Deploying Identity Services within a Converged Plantwide Ethernet Architecture

White Paper

May 2015
Deploying Identity Services within a Converged Plantwide Ethernet Architecture

As access methods to the 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 contractors (such as OEMs and System Integrators), plant-wide networks face continued security threats.

Industrial Automation and Control System (IACS) networks are generally open by default, which facilitates both technology coexistence and IACS interoperability. IACS networks must be secured by configuration and architecture since unknown contractor computers present challenges to the security of plant-wide operations.

The management and security of the evolving coexistence of technologies within the plant require a different approach. Converged Plantwide Ethernet (CPwE) uses Cisco Identity Services Engine (ISE) to support centrally managed secure wired or wireless computer access to the IACS networks by plant personnel and contractors.

CPwE is the underlying architecture that provides standard network 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 Microsoft®-based computer, operating system and logged-on user to push security policies to the network infrastructure that the computer is accessing. The CPwE architecture provides design and implementation guidance to achieve the real-time communication, reliability, scalability, security and resiliency requirements of the IACS. 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 Services is brought to market through a strategic alliance between Cisco Systems® and Rockwell Automation. The CPwE Identity Services Cisco Validated Design (CVD) provides design and implementation guidance for Cisco Identity Services Engine within the Industrial Zone.
Secure Access Control

As the number of known and unknown computers connecting to the IACS network continues to increase, methods for managing disparate security solutions and mitigation of risks continue to mature. Physical security is no longer adequate to prevent attempts to access an IACS network. With the continued proliferation of contractor computer connectivity and the already constrained plant-wide operational resources, the potential impact of failing to identify and re-mediate security threats introduces significant risk to plant-wide operations. CPwE Identity Services is a new approach for both the management and security of the evolving plant.

Protecting IACS assets requires a centrally manageable defense-in-depth security approach that addresses internal security threats. Cisco ISE supports both wired and wireless access methods to secure different access methods to the IACS networks by plant personnel and contractors.

The CPwE Industrial Network Security Framework (Figure 1) uses a defense-in-depth approach and is aligned to industrial security standards such as ISA/IEC-62443 (formerly ISA-99) IACS Security and NIST 800-82 Industrial Control System (ICS) Security.

Designing and implementing a comprehensive IACS network access security framework should be a natural extension to the IACS and not be 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.

CPwE defense-in-depth layers (Figure 1) include:

- **Control System Engineers** (highlighted in tan)—IACS device hardening (for example, physical and electronic), infrastructure device hardening (for example, port security), network segmentation, IACS application authentication, authorization and accounting (AAA)

- **Control System Engineers in collaboration with IT Network Engineers** (highlighted in blue)—Zone-based policy firewall at the IACS application, operating system hardening, network device hardening (such as access control, resiliency), wired and wireless LAN access policies

- **IT Security Architects in collaboration with Control Systems Engineers** (highlighted in purple)—Identity Services (wired and wireless), Active Directory (AD), Remote Access Servers, plant firewalls, Industrial Demilitarized Zone (IDMZ) design best practices
Unified Network Access Policy Management for CPwE

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

- Comprehensive centralized policy management
- Streamlined device onboarding
- Dynamic enforcement

A rules-based, attribute-driven policy model is provided to create access control policies. Cisco ISE includes the ability to create fine-grained policies. 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 2, CPwE Identity Services supports 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 contractors, 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.
Converged Plantwide Ethernet Identity Services

Device profiling within the Industrial Zone is based upon a device profiler service, which identifies specific computers connecting to the plant-wide network. The profiling service within Cisco ISE identifies specific computers that connect to a switch convenience port within the Cell/Area Zone and their location, or upon initial connection to the plant wireless network. The specific devices are profiled based on the endpoint profiling policies configured within Cisco ISE, which then grants permission to the specific computers to access the plant-wide network based on the result of the policy evaluation or routes the untrusted computer to an administratively defined safe destination. The profiling service facilitates management of authentication by using IEEE standard 802.1X port-based authentication access control supported within the Stratix and Cisco industrial Ethernet switches (IES) supported within the CPwE architecture.

Through computer profiling, Cisco ISE will ensure that only trusted plant personnel and contractor computers access the plant-wide network. Based on the user’s or computer’s identity, Cisco ISE sends secure access rules to the Stratix or Cisco IES so plant-wide operations are assured of consistent policy enforcement from wherever the user or computer is trying to access the network.
CPwE Identity 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—according to the business policies defined by the plant-wide operations—automatically. CPwE Identity Services enables IT to establish automated plant-wide device provisioning and profiling, while keeping the process simple for plant personnel to get their computers onto the plant-wide network with limited IT help.

Summary

Within the Industrial Zone, CPwE Identity Services:

- Provides centralized context-aware identity management critical to managing access control within an Industrial Zone.
- Determines if users are accessing the network on an authorized, policy-compliant computer, and assigns access based on the assigned user role, group and associated policy. Variables such as employee, vendor, partner, job role, location and device type are taken into consideration.
- Grants authenticated users access to specific segments of the Industrial Zone based upon authentication results.

IACS networks rely upon technology coexistence and IACS interoperability. In the same manner, IACS networks must also be secure, preventing unknown and untrusted devices from threatening plant-wide operations. CPwE Identity Services is a centrally managed layer of network access protection atop wired and wireless industrial networks distributed across the Industrial Zone. Identity Services integration into the Industrial Zone provides a range of access control options for plant-wide operations. CPwE Identity Services creates and distributes access policies in real-time, allowing plant personnel and contractors to experience consistent access from anyplace they access the plant-wide network.

Note

This release of the CPwE architecture focuses on EtherNet/IP, which is driven by the ODVA Common Industrial Protocol (CIP). Refer to the IACS Communication Protocols section of the *CPwE Design and Implementation Guide*.

Rockwell Automation site

Cisco site: