

CHAPTER 1

CPwE Architecture

This chapter, which introduces the CPwE architecture and then provides a closer look at the how sub-zones in the Cell/Area Zone are important to OEM machine, skid and equipment builders, includes the following major topics:

- [Plant-wide Zoning, page 1-1](#)
- [Cell/Area Zone, page 1-5](#)

For additional information about CPwE architectures as a whole, readers should review the *CPwE Design and Implementation Guide*, which can be found at the following URLs:

- Cisco site:
 - <http://www.cisco.com/c/dam/en/us/td/docs/solutions/Verticals/CPwE/CPwE-CVD-Sept-2011.pdf>
- Rockwell Automation site:
 - http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf

Plant-wide Zoning

The CPwE logical model employs the commonly used industry standards such as Purdue Model for Control Hierarchy (reference ISBN 1-55617-265-6) to organize the plant functions into Levels, and IEC-62443 (formerly ISA99) to organize the Levels into functional and security Zones, as shown in [Figure 1-1](#).

Figure 1-1 CPwE Logical Zoning Based on Purdue Model and IEC-62443

Enterprise Zone	Enterprise Network	Level 5
	Site Business Planning and Logistics Network	Level 4
IDMZ	Industrial Demilitarized Zone — Shared Access	
Industrial Zone	Site Manufacturing Operations and Control	Level 3
	Area Supervisory Control	Level 2
Cell/Area Zone	Basic Control	Level 1
	Process	Level 0

377943

Starting at the bottom of the CPwE logical model, the Cell/Area Zone contains three levels of IACS devices:

- **Level 0 Process**—Industrial sensors, drives, actuators and similar devices that interact with the physical environment by taking measurements or performing actions such as starting a motor or moving a robot arm.
- **Level 1 Basic Control**—Controllers, such as programmable logic controllers, distributed control system and programmable automation controllers that communicate directly with the Level 0 devices, other controllers and higher level IACS applications.
- **Level 2 Area Supervisory Control**—Operator interfaces including human machine interface (HMI), alarm systems and control room workstations.

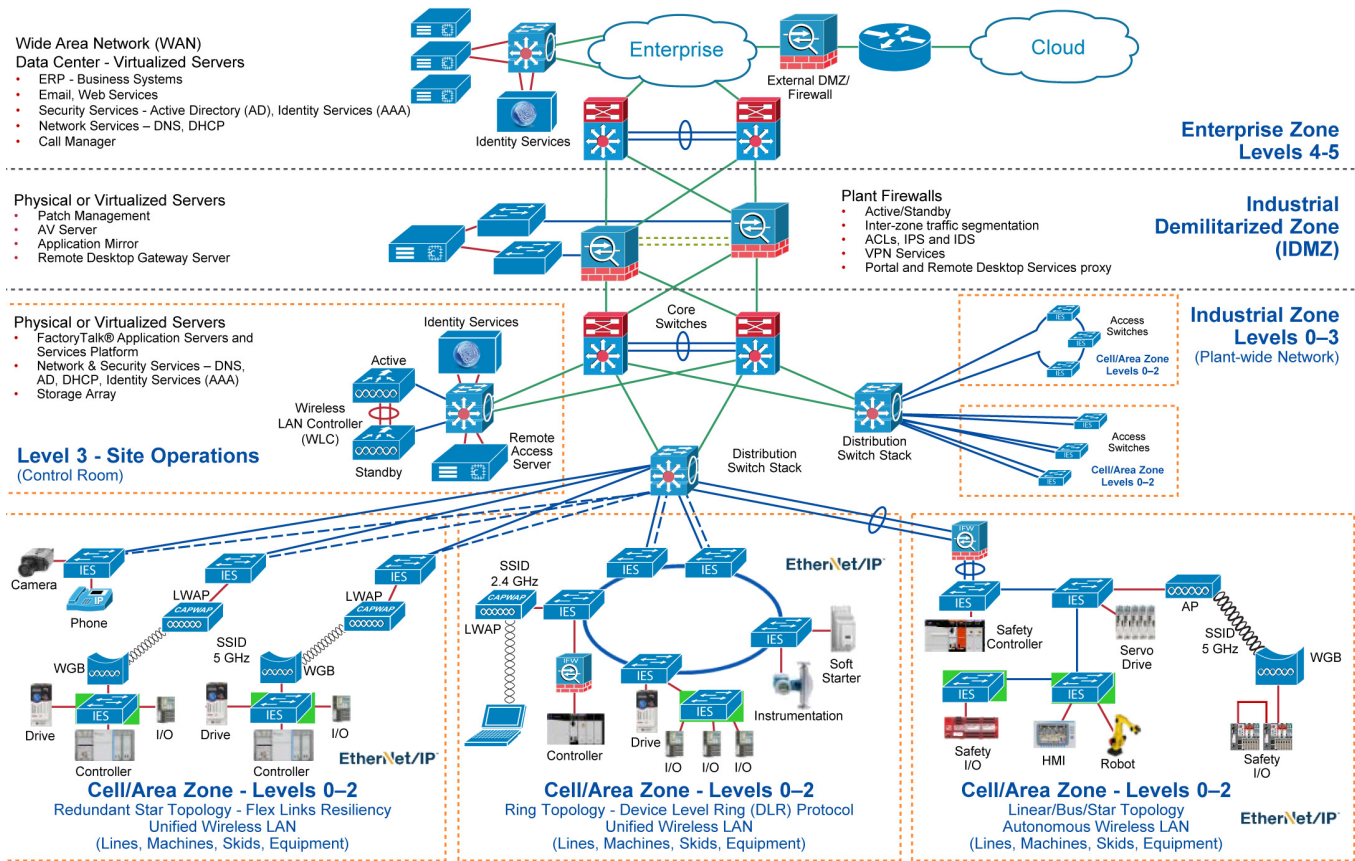
The Industrial Zone contains (Levels 0-3) IACS applications that maintain site level control of the lower level IACS applications and include reporting, scheduling, file and patch servers, and network services such as Network Time Protocol (NTP), Domain Name Server (DNS), Dynamic Host Configuration Protocol (DHCP) and Active Directory. One or more of the Cell/Area Zones (described above) actually reside within the Industrial Zone, as depicted in [Figure 1-1](#).

CPwE includes an additional zone, based on IEC-62443, sitting between the Industrial and Enterprise Zones called the Industrial Demilitarized Zone (IDMZ). The IDMZ provides a layer of separation between the traditional IT and OT operated areas of the network, allowing only traffic that is absolutely required to securely traverse the zone.

The Enterprise Zone, which contains Level 4 and Level 5, provides access to the Internet and higher-order network applications such as email, database, business-to-business (B2B) and business-to-consumer (B2C) applications and other non-critical resources. This zone, which is often seen as a source of security threats to the Industrial Zone resources, is typically managed by the IT department..

[Figure 1-2](#) depicts the CPwE architecture network topology. Notice the separation of the zones within the network, and the different IACS devices and applications residing in each.

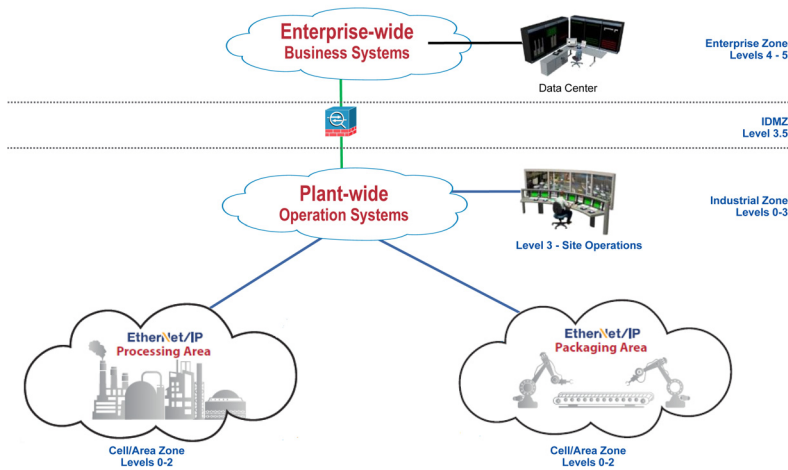
Figure 1-2 CPwE Architecture



Multiple Cell/Area Zones, each containing different types of connectivity topologies, reside at the edge of the IACS application and overall CPwE architecture. The lightly managed IES that are highlighted by a green rectangle representing where a lightly managed IES could be placed. As discussed in [Cell/Area Zone, page 1-5](#), several different supported topologies exist for connecting these lightly managed IES to the rest of the plant-wide network.

