



Cloud Connectivity to a Converged Plantwide Ethernet Architecture

White Paper

February 2020

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, Panduit, 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, reliable, safe, secure, and future-ready plant-wide industrial network infrastructure.
- **Joint Product Collaboration:**
Stratix® 5950 industrial firewall, FactoryTalk® Network Manager™ software, Stratix 5700, Stratix 5400, Stratix 5410, and Stratix 5800 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, which can assist with successful architecture deployment, and helps to enable efficient operations that allow critical resources to focus on increasing innovation and productivity.

Cloud Connectivity to 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 and security technology convergence, including OT-IT persona convergence, by using standard Ethernet, Internet Protocol (IP), network services, security services, and EtherNet/IP. A reliable and secure converged plant-wide or site-wide IACS architecture helps to enable the Industrial Internet of Things (IIoT)..

IIoT helps offer the promise of business benefits by using innovative technology such as mobility, collaboration, analytics and cloud-based services. The challenge for industrial operations 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.

Cloud-based services help to enable data collaboration and remote monitoring of dashboards by industrial operations and/or trusted industry partners (for example, system integrator, OEM or IACS vendor) for IACS applications within the CPwE architecture (Figure 1). A holistic industrial security stance is necessary to help protect the integrity of safety and security best practices while also helping to enable restricted cloud-based 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), utilizing diverse technologies for threat detection and prevention, implemented by different personas, and applied at separate levels of the IACS architecture.

Defense-in-depth applies policies and procedures that address many different types of threats. The CPwE Industrial Security Framework (Figure 2), using a 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) Cybersecurity Framework (CSF).

The *Cloud Connectivity to a Converged Plantwide Ethernet Architecture* Design Guide outlines several security architecture use cases for designing and deploying restricted end-to-end outbound connectivity with FactoryTalk applications from within industrial operations to the Rockwell Automation cloud within a CPwE architecture (Figure1).

**Note**

The *Cloud Connectivity to a Converged Plantwide Ethernet Architecture* Design Guide helps with meeting the following IEC-62443 3-3 Functional Requirements:

FR3 SR 3.2 RE1: Malicious code protection on entry and exit points

FR5 SR 5.2: Zone boundary protection

FR5 SR 5.3 General purpose person-to-person communication restrictions

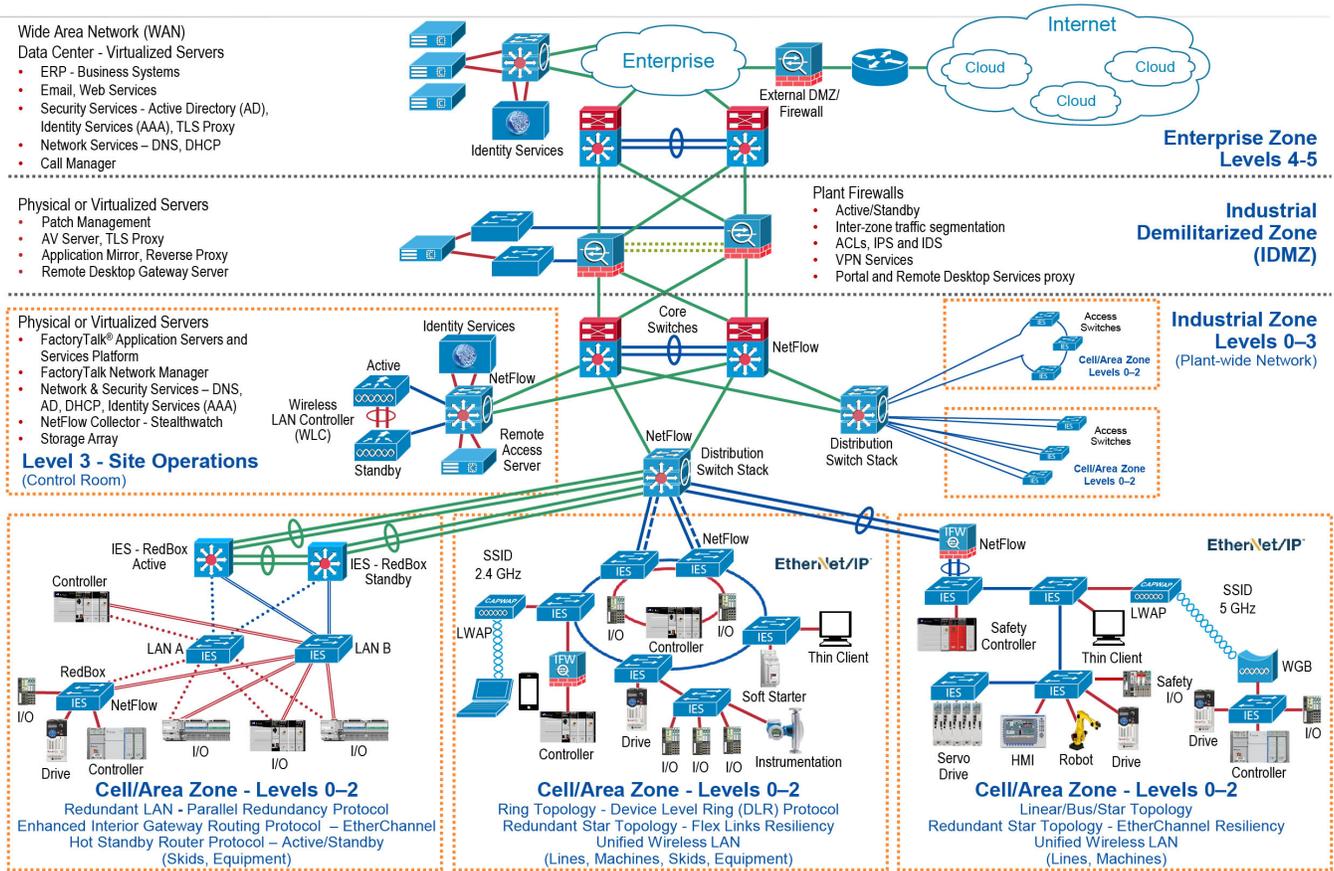
CPwE Overview

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. The CPwE architectures (Figure 1) were architected, tested, and validated to provide design and implementation guidance, test results, and documented configuration settings. This can help to achieve the real-time communication, reliability, scalability, security, and resiliency requirements of modern IACS applications. The content and key tenets of CPwE are relevant to both OT and IT disciplines.

CPwE key tenets include:

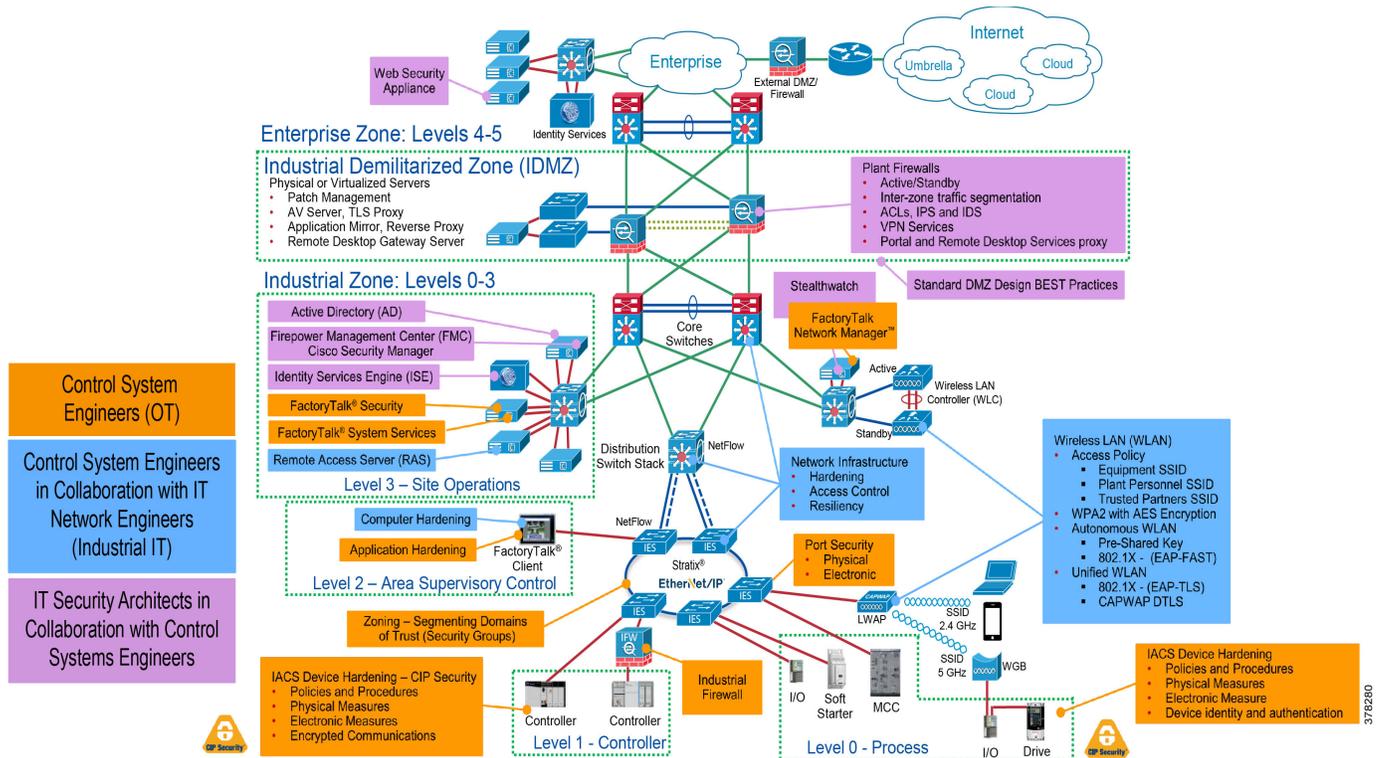
- **Smart IIoT devices**—Controllers, I/O, drives, instrumentation, actuators, analytics, and a single IIoT network technology (EtherNet/IP)
- **Zoning (segmentation)**—Smaller connected LANs, functional areas, and security groups
- **Managed infrastructure**—Managed Allen-Bradley® Stratix industrial Ethernet switches (IES), Cisco Catalyst distribution/core switches, FactoryTalk Network Manager software, and Stratix industrial firewalls
- **Resiliency**—Robust physical layer and resilient or redundant topologies with resiliency protocols
- **Time-critical data**—data prioritization and time synchronization via CIP Sync™ and IEEE-1588 Precision Time Protocol (PTP)
- **Wireless**—Unified wireless LAN (WLAN) to enable mobility for personnel and equipment
- **Holistic defense-in-depth security**—Multiple layers of diverse technologies for threat detection and prevention, implemented by different persona (e.g., OT and IT) and applied at different levels of the plant-wide or site-wide IACS architecture
- **Convergence-ready**—Seamless plant-wide or site-wide integration by trusted partner applications

Figure 1 CPwE Architectures



256705

Figure 2 CPwE Industrial Security Framework



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, CIP, CIP Safety™, CIP Security™, or CIP Sync, see [odva.org](http://www.odva.org) at the following URL:

- <http://www.odva.org/Technology-Standards/EtherNet-IP/Overview>

CPwE Cloud Connectivity

An IACS is deployed in a wide variety of industries such as automotive, pharmaceuticals, consumer packaged goods, distribution, pulp and paper, oil and gas, 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 industrial operations and OEMs is the need to establish and secure connectivity from IACS applications to cloud-based services in order to take advantage of the business benefits associated with the IIoT.

CPwE Cloud Connectivity describes several security architecture use cases that are addressed using diverse security solutions and technologies, managed by different persona, at different levels of the plant-wide security architecture as shown in Figure 2.

- Control System Engineers (highlighted in tan)—IACS asset hardening (for example, physical and electronic), IACS application hardening (for example, CIP Security), infrastructure device hardening (for example, port security), network monitoring and change management (for example, FactoryTalk Network Manager), network segmentation (trust zoning), industrial firewalls (with inspection) at the IACS application edge, and IACS application authentication, 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.

