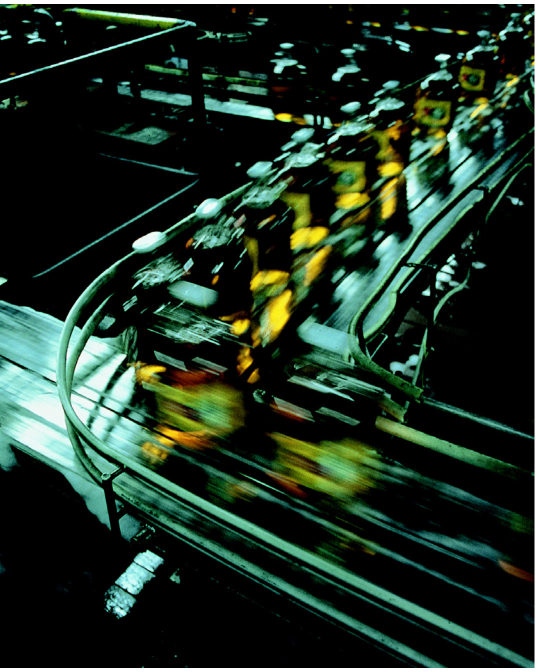


Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture

White Paper

May 2018

Rockwell Automation and Cisco Four Key Initiatives:

- Common Technology View:
  A single scalable architecture, using open EtherNet/IP™ standard networking technologies, is paramount to enable the Industrial Internet of Things for achieving the flexibility, visibility and efficiency required in a competitive manufacturing environment.
- Converged Plantwide Ethernet Architectures:
  Collection of tested and validated architectures developed by subject matter authorities at Cisco and Rockwell Automation. The content of CPwE is relevant to both Operational Technology (OT) and Information Technology (IT) disciplines and consists of documented architectures, best practices, guidance and configuration settings to help manufacturers with design and deployment of a scalable, robust, secure and future-ready plant-wide industrial network infrastructure.
- Joint Product Collaboration:
  Stratix® 5950 Industrial Firewall, Stratix 5100 Wireless Access Point/Workgroup Bridge, and Stratix 5700, Stratix 5400 and Stratix 5410 Industrial Ethernet Switches, incorporating the best of Cisco and the best of Rockwell Automation.
- People and Process Optimization:
  Education and services to facilitate Operational Technology (OT) and Information Technology (IT) convergence, assist with successful architecture deployment, and enable efficient operations that allow critical resources to focus on increasing innovation and productivity.

Document Reference Number: ENET-WP037C-EN-P

Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture

The prevailing trend in Industrial Automation and Control System (IACS) networking is the convergence of technology, specifically IACS operational technology (OT) with information technology (IT). Converged Plantwide Ethernet (CPwE) helps to enable IACS network technology convergence through the use of standard Ethernet, Internet Protocol (IP), network services, security services, and EtherNet/IP. A reliable and secure converged IACS network technology helps to enable the Industrial Internet of Things (IIoT).

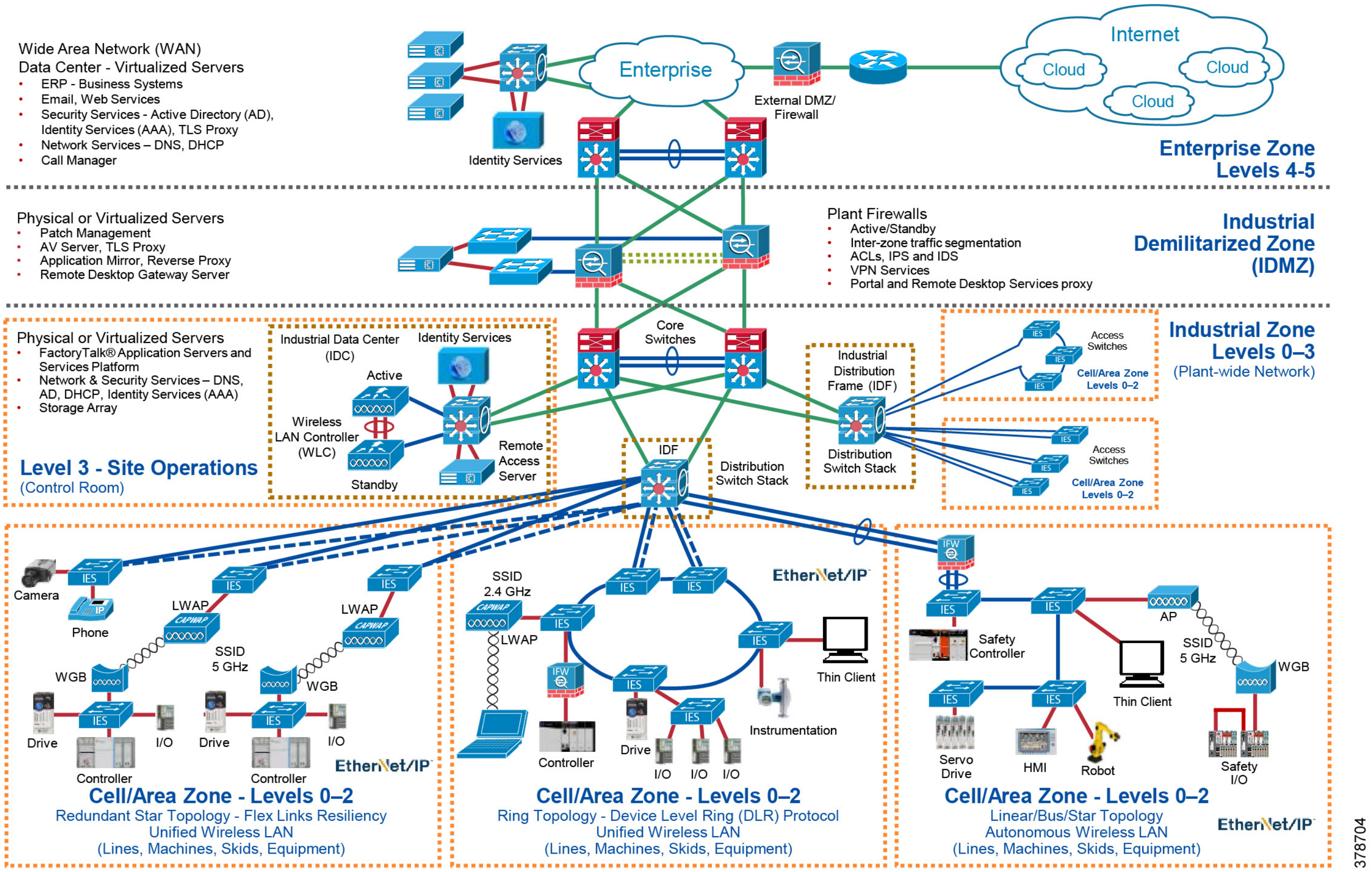
IIoT offers the promise of business benefits through the use of innovative technology such as mobility, collaboration, analytics, and cloud-based services. The challenge for manufacturers is to develop a balanced security stance to take advantage of IIoT innovation while maintaining the integrity of industrial security best practices. Business practices, corporate standards, security policies and procedures, application requirements, industry security standards, regulatory compliance, risk management policies, and overall tolerance to risk are all key factors in determining the appropriate security stance.

As access methods to the plant-wide industrial network expand, the complexity of managing network access security and controlling unknown risks continues to increase. With a growing demand for in-plant access by trusted industry partners (for example, system integrator, OEM, or vendor), IACS applications within the CPwE architecture (Figure 1) face continued security threats. A holistic industrial security stance is necessary in order to help protect the integrity of safety and security best practices while also helping to enable identity and mobility services. No single product, technology, or methodology can fully secure plant-wide architectures. Protecting IACS assets requires a holistic defense-in-depth security approach that addresses internal and external security threats. This approach uses multiple layers of defense (administrative, technical, and physical), using diverse technologies at separate IACS levels, by applying policies and procedures that address different types of threats. The CPwE Industrial Security Framework (Figure 2), which applies a holistic defense-in-depth approach, is aligned to industrial security standards such as IEC-62443 (formerly ISA99) Industrial Automation and Control Systems (IACS) Security and NIST 800-82 Industrial Control System (ICS) Security.