A simplified view of the logical CPwE architecture is depicted in [Figure 1-3](#). It shows how multiple Cell/Area Zones (for example, packaging and processing), all aggregated and communicating with IACS applications in higher levels of the CPwE Logical Model when necessary, are possible.

Figure 1-3 Simplified CPwE Architecture



Zooming in on the Industrial Zone (Levels 0-3) shows how a Cell/Area Zone (packaging) can in fact be sub-divided into multiple sub-zones (for example, Lines 1, 2 and 3), as shown in Figure 1-4, and then into further sub-zones for each function within each line (for example, labeling, filling and packaging).


Note

The overlapping IP subnets for each sub-zone are possible by using network address translation (NAT), as discussed in Chapter 2, “Lightly Managed IES in the Sub-Zone.”

Figure 1-4 Multiple Sub-Zones within a Cell/Area Zone

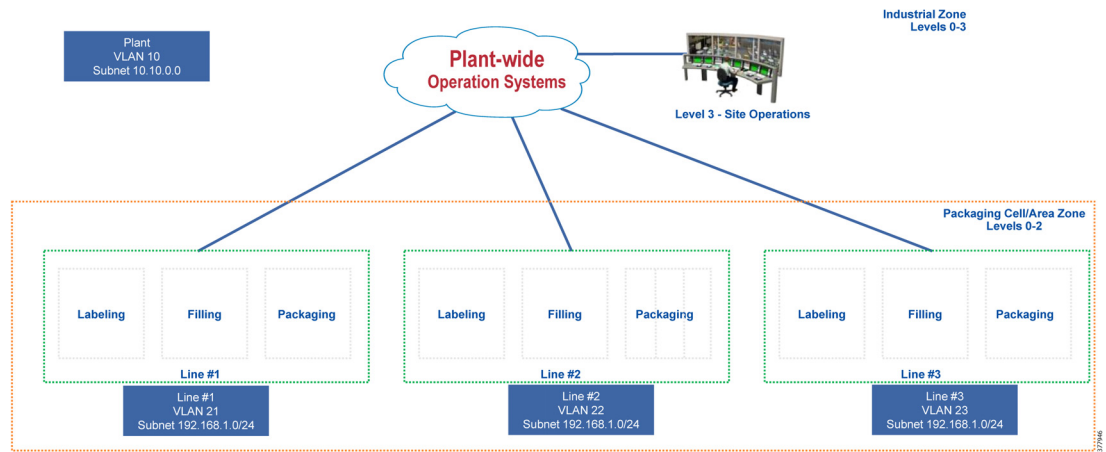
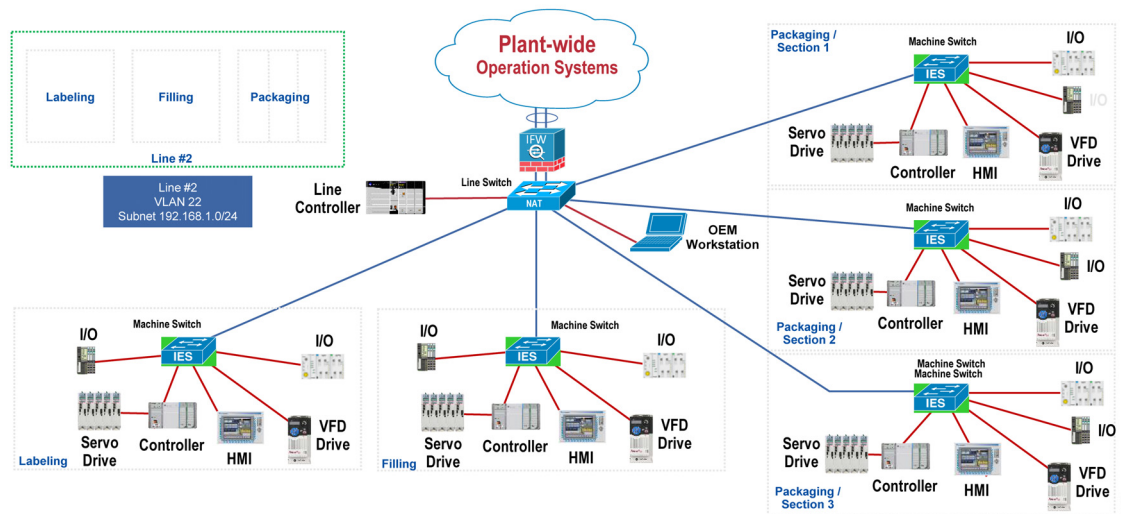