CPwE Cloud Connectivity outlines the concepts, requirements and technology solutions for reference designs developed around a specific set of security architecture use cases. These use cases were tested for solution functional validation by Cisco Systems and Rockwell Automation with assistance by Panduit. The following is a synopsis for this release of CPwE Cloud Connectivity:

- End-to-end outbound cloud connectivity
 - Tested and verified as part of this design guide: end-to-end FactoryTalk solution use cases—Platinum, Gold, Silver, and Bronze
 - Referenced only: Cisco Kinetic, Cisco IoT Gateway, any public cloud service
- Security Stance Overview
 - Risk management—Risk assessment considerations, risk tolerance, and risk mitigation
 - One size does not fit all
 - Trusted versus untrusted security zones
 - Policies and procedures to balance business benefits (such as innovation) with risk management
- End-to-end FactoryTalk Solutions Capabilities Overview
 - FactoryTalk AssetCentre
 - ControlFLASH Plus
 - FactoryTalk Activation Manager
 - Rockwell Automation Cloud API—Currently this API is used to ascertain product life cycle status and acts as the cloud endpoint.
- Design and Deployment Considerations for End-to-End FactoryTalk Solution
 - Establishing the restricted outbound path from the Industrial Zone to the Rockwell Automation cloud
 - Securing the restricted outbound path from the Industrial Zone to the Rockwell Automation cloud
 - Securing the plant-wide IACS network from the Industrial Zone ingress/egress point
 - Securing access to the Rockwell Automation cloud
 - Securing access to the Industrial Demilitarized Zone (IDMZ) Cisco Web Security Appliance acting as the Transport Layer Security (TLS) proxy

Security Architecture Use Cases

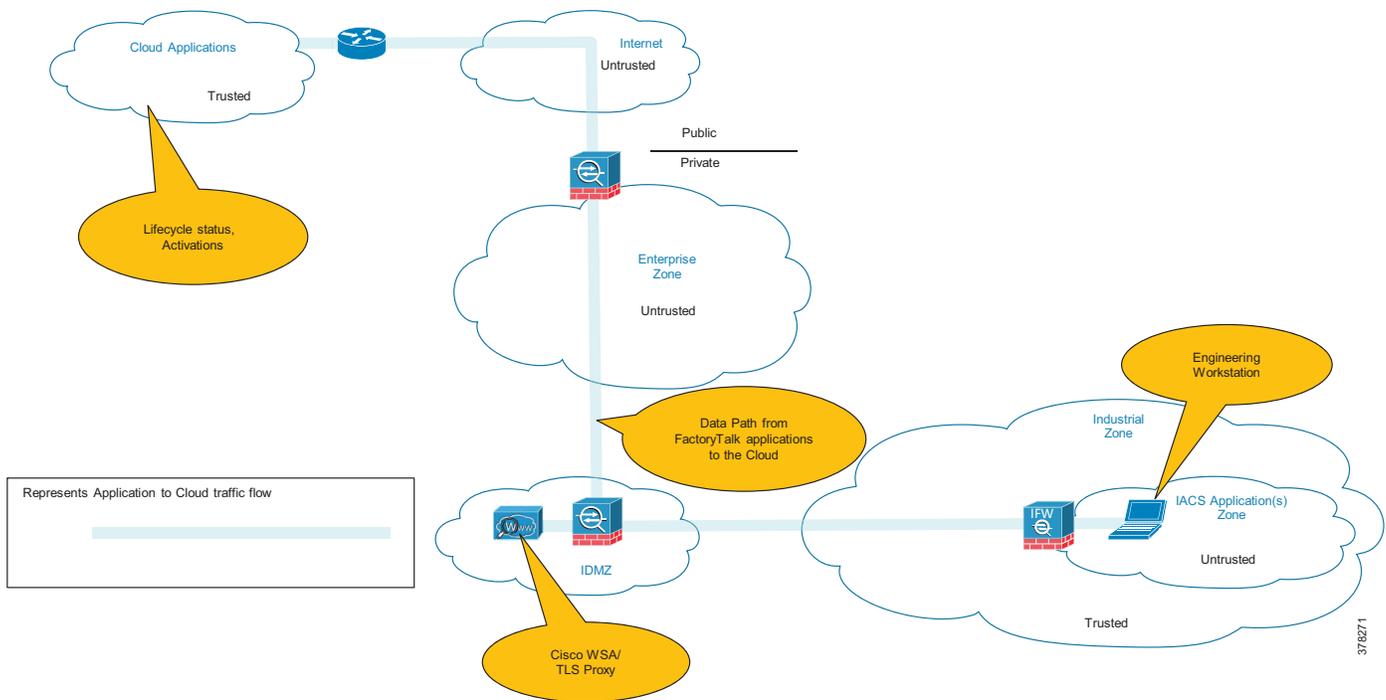
One size does not fit all when it comes to risk tolerance. What's acceptable by one industrial operator may be unacceptable to another and vice versa. The CPwE architecture supports scalability, which includes the degree of holistic and diverse industrial security technologies (Figure 2) applied to a plant-wide security architecture. Scalable security comes in many forms. Based on risk mitigation requirements, several diverse technology options are available for threat detection and prevention to help industrial operations meet their

tolerance to risk. Industrial operators should also ensure that the cloud provider and internet service provider (ISP) are trusted. They are required to protect connectivity and data per the industrial operator’s security policies.

- Platinum Security Architecture**—The Industrial Zone communicates with the Rockwell Automation Cloud via Transport Layer Security (TLS). In keeping with the Industrial Demilitarized Zone (IDMZ) concept of brokered services, a TLS proxy is located in the IDMZ (Figure B-1). For testing and verification purposes, the TLS proxy that was used is the Cisco Web Security Appliance (Cisco WSA). This security architecture uses the IDMZ with Firewall(s) and replicated services to buffer the Industrial Zone from the Enterprise Zone. Industrial Firewall(s) are also implemented to enforce security policies within a Cell/Area Zone to protect the Industrial Zone from the ingress/egress point of the TLS traffic.

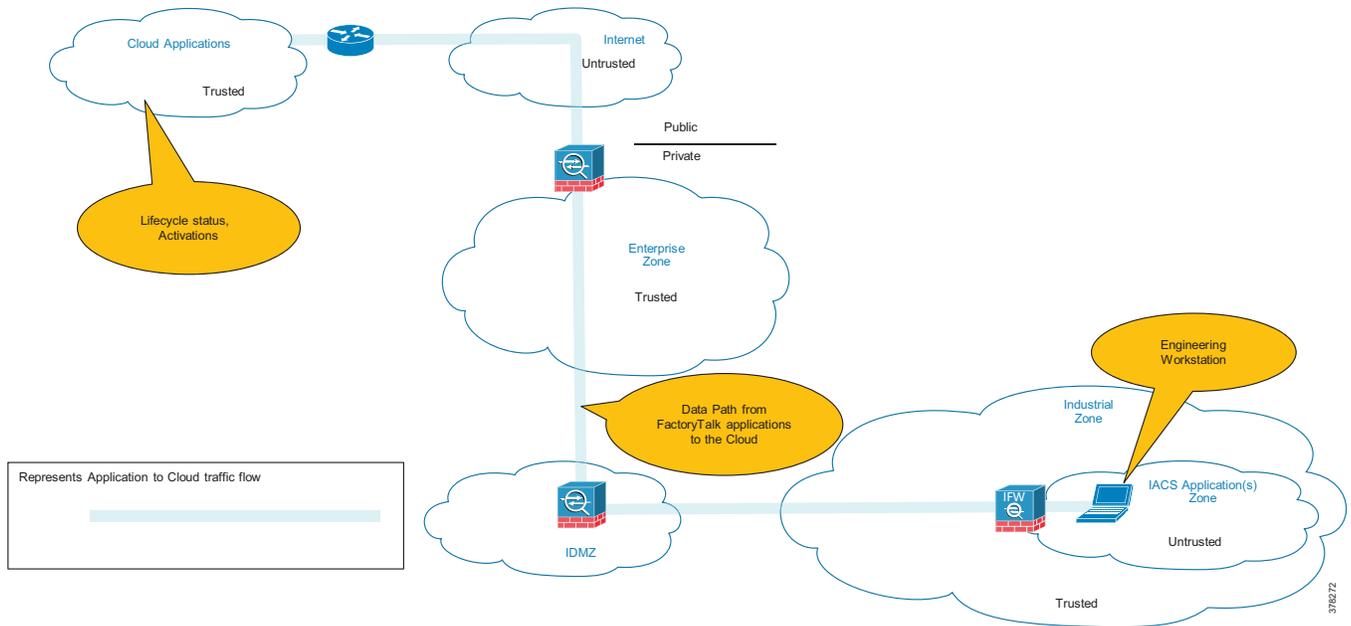
This is the security architecture recommended by Cisco, Panduit, and Rockwell Automation for industrial operations that require cloud-based connectivity yet have a lower tolerance to risk. Some industrial operators may already have a TLS proxy located in their Enterprise DMZ that buffers their Enterprise Zone from the Internet. This security architecture could be implemented to leverage that existing TLS proxy. A third option is to have a TLS Proxy located in the cloud like the Cisco Umbrella Intelligent Proxy. This solution only proxies the traffic that is destined for domains that are proven to be harmful.

