Physical Infrastructure for the Converged Plantwide Ethernet Architecture

Application Guide

February 2023

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 using proven designs that can facilitate quicker deployment while helping to minimize risk in deploying new technology. CPwE is brought to market through a CPwE ecosystem consisting of Cisco, Panduit, and Rockwell Automation emergent from the strategic alliance between Cisco Systems and Rockwell Automation.

Resilient plant-wide or site-wide network architectures play a pivotal role in helping to confirm overall plant/site uptime and productivity. Industrial Automation and Control System (IACS) application requirements such as availability and performance drive the choice of resiliency technology. A scalable, holistic, and reliable plant-wide or site-wide network architecture is composed of multiple technologies (logical and physical) deployed at different levels within plant-wide or site-wide architectures. When selecting resiliency technology, various IACS application factors should be evaluated, including physical layout of IACS devices (geographic dispersion), recovery time performance, uplink media type, tolerance to data latency and jitter and future-ready requirements.

Physical Infrastructure for the Converged Plantwide Ethernet Architecture, which is documented in this Application Guide, outlines several physical layer use cases for designing and deploying reliable OEM, plant-wide or site-wide architectures for Industrial Automation and Control System (IACS) applications.

Release Notes

This section summarizes this February 2023 release:

- Standalone fiber optic cabling guide merge with this physical infrastructure guide

- Expanded coverage of industrial wireless guidance

- Inclusion of SPE (Single Pair Ethernet) and Ethernet-APL

- Additional topics added: minimum/maximum cable length, high speed SFPs, and cable entry systems

- Updated part numbers

Document Organization

This document is composed of the following chapters and appendices:

	Description
CPwE Physical Layer Overview	Provides an overview of CPwE Physical Layer and the uses cases in this release.
Physical Infrastructure Network Design for CPwE Logical Architecture	Introduces key concepts and addresses common design elements for mapping the physical infrastructure to the CPwE Logical Network Design, key requirements and considerations, link testing, and wireless physical infrastructure considerations.
Physical Infrastructure Design for the Cell/Area Zone	Describes the Cell/Area Zone physical infrastructure for applications and the locations for the Allen-Bradley® Stratix® Industrial Ethernet Switches (IES), including IES in control panels and/or PNZS components.
Physical Infrastructure Design for the Industrial Zone	Describes the physical infrastructure for network distribution across the Industrial Zone (one or more Cell/Area Zones) through use of Industrial Distribution Frames (IDF), industrial pathways, and robust media/connectivity.
Physical Infrastructure Deployment for Level 3 Site Operations	Describes the physical infrastructure for Level 3 Site Operations, including Industrial Data Centers (IDCs) for compute, storage, and switching resources for software and services within industrial operations.
References	Links to documents and websites that are relevant to this Application Guide.
Acronyms and Initialisms	List of acronyms and initialisms used in this document.

For More Information

More information on CPwE Design and Implementation Guides can be found at the following URLs:

- Rockwell Automation site:

  – https://www.rockwellautomation.com/en-us/capabilities/industrial-networks/network-architectures.html

- Cisco site:

  – http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

- Panduit site:

  – www.panduit.com/cpwe

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 Sync™, CIP Security™, and DLR, see odva.org at the following URL:

- http://www.odva.org/Technology-Standards/EtherNet-IP/Overview

CPwE Physical Layer Overview

This chapter includes the following major topics:

The prevailing trend in Industrial Automation and Control System (IACS) networking is the convergence of technology, specifically IACS operational technology (OT) with information technology (IT). Converged Plantwide Ethernet (CPwE) helps to enable IACS network and security technology convergence, including OT-IT persona convergence, by using standard Ethernet, Internet Protocol (IP), network services, security services, and EtherNet/IP. A reliable and secure converged OEM, plant-wide or site-wide IACS architecture helps to enable the Industrial Internet of Things (IIoT).
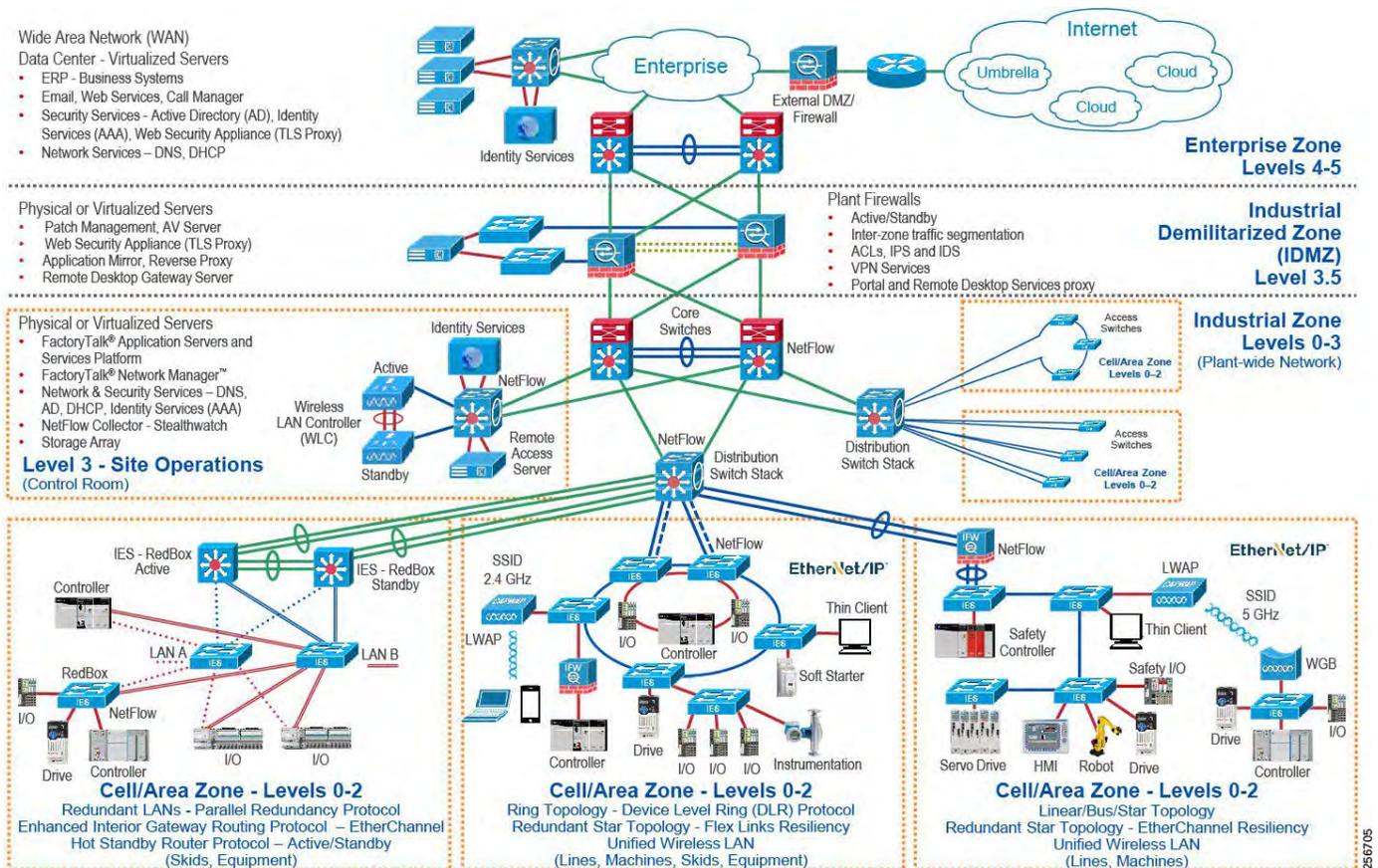
CPwE Overview

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 architectures (Figure 1-1) were architected, tested, and validated to provide design and implementation guidance, test results, and documented configuration settings. This can help to achieve the real-time communication, reliability, scalability, security, and resiliency requirements of modern IACS applications. The content and key tenets of CPwE are relevant to both OT and IT disciplines. CPwE key tenets include:

- Smart IIoT devices—Controllers, I/O, drives, instrumentation, actuators, analytics, and a single IIoT network technology (EtherNet/IP), facilitating both technology coexistence and IACS device interoperability, which helps to enable the choice of best-in-class IACS devices.

- Zoning (segmentation)—Smaller connected LANs, functional areas, and security groups.

- Managed infrastructure—Managed Allen-Bradley Stratix industrial Ethernet switches (IES) and Cisco Catalyst® distribution/core switches.

- Resiliency—Robust physical layer and resilient or redundant topologies

with resiliency protocols.

- Time-critical data—Data prioritization and time synchronization via CIP Sync and IEEE-1588 Precision Time Protocol (PTP).

- Wireless—Unified wireless LAN (WLAN) to enable mobility for personnel and equipment.

- Holistic defense-in-depth security—Multiple layers of diverse technologies for threat detection and prevention, implemented by different persona (for example, OT and IT) and applied at different levels of the plant-wide or site-wide IACS architecture.

- Convergence-ready—Seamless plant-wide or site-wide integration by trusted partner applications.

Figure 1-1   CPwE Architectures

CPwE Resilient IACS Architectures Overview

An IACS is deployed in a wide variety of industries such as automotive, pharmaceuticals, consumer packaged goods, pulp and paper, oil and gas, mining, and energy. IACS applications are composed of multiple control and information disciplines such as continuous process, batch, discrete, and hybrid combinations. One of the challenges facing industrial operations is the industrial hardening of standard Ethernet and IP-converged IACS networking technologies to take advantage of the business benefits associated with IIoT. A resilient LAN

architecture can help to increase the overall equipment effectiveness (OEE) of the IACS by helping to reduce the impact of a failure and speed recovery from an outage, which lowers Mean-Time-to-Repair (MTTR).

Protecting availability for IACS assets requires a scalable defense-in-depth approach where different solutions are needed to address various network resiliency requirements for OEM, plant-wide or site-wide architectures. This section summarizes the Cisco, Panduit, and Rockwell Automation CPwE application guidance that address different aspects of availability for IIoT IACS applications.

- *Deploying Device Level Ring within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several use cases for designing and deploying DLR technology with IACS device-level, switch-level, and mixed device/switch-level single and multiple ring topologies across OEM and plant-wide or site-wide resilient LAN IACS applications.

  - Rockwell Automation site:
    https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td015_-en-p.pdf

  - Cisco site:
    https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

- *Deploying Parallel Redundancy Protocol within a Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several use cases for designing and deploying Parallel Redundancy Protocol (PRP) technology with redundant LANs across plant-wide or site-wide IACS applications.

  - Rockwell Automation site:
    https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td021_-en-p.pdf

  - Cisco site:
    https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

- *Deploying A Resilient Converged Plantwide Ethernet Architecture Design and Implementation Guide* outlines several use cases for designing and deploying resilient plant-wide or site-wide architectures for IACS applications, utilizing a robust physical layer and resilient LAN topologies with resiliency protocols.

  - Rockwell Automation site:
    https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td010_-en-p.pdf

  - Cisco site:
    http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

CPwE Physical Layer Solution Use Cases

Successful deployment of CPwE logical architectures depends on a robust physical infrastructure network design that addresses environmental and performance challenges with best practices from Operational Technology

(OT) and Information Technology (IT). Cisco, Panduit, and Rockwell Automation have collaborated to reference Panduit's building block approach for physical infrastructure (Figure 1-2) deployment. This approach helps customers address the physical deployment associated with converged OEM, plant-wide or site-wide EtherNet/IP architectures. As a result, users can achieve resilient, scalable networks that can support proven and flexible CPwE logical architectures designed to help optimize OEM, plant-wide or site-wide IACS network performance.

The following use cases were documented by Panduit:

- Robust physical infrastructure design considerations and best practices
    - Long reach cable applications, minimum/maximum cable lengths
    - Single Pair Ethernet (SPE) and Ethernet-APL
    - Wireless deployments
- Control Panel:
    - Electromagnetic interference (EMI) noise mitigation through bonding, shielding, and grounding
    - Industrial Ethernet Switch (IES) deployment within the Cell/Area Zone
- Physical Network Zone System:
    - IES and Access Point (AP) deployment within the Cell/Area Zone
- Cable distribution across the Industrial Zone
- Industrial Distribution Frame (IDF):
    - Industrial aggregation/distribution switch deployment within the Industrial Zone
- Industrial Data Center (IDC):
    - Physical design and deployment of the Level 3 Site Operations

Figure 1-2   Panduit Robust Physical Infrastructure for the CPwE Architecture

CHAPTER **2**

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 2-17
- Wireless Physical Infrastructure Considerations, page 2-18

# 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.

Figure 2-1 Network Overlay on Building Locations
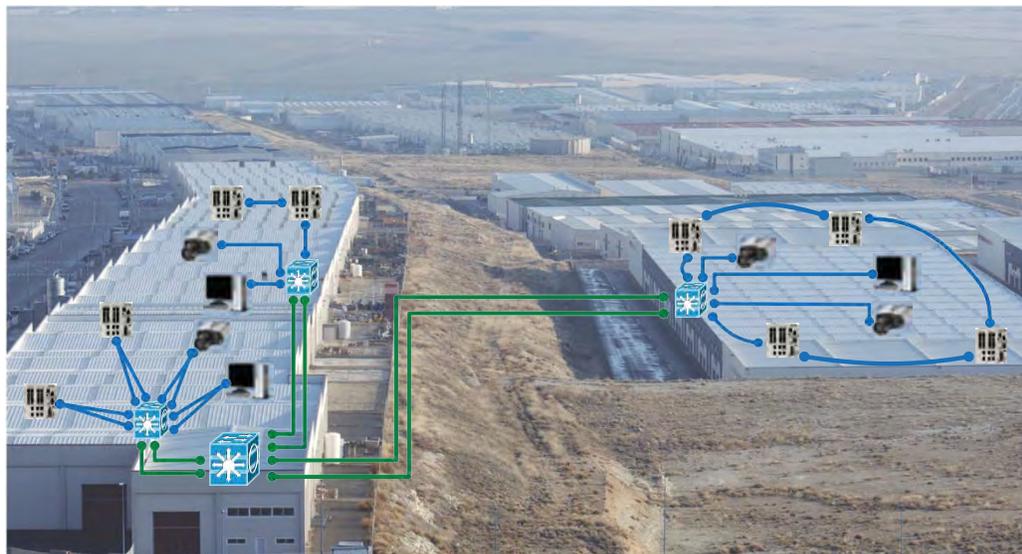
- **Brownfield or Legacy Network**—Additional design considerations are necessary to transition from or work alongside a legacy network. Existing installations have many challenges, including bandwidth concerns, poor grounding/bonding, inadequate media pathways, and limited space for new areas to protect 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.

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, device 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
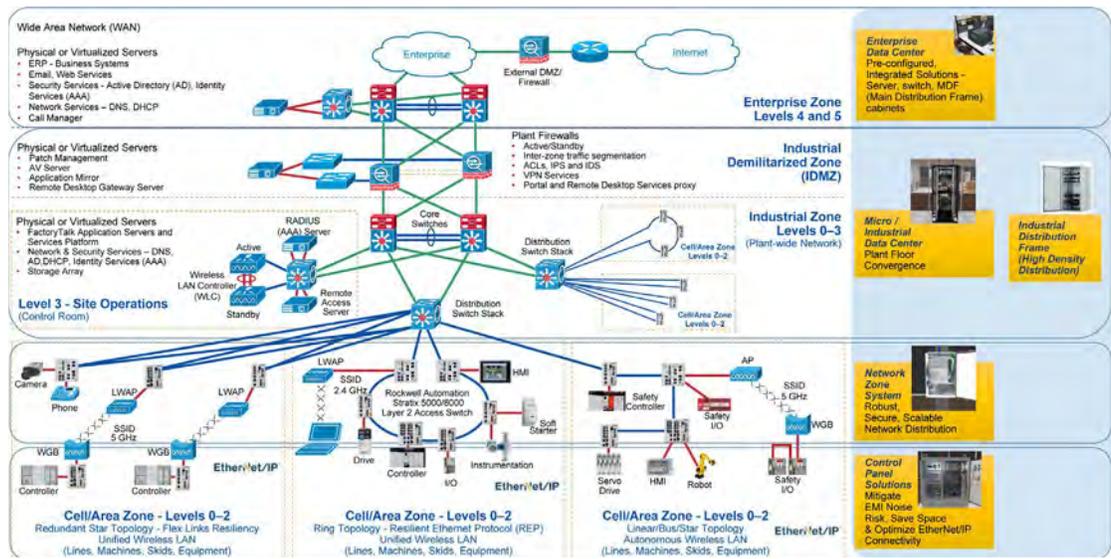
Key Requirements and Considerations

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. Controlling access of personnel to network enclosures is a key consideration of a defense in depth security strategy. Use of a card reader system is an alternative to key lock solutions which controls access to the enclosure and provides physical status of door. 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 controls access to the enclosure and provides physical status of door. 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. Controlling access of personnel to network enclosures is a key consideration of a defense in depth security strategy. Use of a card reader system is an alternative to key lock solutions which controls access to the enclosure and provides physical status of door. 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. Legacy802.11 a/b/g devices are likely to exist. New wireless APs deployed today are likely to be 802.11 n/ac/ax (WiFi 4, 5, or WiFi 6 certified) with speeds up to 10Gbps. Cable requirements for new installations are recommended to be Category 6 (WiFi 4) to Category 6A. As higher performance wireless standards such as 802.11be (also known as Wi-Fi 7) 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. Industrial Network switches are available that offer PoE (IEEE 802.3af (802.3at Type 1)) and PoE+ (IEEE 802.3at Type 2) ports with between 15.4W to 30W available to devices. 23AWG Category 6 cabling is recommended for these installations. The IEEE 802.3bt-2018 standard further expands the power capabilities for PoE++ (IEEE 802.3bt Type 3) at 60W and 4PPoE (IEEE 802.3bt Type 4) at 99W. 23 AWG Category 6A cabling will be required to support these device connections. 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.

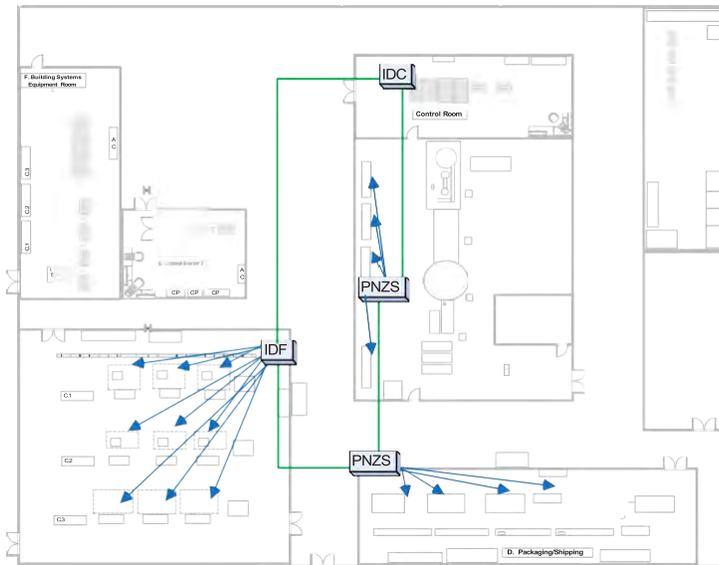# Physical Zone Cabling Architecture

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.

Figure 2-3   Example of 'Home Run' Cabling from Control Panels and Machines back to IT Closet
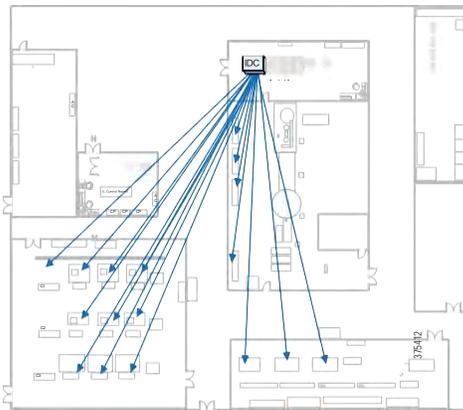
PNZS cabling architectures are well proven in Enterprise networks across offices and buildings for distributing networking in a structured, distributed manner. These architectures have evolved to include active switches at the distributed locations. For an IACS application as depicted in Figure 2-4, 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.

Figure 2-4   Example Use of PNZS and IDFs to Efficiently Distribute Cabling Using a Physical Zone Cabling Architecture

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 4-pair copper installations have a maximum link length of 100 m (328 feet). Single Pair

Ethernet (per IEEE 802.3cg) utilizing 10BASE-T1L PHYs can provide a maximum link length of 1000 m (3280 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 key feature of a PNZS architecture is scalability because spare ports 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 ensures 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.

- **PoE Network Extender**—Utilizing a PoE-powered port from an IES a network connection can be extended beyond the 100-meter limitation by installing a PoE network extender module. This setup includes a transmitter and receiver device that leverages standard physical infrastructure.

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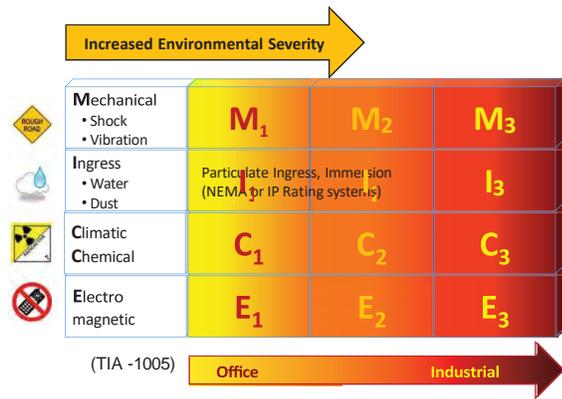
It is important to understand that M.I.C.E. rates the environment, not the product. The result of a M.I.C.E. evaluation is used as a benchmark for comparing product specifications. Each product used in the system design should at least be equal to or exceed the M.I.C.E. evaluation for that space.

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
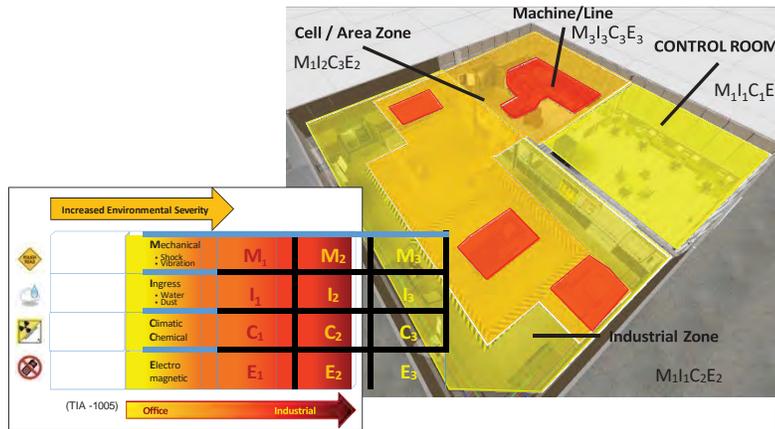
Cable Media and Connector Selection

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, OM5, 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 dielectric double jacketed.

