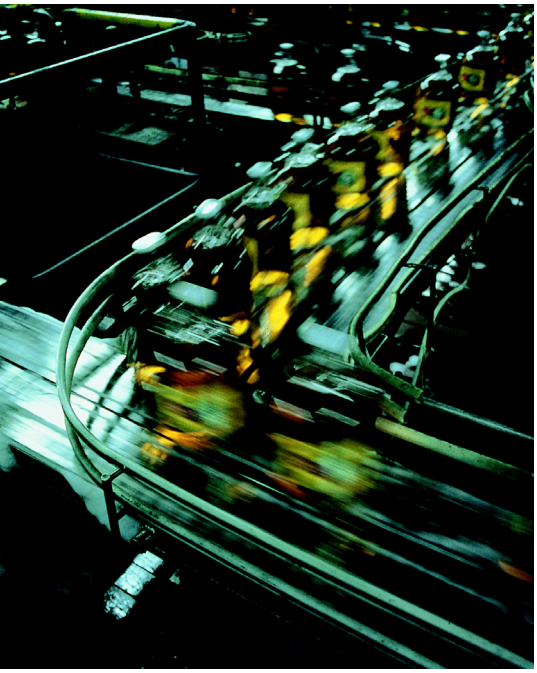


Deploying Industrial Data Center within a Converged Plantwide Ethernet Architecture

Design Guide

May 2018

Cisco Reference Design

Document Reference Number: ENET-TD014A-EN-P

Preface

Converged Plantwide Ethernet (CPwE) is a collection of tested and validated architectures that are developed by subject matter authorities at Cisco and Rockwell Automation. The testing and verification 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 manufacturers with the design and deployment of a scalable, reliable, secure, and future-ready plant-wide industrial network infrastructure. CPwE can also help manufacturers 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 a strategic alliance between Cisco Systems and Rockwell Automation.

Expanding on the existing collection of CPwE CVDs, this CPwE CRD outlines key requirements and application considerations to help with the integration of the Industrial Data Center (IDC) product within a CPwE architecture. The IDC is a purpose-built resource that provides compute, storage, and multi-layer network switching in a pre-engineered and validated package. This *Deploying Industrial Data Center within a Converged Plantwide Ethernet Architecture Design Guide* describes the IDC and validates some potential use cases within a CPwE architecture. CPwE IDC CRD was architected, tested, and documented by Cisco Systems, Panduit, and Rockwell Automation.

Document Organization

This document is composed of the following chapters and appendices.

Chapter/Appendix	Description
CPwE Architecture with Industrial Data Center	Introduces the CPwE architecture and provides a closer look at how the IDC operates in the greater architecture.
Virtualization, Thin Clients, and Industrial Data Center Description Virtualization	Describes the equipment and capabilities of the IDC.
Industrial Data Center Use Cases	Describes the use cases for which the IDC was tested.
Industrial Data Center Verification	Describes the testing performed on the IDC.

Chapter/Appendix	Description
Appendix A, “References”	Link to documents and websites that are relevant to the IDC within a Converged Plantwide Ethernet Architecture CRD.
Appendix B, “Acronyms and Initialisms”	Lists the acronyms and initialisms commonly used in CPwE documentation.
Appendix C, “About the Cisco Validated Design (CVD) Program”	Describes the Cisco Validated Design (CVD) process and the distinction between CVDs and Cisco Reference Designs (CRDs).

Audience

The main intended audience for this document are IT and engineers at manufacturers looking for guidance for implementing an Industrial Data Center product and integrating it into the larger CPwE architecture.

Readers should already be familiar with the CPwE architectures.

Document Objective and Scope

This document briefly discusses the CPwE architecture and then focuses on the Level 3 Site Operations and the Cell/Area Zone(s), where the Industrial Data Center (IDC) solution from Rockwell Automation provides services to end users. This document is not intended to be an exhaustive analysis of every feature and option available, but instead is designed to highlight the most important use cases of the Rockwell Automation Industrial Data Center.

For More Information

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
- Panduit site:
  - http://www.panduit.com/cpwe

CHAPTER 1

CPwE Architecture with Industrial Data Center

Business practices, corporate standards, industry standards, policies, and risk tolerance are key factors in determining the need for an IDC within a plant-wide architecture. Most network architectures supporting an Industrial Automation and Control System (IACS) application require this pivotal piece of equipment to minimize risk while maximizing overall plant uptime.

An IACS is deployed to support a variety of industry applications such as automotive, pharmaceuticals, consumer goods, 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. An IACS architecture that includes an IDC can help to increase Overall Equipment Effectiveness (OEE) by reducing the impact of a failure and speed recovery from an outage, in turn lowering the Mean Time To Repair (MTTR).

The IDC functions best as part of a holistic, resilient plant-wide network architecture made up of multiple technologies, both logical and physical, deployed at different levels within the plant.

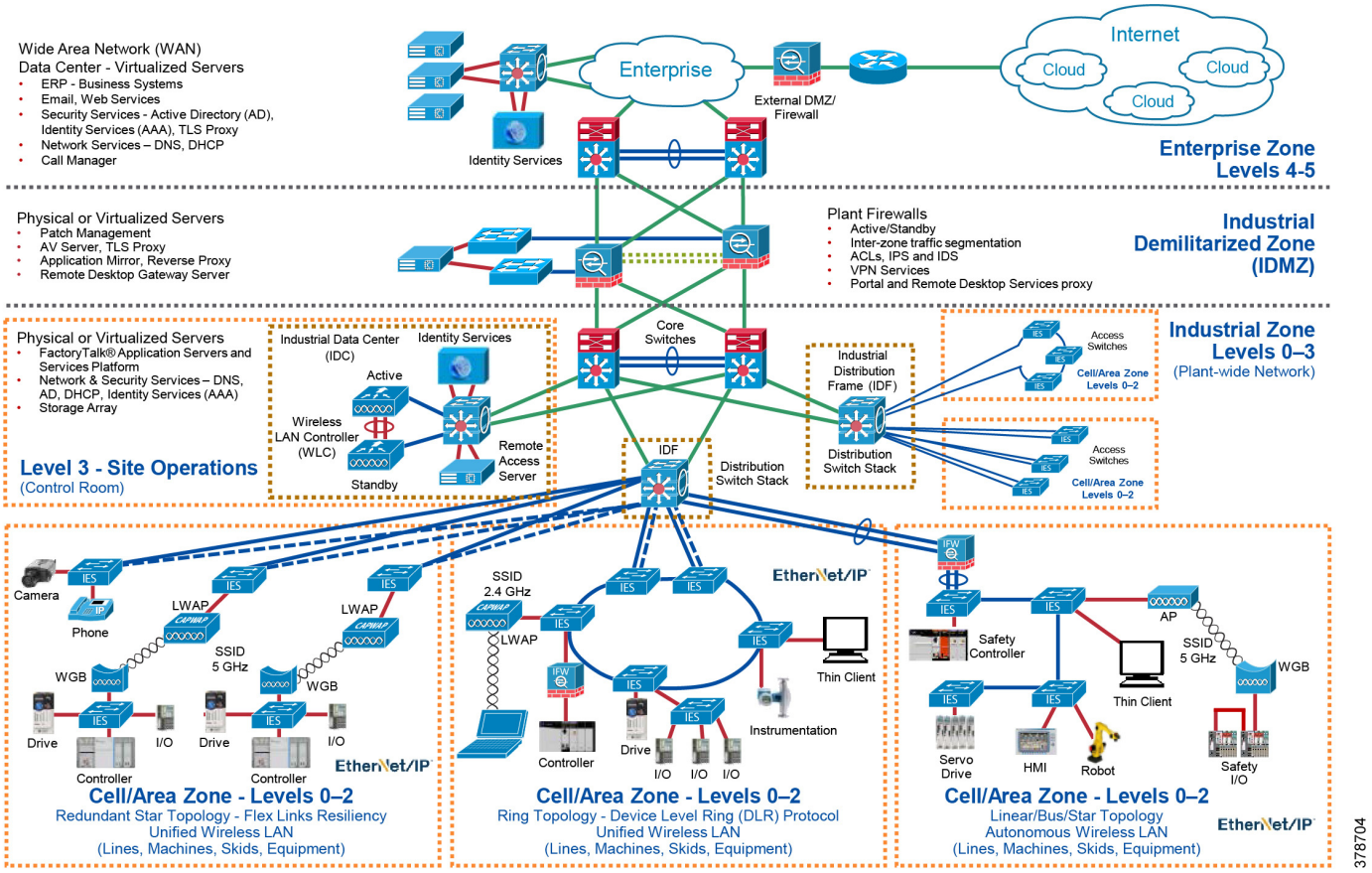
- Robust physical infrastructure
- Topologies and protocols
- Switching and routing
- Wireless LAN controllers
- Firewalls
- Network and device management

Converged Plantwide Ethernet (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 architecture (Figure 1-1) provides design and implementation guidance to achieve the real-time communication, reliability, scalability, security and resiliency requirements of the IACS. The CPwE Industrial Data Center for IACS applications is brought to market through collaboration between Cisco Systems, Panduit Corp., and Rockwell Automation.

The Level 3 Site Operations Area (Figure 2-1) provides the switching, compute, and storage resources needed to efficiently operate a manufacturing facility. This area is the foundation for data collection and application hosting in the Industrial setting. This Level 3 equipment is housed in the IDC solution. Level 3 Site Operation applications range from Manufacturing Execution Systems (such as FactoryTalk® ProductionCentre®), applications like FactoryTalk and PlantPAx®, key performance indicators like OEE, lot traceability, preventive maintenance schedules, process monitoring and management, safety and security dashboards, and

productivity KPIs. Continuity of service is imperative as these functions are used for daily decision making on an ever-increasing basis. Reliable and secure network support for these applications keeps production flowing and business communication running smoothly. Manufacturing network outages are readily visible and easily monetized in thousands of dollars from missed customer commitments.

Figure 1-1 CPwE Architectures



CHAPTER 2

Virtualization, Thin Clients, and Industrial Data Center Description Virtualization

Virtualization is the creation of virtual resources such as a server, desktop, operating system, file, storage, or network. The main goal of virtualization is to manage workloads by transforming traditional computing to make it more scalable. Virtualization has been around for quite some time and today is being applied to a wide variety of system levels, including operating system-level virtualization, hardware-level virtualization, and server virtualization.

Some items to consider that are good and bad for virtualization include:

- Virtualization opportunities:
  - Flexibility—Old operating systems, Linux on Windows, etc.
  - Availability—VMs can migrate to another host should their host fail.
  - Speed—Server and desktop provisioning
- Virtualization challenges:
  - Anything (process, application, etc.) that requires a dongle or physical hardware.
  - Systems that require extreme performance, e.g., systems that use a lot of the resources.
  - Applications and operating systems with license or support agreements that do not permit virtualization.

Benefits of Virtualization

Benefits of virtualization include:

- **Energy Saving**—Migrating physical servers over to virtual machines and consolidating them onto far fewer physical machines means lower power and cooling costs.
- **Reduces the Data Center Footprint**—Server consolidation with virtualization reduces the overall footprint of the data center, which means fewer physical machines, less networking gear, and fewer racks and hence less required floor space.
- **QA, Test, and Lab Environments**—Virtualization allows for an easy build out of a self-contained lab or test environment operating in its own isolated network, which should be considered when rolling out patches or updates both to the OS and the IACS software.

- **Faster Provisioning**—Virtualization enables flexible capacity to provide systems (servers and desktops) very quickly as opposed to purchasing additional physical machines. This process can be done within a few minutes by simply closing an existing "master" image, template, or existing virtual machine.
- **Increased Uptime**—With the use of advanced features that are not available on physical servers, virtualization allows for better continuity and uptime. Capabilities such as VM and storage migration, fault tolerance, high availability, and resource scheduling keep virtual machines running or allow for fast recovery from failures and unplanned outages.
- **Improve Disaster Recovery**—By removing the dependency on specific hardware or server models, a disaster recovery site no longer needs to keep identical hardware that matches the production environment. Operations can save money by purchasing less expensive hardware for disaster recovery since it rarely gets used. Also, because virtualization allows for fewer physical machines, replication sites are more affordable.
- **Application Isolation**—Application isolation is usually achieved by using a "one app/one server" model. Virtualization can use components (e.g., application farms) to support specific applications and allow only specified users.
- **Extend the Life of Older Applications**—Older applications than are not able to be upgraded and will only run on older operating systems (and therefore older hardware) can be maintained on virtual machines, avoiding the need to keep and maintain outdated or non-replaceable hardware.

Thin Client Technology

A thin client is a lightweight computer which is optimized for accessing applications or desktops from a remote server-based computing platform. The server provides the majority of the computing power, including launching software programs, running calculations, and storing data. The thin client provides I/O for a keyboard, mouse, monitor, sound, and USB ports for access to USB devices.

Thin clients are used to access applications or desktops from remote locations (e.g., IDC). Some benefits of using thin clients include cost savings, reduced energy consumption (versus a PC), simplified management, enhanced security, and overall increased productivity.

Thin client technology types include:

- PC over IP (PCoIP)
- Remote Desktop Protocol (RDP)
- ThinManager® software

PC over IP (PCoIP)

PCoIP or PC-over-IP is a display protocol that permits total compression of a desktop, which is then displayed using a zero-client device over a standard IP network. With PCoIP, the entire computing experience is compressed, encrypted, and encoded in the data center before being transmitted across a standard IP network to PCoIP-enabled endpoint devices.

Remote Desktop Protocol (RDP)

RDP is used for communication between the Terminal Server Client and the Terminal Server. With RDP a remote user can add a graphical interface to another computer's desktop. This secure network communications protocol is designed for Windows-based applications that run on a server. It facilitates

encryption and application data transfer security between devices, client users, and a virtual network server. Network administrators can use RDP to remotely identify and resolve problems faced by individual subscribers.

PCoIP versus RDP

The choice of PCoIP versus RDP is based on how well either PCoIP or RDP meet your requirements.

Choose PCoIP if any of the following are applicable:

- You are using a high-speed connection and bandwidth is not a problem.
- You want to display better quality videos, graphics, and sound.

Choosing RDP would be a good decision if:

- You are unaware of your network quality; in such a case, RDP would be a better choice than PCoIP.
- The quality of sound, graphics, and video is not an issue.

ThinManager

ThinManager® software provides software solutions for IACS networks that enable secure, centralized configuration and deployment of applications and content to every PC, thin client, mobile device, and user.

ThinManager Relevance® software is a location-based mobile management platform that allows applications and content to be securely delivered to specific locations within the manufacturer's facility. ThinManager Relevance uses location resolvers and geofences like QR codes, Bluetooth beacons, Wi-Fi, and GPS to confirm that mobile users and devices only receive content in authorized areas. Content specific to a user's role can be delivered based on Relevance user credentials which can be linked to Active Directory accounts.

Within the CPwE IDC, ThinManager can be used to securely manage content delivery to thin clients from various applications and data sources in the Industrial Zone: FactoryTalk View SE and ME applications, FactoryTalk VantagePoint data, Studio 5000 Logix Designer® software, terminal shadowing, streaming video, and many others. Thin clients can receive content from Microsoft® Remote Desktop servers running these applications, as well as VNC servers (for example, FactoryTalk View ME terminals) and IP cameras.