Figure B-1 Platinum Security CPwE Cloud Connectivity Use Case



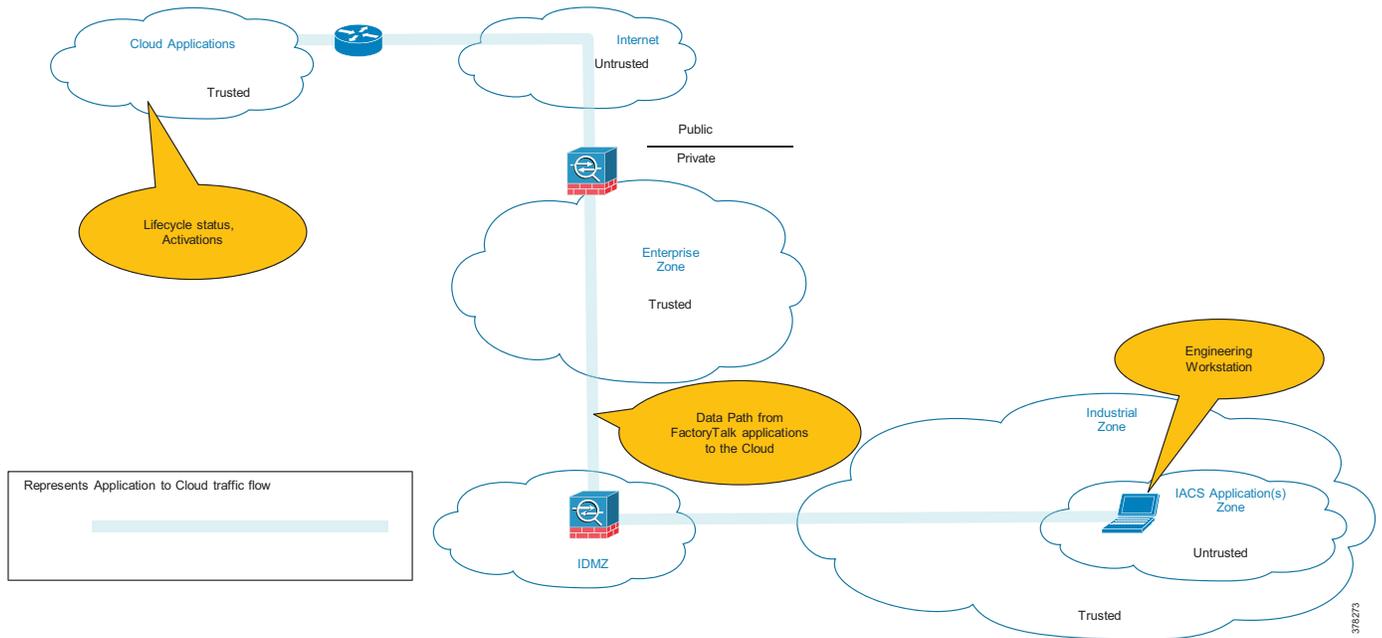
- Gold Security Architecture**—This security architecture could be deployed when a TLS proxy is not present and when multiple layers of diverse industrial security best practices (Figure 2) have been followed. This security architecture uses the IDMZ with Firewall(s) and replicated services to buffer the Industrial Zone from the Enterprise Zone. Industrial Firewall(s) are also implemented to enforce security policies within a Cell/Area Zone to protect the Industrial Zone from the ingress/egress point of the TLS traffic (Figure B-2).

