Physical Infrastructure Network Design for CPwE Logical Architecture

Successful deployment of a Converged Plantwide Ethernet (CPwE) logical architecture depends on a solid physical infrastructure network design that addresses environmental, performance, and security challenges with best practices from Operational Technology (OT) and Information Technology (IT). Panduit collaborates with industry leaders such as Rockwell Automation and Cisco to help customers address deployment complexities that are associated with plant-wide Industrial Ethernet. As a result, users achieve resilient, scalable networks that support proven and flexible logical CPwE architectures that are designed to optimize industrial network performance. This chapter provides an overview of the key recommendations and best practices to simplify design and deployment of a standard, highly capable industrial Ethernet physical infrastructure. It introduces key concepts and addresses common design elements for the other chapters, specifically:

- Mapping Physical Infrastructure to the CPwE Logical Network Design, page 2-2
- Key Requirements and Considerations, page 2-3:
  - Essential physical infrastructure design considerations
  - Physical Network Zone System cabling architecture, the use of structured cabling versus point-to-point cabling and network topology
  - M.I.C.E. assessment for industrial characteristics
  - Physical infrastructure building block systems
  - Cable media and connector selection
  - Effective cable management
  - Network cabling pathways
  - Grounding and bonding industrial networks
- Link Testing, page 2-14
- Wireless Physical Infrastructure Considerations, page 2-16
Physical Infrastructure for the Converged Plantwide Ethernet Architecture

Chapter 2  Physical Infrastructure Network Design for CPwE Logical Architecture

Mapping Physical Infrastructure to the CPwE Logical Network Design

Network designers are being challenged to implement a reliable, secure, and future-ready network infrastructure across the varied and harsh environments of industrial plants/sites. The networking assets must be placed across the plant/site with consideration of difficult environmental factors such as long distances, temperature extremes, humidity, shock/vibration, chemical/climatic conditions, water/dust ingress and electromagnetic threats. These factors introduce threats that can potentially degrade network performance, affect network reliability, and/or shorten asset longevity. Figure 2-1 shows the CPwE logical framework mapped to a hypothetical plant/site footprint.

Mapping CPwE Logical to Physical

The physical impact on network architecture includes:

- **Geographic Distribution** — The selection of IES and overall logical architecture is also heavily influenced by the geographic dispersion of IACS devices, switches, and compute resources, and the type and amount of traffic anticipated between IACS devices and switches. Figure 2-1 shows the network architecture superimposed over the building locations and the campus-type connectivity between buildings that may require the long-reach capabilities of single-mode fiber.

- **Brownfield or Legacy Network** — Additional design considerations are necessary to transition from or work alongside a legacy network. Existing installations have many challenges, including bandwidth concerns, poor grounding/bonding, inadequate media pathways, and limited space for new areas to protect networking gear. Additional cabling and pathways are often needed during the transition to maintain existing production while installing new gear.

- **Greenfield or New Construction** — Critical deadlines must be met within short installation time frames. In addition, installation risk must be minimized. Mitigating these concerns requires a proven, validated network building block system approach that uses pre-configured, tested, and validated network assets built specifically for the application.

Figure 2-1  Network Overlay on Building Locations
Physical Infrastructure Building Block Systems

Industrial physical infrastructure cabling systems and enclosures are often designed and built without attention to detail. Poorly deployed industrial networks frequently fail because growth, environmental impact, incompatibility and poor construction were not anticipated. A better approach is to specify tested, validated industrial network building block systems that are built for industrial network deployment. A standardized approach to industrial network design speeds deployment and reduces risk, leading to a cost-effective solution. Also, as the network is expanded, the consistency of standardized, validated systems is rewarded with lower maintenance and support costs.

Industrial physical infrastructure network building block systems comprised of integrated active gear can be deployed at most levels of the CPwE logical architecture. An industrial network building block system simplifies deployment of the network infrastructure required at each level of CPwE by containing the specified switching, routing, computing and/or storage elements required for a given zone housed in an enclosure, cabinet, or rack complete with cabling, cable management, identification, grounding, and power. These building block systems can be ordered pre-configured with all the components and parts to be assembled on site or as an integrated, ready-to-install solution.

Figure 2-2 shows various building block systems as they relate to the CPwE architecture. At the Level 3 Site Operations or IDMZ, the building block system may consist of a network, compute, and storage system and may be delivered as both pre-configured and integrated. The integrated solution is basically an appliance compute system, such as an IDC, which is described in more detail in Chapter 5, “Physical Infrastructure Deployment for Level 3 Site Operations.” In the Cell/Area Zone, a Physical Network Zone System (PNZS) with a DIN-mount IES can be deployed as a building block system. These building block systems can be both pre-configured and integrated. Building block systems in the Industrial Zone are addressed in Chapter 5, “Physical Infrastructure Deployment for Level 3 Site Operations.” The Cell/Area Zone building block systems are described in Chapter 4, “Physical Infrastructure Design for the Industrial Zone.”

Figure 2-2 Various CPwE Building Block Systems

Key Requirements and Considerations

The following are key considerations for helping to ensure the success of CPwE logical architecture:
• **Reach**—The distance the cable must travel to form the connections between the IACS device and IES ports. Distance includes all media between ports, including patch cables.

• **Industrial Characteristics**—Environmental factors that act upon networking assets and cabling infrastructure installed in the plant/site.

• **Physical Infrastructure Life Span**—IACS and the plant/site network backbone can be in service 20 years or more. Therefore, cabling, connectivity, and the PNZS must survive the expected lifespan. During its lifespan, changes and upgrades to the IACS served by the network can occur. As a result, the physical infrastructure and logical aspects of the network must be engineered to adapt.

• **Maintainability**—Moves, Adds, and Changes (MACs) have dependencies and may affect many Cell/Area Zones. Also, changes must be planned and executed correctly because errors can cause costly outages. Proper cable management practices, such as use of patch panels, secure bundling and routing, clear and legible permanent identification with accurate documentation, and revision control are vital to effective network maintenance and operation and rapid response to outages.

• **Scalability**—In general, the explosive growth of EtherNet/IP and IP connections strains legacy network performance. In addition, rapid IACS device growth causes network sprawl that can threaten uptime and security. A strong physical infrastructure design accounts for current traffic and anticipated growth. Forming this forecast view of network expansion simplifies management and guides installation of additional physical infrastructure components when necessary.

• **Designing for High Availability**—PNZSs can either be connected in rings or redundant star topologies to achieve high availability. Use of an uninterruptible power supply (UPS) for backup of critical switches prevents network downtime from power bumps and outages. New battery-free UPS technologies leverage ultra-capacitors with a wide temperature range and a long lifetime for IACS control panel and PNZSs. Intelligent UPS backup devices with EtherNet/IP ports and embedded CIP (ODVA, Inc. Common Industrial Protocol) object support allow for faceplates and alarm integration with IACS to improve system maintainability and uptime.

• **Network Compatibility and Performance**—Network compatibility and optimal performance are essential from port to port. This measurement includes port data rate and cabling bandwidth. Network link performance is governed by the poorest performing element within a given link. These parameters take on greater importance when considering the reuse of legacy cabling infrastructure.

• **EMI (Noise) Mitigation**—The risks from high frequency noise sources (such as variable-frequency drives, motors, power supplies and contractors) causing networking disruptions must be addressed with a defense-in-depth approach that includes grounding/bonding/shielding, well-balanced cable design, shielded cables, fiber-optics and cable separation. The importance of cable design and shielding increases for copper cabling as noise susceptibility and communication rates increase. Industry guidelines and standards from ODVA, Telecommunications Industry Association (TIA), and International Electrotechnical Commission (IEC) provide guidance into cable spacing, recommended connectors and cable categories to enable optimum performance.

• **Grounding and Bonding**—Grounding and bonding is an essential practice not only for noise mitigation but also to help enable worker safety and help prevent equipment damage. A well-architected grounding/bonding system, whether internal to control panels, across plants/sites, or between buildings, helps to greatly enhance network reliability and helps to deliver a significant increase in network performance. A single, verifiable grounding network is essential to avoid ground loops that degrade data transmission. Lack of good grounding and bonding practices risks loss of equipment availability and has considerable safety implications.

• **Security**—A security incident can cause outages resulting in high downtime costs and related business costs. Many industry security practices and all critical infrastructure regulations require physical infrastructure security as a foundation. Network security must address not only intentional security breaches but inadvertent security challenges. One example of an inadvertent challenge is the all-too-frequent practice of plugging into live ports when attempting to recover from an outage. A
successful security strategy employs logical security methods and physical infrastructure practices such as lock-in/block-out (LIBO) devices to secure critical ports, keyed patch cords to prevent inappropriate patches, and hardened pathways to protect cabling from tampering.

- **Reliability Considerations**—Appropriate cabling, connectivity, and enclosure selection is vital for network reliability, which must be considered over the design life span, from installation through operational phase(s) to eventual decommissioning/replacement. Designing in reliability protocols helps prevent or minimizes unexpected failures. Reliability planning may also include over-provisioning the cabling installation. Typically, the cost of spare media is far less than the labor cost of installing new media and is readily offset by avoiding outages.

- **Safety**—During the physical infrastructure deployment of IES, it is important to consider compliance with local safety standards to avoid electrical shock hazards. IT personnel may occasionally require access to industrial network equipment and may not be familiar with electrical and/or other hazards contained by PNZSs deployed in the industrial network. Standards such as National Fire Protection Association (NFPA) 70E provide definitions that help clarify this issue. Workers are generally categorized by NFPA-70E as qualified or unqualified to work in hazardous environments. In many organizations, IT personnel have not received the required training to be considered qualified per NFPA-70E. Therefore, network planning and design must include policies and procedures that address this safety issue.

- **Wireless**—The deployment of wireless in the PNZS requires design decisions on cabling and installation considerations for access points (APs) and Wireless Local Area Networks (WLANs). The PNZS backbone media selection and the selection of cabling for APs using Power over Ethernet (PoE) are critical for future readiness and bandwidth considerations. Another planning aspect in the wireless realm involves legacy cabling connected to current wireless APs. Many wireless APs deployed today are 802.11 a/b/g/n. As higher performance wireless standards such as 802.11ac are considered, it is important to understand that in some cases, existing cabling may not support increased uplink bandwidths necessary to support higher bit rate APs.

- **PoE**—PoE is a proven method for delivering commercial device power over network copper cabling. DC power, nominally 48 volts, is injected by the network switch. PoE switch capabilities have evolved to help deliver higher levels of power over standards-compliant Ethernet copper cabling. In time, the scope of PoE will expand to become a viable power source for other elements of industrial networks. Accordingly, consideration of conductor gauge and bundling density will grow in importance.