- **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

Parameter	Copper Cable	Multimode Fiber	Single-mode Fiber
Reach (maximum)	100 m 1000m (SPE)	2,000 m (1 Gbps) 400 m (10 Gbps)	70 km (1 Gbps) 10 km (10 Gbps)
Noise Mitigation Option	Foil shielding	Noise immune*	Noise immune*
Data Rate (Industrial)	10Mbps (SPE) 100 Mbps (Cat 5e) 1 Gbps (Cat 6) 10 Gbps (Cat 6a)	1 Gbps 10 Gbps	1 Gbps 10 Gbps

Table 2-1   General Cable Characteristics

Parameter	Copper Cable	Multimode Fiber	Single-mode Fiber
Cable Bundles	Large	Small	Small
Power over Ethernet (PoE) capable	Yes Yes, PoDL for SPE applications	Yes, with media conversion	Yes, with media conversion

*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 either Single Pair Ethernet (a copper cabling technology), non-standard long reach cable, PoE network extender, or optical fiber cable. Four-pair copper Ethernet cable is limited to a maximum link length of 100 m. Single Pair Ethernet (SPE) with a media converter extends the reach of copper cabling for specific applications, typically those found at the network edge, and can be used to form point-to-point links at distances up to 1000 meters (3280 feet). However, other considerations may be important for distances less than 100 m, such as extreme EMI, for which fiber-optic cable is preferred due to its inherent noise immunity.

Another consideration that warrants the use of fiber optic cabling network switch uplinks. Laboratory studies show that using optical fiber for these connections 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. A possible exception to the "copper/fiber" speed statement is Single Pair Ethernet. SPE, as defined by IEEE 802.3cg, has a maximum speed of 10 Mbps. However, this apparent speed penalty versus 4-pair performance comes with the advantage of 10x link length if the IACS application can tolerate the speed penalty.

Network life span is a significant consideration for media performance. For instance, installing a network with Cat 6 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.

Long Reach applications

ANSI/TIA 568 standard defines that an Ethernet channel (structured cable plus patch cords) should not exceed 100 meters due to the amount of time it takes the electrical signal, at high bandwidth speed, to traverse the entire channel. However, with advancements in cable technology and the proliferation of IIoT sensors that don't require high bandwidth, there are cable solutions that can provide longer reach due to UL validation testing but do not comply with the current ANSI/TIA 568 standard.

IIoT sensors are typically lower bandwidth, around 10 or 100 Mbps and therefore the signal can operate reliably at longer distances when using a higher quality cable that has been validated through testing. Additional long-reach applications, that benefit from this cable technology, include video cameras and wireless access points. Often these devices require greater than 100 meters of cabling and require power, such as PoE.

These long-reach applications are where cable construction and the corresponding performance are essential. The specified cable should have proof that a third party*, such as UL, has tested and approved the cable for the required installation, and provide a performance warranty. In addition, it is good practice to verify the performance of the installed cable with a network tester (this testing is often required for establishing the warranty). These long-reach cables may

eliminate the need for additional zone enclosures or fiber runs and when properly specified and installed will provide years of reliable cable infrastructure.

Long reach cables are also capable of supplying Power over Ethernet (PoE) for remote sensors, wireless access points, and cameras. As expected, the lower the required PoE power, the longer the cable distance. The table below shows the results of a UL test that addresses distance, power, and wireless access points on a high-quality Cat 6 and Cat 6a cable.

Maximum horizontal transmission distance	High-Quality Cat 6	High-Quality Cat 6a
10 Mbps	185m (606 ft.)	185m (606 ft.)
100 Mbps	150m (492 ft.)	150m (492 ft.)
1 Gbps	100m (328 ft.)	100m (328 ft.)
10 Gbps	50m (164 ft.)	100m (328 ft.)

PoE Specifications	High-Quality Cat 6/Cat 6a
Type 1 – 15.4 watts	185m (606 ft.)
Type 2 – 30 watts	150m (492 ft.)
Type 3 – 60 watts	100m (328 ft.)
Type 4 – 100 watts	100m (328 ft.)

Wireless Specifications	High-Quality Cat 6	High-Quality Cat 6a
WiFi (IEEE 802.11 ac)	10 Gbps 37-50m (121-164 ft.)	10 Gbps 100m (328 ft.)
WiFi (IEEE 802.11 ax)	10 Gbps 37-50m (121-164 ft.)	10 Gbps 100m (328 ft.)

* Refer to verify.UL.com V558491 & V685853 for details on the above specifications

Network extenders

A network extender, also known as Power over Ethernet (PoE) Extender, is the simplest and most cost-effective method to extend data, and optionally PoE power, well beyond the 100-meter limitation of a traditional switch using standard twisted-pair cabling or long reach cabling described in the previous section. In fact, a network extender distance of up to 2,000 feet at a speed of 100 Mbps can be achieved.

