Preface

Converged Plantwide Ethernet (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 achieve the design and deployment of a scalable, reliable, secure, and future-ready plant-wide or site-wide industrial network infrastructure. CPwE can also help industrial operations and OEMs achieve cost reduction benefits by 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.

Deploying CIP Security within a Converged Plantwide Ethernet Architecture (CPwE CIP Security™), which is documented in this Design Guide outlines several security architecture use cases for designing and deploying CIP Security technology across plant-wide or site-wide Industrial Automation and Control System (IACS) applications. CPwE CIP Security was architected, tested, and validated by Rockwell Automation with assistance by Cisco Systems and Panduit.

CPwE CIP Security provides a comprehensive explanation of the CIP Security application design. It includes information about key requirements, possible deployment models, potential challenges, technology considerations, and guidelines for implementation and configuration of these specific use security cases within the CPwE framework.

Document Organization

This document contains the following chapters and appendices:

Chapter	Description
Chapter 1, “CPwE CIP Security Overview”	CPwE Overview, CPwE Industrial Security Framework Overview, CPwE CIP Security in alignment with ISA/IEC 62443, and CIP Security Solution Use Cases
Chapter 2, “CPwE CIP Security Design Considerations”	System Components, IACS Security Policy Considerations, Technology Considerations, and Architectural Considerations

Chapter	Description
Chapter 3, “CPwE CIP Security Configuration”	Describes how to configure CPwE CIP Security within the CPwE architecture based on the design considerations and recommendations of the previous chapter. This includes deploying, changing, and removing CIP Security properties using FactoryTalk® Policy Manager.
Chapter 4, “Verifying and Troubleshooting the Deployment”	Information on verifying and troubleshooting CPwE CIP Security.
Appendix A, “References”	Links to documents and websites that are relevant to *Deploying CIP Security within a Converged Plantwide Ethernet Architecture Design Guide*.
Appendix B, “Acronyms and Initialisms”	List of acronyms and initialisms used in this document.
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).

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

Note This release of the CPwE architecture focuses on EtherNet/IP™, which uses the ODVA, Inc. 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 the following URL: http://www.odva.org/Technology-Standards/EtherNet-IP/Overview