The ThinManager solution provides additional security when introducing thin clients into the industrial environment since no production data is stored locally and content delivery can be authorized by any combination of user, location, and device.

Industrial Data Center

The IDC is a purpose-built resource that provides compute, storage, and multi-layer network switching in a pre-engineered and validated package. The IDC is located in Level 3 Site Operations where it houses the virtualized servers used in the IACS. Most IDC designs also have backup power provisions as well as smart power distribution units with dual-power source provisions. Design parameters and verification methodologies are established by CPwE architects, Rockwell Automation application specialists, and Panduit engineers to ensure that the IDC meets requirements in a robust and reliable fashion.

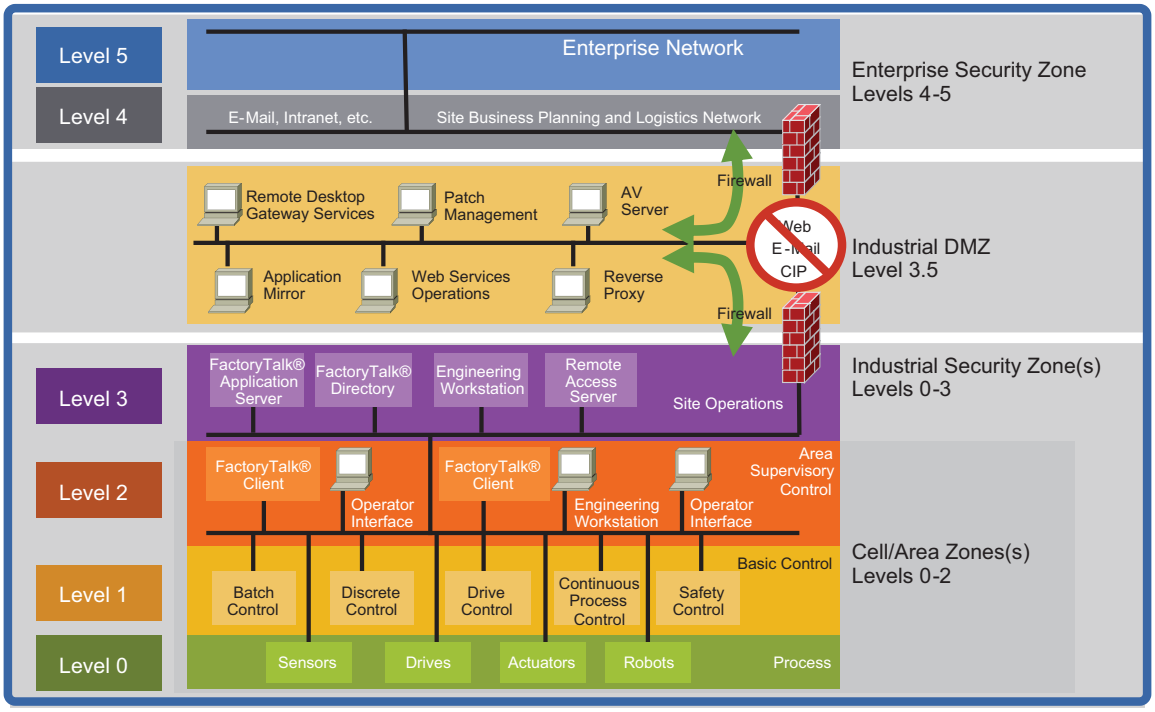
The IDC provides many key functions for a well-designed IACS network. It can provide an operating platform for enterprise grade software applications like MES software, hosts patch and version servers, etc.

There is open rack unit (RU) space within the IDC that may be used for mounting additional items such as security appliances (e.g., ISE), networking appliances, etc.

In support of the performance of the industrial network, there are many infrastructure aspects of the IDC that play an important role and must be considered in the design and implementation of it within the network.

- **Industrial Characteristics**—The IDC is typically deployed within Level 3 Site Operations of CPwE architectures (Figure 2-1). Plant networking assets and cabling used in Level 3 Site Operations are not environmentally hardened but are almost exclusively installed in IP20 or better environments. Environmental risks at Level 3 Site Operations involve thermal management of equipment heat dissipation, redundant network connections, redundant power connections, and power quality considerations.

Figure 2-1 CPwE Logical Model



- **Physical Network Infrastructure Life Span**—Industrial automation and control systems (IACS) and the plant backbone can be in service 20 years or longer. Hardware used in Level 3 Site Operations, being IT gear, has a much shorter life span, generally 3-5 years. This nominal life span is related to the technology age of the equipment rather than its ability to function past this time frame. The infrastructure used to connect and house hardware such as cabinets, cabling, connectivity, and enclosures has a much longer life span, generally 10-15 years. Consideration of higher performance cabling enables the data communications needs of tomorrow as well as today to be fully met. Choosing supporting infrastructure wisely at the time of IDC installation and commissioning avoids the future cost and disruption of installing upgraded media that matches the capabilities of the new IT equipment that is installed. Choices in media between copper and fiber optic cabling ensure higher data rate transport requirements.
- **Maintainability**—Be aware that Move, Adds, and Changes at Level 3 have dependencies that affect many Cell/Area Zones. Also, changes need to be planned and executed correctly as an error can bring down manufacturing. Proper cable management such as bundling, identification, access, etc. is vital. Use of structured cabling techniques provides maintainability benefits and provides measurable value in terms of quickly recovering from outages related to media cuts as well as delivering a high level of agility when the network must adapt to meet manufacturing process changes.

- **Scalability**—The high growth of EtherNet/IP and IP connections can strain network performance as well as cause network sprawl that threatens uptime and security. A strong physical building block design accounts for traffic growth as well as management of additional cabling to support designed network growth. Use a zone topology together with structured copper and fiber optic cabling chosen for high data throughput. The CPwE architecture lends itself readily to deployment across a zone architecture. Choose building block pre-configured solutions to enable a network infrastructure comprised of modular components that scale to meet increasing Ethernet communications needs in your IACS network.
- **Designing for High Availability**—A robust, reliable physical infrastructure achieves service levels required of present and future IACS networks. The use of standards-based cabling together with measured, validated performance ensures reliable data throughput. Use of redundant logical and physical networks assures highest availability. Properly designed and deployed pathways should be employed to ensure redundant cables paths are also resilient cables paths.
- **Network Compatibility and Performance**—Network performance is governed by the poorest performing element in any link. Network compatibility and optimal performance is essential from port to port. This compatibility requirement includes port data rate and cabling bandwidth. Cable selection is the key to optimal physical network performance.
- **Grounding and Bonding**—A well architected grounding and bonding system is crucial for industrial network performance at every level whether internal to control panels, across plants, or between buildings. A single, verifiable grounding network avoids ground loops that can degrade data and has implications for equipment uptime and even safety. In high EMI areas, where the use of shielded cabling is advisable, the performance of the shielding is inexorably tied to the quality of the grounding network that supports it.
- **Security**—Network security is a critical element of network uptime and availability. Physical layer security measures, like logical security measures, should follow a defense-in-depth hierarchy. Your Level 3 physical defense in depth strategy could take the form of locked access to data center and control room spaces and cabinet key card access to help limit access, use of Lock In Block Out (LIBO) devices to control port usage, and keyed patch cords to avoid inadvertent cross patching. Using a physical strategy in concert with your logical strategy helps prevent inadvertent or malicious damage to equipment and helps achieve connectivity service level goals.
- **Wireless**—Unified operation of wireless access points requires a Wireless LAN Controller (WLC) at Level 3 Site Operations and distribution of lightweight wireless access points across Industrial Zone and Cell/Area Zones. Autonomous wireless access points, typically Work Group Bridges, in Cell/Area Zones involves cabling for access points and Workgroup bridges. The selection of media for the industrial zone backbone as well as for cabling for access points using POE is critical for future readiness and bandwidth considerations. PoE is evolving to deliver more power over copper cabling so understanding industrial applications with scalability and environmental considerations is critical.
- **Panduit SmartZone™ Cabinet**—The IDC used in testing utilized a Panduit SmartZone Cabinet. SmartZone Cabinets enable Level 3 Site Operation data centers, co-location facilities, and remote sites with limited technical expertise and financial resources to easily order, rapidly install, and deploy fully integrated cabinets. The SmartZone Cabinet is pre-installed with SmartZone Power Solutions to provide a range of standardized, factory-integrated intelligent cabinets with pre-tested, validated access control, power, and thermal monitoring capabilities. SmartZone Rack Monitoring Software uses operational data consolidated by the SmartZone Gateway and displays it on the intuitive dashboard to provide a precise and logical reflection of the “actual” power and thermal data as well as the ability to send alerts to identify rising temperatures or other issues that may impact business resilience. This ready-to-deploy cabinet solution provides data centers with a complete Data Center Infrastructure Management (DCIM) solution that is immediately ready to begin delivering the transparency and actionable information needed to optimize energy and operational efficiencies, fully maximize existing capacity, and protect service uptime.