The network extender hardware, consisting of a transmitter and receiver, is used to extend the Ethernet signal and, if using a PoE-powered switch, the power can be extended as well. Network extenders can be powered using a PoE port on a switch or with a local DC power supply. The extender works by converting the standard Ethernet to a long-range signal and then converting it back to standard Ethernet. Therefore, the sourcing switch and end device are unaware the extender is being used and maintain operation with standard Ethernet protocol. The extenders do not require any configuration setup and therefore are easy to install.

Industrial environments are often more demanding for network transmission due to nearby electrical noise that can interfere with the integrity of the signal. In some cases, a shielded cable is recommended to protect the network transmission from this electrical noise, often referred to as Electromagnetic Interference (EMI). When running a cable long distance for a network extender application it is best to avoid areas where EMI is present. However, avoiding the EMI area is not always possible and mitigation methods, such as using shielded cable, must be implemented. Cisco, Panduit, and Rockwell Automation recommend installing the cabling system using patch panels. Using patch panels requires some additional physical infrastructure as shown in figure 4. 'Patching' refers to interconnecting the cables through patch panels so

that standard patch cables can be used, and a structured cable can be set up to connect the patch panels. Structured horizontal cable is typically a solid conductor and can be conveniently tested with handheld test equipment. Patching can be set up with shielded or unshielded copper cabling, and it is recommended to follow structured cabling standards, such as TIA 1005.

Figure 2-7   Typical PoE network extender application
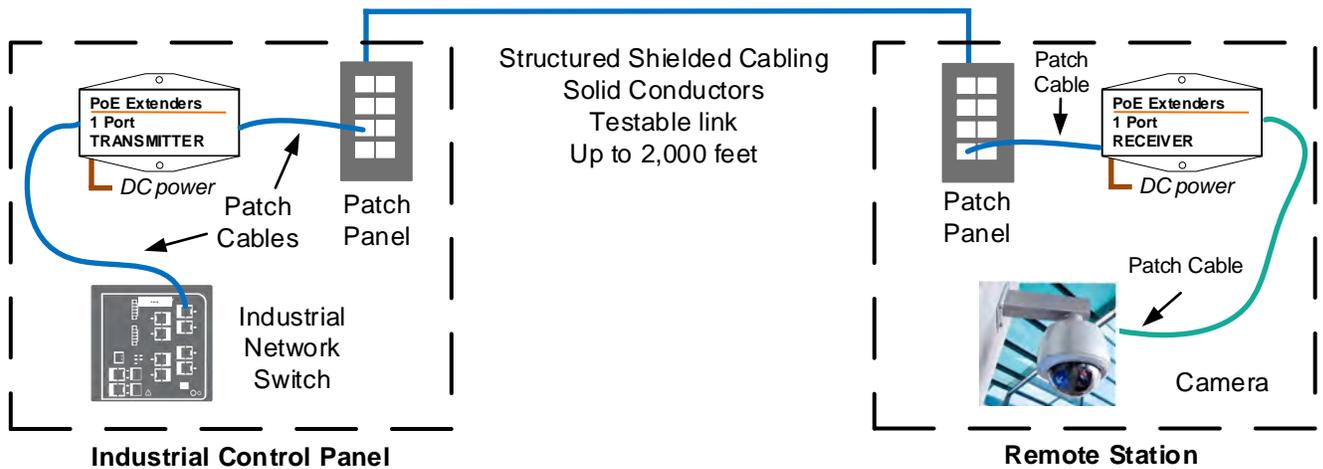
Optical Fiber Cable Basics

Single-mode and multimode are the two fiber types. Multimode fiber has glass grades of OM1 to OM5. 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 6A (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 28 AWG may be used in some cases for patching. Larger gauge wires are available, and the conductors 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. Select higher strand counts 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
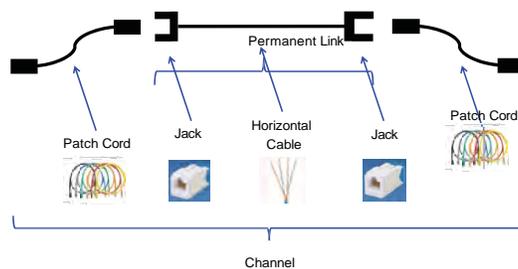
Minimum copper patch cord length

As network infrastructures continue to have a higher impact on an organization's productivity and competitive position, it becomes increasingly important to select a reliable end-to-end structured cabling system that allows for future network growth. To maximize usable network bandwidth, it is critical that patch cords properly support the performance, quality, and dependability of the entire structured cabling system. The performance of the link between the IES and IACS device is most impacted by noise generated in the portion of the channel closest to the active equipment. This is where the patch cords are located and where quality should never be compromised.

It is vital that patch cords have the following design features:
- Mated performance with connecting hardware to maximize cancellation of near-end-crosstalk
- Robust construction to ensure long-term reliability of the network under day-to-day moves, adds and change conditions
- Certified component performance to ensure maximum network availability.