Figure B-2 Gold Security CPwE Cloud Connectivity Use Case



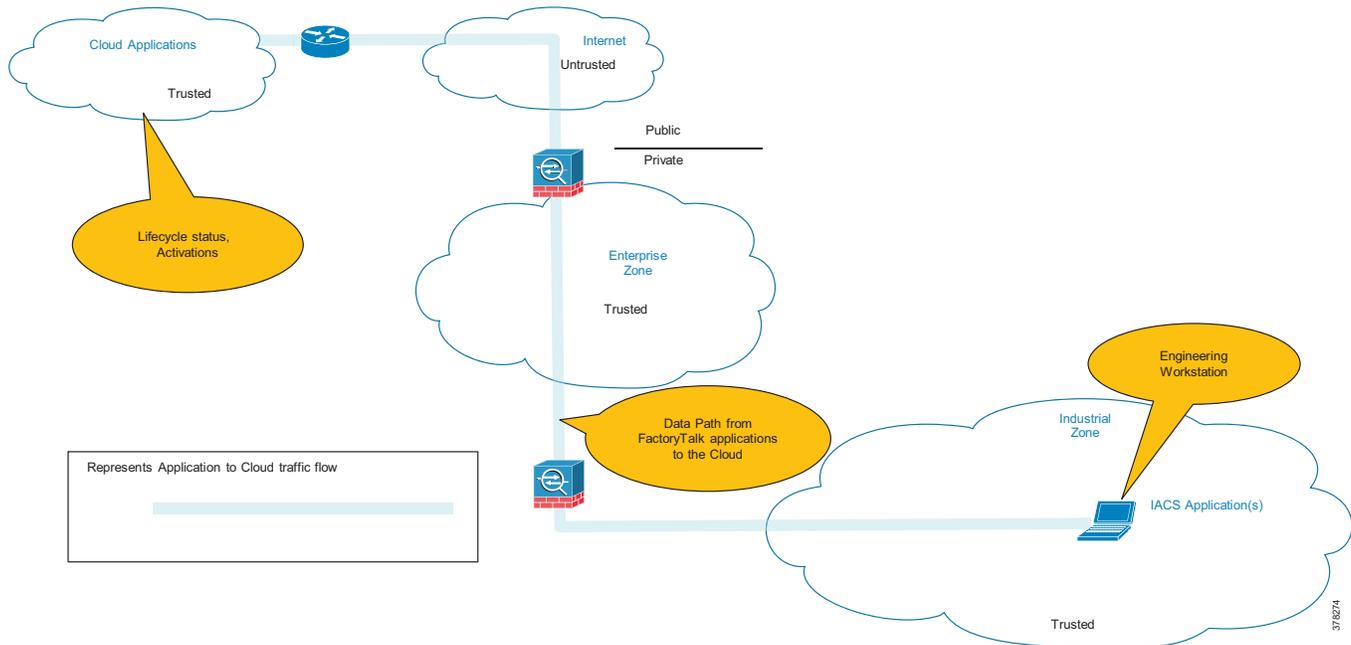
- Silver Security Architecture**—This security architecture has an IDMZ with Firewall(s) and replicated services to buffer the Industrial Zone from the Enterprise Zone. No additional Industrial Firewall(s) exist to enforce security policies to help protect the Industrial Zone from the ingress/egress point of the TLS traffic (Figure B-3).

Figure B-3 Silver Security CPwE Cloud Connectivity Use Case



- Bronze Security Architecture**—This security architecture has the fewest defensive layers of diverse industrial security best practices for threat protection and detection. A Firewall is the only buffer between the Enterprise and Industrial Zone. No additional Industrial Firewall(s) exist to enforce security policies to help protect the Industrial Zone from the ingress/egress point of the TLS traffic. Only industrial operations with a higher tolerance to risk should consider this security architecture for cloud-based connectivity (Figure B-4).

Figure B-4 Bronze Security CPwE Cloud Connectivity Use Case



CPwE Industrial Security Overview

Protecting IACS assets requires a defense-in-depth security approach (Figure 2) where different solutions are needed to address various network and security requirements for a plant-wide architecture. This section summarizes the existing Cisco, Panduit, and Rockwell Automation CPwE security CVDs and CRDs that address different aspects of industrial security.

- *Deploying Network Security within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several network security use cases for plant-wide IACS network infrastructure to help enable IIoT innovation within the CPwE framework.
 - Rockwell Automation site:
https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network_Security/DIG/CPwE-5-1-NetworkSecurity-DIG.html
- *Deploying Identity and Mobility Services within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several industrial 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.
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.html

- *Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide* details design considerations to help with the successful design and implementation of an IDMZ to securely share IACS data across the IDMZ.
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf
 - Cisco site:
https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html
- *Deploying Industrial Firewalls within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several use cases for designing, deploying, and managing industrial firewalls throughout a plant-wide IACS network. The Industrial Firewall is ideal for IACS applications that need trusted zone segmentation.
 - Rockwell Automation site:
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td002_-en-p.pdf
 - Cisco site:
<https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-0/Firewalls/DIG/CPwE-5-IFS-DIG.html>

Summary

CPwE is a collection of architected, tested, and validated designs. 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 operational technology (OT) and informational technology (IT) disciplines, consists of documented architectures, best practices, guidance, and configuration settings to help industrial operations and OEMs with the design and deployment of a scalable, reliable, secure, and future-ready plant-wide industrial network infrastructure. CPwE can also help industrial operations and OEMs achieve cost reduction benefits using proven designs that can facilitate quicker deployment while helping to minimize risk in deploying new technology. CPwE is brought to market through an ecosystem consisting of Cisco, Panduit, and Rockwell Automation emergent from the strategic alliance between Cisco Systems and Rockwell Automation.

The *Cloud Connectivity to a Converged Plantwide Ethernet Architecture Design Guide* outlines several security architecture use cases for designing and deploying restricted end-to-end outbound connectivity with FactoryTalk® applications from industrial operations to the Rockwell Automation cloud within a CPwE architecture. CPwE Cloud Connectivity highlights the key IACS application requirements, technology, and supporting design considerations to help with the successful design and deployment of these specific security architecture use cases within the CPwE framework. CPwE Cloud Connectivity was architected, tested, and verified by Cisco Systems and Rockwell Automation with assistance by Panduit.

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

- Rockwell Automation site:
 - https://www.rockwellautomation.com/en_NA/capabilities/industrial-networks/overview.page?pagetitle=Network-Architectures&docid=04cf49e1d6b46f5d3dcbf777464e6e53
- Cisco site:
 - http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

Panduit Corp. is a world-class provider of engineered, flexible, end-to-end electrical and network connectivity infrastructure solutions that provides businesses with the ability to keep pace with a connected world. Our robust partner ecosystem, global staff, and unmatched service and support make Panduit a valuable and trusted partner.

www.panduit.com

US and Canada:
Panduit Corp.
World Headquarters
18900 Panduit Drive
Tinley Park, IL 60487
iai@panduit.com
Tel. 708.532.1800

Asia Pacific:
One Temasek Avenue #09-01
Millenia Tower
039192 Singapore
Tel. 65 6305 7555

Europe/Middle East/Africa:
Panduit Corp.
West World
Westgate London W5 1XP Q
United Kingdom
Tel. +44 (0) 20 8601 7219

Latin America:
Panduit Corp.
Periférico Pte Manuel Gómez
Morin #7225 - A
Guadalajara Jalisco 45010
MEXICO
Tel. (33) 3777 6000

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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

Allen-Bradley, Control FLASH Plus, FactoryTalk, FactoryTalk Network Manager, Rockwell Automation, and Stratix are trademarks of Rockwell Automation, Inc.. Trademarks not belonging to Rockwell Automation are property of their respective companies.

CIP, CIP Safety, CIP Security, CIP Sync, and EtherNet/IP are trademarks of the ODVA, Inc.