The above considerations are addressed in this chapter with various design, installation, and maintenance techniques, such as PNZS architecture and cabling methods (structured and point-to-point). The following sections describe these methodologies.

### Physical Zone Cabling Architecture

A common approach to deploying industrial Ethernet networks was to cable infrastructure as a home run from the IES back to a centralized IT closet switch, to an IDC, as shown in Figure 2-3. This was a reasonable approach because fewer cable runs existed and the Ethernet network was for IACS information only. As industrial networks grew in size and scope, with Ethernet becoming pervasive in many layers of the network (control and information), this home run methodology became difficult to scale and developed into a more expensive choice. Adding a new IES to the edge of the IACS may require a major cable installation to help overcome obstacles, route in pathways, and so on. In addition, this growth in home run networks has led to significant network cabling sprawl, impacting the reliability of the network. A better approach is a PNZS cabling architecture.
PNZS cabling architectures are well proven in Enterprise networks across offices and buildings for distributing networking in a structured, distributed manner. These architectures have evolved to include active switches at the distributed locations. For an IACS application as depicted in Figure 2-4, PNZS architecture helps mitigate long home runs by strategically locating IES around the plant to connect equipment more easily. The IES switches are located in control panels, IDF enclosures, and in PNZS enclosures. IDF enclosures house higher density 19" rack-mounted IES and related infrastructure while PNZSs house DIN rail-mounted IES and related infrastructure. PNZS architectures can leverage a robust, resilient fiber backbone in a redundant star or ring topology to link the IES in each enclosure location. Shorter copper cable drops can then be installed from each IDF or PNZS to control panels or on-machine IACS devices in the vicinity rather than back to a central IT closet.

TIA/EIA and related ISO/IEC standards support PNZS cabling architectures. A specific example of cabling support appears in Work Area Section 6.1 of TIA 568-C.1: "Work area cabling is critical to a well-managed distribution system; however, it is generally non-permanent and easy to change." These standards define work areas to be the locations where end device connections are made. For office buildings, the work area can be desks in offices and cubicles. In industrial settings, the work area is often in harsh areas on the machine or process line within Cell/Area Zones. These standards require structured cabling that eases management and enables performance by connecting equipment with patch cords to horizontal cabling terminated to jacks.
Structured and Point-to-Point Cabling Methods

Networked IACS devices can be connected in two ways for both copper conductor and optical fiber:

- Structured
- Point-to-point or Direct Attached

The preferred approach to deploy an industrial network is a standards-based (TIA-1005) structured cabling approach. Structured cabling has its roots in Enterprise and data center applications and can be reliable, maintainable and future-ready. Although point-to-point connectivity was the practice for slower proprietary networks for over 25 years, as networks move to higher-performing industrial Ethernet networks, weaknesses occur. In general, point-to-point is less robust than structured cabling because testable links don't exist, spare ports cannot be installed, and the use of stranded conductors means reduced reach. However, good use cases exist for point-to-point connectivity, such as connecting devices to a switch in a panel or short single-connection runs. For more detail on this topic, see Chapter 5, “Physical Infrastructure Deployment for Level 3 Site Operations.”

A PNZS cabling architecture addresses the following key considerations:

- **Reach**—Media selection is a significant aspect of network reach. Standards-compliant copper installations have a maximum link length of 100 m (328 feet). A fiber backbone can reach 400 m to 10 km along with the downlinks. PNZS cabling architecture has a unique ability to extend the practical reach of copper links beyond the 100 m home run copper cabling limitation. For an all-copper installation, the uplink can travel up to 100 m while the downlink can reach another 100 m for a total of 200 m.

- **Industrial Characteristics**—Media selection can be more granular and cost-effective in a PNZS architecture because only the necessary harsh environment drops from IES to IACS end devices are run in hardened media and connectivity.

- **Physical Network Infrastructure Life Span**—A PNZS cabling infrastructure has a longer potential life span than home run cabling. Where it may be too expensive to install state-of-the-art cabling to each IACS device in a home run scenario, a physical zoned architecture can have high-bandwidth uplinks in the backbone and downlinks/IES can be upgraded as needed, extending the effective life span of a PNZS cabling infrastructure.

- **Maintainability**—MACs are faster, easier, and less expensive with a PNZS architecture because only shorter downlink cables are installed, removed, or changed. A home run change requires greater quantities of cable and installation/commissioning labor.

- **Scalability**—A main feature for a PNZS architecture is the ability to help scale because spares are automatically included in the design with a structured cabling approach.

- **Designing for High Availability**—PNZSs can be connected in either a resilient ring or redundant star topology to achieve higher availability.

- **Network Compatibility and Performance**—A key feature of a PNZS-deployed IES is the ability to place the machine/skid IES in a dedicated enclosure with power always on. This helps eliminate network degradation to rebuild address tables caused by powering up/down IES in a control panel for production runs.

- **Grounding and Bonding**—A PNZS enclosure must have a grounding system with a ground bar tied to the plant ground network. In addition to addressing worker safety considerations, an effective grounding/bonding strategy's maximum transmission quality for the network.

- **Security**—PNZSs typically have a keyed lock to control access to the equipment housed within. In addition, port blocking and port lock-in accessories can secure IES ports, helping prevent problems that may be caused by inadvertent connections made when recovering from an outage.

- **Reliability Considerations**—A PNZS architecture with a structured cabling system helps deliver high reliability because it provides testable links. Built-in spare ports can resolve outages rapidly.
- **Safety**—An IES in a PNZS enclosure separates personnel from hazardous voltages in a control panel connected to the IES.
- **Wireless**—APs can be connected to IES in a PNZS architecture.
- **PoE**—IES can have PoE-powered ports. Typical applications for PoE include cameras, APs, and other IP devices that can use PoE power. PNZS cabling architectures can help easily support the addition of PoE devices from the IES while minimizing cost and complexity of a home run.

### M.I.C.E. Assessment for Industrial Characteristics

Cabling in IACS environments frequently is exposed to caustic, wet, vibrating, and electrically noisy conditions. During the design phase, network stakeholders must assess the environmental factors of each area of the plant where the network is to be distributed. A systematic approach to make this assessment, called Mechanical Ingress Chemical/Climatic Electromagnetic (M.I.C.E.), is described in TIA-1005A and other standards ANSI/TIA-568-C.0, ODVA, ISO/IEC24702 and CENELEC EN50173-3.

M.I.C.E. assessment considers four areas:
- **Mechanical**—Shock, vibration, crush, impact
- **Ingress**—Penetration of liquids and dust
- **Chemical/Climatic**—Temperature, humidity, contaminants, solar radiation
- **Electromagnetic**—Interference caused by electromagnetic noise on communication and electronic systems

M.I.C.E. factors are graded on a severity scale from 1 to 3, where 1 is negligible, 2 is moderate and 3 is severe (see Figure 2-5). Understanding exposure levels helps to enable the appropriate connectivity and pathways are specified to guarantee long-term performance. For example, exposure to shock, vibration, and/or UV light may require use of armored fiber cabling suitable for outdoor environments.

![Figure 2-5 TIA-1005A MICE Criteria](image)

It is important to understand that M.I.C.E. rates the environment, not the product. The result of a M.I.C.E. evaluation is used as a benchmark for comparing product specifications. Each product used in the system design should at least be equal to or exceed the M.I.C.E. evaluation for that space.

M.I.C.E diagramming allows the design to balance component costs with mitigation costs to build a robust, yet cost-effective system. The process starts by assessing the environmental conditions in each Cell/Area Zone within the Industrial Zone. A score is determined for each factor in each area. For example, the
Machine/Line is a harsh environment with a rating of M3I3C3E3. Since the E factor, electromagnetic, is high, the likely cabling would be optical fiber. Since the other factors, M, I and C, are high as well, the cabling would require armor and a durable jacket. Figure 2-6 shows an example of M.I.C.E. diagramming.

![Figure 2-6 Sample Environmental Analysis Using the M.I.C.E. System](image)

### Cable Media and Connector Selection

Many considerations exist for media selection, such as reach, industrial characteristics, life span, maintainability, compatibility, scalability, performance, and reliability, all of which depend on the construction of the cable. The four main options for the cable construction are:

- **Media**—Copper (shielded or unshielded, solid or stranded) or optical fiber
- **Media Performance**—For copper, Cat 5e, Cat 6, Cat 6A, Cat 7; for fiber-optic cable, OM1, OM2, OM3, OM4, single-mode
- **Inner Covering/Protection**—A number of media variants are designed to allow copper and fiber-optic cable to survive in harsh settings. These include loose tube, tight buffer, braided shield, foil, aluminum-clad, and all-dielectric conduit.
- **Outer Jacket**—TPE, PVC, PUR, PE, LSZH

In addition, regulations and codes may govern the use of cabling in certain areas based on characteristics such as flammability rating, region deployed (such as low-smoke zero-halogen in Europe) and voltage rating (600 v). Table 2-1 shows some general cable characteristics.

### Table 2-1  General Cable Characteristics

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Copper Cable</th>
<th>Multimode Fiber</th>
<th>Single-mode Fiber</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reach (maximum)</td>
<td>100 m</td>
<td>2,000 m (1 Gbps)</td>
<td>10 km (1 Gbps)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>400 m (10 Gbps)</td>
<td>10 km (10 Gbps)</td>
</tr>
<tr>
<td>Noise Mitigation Option</td>
<td>Foil shielding</td>
<td>Noise immune*</td>
<td>Noise immune*</td>
</tr>
<tr>
<td>Data Rate (Industrial)</td>
<td>100 Mbps (Cat 5e)</td>
<td>1 Gbps</td>
<td>1 Gbps</td>
</tr>
<tr>
<td></td>
<td>1 Gbps (Cat 6)</td>
<td>10 Gbps</td>
<td>10 Gbps</td>
</tr>
<tr>
<td></td>
<td>10 Gbps (Cat 6a)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cable Bundles</td>
<td>Large</td>
<td>Small</td>
<td>Small</td>
</tr>
<tr>
<td>Power over Ethernet (PoE)</td>
<td>Yes</td>
<td>Yes, with media conversion</td>
<td>Yes, with media conversion</td>
</tr>
</tbody>
</table>

*Fiber-optic media is inherently noise immune; however, optical transceivers can be susceptible to electrical noise.*
Fiber and Copper Considerations

When cabling media decisions are made, the most significant constraint is reach (see Table 2-1). If the required cable reach exceeds 100 m (328 feet), then the cable media choice is optical fiber cable. Copper Ethernet cable is limited to a maximum link length of 100 m. However, other considerations may be important for distances less than 100 m, such as EMI, for which fiber-optic cable is preferred due to its inherent noise immunity. Another consideration is the fact that switch uplinks connected with optical fiber help to provide faster convergence after a switch power interruption, lessening the duration of the network outage. In a comparison of data rates, copper and fiber are similar for typical industrial applications (see Table 2-1); however, other higher performing optical fiber cables are available for high demand networks.

Network life span is a significant consideration for media performance. For instance, installing a network with Cat 5e cabling is not recommended if growth is expected within 10 years, especially if the network will be transporting video. If the expectation is 10 or more years of service, a higher performance category cabling (such as Cat 6a) should be considered.

Optical Fiber Cable Basics

Single-mode and multimode are the two fiber types. Multimode fiber has glass grades of OM1 to OM4. When selecting any optical fiber, the device port must first be considered and must be the same on both ends, (that is, port types cannot be mixed). In general, the port determines the type of fiber and glass grade. If the device port is SFP, it is possible to select compatible transceivers and the optimal transceiver for the application. Also, considerations for number of strands, mechanical protection, and outer jacket protection exist. See Chapter 5, “Physical Infrastructure Deployment for Level 3 Site Operations” for a more detailed explanation of optical fiber.

Optical Fiber Link Basics

The optical fiber link (that is, channel) is formed with a patch cord from the device to an adapter. Adapters hold connector ends together to make the connection and are designed for a single fiber (simplex), a pair (duplex), or as a panel containing many adapter pairs. One end of the adapter holds the connector for the horizontal cable that extends to an adapter on the opposite end. A patch cord from the end adapter connects to the device on the opposite end, completing the link. Various connectors and adapters exist in the field where Lucent Connector (LC) is the predominate choice due to the SFP and performance. However, many legacy devices may have older-style Subscriber (SC) or Straight Tip (ST) connectors. See Chapter 5, “Physical Infrastructure Deployment for Level 3 Site Operations” for a more detailed explanation of connectors and adapters.

Copper Network Cabling Basics

Copper network cabling performance is designated as a category (that is, Cat). Higher category numbers indicate higher performance. Currently, the predominant choice is Cat 6 (especially for video applications) where higher categories are beginning to be deployed. The copper conductor is typically 23 American wire gauge (AWG), although smaller diameter 27 AWG may be used in some cases for patching. Larger gauge wires are available and the conductor can be stranded or solid. Typically, a solid conductor is used to help achieve maximum reach for the horizontal cable/permanent links, while a stranded conductor is used for patching or flex applications. Different strand counts are available in stranded Ethernet cable, and higher strand counts are for high flex applications. Another consideration is EMI shielding. Various shielding possibilities can be employed to suppress EMI noise with foil and/or braided outer jacket or pairs with foil. Mechanical protection and outer jacket protection also must be considered when selecting copper network cables. See Chapter 4, “Physical Infrastructure Design for the Industrial Zone” for a more detailed explanation of copper network cabling.
Copper Network Channel Basics

A structured copper network channel is formed with a patch cord plugged into the device and the other end of the patch cord plugged into a jack in a patch panel. The jack is terminated to solid copper horizontal cable that extends to a jack on the other end. A patch cord is plugged into the jack, and the other end of the patch cord is plugged into the device, completing the channel (see Figure 2-7). Two predominant, proven connectors or jacks exist for copper industrial networks:

- **RJ45**—Part of validated and tested patch cord or field terminable
- **M12**—Over-molded patch cord or field terminable

The RJ45 plug and jack have been adapted for industrial networks, where they can be deployed in a DIN patch panel. If the connector is located inside a protected space or enclosure, standard RJ45 connectivity is preferred. The plug could be part of a tested and validated patch cord or a durable field-attachable plug. The RJ45 bulkhead versions are available for quick connect/disconnect and versions that are sealed from ingress of liquids and particulates. The M12 is a screw-on sealed connector well suited for splashdown and harsh environments and can be a two-pair D-Code or a four-pair X-Code. See Chapter 4, “Physical Infrastructure Design for the Industrial Zone” for a detailed explanation of copper network cabling and connectivity.

Figure 2-7  Simplified Example of Copper Structured Cabling

---

Cable Management

Proper cable management helps to provide a converged network with high system performance, availability, and reliability across all zones of the CPwE architecture. Cable management impacts MACs, signal performance and cable life in infrastructure locations that range from harsh industrial areas to air conditioned, protected areas. Cable management features include:

- **Bend Radius Control**—Maintaining the cable bend radius (that is, change in direction) within specifications minimizes signal attenuation for both fiber and copper. All bends should be controlled from port to port with slack spools, pathway waterfalls, enclosure spools or features built into products. Cable runs through conduit must maintain bend radius, and some conduit fittings may not be appropriate.

- **Panel, Rack, and Cabinet Cable Routing and Protection**—Cable routing and protection is essential in server cabinets, switch racks, enclosures, control panels, and so on. For cabinets and racks, cables must be managed both horizontally (such as D rings) and vertically (such as cabinet fingers). Network cables in enclosures and control panels should be routed in duct and may need shielding from noise. Standard distribution fiber cabling may need to be routed through a corrugated loom tube or conduit for protection.

- **Slack Management**—Slack cabling should be properly coiled and secured to help prevent tangling, snagging, and poor appearance.
• **Bundling**—Cable ties specific for network cables, such as hook and loop or elastomeric cable ties, should be used only to prevent cable deformation that can lead to signal loss.

• **Identification**—Identification can be accomplished with printed labels and color coding of cables, cable ties, labels and icons. Intuitive and standard methods reduce errors for moves/adds/changes and aid in troubleshooting by helping to identify cabling and upgrade planning.

Cable inside PNZS architecture, freestanding enclosures, and control panels are addressed in Chapter 4, “Physical Infrastructure Design for the Industrial Zone.”. See Chapter 5, “Physical Infrastructure Deployment for Level 3 Site Operations” for information about cable management for an IDF and routing to the Cell/Area Zone. See Chapter 5, “Physical Infrastructure Deployment for Level 3 Site Operations” for information on network cable management for switches, servers, storage, and other gear.

### Network Cabling Pathways

Pathways for cables are critical for distributing copper and fiber cabling securely across the plant/site while protecting it from physical infrastructure threats. The TIA-1005 standard, the *ODVA Media Planning and Installation Manual*, and other guides provide recommendations on pathways, including cable spacing and installation guidance to minimize risks from environmental threats. Several options of routing cables via pathways simplify deployment using best practices for various environments across the plant. Figure 2-8 describes some of these options.

**Figure 2-8 Pathway Considerations**

<table>
<thead>
<tr>
<th>Installation Consideration</th>
<th>J-Hook</th>
<th>Wyr-Grid®</th>
<th>FiberRunner®</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable Protection Environment</td>
<td>Mild</td>
<td>Moderate</td>
<td>Moderate to harsh</td>
</tr>
<tr>
<td>Cable Density</td>
<td>Light to medium</td>
<td>Medium to heavy</td>
<td>Light to heavy</td>
</tr>
<tr>
<td>Applicable in Constrained Spaces</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Installation Complexity</td>
<td>Simple</td>
<td>Moderate</td>
<td>Moderate to strong</td>
</tr>
<tr>
<td>Ease of Moves, Adds, Changes</td>
<td>Simple</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

The simplest and lowest-cost pathways are J-Hooks. J-Hooks can be mounted to a wall, beam, or other surface. Network cables are held in place by the hook feature and are often secured with a cable tie. The J-Hook hook feature is designed to achieve proper bend radius control when transitioning down. J-Hook systems should be used with cables with enough rigidity to have an acceptable bend between spans and are suitable for a small bundle. Standard fiber distribution cable is not suitable for J-Hooks unless supported by corrugated loom tube.

When routing large or many cable bundles, a tray or wire basket can be installed overhead to form a solid and continuous pathway. Since cabling is exposed to the plant environment, cable jackets must be specified for the environment. An enclosed tray, such as a fiber tray, provides a high level of environmental protection for light to heavy cable densities. For the highest protection with few network cables, conduit is the preferred choice and care must be taken to maintain the proper bend radius.
Grounding and Bonding Industrial Networks

A proper grounding and bonding system is essential for personnel safety, equipment protection, equipment operation, and reliable network communication. An appropriately designed grounding and bonding system is intentional (designed and specified), visually verifiable (such as green and yellow cable jacket), and consists of adequately sized conductors to safely handle expected electrical currents and dissipate electrical noise.

Earthing, Grounding, and Bonding

The terms earthing, grounding, and bonding are often interchanged; however, each has a specific meaning:

- **Earthing**—Connecting to earth or a conductive body that is connected to earth
- **Grounding**—The point at which all bonded conductors come together at earth
- **Bonding**—Electrically connecting all exposed metallic items not designed to carry electricity, like enclosures, trays, racks, and cable armor to a ground

Grounding for Safety

Cable trays, enclosures, communication/control cable, chassis, or metallic surfaces can be inadvertently energized by a power cable short or lightning, potentially leading to shock that causes injury or equipment damage. A dedicated grounding conductor safely directs the hazardous stray electrical current to ground.

Ground Loop

A ground loop is an unwanted current in a conductor connecting two points that should be at the same potential. Ground loops result from multiple ground connections to earth, creating a potential difference.

Grounding and Bonding for Network Communication

Stray electrical noise and ground loops can disrupt electronic equipment, especially Ethernet gear. Varying methods exist to suppress these elements. Unshielded Twisted Pair (UTP) Ethernet cable has limited noise cancellation. Shielded Twisted Pair (STP) cable is more effective because it has a metallic sheath that is bonded to dissipate the electrical noise. The challenge is to maintain equipotential, and an equalizing potential conductor (EPC) may be necessary. Network cable protected by a grounded noise shield or shielded duct is designed to dissipate electrical noise in an enclosure. Also, a flat, wide bonding strap bonded to the enclosure door and side panels dissipates noise more effectively than standard cable (skin effect of high frequency noise). The goal is to implement a single ground reference throughout.

Equalizing Potential Conductor

If a potential difference exists between the cable shield and equipment ground greater than one volt, a ground loop can form, disrupting transmission. An EPC restores ground and limits potential differences between network segments. (See Figure 2-10).
Applicable Grounding and Bonding Standards

- NEC Article 250 and 645.15
- IA 607-B and 1005
- BICSI
- Industrial Grounding Network

Figure 2-10  Industrial Grounding Network

Link Testing

Link testing verifies baseline performance and helps with efficient network maintenance over its life span. Two forms of link testing are used:

- **Static**—Typically used at installation and commissioning phases and some maintenance tasks
- **Dynamic**—Network monitoring solution that resides on the network and provides real-time performance data and analytics

Static link testing (see Figure 2-11) involves test instrumentation attached to each link.

Figure 2-11  TIA568 Static Link Testing Set Up

This step is important at installation and commissioning of the network to confirm that any challenges relating to media installation are uncovered before the network moves into the operational phase. Performance measurements are made and recorded for each link. This baseline performance information is archived and can greatly speed diagnosis and correction. Finally, having the installer provide link test data as part of acceptance criteria can greatly reduce the likelihood of billing disputes if the test data is included as acceptance criteria.
Dynamic link testing solutions reside in the network and provide real-time monitoring and analysis of network performance. Dynamic solutions should include discovery and visualization functions in addition to staple functions such as bandwidth indication. Visualization is especially important as a maintenance adjunct to expedite correction of challenges as they are discovered. Many networks are mixture of various manufacturers' equipment, therefore, it is advisable to choose a vendor-neutral solution.

A key advantage of dynamic link testing is that many conventional tools are unable to detect some forms of network interruptions, especially intermittent challenges and/or challenges that manifest only under actual network operation. Dynamic monitoring solutions provide daily around-the-clock performance data and analysis, permitting trending and other forms of long-term analytics that can weed out difficult challenges. Another advantage of dynamic solutions is gaining the ability to detect and respond quickly to issues such as duplicate IP addresses, device or cable moves, connection or applications faults, and unauthorized connections.

Channel

All segments in the cabling system must be subject to link loss testing. A segment consists of media and connectivity, like connectors, adapters, splice points, and so on, joining different segments of the network. The link testing measurement includes the insertion loss of connectors at the panels (termination bulkheads) on either end of the link, but excludes the attenuation of any short jumpers attached to terminating electronics or to the performance of the connector at the equipment interface. Although the channel is defined as all the components in the permanent link and additional jumpers attached to terminating electronics, only the permanent link is measured against the standard's expectations.

ISO/IEC and TIA standards define the permanent link as the permanent fiber cabling infrastructure over which the active equipment must communicate. This excludes equipment patch cords to connect the active network devices in control panels or the patch cords in other switch patching areas. ISO/IEC and TIA standards define specific permanent link testing to verify the performance of the fixed (permanent) segments of installed cabling as accurately as possible.

The permanent link segment constitutes the cabling infrastructure: the fiber cabling and the connectivity that joins patch panel to patch panel, and the connectivity residing in the patch panels. A permanent link excludes any patch cords to the line-terminating electronics. Testing of a permanent link should be completed before any patch cords are connected to the panels.

Unless otherwise stated, all permanent link loss testing should be performed with a handheld power meter/source. This equipment measures link attenuation, which is the most important performance parameter when installing components.

For backbone cabling, permanent link testing is recommended for all links at both specified wavelengths. Multimode fibers must be tested in one direction at 850 nm (the SX operating window) and at 1300 nm to account for fiber attenuation differences due to wavelength and to reveal potential issues associated with installation. Similarly, for LX applications, window testing should first be performed at the application operating wavelength and the second window at the higher wavelength (1550 nm).

Significant differences in link test results between these windows can aid in troubleshooting failing links. Link failures predominately at the first window may indicate challenges with connector systems, while second window failures may indicate fiber macrobend sites in the installed cabling; that is, large-radius bends in the cable that can cause incremental attenuation.

To verify that fiber links are tested and cleaned properly according to the standards, Panduit provides the following best practices documents:
Wireless Physical Infrastructure Considerations

Secure and robust wireless access networks have become a necessity in industrial environments. As these networks are being stretched to maximum capacity with various new trends, it is important to consider during the planning and design stages the specific tasks that must be accomplished wirelessly. It is also important to have a forecast of future growth. Currently, two main client applications are served wirelessly: mobility and workgroup bridge (WGB) communications. This section discusses important topics relating to the physical infrastructure and deployment of wireless APs.

Site Survey

The first step to the design and successful operation of a WLAN network is the site survey. The survey characterizes and identifies the RF environment over the entire coverage area to confirm that performance requirements of the wireless APs are met. The survey can be conducted using measured data from APs arranged throughout the coverage area, or may be predictive where a computer model of the detailed coverage area is created and performance is determined.

Wireless Spectrum

The 5 GHz frequency band is recommended for industrial wireless applications. Because of the limited number of channels and a much higher chance of interference, the 2.4 GHz band is not recommended for critical IACS applications, such as machine control. However, 2.4 GHz band can be used for personnel access and low throughput, non-critical applications. Use only channels 1, 6, and 11 in the 2.4 GHz band. Use of non-standard channels or more than three channels in a 2.4 GHz band will cause adjacent channel interference and lower throughput.

The guidelines constantly change, therefore it is important to refer to the local regulatory authority and product documentation for the most recent compliance information and channel availability for a particular country.

Many sources of interference are intermittent, and new sources may appear over time. It is important to proactively monitor for radio interference in the industrial environment, before and after the deployment. Properly defined and enforced spectrum policy on site is critical for interference prevention.