Figure 1-5 zooms further into the individual sub-zones for each packaging line. Zones and sub-zones allows plant operators to achieve scalability through a building block approach. A machine or skid are examples of how these sub-zones could be used.

Figure 1-5 Close-up View of Line 2 within the Packaging Cell/Area Zone



Once the process skid or machine is built and connected internally using a light managed IES, it can be used as a self-contained unit from the network perspective, ready to be installed on the plant floor by simply plugging it into the existing Cell/Area Zone network aggregation IES. As discussed in detail in [Chapter 2](#), “Lightly Managed IES in the Sub-Zone,” this approach helps produce secure, resilient and easily repeatable and scalable networks in the Industrial Zone.

Lightly managed IES are ideally deployed at the edge of the Cell/Area Zone of the CPwE architecture, specifically for sub-zones of OEM skids, machines and equipment, with some restrictions.

- Deploy lightly managed IES to aggregate single IACS devices on each downlink port. It is not recommended to cascade IACS devices with embedded switches off the lightly managed IES.
- The uplink port of the lightly managed IES should be connected to a fully managed IES or possibly an IACS device with embedded switch.
- Keep CIP motion servo drives closer to the controller, as shown in [Figure 1-5](#).
- Network services for the lightly managed IES are a subset of a fully managed IES—that is, resiliency, data prioritization and time synchronization.

Cell/Area Zone

Within the Cell/Area Zone, several options exist for network topologies to connect the end IACS devices to the higher level network. The following factors should be considered when choosing a topology for the access switches:

- Physical layout of the manufacturing environment. For example, a long conveyor belt system does not lend itself to a star configuration, but rather to a linear or ring topology.
- Availability/resiliency provided by multiple available paths for the traffic. If an IES or cable fails, alternative paths are helping to provide increased uptime.

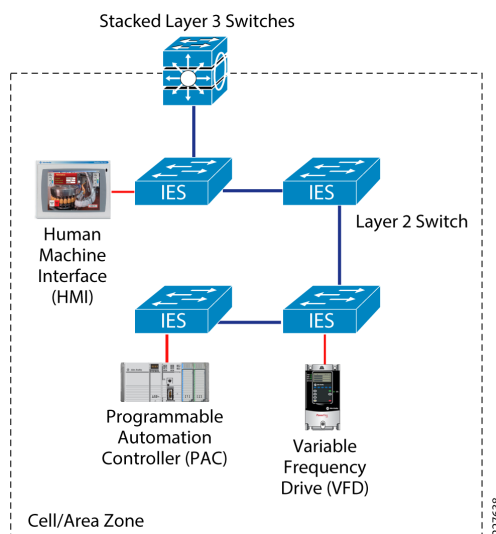
- Latency and jitter should be minimized in general, but especially when connected devices are relying on real-time communication for proper operation. This is done by applying data prioritization through quality of services (QoS), time synchronization through IEEE 1588 precision time protocol (PTP), and reducing the number of hops the traffic must traverse and by making sure the network devices in the path are not congested or over-utilized.