CHAPTER 3

Industrial Data Center Use Cases

This chapter examines four potential use cases for the IDC:

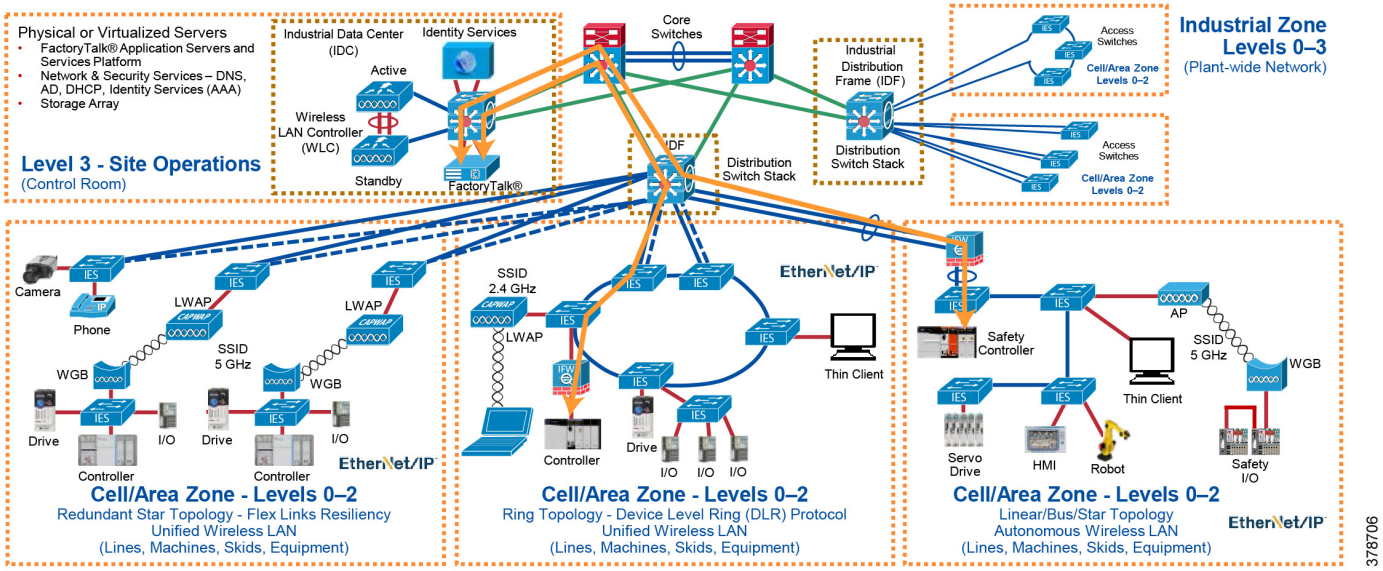
- CPwE IDC EtherNet/IP Connectivity Use Case
- CPwE IDC ThinManager Operator Workstations Connectivity Use Case
- CPwE IDC ThinManager Engineering Workstations Connectivity Use Case
- CPwE IDC Active Directory Connectivity Use Case

CPwE IDC EtherNet/IP Connectivity Use Case

Virtualization of Industrial Automation and Control System (IACS) application servers is a common practice. IACS applications that can be virtualized include HMI servers, Historians, and Asset Management.

The IDC is located at Level 3 - Site Operations. This potentially separates the IDC—and the virtualized application servers—from the IACS assets at Levels 0-2 - Cell/Area Zone by multiple network hops.

Figure 3-1 CPwE IDC EtherNet/IP Connectivity Use Case



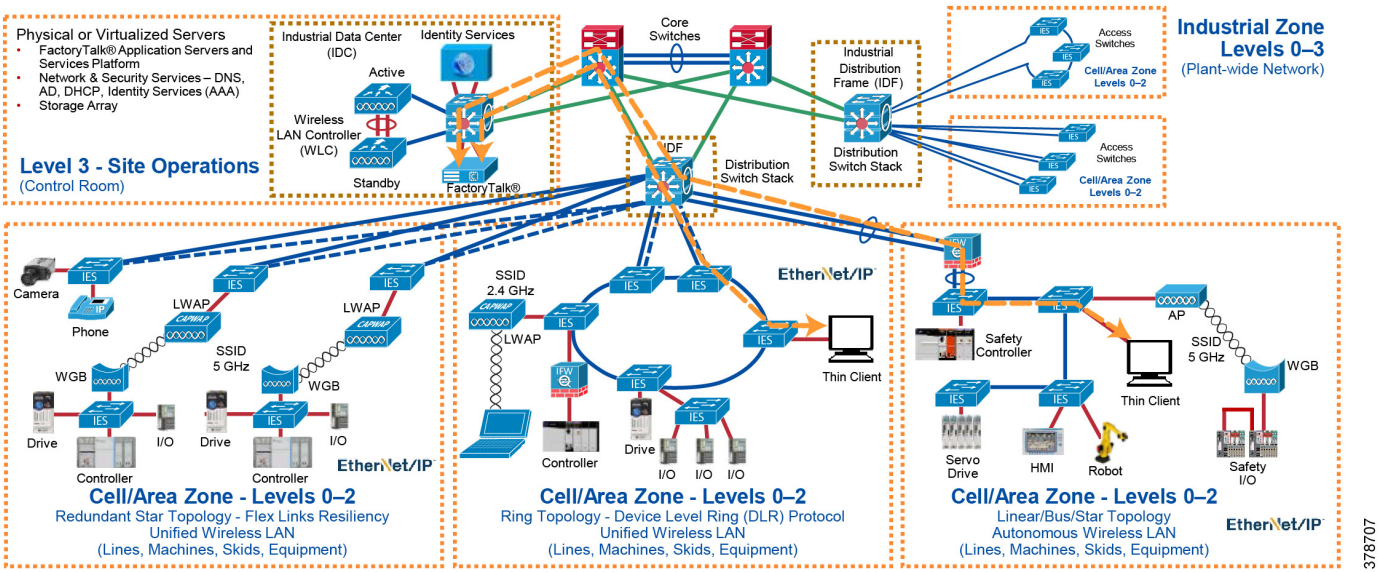
This use case demonstrates EtherNet/IP connectivity from the virtualized application servers (with proper network configuration) from Level 3 Site Operations to the IACS assets located in Levels 0-2 - Cell/Area Zone.

CPwE IDC ThinManager Operator Workstations Connectivity Use Case

Operator workstations (OWS) allow an operator to monitor and control the IACS. They present data acquired by the application servers to allow visibility to the IACS by an operator.