Wireless Coverage

The AP coverage area where the desired data rate can be supported depends on many factors and can only be determined during the site survey. Changes in the environment and interference levels also dynamically change the coverage.
For EtherNet/IP applications, confirm that minimum levels of parameters such as Received Signal Strength Indication (RSSI) and Signal to Noise Ratio (SNR) are met. For CIP Sync traffic, the cell coverage area should be designed to sustain a 54 Mbps data rate.

RF Parameters

Spatial Division Multiplexing has limited benefit for the real-time EtherNet/IP traffic. Multiple spatial streams make communication less reliable, dependent on higher SNR, and more susceptible to multipath fading. Single spatial stream is more suitable for EtherNet/IP control communication. In this case, 20 MHz channel width (no channel bonding) is recommended with IACS applications.

It is not always desirable to use the maximum transmit power in the Cell/Area Zone. Limiting transmit power creates smaller coverage Cell/Area Zone size with less signal propagation outside the intended area and less chance for distant clients to join the AP.

Note

For more information, see the Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide at the following URLs:


Location of Wireless Access Points

The location of wireless access points are determined by wireless coverage and performance modeling software. These findings are then validated during the commissioning phase. On occasion, thorough initial testing of the WLAN during the commissioning phase reveals that the location of the AP has to be moved slightly to accommodate building layouts, obstacles, and so on, that were not considered. Typically, these interferences were changed or moved after the time of software modeling. The structured cabling used to connect the AP to the IES port can be designed considering the need for change by the use of patch cords connecting the AP to fixed equipment outlets (EO) that are connected to the horizontal cable run. This concept is introduced in TIA Technical Services Bulletin (TSB) 162-A, *Telecommunications Cabling Guidelines for Wireless Access Points*.

TSB-162-A bases initial design on the deployment of APs on a square grid model, and emphasizes that after initial design, software prediction of performance should be conducted to determine any deviation of AP locations from this grid. Frequently, in larger plant/site deployments, vertical structural beams that support the roof and give strength to the overall building are used, and these form a potential array of supporting locations for APs. These beams also can provide convenient support locations for the PNZS enclosure located in the Cell/Area Zone.

Cabling for Wireless Access Points

From the original release in 1997 of IEEE 802.11 standards for WLAN, IEEE 802.11-1997 and supported data rates of up to 2 Mbps, the IEEE has been developing technology and WLAN systems capable of increasingly higher data rates. Through progression of 802.11b, 802.11g, 802.11a and 802.11n, the most recent standard to be released is IEEE 802.11ac. Up until IEEE 802.11n, backhaul data rates were less than 1 Gbps, which indicates that Cat 5e or 6 cabling could be used. With the release of IEEE 802.11ac, however, Generation 2 APs (often referred to as the second wave) will experience the backhaul rate increasing to over
1 Gbps. Therefore, it will be necessary to deploy Cat 6A cabling that will support data rates of up to 10 Gbps and is recommended for new deployments. Some references have been made to the use of two Cat 6A cables for each AP, thereby increasing reliability and availability in the event of channel failure. The IEEE standards development groups are establishing lower data rates that can support Wave 2 data rates, focusing on the use of 2.5 Gbps and 5 Gbps and using existing Cat 5e and 6 cabling. The standards are still in development at the time of writing and will be reviewed closer to the time of WLAN design and deployment. Since the original release of IEEE 802.11 standards for WLAN, new technology includes WLAN systems capable of increasingly higher data rates. The current standard is IEEE 802.11ac. Until the previous standard, IEEE 802.11n, backhaul data rates were less than 1 Gbps, therefore Cat 5e or 6 cabling could be used. With the release of IEEE 802.11ac, however, second-generation APs (often referred to as the second wave) will experience the backhaul rate increasing to over 1 Gbps. As a result, it will be necessary to deploy Cat 6A cabling, which supports data rates of up to 10 Gbps and is recommended for new deployments. Two Cat 6A cables can be used for each AP, thereby increasing reliability and availability if channel failure occurs. The IEEE standards development groups establishing lower backhaul data rates that can support second wave APs, focusing on the use of 2.5 Gbps and 5 Gbps and using existing Cat 5e and 6 cabling. The standards are still in development at the time of writing and will need to be reviewed closer to the time of WLAN design and deployment.

Power over Ethernet

Copper cabling used for the backhaul for the AP can also be used to supply power to the AP with PoE. PoE has been developed by the IEEE standards bodies, and currently two versions exist:

- IEEE 802.3af, delivering up to 12.95 watts at the end of a maximum-length channel
- IEEE 802.3at, delivering up to 25.5 watts at the end of a maximum-length channel.

The detailed design of the cabling must be considered since higher data rate APs typically require a higher power feed, and on occasions may require more power than would be available from one PoE source. In this case, two cables would be required and power combining would be used in the AP.

Access Points in Harsh Environments

APs used in plant/site deployments are frequently located in harsh, or even outdoor, environments. In these cases, the APs must be placed into a protective enclosure. Consideration of the design of the enclosure must be made, since the proximity of additional material associated with an enclosure made from metal can affect the radiation pattern and hence the coverage behavior of the AP. In addition, the antennas must be located outside the enclosure or the enclosure must include an RF-transparent window.
Wireless Physical Infrastructure Considerations