The management and security of the evolving coexistence of technologies within the plant require a different approach. CPwE uses the Cisco Identity Services Engine (ISE) to support centrally managed secure wired computer or wireless mobile device (computer, tablet, smartphone) access to the IACS networks by plant personnel and trusted partners.

This release of Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture CVD (Cisco Validated Design), which is documented the *Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide (DIG)*), outlines several security and mobility architecture use cases, with Cisco ISE, for designing and deploying mobile devices, with FactoryTalk® software applications throughout a plant-wide IACS network infrastructure. The CPwE Identity and Mobility Services CVD is brought to market through a strategic alliance between Cisco Systems and Rockwell Automation.

Figure 1 CPwE Architectures


Wide Area Network (WAN)
Data Center - Virtualized Servers
ERP - Business Systems
Email, Web Services
Security Services - Active Directory (AD), Identity Services (AAA), TLS Proxy
Network Services – DNS, DHCP
Call Manager
Identity Services
Enterprise
External DMZ/ Firewall
Internet
Cloud
Cloud
Cloud
Enterprise Zone
Levels 4-5
Physical or Virtualized Servers
Patch Management
AV Server, TLS Proxy
Application Mirror, Reverse Proxy
Remote Desktop Gateway Server
Plant Firewalls
Active/Standby
Inter-zone traffic segmentation
ACLs, IPS and IDS
VPN Services
Portal and Remote Desktop Services proxy
Industrial
Demilitarized Zone
(IDMZ)
Physical or Virtualized Servers
FactoryTalk® Application Servers and Services Platform
Network & Security Services – DNS, AD, DHCP, Identity Services (AAA)
Storage Array
Level 3 - Site Operations
(Control Room)
Industrial Data Center (IDC)
Identity Services
Active
Wireless LAN Controller (WLC)
Standby
Remote Access Server
Core Switches
IDF
Distribution Switch Stack
Industrial Distribution Frame (IDF)
Distribution Switch Stack
Access Switches
Cell/Area Zone Levels 0–2
Access Switches
Cell/Area Zone Levels 0–2
Industrial Zone
Levels 0–3
(Plant-wide Network)
IES
Camera
IP
Phone
LWAP
CAPWAP
SSID 5 GHz
LWAP
WGB
WGB
Drive
I/O
Drive
I/O
Controller
Controller
EtherNet/IP
Cell/Area Zone - Levels 0–2
Redundant Star Topology - Flex Links Resiliency
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
SSID 2.4 GHz
LWAP
EtherNet/IP
IFW
Thin Client
Instrumentation
Controller
Drive
I/O
I/O
I/O
Cell/Area Zone - Levels 0–2
Ring Topology - Device Level Ring (DLR) Protocol
Unified Wireless LAN
(Lines, Machines, Skids, Equipment)
Safety Controller
AP
SSID 5 GHz
WGB
Thin Client
Servo Drive
HMI
Robot
Safety I/O
Cell/Area Zone - Levels 0–2
Linear/Bus/Star Topology
Autonomous Wireless LAN
(Lines, Machines, Skids, Equipment)
EtherNet/IP
378704

Note This release of the CPwE architecture focuses on EtherNet/IP, which uses the ODVA Common Industrial Protocol (CIP™) and is ready for the Industrial Internet of Things (IIoT). For more information on EtherNet/IP, see odva.org at the following URL:
http://www.odva.org/Technology-Standards/EtherNet-IP/Overview

Secure Access Control

As the number of known and unknown mobile devices (computer, tablet, smartphone) connecting to the IACS network continues to increase, methods for managing disparate security solutions and mitigating risks continue to mature. Physical security is no longer adequate to prevent attempts to access an IACS network. With the continued proliferation of trusted partner mobile device connectivity and the already constrained plant-wide operational resources, the potential impact of failing to identify and remediate security threats introduces significant risk to plant-wide operations. Protecting IACS assets from mobile devices requires a centrally manageable defense-in-depth security approach. Cisco ISE supports different levels of secure wired and wireless access to the IACS networks by plant personnel and trusted partners.

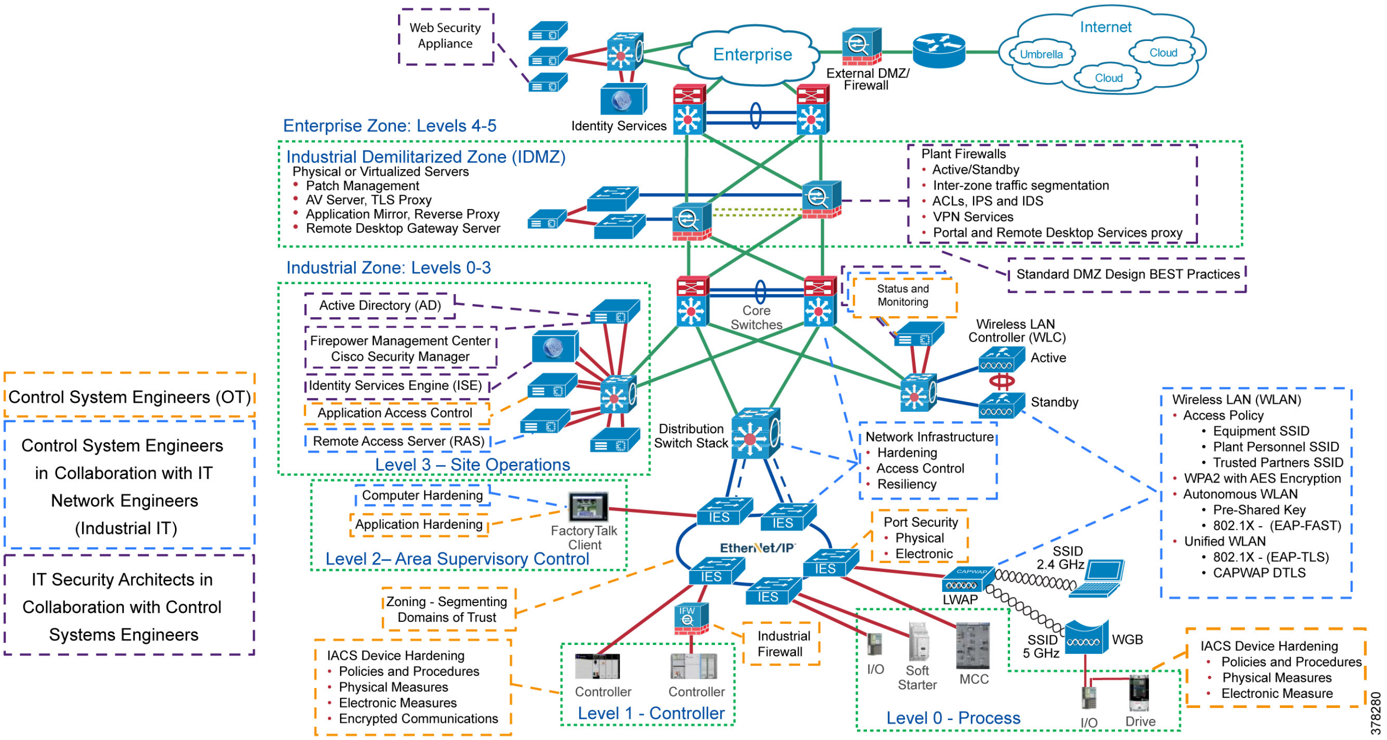
Designing and implementing a comprehensive IACS network access security framework (Figure 2) should be a natural extension to the IACS and not implemented as an afterthought. The industrial network access security framework should be pervasive and core to the IACS. However, atop existing IACS deployments, the same defense-in-depth layers can be applied incrementally to help improve the access security stance of the IACS.