An operator may need to remotely access an OWS in the IDC (Level 3 - Site Operations) from a thin client (e.g., ThinManager) located at Level 2 within the Cell/Area Zone.

Figure 3-2 CPwE IDC ThinManager OWS Connectivity Use Case



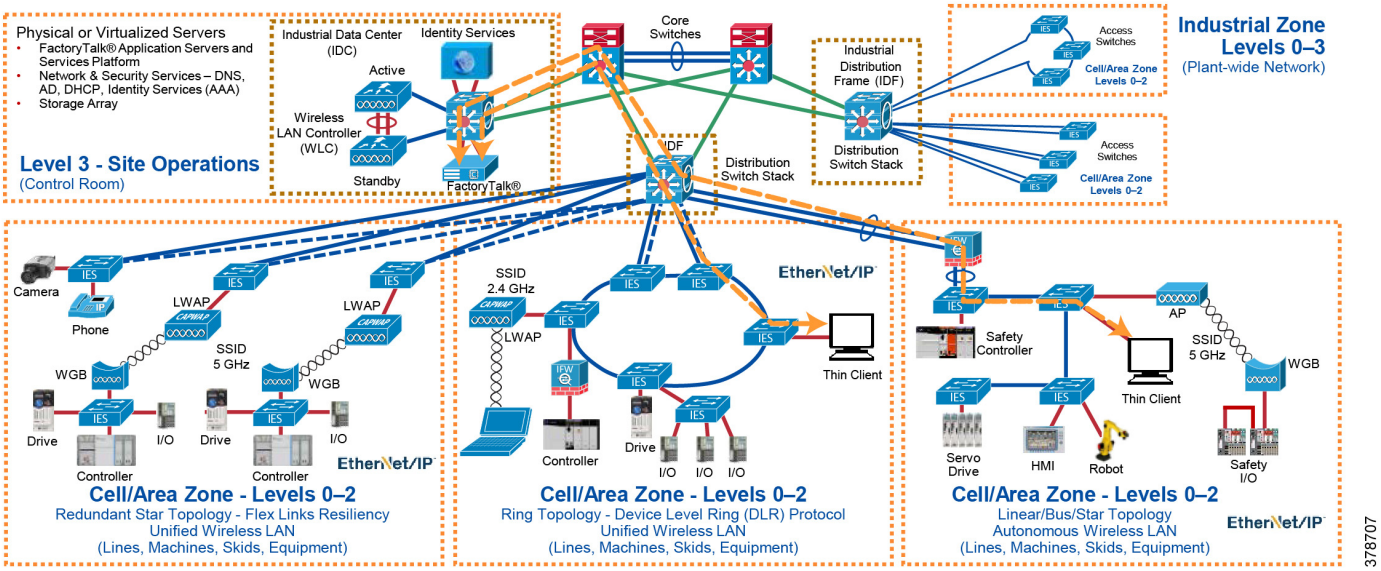
This use case demonstrates that a user/operator can remotely access an OWS in the IDC from a thin client located at Level 2 within the Cell/Area Zone.

CPwE IDC ThinManager Engineering Workstations Connectivity Use Case

Engineering workstations (EWS) are used by proper, authorized personnel (e.g., OT engineers) to configure, correct, and troubleshoot the IACS. They will typically have specialized software installed to allow programming and configuration of the IACS and network devices.

An engineer may need to remotely access an EWS in the IDC (Level 3 - Site Operations) from a thin client (e.g., ThinManager) located at Level 2 within the Cell/Area Zone.

Figure 3-3 CPwE IDC ThinManager EWS Connectivity Use Case

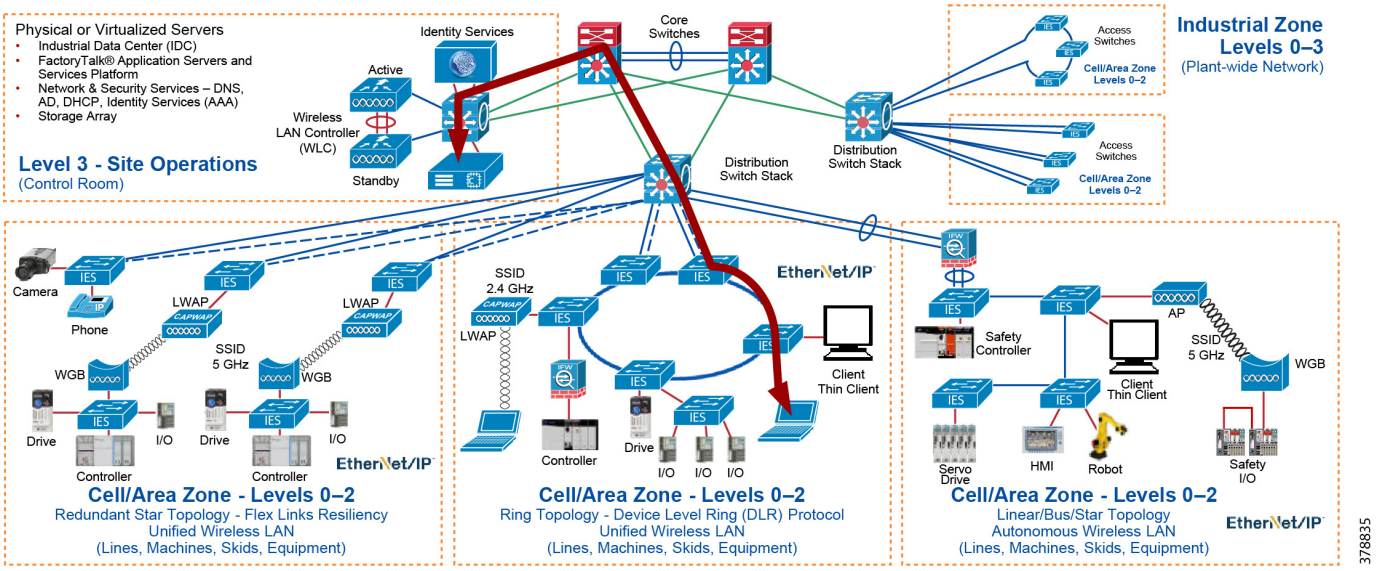


This use case demonstrates that an engineer can remotely access an EWS in the IDC from a thin client located in Level 2 within the Cell/Area Zone.

CPwE IDC Active Directory Connectivity Use Case

A virtualized Active Directory server in the IDC can be used to authenticate users at Level 3 - Site Operations and Level 2 within a Cell/Area Zone without requiring the authentication process to traverse the industrial DMZ (IDMZ).

Figure 3-4 CPwE IDC Active Directory Connectivity Use Case



This use case demonstrates user authentication using the virtuliazed Active Directory server located in the IDC at Level 3 - Site Operations from a PC/Thin Client/terminal located at Level 2 within the Cell/Area Zone.

CHAPTER 4

Industrial Data Center Verification

This chapter, which documents the testing performed on the IDC, includes the following major topics:

- System Verification Coverage
- System Verification Results

The scope of the verification for this CRD is limited compared to the extensive Cisco Validated Design process typically performed by Cisco, Rockwell Automation, and Panduit subject matter authorities. The scope of proof of concept (PoC) testing is more narrowly focused on the IDC itself, and to a limited degree, the directly attached devices. All PoC testing was performed in the full CPwE test lab, which is a comprehensive end-to-end architecture, and the testing documented here should be viewed as an extension to the existing collection of CPwE architectures.

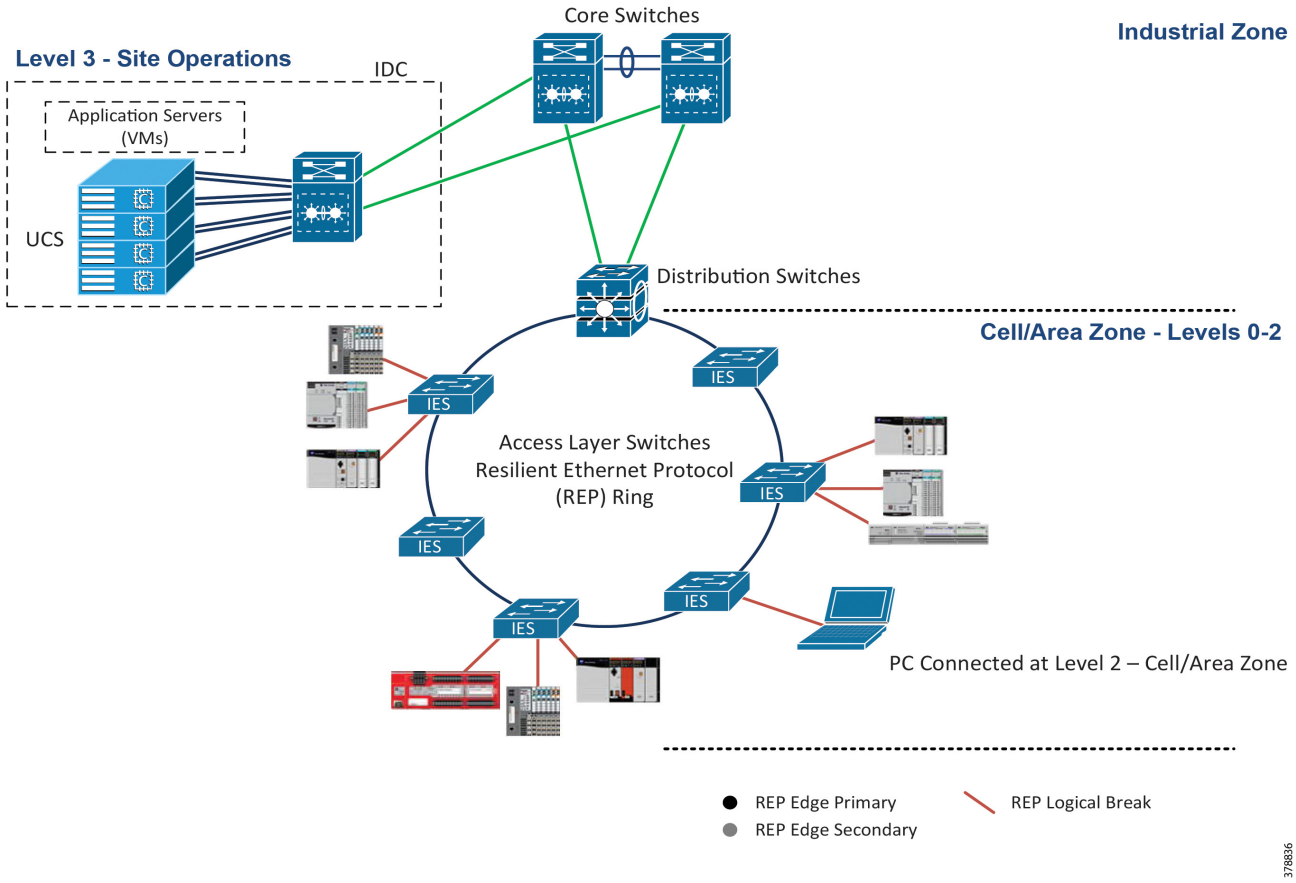
System Verification Coverage

PoC test coverage of the IDC was divided into the four areas described below:

- CPwE IDC EtherNet/IP Connectivity Use Case—Verification of IDC virtualized application server functionality using an HMI Server, Data Server (RSLinx®), FactoryTalk Services Platform, and EtherNet/IP to communicate to the IACS end devices located at Cell/Area Zone (Levels 0-2).
- CPwE IDC ThinManager Operator Workstations Connectivity Use Case—Verification of IDC virtualized operator workstation (OWS) functionality using a PC with RDP client, ThinManager, and a Client installed on an HMI.
- CPwE IDC ThinManager Engineering Workstations Connectivity Use Case—Verification of IDC virtualized engineer workstation (EWS) functionality using a PC at Level 2, Thin Client at Level 2, RDP, PCoIP, and ThinManager.
- CPwE IDC Active Directory Connectivity Use Case—Verification of IDC virtualized Active Directory using Authentication (AAA) for the IACS.

System and Application Setup

Figure 4-1 Testbed Setup



Application/Software	Version
VMware vSphere	6.5 update 1
VMware Horizon View Administrator	7.3.2
VMware View Agent	7.3.2
FactoryTalk Activation Manager	4.00.02
FactoryTalk View Site Edition Server	9.00.00
FactoryTalk View Studio	9.00.00
RSLinx Enterprise	5.90.00
RSLinx Classic	3.74.00
Studio 5000 Logix Designer	20.04/21.00/26.01/27.00/28.00/29.00
ThinManager Server	10.0
ThinManager Client	4.0.0

System Verification Results

Test Case 1—CPwE IDC EtherNet/IP Connectivity Use Case

Use RSLinx data server hosted on a virtual machine (VM) at Level 3 - Site Operations to acquire data from IACS devices at Levels 0-2 - Cell/Area Zone.

Test Setup

Virtual Machine in the IDC—Level 3-Site Operations	
OS Installed	Windows Server 2008 R2
Software	• FactoryTalk View Site Edition Server (RSLinx Enterprise) • RSLinx Classic • FactoryTalk Activation Manager
Configuration	• Network • RSLinx Classic can browse remote subnets • Server: PLN-CPWE-AS1 (Application Server 1)

Verification Procedure

Virtual Machine in the IDC—Level 3-Site Operations			
	Action	Pass/Fail	Comments
1.	Verify RSLinx on server PLN-CPWE-AS1 (Application Server 1) can browse/see devices at Levels 0-2 - Cell/Area Zone.	PASS	See Lab Setup for network configuration.
2.	Verify RSLinx Enterprise PLN-CPWE-AS1 (Application Server 1) can poll data [HMI/SCADA Applications] from devices at Levels 0-2 - Cell/Area Zone.	PASS	

Test Case 2—CPwE IDC ThinManager Operator Workstations Connectivity Use Case

Use PC at Level 2 - Cell/Area Zone to connect to specified OWS applications in the IDC at Level 3 Site Operations.

Test Setup

Part A—Windows RDS Host	
Virtual Machine in the IDC—Level 3-Site Operations	
OS Used	Windows Server 2008 R2
Software	• Windows Remote Desktop Services (Role) • FactoryTalk View Site Edition Client • FactoryTalk Activation Manager
Configuration	A remote user configured so a specified application (HMI) launches when that user connects (via RDP).
Part B—RDP-Windows 7	
Virtual Machine in the IDC—Level 3-Site Operations	
OS Used	Windows 7 Professional
Software	• FactoryTalk View Site Edition Client • FactoryTalk Activation Manager • Desklock
Configuration	Desklock configured to launch applications(s) and prevent the user from accessing the desktop.
Part C—VDI-Windows 7	
Server—Virtual Machine in the IDC—Level 3-Site Operations	
OS Used	Windows 7 Professional
Software	• FactoryTalk View Site Edition Client • FactoryTalk Activation Manager • Desklock
Configuration	Desklock configured to launch applications(s) and prevent the user from accessing the desktop.
Client—PC—Level 2-Cell/Area Zone	
OS Used	Windows 7 Professional
Software	Horizon View Client
Part D—VDI-Application Pool configured in Horizon View Connection Server	
Server—Virtual Machine Server Farm in the IDC—Level 3-Site Operations	
OS Used	Windows Server 2008 R2
Software	• FactoryTalk Site Edition Client • FactoryTalk Activation Manager
Configuration	• Application Pool (Server Farm) is configured in Horizon View Server. • Entitlement for a remote user is added to the Application Pool.
Client—PC—Level 2-Cell/Area Zone	
OS Used	Windows 7 Professional

Software	Horizon View Client
Part E—ThinManager	
ThinManager Server in the IDC—Level 3-Site Operations	
OS Installed	Windows Server 2008 R2
Software	ThinManager Server - ThinManager 10.0
Configuration	Configure Application Link for ThinManager
PC—Level 2-Cell/Area Zone	
OS Installed	Windows 7 Professional
Software	ThinManager Client - WinTMC 4.0.0

Verification Procedure

Part A—Windows RDS Host			
	Action	Pass/Fail	Comments
1.	Use Windows RDP to connect to the remote server.	PASS	
2.	Verify when the user connects, the HMI application is launched.	PASS	
3.	Verify when the user closes the HMI application, the user is disconnected from the server and logged off.	PASS	
Part B—RDP-Windows 7			
	Action	Pass/Fail	Comments
1.	Use Windows RDP to connect to the remote Windows 7 desktop.	PASS	
2.	Verify when the user connects, the only item available is Desklock, and there is no access to the remote Windows 7 desktop.	PASS	Connection passed but had issues with Desklock software: • Not saving/maintaining its configuration. • Desklock software troubleshooting exceeds the scope of this document.
Part C—VDI-Windows 7			
	Action	Pass/Fail	Comments
1.	Use Horizon View Client to connect to the remote Windows 7 desktop.	PASS	
2.	Verify when the user connects, the only item available is Desklock, and there is no access to the remote Windows 7 desktop.	PASS	Connection passed but had issues with Desklock software: • Not saving/maintaining its configuration. • Desklock software troubleshooting exceeds the scope of this document.
Part D—VDI-Application Pool configured in Horizon View Connection Server			

	Action	Pass/Fail	Comments
1.	Use Horizon View Client to connect to the remote Horizon View Server. Application Pool applications are visible and available.	PASS	
2.	Verify when the user can select and open/run the specified application(s) from the Application Pool.	PASS	
Part E—ThinManager			
	Action	Pass/Fail	Comments
1.	Verify the client PC with ThinManager Client (Level 2 - Cell/Area Zone) can connect to the ThinManager Server (Level 3 - Site Operations).	PASS	
2.	Verify the ThinManager client is restricted to the application configured using the Application Link option.	PASS	

Test Case 3—CPwE IDC ThinManager Engineering Workstations Connectivity Use Case

Use PC at Level 2 - Cell/Area Zone to connect to specified EWS applications in the IDC at Level 3 Site Operations.

Test Setup

Part A—Windows RDS Host	
Virtual Machine in the IDC—Level 3-Site Operations	
OS Installed	Windows Server 2008 R2
Software	• Windows Remote Desktop Services (Role) • FactoryTalk View Studio • Studio 5000 Logix Designer • FactoryTalk Activation Manager
Configuration	A remote user configured to have full access to the desktop when that user connects (via RDP).
Part B—RDP-Windows 7	
Virtual Machine in the IDC—Level 3-Site Operations	
OS Installed	Windows 7 Professional
Software	• FactoryTalk View Studio • Studio 5000 Logix Designer • FactoryTalk Activation Manager
Configuration	A remote user configured to have full access to the desktop when that user connects (via RDP).
Part C—VDI-Windows 7	

Virtual Machine in the IDC—Level 3-Site Operations	
OS Installed	Windows 7 Professional
Software	• FactoryTalk View Studio • Studio 5000 Logix Designer • FactoryTalk Activation Manager
Configuration	• Desktop Pool is created/configured in Horizon View Server. • Entitlement for a remote user is added to the Desktop Pool.
PC—Level 2-Cell/Area Zone	
OS Installed	Windows 7 Professional
Software	Horizon View Client
Part D—VDI-Application Pool configured in Horizon View Connection Server	
Virtual Machine Server Farm in the IDC—Level 3-Site Operations	
OS Installed	Windows Server 2008 R2
Software	• FactoryTalk View Studio • Studio 5000 Logix Designer • FactoryTalk Activation Manager
Configuration	• Application Pool [Server Farm] is configured in Horizon View Server. • Entitlement for a remote user is added to the Desktop Pool.
PC—Level 2-Cell/Area Zone	
OS Installed	Windows 7 Professional
Software	Horizon View Client
Part E—ThinManager	
ThinManager Server in the IDC—Level 3-Site Operations	
OS Installed	Windows Server 2008 R2
Software	ThinManager Server - ThinManager 10.0
Configuration	Default settings for ThinManager Server
PC—Level 2-Cell/Area Zone	
OS Installed	Windows 7 Professional
Software	ThinManager Client - WinTMC 4.0.0

Verification Procedure

Part A—Windows RDS Host			
	Action	Pass/Fail	Comments
1.	Use Windows RDP to connect to the remote server.	PASS	

2.	Verify when the user connects, the user has full access to the remote desktop.	PASS	
Part B—RDP-Windows 7			
	Action	Pass/Fail	Comments
1.	Use Windows RDP to connect to the remote Windows 7 desktop.	PASS	
2.	Verify when the user connects, the user has full access to the remote desktop.	PASS	
Part C—VDI-Windows 7			
	Action	Pass/Fail	Comments
1.	Use Horizon View Client to connect to the remote Windows 7 desktop in the desktop pool.	PASS	
2.	Verify when the user connects, the user has full access to the remote desktop.	PASS	
Part D—VDI-Application Pool configured in Horizon View Connection Server			
	Action	Pass/Fail	Comments
1.	Use Horizon View Client to connect to the remote Horizon View Server. Application Pool applications are visible and available.	PASS	
2.	Verify when the user can select and open/run the specified application(s) from the Application Pool.	PASS	
Part E—ThinManager			
	Action	Pass/Fail	Comments
1.	Verify the client PC with ThinManager Client (Level 2 - Cell/Area Zone) can connect to the ThinManager Server (Level 3 - Site Operations).	PASS	

Test Case 4—CPwE IDC Active Directory Connectivity Use Case

Configure Active Directory on a server (VM) in the IDC at Level 3—Site Operations.

Test Setup

Active Directory	
OS Installed	Windows Server 2012
Configuration	Active Directory Services (Role)

Verification Procedure

Active Directory			
	Action	Pass/Fail	Comments
1.	Verify a user at Level 2 - Cell/Area Zone can authenticate to the Active Directory.	PASS	

APPENDIX A

References

The following documents and web sites are relevant to the *Deploying Industrial Data Center within a Converged Plantwide Ethernet Architecture CRD*:

- Rockwell Automation IDC specification sheet: http://literature.rockwellautomation.com/idc/groups/literature/documents/pp/gsmn-pp001_-en-p.pdf
- Design Zone for Manufacturing—Converged Plantwide Ethernet: https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html
- Industrial Network Architectures—Converged Plantwide Ethernet: http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page
- Panduit Industrial Products: https://www.panduit.com/en/solutions/industrial-networks-and-IoT.html
- SmartZone Cabinet Specification Sheet: http://www.panduit.com/ccurl/423/887/smartzone-cabinet-pvsp124.pdf?_ga=2.19373240.1096428009.1517953389-1567405429.1470069321

APPENDIX B

Acronyms and Initialisms

Table B-1 lists the acronyms and initialisms commonly used in CPwE documentation.

Table B-1 Acronyms and Initialisms

Term	Description
1:1	One-to-One
AAA	Authentication, Authorization, and Accounting
AD	Microsoft Active Directory
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
AES	Advanced Encryption Standard
ACL	Access Control List
AH	Authentication Header
AIA	Authority Information Access
AMP	Advanced Malware Protection
AP	Access Point
ASDM	Cisco Adaptive Security Device Manager
ASIC	Cisco Application-Specific Integrated Circuit
ASR	Cisco Aggregation Services Router
AWG	American Wire Gauge
BYOD	Bring Your Own Device
CA	Certificate Authority
CAPWAP	Control and Provisioning of Wireless Access Points
CDP	CRL Distribution Points
CFD	Computational Fluid Dynamics
CIP™	ODVA, Inc. Common Industrial Protocol
CLI	Command Line Interface
CoA	Change of Authorization
CPwE	Converged Plantwide Ethernet
CRAC	Computer Room Air Conditioning
CRD	Cisco Reference Design
CRL	Certificate Revocation List
CSR	Certificate Signing Request

Table B-1 Acronyms and Initialisms (continued)

Term	Description
CSSM	Cisco Smart Software Manager
CTL	Certificate Trust List
CVD	Cisco Validated Design
DACL	Downloadable Access Control List
DC	Domain Controller
DCF	Dielectric Conduited Fiber
DHCP	Dynamic Host Configuration Protocol
DIG	Design and Implementation Guide
DLR	Device Level Ring
DMVPN	Dynamic Multipoint Virtual Private Network
DNS	Domain Name System
DPI	Deep Packet Inspection
DSRM	Directory Services Restoration Mode
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
EIGRP	Enhanced Interior Gateway Routing Protocol
EMB	Effective Modal Bandwidth
EMI	Enterprise Manufacturing Intelligence, ElectroMagnetic Interference
EO	Equipment Outlet
EoIP	Ethernet over IP
EPC	Equalizing Potential Conductor
ERP	Enterprise Resource Planning
ESP	Encapsulating Security Protocol
ESR	Embedded Services Router
FAP	Fiber Adapter Panel
FHRP	First Hop Redundancy Protocols
FIB	Forwarding Information Base
FQDN	Fully Qualified Domain Name
FVRF	Front-door Virtual Route Forwarding
GRE	Generic Routing Encapsulation
HDPE	High-Density Polyethylene
HMAC	Hash Message Authentication Code
HMI	Human-Machine Interface
HSRP	Hot Standby Routing Protocol
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IDC	Industrial Data Center
IDF	Industrial Distribution Frame
IDMZ	Industrial Demilitarized Zones
IEC	International Electrotechnical Commission
IES	Industrial Ethernet Switch (Allen-Bradley® Stratix®, Cisco IE)
IIoT	Industrial Internet of Things
IKE	Internet Key Exchange
IoT	Internet of Things

Table B-1 Acronyms and Initialisms (continued)

Term	Description
IP	Internet Protocol
IPDT	IP Device Tracking
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Internet Service Provider
ISE	Cisco Identity Services Engine
ISR	Integrated Service Router
IT	Information Technology
LACP	Link Aggregation Control Protocol
LBS	Location Based Services
LIBO	Lock In/Block Out
LOS	Loss of Signal
LWAP	Lightweight Access Point
MAB	MAC Authentication Bypass
MAC	Media Access Control; Moves, Adds, and Changes
MDF	Master Distribution Frame
MDM	Mobile Device Management
ME	FactoryTalk View Machine Edition
MEC	Multi-Chassis Ethernet Channel
mGRE	Multipoint Generic Routing Encapsulation
M.I.C.E.	Mechanical Ingress Chemical/Climatic Electromagnetic (see TIA-1005)
MMC	Microsoft Management Console
MnT	Monitoring Node
MPLS	Multiprotocol Label Switching
MSE	Mobile Service Engine
MSS	Maximum Segment Size
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDES	Network Device Enrollment Service
NFPA	National Fired Protection Association
NHRP	Next Hop Routing Protocol
NOC	Network Operation Center
NPS	Microsoft Network Policy Server
NSF	Nonstop Forwarding
NSP	Native Supplicant Profile
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OD	Outer Cable Diameter
ODVA	Open DeviceNet Vendors Association
OEE	Overall Equipment Effectiveness
OEM	Original Equipment Manufacturer
OIR	Online Insertion and Removal
OM	Optical Multimode

Table B-1 Acronyms and Initialisms (continued)

Term	Description
OpEx	Operational Expense
OT	Operational Technology
OTA	Over-the-Air
OU	Organizational Unit
PAC	Programmable Automation Controller
PAgP	Port Aggregation Protocol
PAN	Policy Administration Node
PAT	Port Address Translation
PC	Personal Computer
PCoIP	PC over IP
PCS	Process Control System
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PNZS	Physical Network Zone System
PoE	Power over Ethernet
POU	Power Outlet Unit
PSK	Pre-Shared Key
PSN	Policy Service Node
PTP	Precision Time Protocol
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Server
RD	Route Descriptor
RDG	Remote Desktop Gateway
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
REP	Resiliency Ethernet Prottocol
RIB	Routing Information Base
RPI	Requested Packet Interval
RSSI	Received Signal Strength Indication
RTT	Round Trip Time
RU	Rack Unit
SA	Security Association
SaaS	Software-as-a-Service
SCEP	Simple Certificate Enrollment Protocol
SE	FactoryTalk View Site Edition
SFP	Small Form Factor Pluggable
SHA	Secure Hash Standard
SIG	Secure Internet Gateway
SNR	Signal to Noise Ratio
SPW	Software Provisioning Wizard
SSID	Service Set Identifier
SSO	Stateful Switch Over
STP	Shielded Twisted Pair; Spanning Tree Protocol

Table B-1 Acronyms and Initialisms (continued)

Term	Description
SVI	Switched Virtual Interface
SYN	Synchronization
TIA	Telecommunication Industry Association
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSB	TIA Technical Services Bulletin
UCS	Cisco Unified Computing System
UDP	User Datagram Protocol
UPS	Uninterruptable Powr Supply
UTP	Unshielded Twisted Pair
VDI	Virtual Desktop Infrastructure
VFD	Variable Frequency Drive
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
VRRP	Virtual Router Redundancy Protocol
VSL	Virtual Switching Link
VSS	Virtual Switching System
WAN	Wide Area Network
WGB	Work Group Bridge
wIPS	wireless Intrusion Prevention Service
WLAN	Wireless LAN
WLC	Cisco Wireless LAN Controller
WSA	Cisco Web Security Appliance
ZFW	Zone-Based Policy Firewall

APPENDIX C

About the Cisco Validated Design (CVD) Program

Converged Plantwide Ethernet (CPwE) is a collection of tested and validated architectures developed by subject matter authorities at Cisco and Rockwell Automation which follows the Cisco Validated Design (CVD) program.

CVDs provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Each one has been comprehensively tested and documented by engineers to help achieve faster, more reliable, and fully predictable deployment.

The CVD process is comprehensive and focuses on solving business problems for customers and documenting these solutions. The process consists of the following steps:

- Requirements are gathered from a broad base of customers to devise a set of use cases that will fulfill these business needs.
- Network architectures are designed or extended to provide the functionality necessary to enable these use cases, and any missing functionality is relayed back to the appropriate product development team(s).
- Detailed test plans are developed based on the architecture designs to validate the proposed solution, with an emphasis on feature and platform interaction across the system. These tests generally consist of functionality, resiliency, scale, and performance characterization.
- All parties contribute to the development of the CVD guide, which covers both design recommendations and implementation of the solution based on the testing outcomes.

Within the CVD program, Cisco also provides Cisco Reference Designs (CRDs) that follow the CVD process but focus on reference designs developed around specific sets of priority use cases. The scope of CRD testing typically focuses on solution functional verification with limited scale.

For more information about the CVD program, please see the Cisco Validated Designs at the following URL::

https://www.cisco.com/c/en/us/solutions/enterprise/validated-design-program/index.html

.

Publication ENET-TD014A-EN-P May 2018