With these considerations in mind, the CPwE architecture supports the following topologies for the Cell/Area Zone, comprised of fully managed IES such as the Cisco IE 2000, Cisco IE 3000, Cisco IE 4000, Allen-Bradley Stratix 5400, Stratix 5700, Stratix 8000 and Stratix 8300 series industrial managed switches.

Linear Topology

In a linear topology, as shown in [Figure 1-6](#), Layer 2 access IES are connected in a chain, with one IES on the end of the chain connecting to a Layer 3 distribution switch. IACS devices and any other endpoints connect to the various IES in the chain of IES. This topology is very common for OEMs and is simple and easy to implement; however, it introduces a bottleneck at the connection to the Layer 3 distribution switch that can lead to degraded performance if the connection is oversubscribed. This topology does not factor in any resiliency. If a single IES or link fails, a loss of connectivity will occur for all IACS devices at or behind the point of failure.

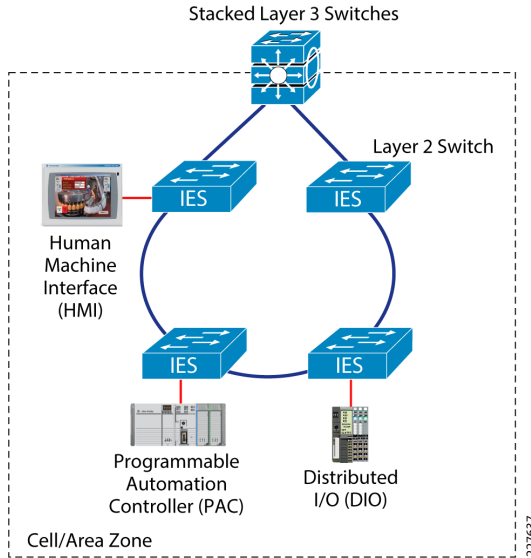
Figure 1-6 Linear Topology



Ring Topology

A ring topology, as shown in [Figure 1-7](#), improves on the linear topology by connecting both ends of the chain of Layer 2 IES back to an IES or the Layer 3 distribution switch as shown. This provides basic resiliency to the IES in the Cell/Area Zone by creating an alternate path for traffic to flow in the event of a single failure. In order to implement this topology, a loop prevention mechanism, such as Rapid Spanning Tree Protocol (RSTP), Resilient Ethernet Protocol (REP), or Device Level Ring (DLR) protocol (all IES ring), must be configured. Note that the lightly managed IES only supports RSTP.

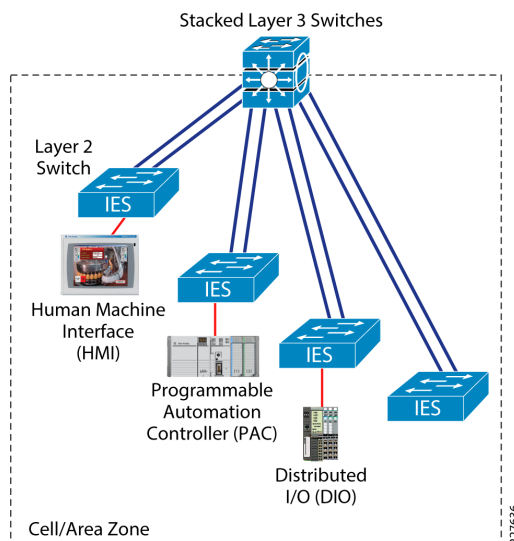
Figure 1-7 Ring Topology



Redundant Star Topology

A redundant star topology, as shown in [Figure 1-8](#), helps provide increased resiliency by connecting each Layer 2 access IES with dual uplinks to the Layer 3 distribution switch. In this topology, the number of hops between devices on different Layer 2 IES within the Cell/Area Zone are reduced. The design of the topology itself helps minimize any bottlenecks because each Layer 2 access IES has dedicated uplinks to the Layer 3 distribution switch.

Figure 1-8 Redundant Star Topology



A star topology without redundant links between the IES is also possible, and can help minimize the number of ports and cables required, at the expense of resiliency in the event of an uplink failure. This topology will still help minimize the number of hops required and bottlenecks that exist in some other topologies.