One size does not fit all when it comes to risk tolerance. What's acceptable to one manufacturer may be unacceptable to another and vice versa. The CPwE architecture supports scalability, which includes the degree of holistic industrial security (Figure 2) applied to a plant-wide security architecture. Scalable security comes in many forms. Choices in multiple layers of diverse technology are available to apply at multiple levels of the IACS application based on risk mitigation requirements to help meet the manufacturer’s tolerance to risk.

CPwE holistic defense-in-depth layers (Figure 2) include:

- **Control System Engineers** (highlighted in tan)—IACS device hardening (for example, physical and electronic), infrastructure device hardening (for example, port security), network monitoring and change management, network segmentation (trust zoning), industrial firewalls (with inspection) at the IACS application edge, IACS application authentication, and authorization and accounting (AAA).
- **Control System Engineers in collaboration with IT Network Engineers** (highlighted in blue)—Computer hardening (OS patching, application white listing), network device hardening (for example, access control, resiliency), network monitoring and inspection, and wired and wireless LAN access policies.
- **IT Security Architects in collaboration with Control Systems Engineers** (highlighted in purple)—Identity and Mobility Services (wired and wireless), network monitoring with anomaly detection, Active Directory (AD), Remote Access Servers, plant firewalls, and Industrial Demilitarized Zone (IDMZ) design best practices.

Figure 2 CPwE Industrial Security Framework



Unified Network Access Policy Management for CPwE

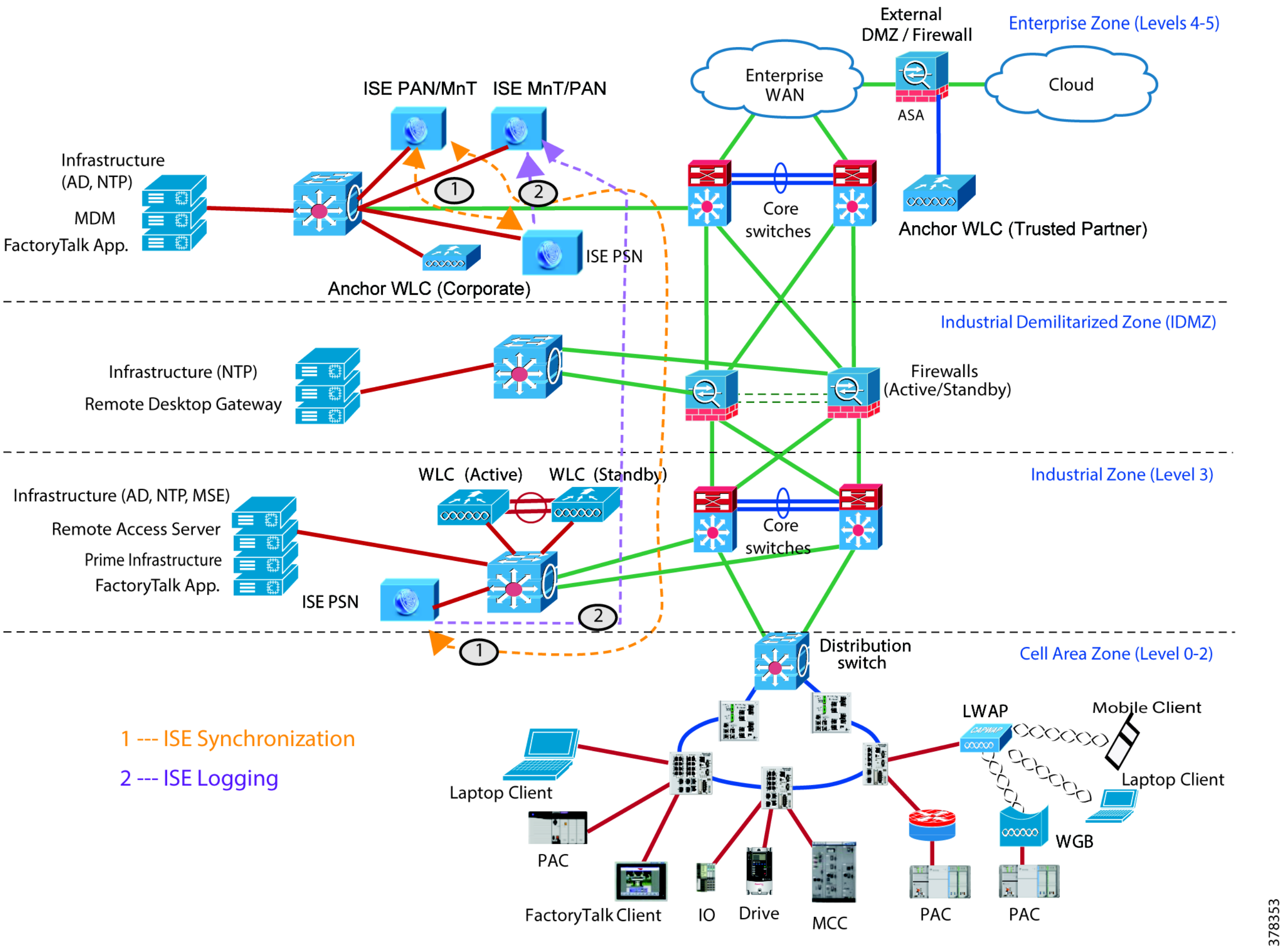
The Cisco Identity Services Engine empowers IT to help achieve highly secure wired and wireless access within the plant by providing:

- Comprehensive centralized policy management
- Streamlined device onboarding
- Dynamic enforcement
- Mobile device (computer, tablet, smartphone) posturing

A rules-based, attribute-driven policy model is provided to create access control based upon IEEE-802.1X authentication and authorization policies. Cisco ISE includes the ability to create fine-grained authorization policies that include the association of a user or a mobile device to an associated VLAN or an associated downloadable access control list (dACL). Attributes can also be created dynamically and saved for later use as new operations and management devices are introduced to the IACS network.

As shown in Figure 3, CPwE Identity and Mobility Services support multiple external identity repositories, including Active Directory for both authentication and authorization. Plant-wide network administrators may centrally configure and manage both wired and wireless access for employees, guests, vendors, and trusted partners, based upon authentication and authorization services available from a web-based GUI console. Cisco ISE simplifies administration by providing integrated central management from a single administrative interface for distributed network environments.

Figure 3 Unified Identity and Mobility Services for Wired and Wireless



Through the incorporation of Cisco ISE, provision and posture policies are applied across the IACS network in real time, so users experience consistent access to their services from wired and wireless connections. Cisco ISE allows IT to define roles such as employees and trusted partners. These roles can be configured to permit and limit access to assets within the Industrial Zone, the Industrial Demilitarized Zone (IDMZ) and the Enterprise Zone:

- Unknown mobile devices are directed to an administratively-defined safe destination, with no access to local resources within the plant-side operations.
- Trusted mobile devices are granted access to essential platforms within the Industrial Zone.

Such device-sensing capabilities are built into Allen-Bradley® Stratix and Cisco® industrial Ethernet switches (IES) for wired connections and Cisco wireless LAN controllers (WLC) for wireless connections. This allows for centralized network-wide profiling at the point of entry and without the costs and management of overlay appliances, stand-alone devices or infrastructure replacement.

CPwE Identity and Mobility Services CVD

An IACS is deployed in a wide variety of discrete and process manufacturing industries such as automotive, pharmaceuticals, consumer packaged goods, pulp and paper, oil and gas, and mining and energy. IACS applications are made up of multiple control and information disciplines such as continuous process, batch, discrete, and hybrid combinations. One of the challenges facing manufacturers and OEMs is the need to enable secure connectivity from mobile devices to plant-wide IACS applications in order to take advantage of the business benefits associated with the IIoT.

CPwE is the underlying architecture that provides standard network and security services for control and information disciplines, devices, and equipment found in modern IACS applications. Cisco ISE is used in conjunction with the CPwE architecture to provide an additional and dynamic layer of network access control security by identifying the mobile device, IACS application (FactoryTalk), and logged-on user to push security policies to the network infrastructure that the mobile device is accessing. The CPwE architecture (Figure 1), through testing and validation by Cisco and Rockwell Automation, provides design and implementation guidance, test results, and documented configuration settings that can help to achieve the real-time communication, reliability, scalability, security, and resiliency requirements of modern IACS applications for manufacturers and OEMs. Cisco ISE builds on top of the defined best practices and network architecture with a centrally managed architectural model where the IT department maintains the management of the Cisco ISE platform that operates in the Industrial Zone.

CPwE Identity and Mobility Services enables centralized plant-wide flexibility in deciding how to implement guest policies. Cisco ISE provides a self-service registration portal for plant personnel, vendors, partners, and guests to register and provision new devices automatically according to the business policies defined by the plant-wide operations. CPwE Identity and Mobility Services enables IT to establish automated plant-wide device provisioning and profiling while keeping the process simple for plant personnel to get their mobile devices onto the plant-wide network with limited IT help.

The following is a synopsis for this release of CPwE Identity and Mobility Services CVD:

- Identity Services Engine (ISE) Overview
- Unified and Autonomous Wireless LAN (WLAN) Architecture Overview
- Mobile Device Management (MDM) and Mobile Service Engine (MSE) Overview
- Mobile IACS Applications Overview
  - Tested and validated: FactoryTalk TeamONE™ software and ThinManager® software
  - Referenced: FactoryTalk View, FactoryTalk ViewPoint, FactoryTalk Batch View, FactoryTalk VantagePoint®, FactoryTalk Analytics for Devices software, Studio 5000® software
- Security and Mobility Architecture Use Case Overview
- Design and Implementation Considerations

Summary

CPwE is a collection of tested and validated architectures that are developed by subject matter authorities at Cisco and Rockwell Automation. The testing and validation follow the Cisco Validated Design (CVD) and Cisco Reference Design (CRD) methodologies.

The content of CPwE, which is relevant to both OT and IT disciplines, consists of documented architectures, best practices, guidance, and configuration settings to help manufacturers and OEMs design and deploy a scalable, reliable, secure, and future-ready plant-wide industrial network infrastructure. CPwE also helps manufacturers and OEMs achieve the benefits of minimizing costs using proven designs that can help lead to quicker deployment and reduced risk in deploying new technology. CPwE is brought to market through a strategic alliance between Cisco Systems and Rockwell Automation.

The *Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture DIG* outlines several security and mobility architecture use cases, with Cisco ISE, for designing and deploying mobile devices with FactoryTalk applications throughout a plant-wide IACS network infrastructure. The DIG highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific security and mobility architecture use cases within the framework of CPwE.

More information on CPwE Design and Implementation Guides can be found at the following URLs:

- Rockwell Automation site:
  http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page?
- Cisco site:
  http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

Cisco is the worldwide leader in networking that transforms how people connect, communicate and collaborate. Information about Cisco can be found at www.cisco.com. For ongoing news, please go to http://newsroom.cisco.com. Cisco equipment in Europe is supplied by Cisco Systems International BV, a wholly owned subsidiary of Cisco Systems, Inc.

www.cisco.com

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 www.cisco.com/go/offices.

Rockwell Automation is a leading provider of power, control and information solutions that enable customers to be more productive and the world more sustainable. In support of smart manufacturing concepts, Rockwell Automation helps customers maximize value and prepare for their future by building a Connected Enterprise.

www.rockwellautomation.com

Americas:
Rockwell Automation
1201 South Second Street
Milwaukee, WI 53204-2496 USA
Tel: (1) 414.382.2000
Fax: (1) 414.382.4444

Asia Pacific:
Rockwell Automation
Level 14, Core F, Cyberport 3
100 Cyberport Road, Hong Kong
Tel: (852) 2887 4788
Fax: (852) 2508 1846

Europe/Middle East/Africa:
Rockwell Automation
NV, Pegasus Park, De Kleetlaan 12a
1831 Diegem, Belgium
Tel: (32) 2 663 0600
Fax: (32) 2 663 0640

Publication ENET-WP037C-EN-P May 2018