Patch cords are an integral component impacting the performance of the entire structured cabling system. Investment should be made in patch cords that utilize advanced features to deliver maximum reliability and usability of the network.

Sub-standard patch cords jeopardize network performance due to:
- High degree of plug variability which leads to degradation of channel performance
- Inferior design features which do not perform over time due to the mechanical stresses of real-world conditions
- Untested, low quality patch cords which may not meet electrical requirements. Often, field-produced patch cords made in the pursuit of expediency cannot come close to the performance of factory-produced cords. In addition, patch cords must be properly mated and tuned to connecting hardware (jacks, panels, and horizontal cable) to keep the network running at peak performance. This directly minimizes the impact of costly network downtime.
- All PHY chips produced to a given standard have a tolerance built in to offset variances in physical layer performance. Be aware that some of this silicon is "sensitive" to physical layer variance. Here sub-standard patch cord performance may result in a poor performing or even non-functional link.

The proven performance of high-quality Panduit copper patch cords, tested to exceed TIA/EIA 568-B.2 specifications as a key component of the complete end-to-end solution, helps ensure maximum network bandwidth. Specifying and installing these patch cords can support critical network demands.

In addition to quality and performance of patch cords, it's important to consider the minimum feasible patch cord length. Patch cords that are too short can cause performance problems in practice. A good rule of thumb is to use cords no shorter than 0.5 meter (approximately 20 inches). Some PHY chips are sensitive to short cords.

While there is not a minimum patch cord length specified, ANSI/TIA 568-B.2 sets an implied minimum length for a certified patch cord at 0.5 meter. That's because the calculation for the insertion loss limit lines does not work well below this length. When selecting patch cords, pay close attention to the chosen supplier. Many suppliers will not certify a patch cord below 1 meter.

From ANSI/TIA 568-B.2, K.7.3.2   Insertion Loss
"For cords or jumpers using stranded 26 AWG conductors, the insertion loss of any pair shall be less than or equal to the value computed by multiplying the result of the insertion loss equation in clause 4.3.4.7 by a factor of 1.5. This is to allow a 50% increase in insertion loss for stranded construction, AWG differences, and design differences."

SPE (Single Pair Ethernet)

SPE (Single Pair Ethernet) is a form of copper-based Ethernet network communications technology for OT networks. SPE is governed by IEEE 802.3cg and provides for Ethernet

communications at speeds of 10 Mbps over a pair of balanced copper conductors. The IEEE standard created two new PHYs, 10BASE-T1L and 10BASE-T1S.

10BASE-T1L	Point-to-point links of up to 1000 meters in length at 10 Mbps, with optional power delivery. This point-to-point link is designed to tolerate up to ten (10) inline connectors.
10BASE-T1S	Multidrop links with up to 8 nodes over a total cabled length of 25 meters. T1S PHYs can also form point-to-point lengths of up to 15 meters in length.

Figure 2-8   Single pair Ethernet architecture
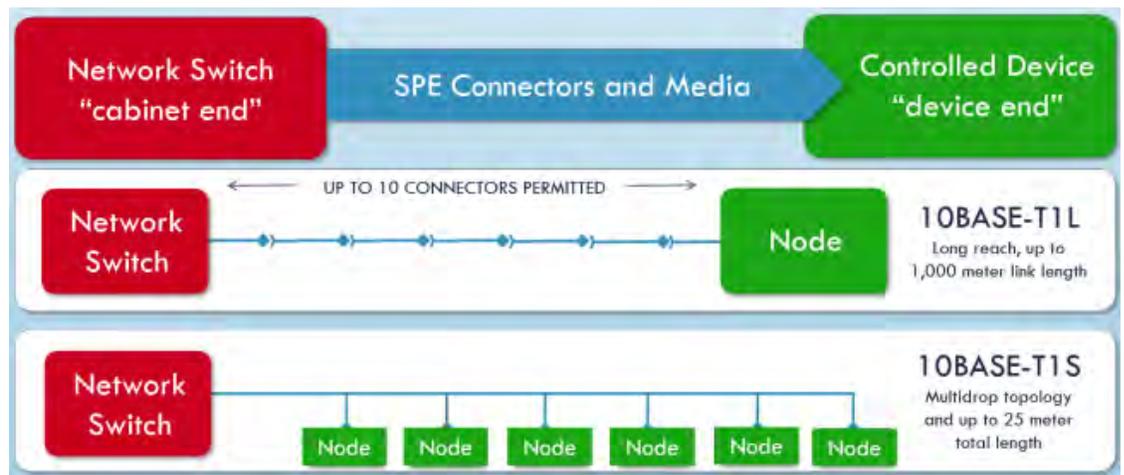
Both PHYs support topologies that the "built for purpose" legacy networks do today. Therefore, a key SPE benefit is building OT networks as you always have and gaining the advantages of Ethernet.

10BASE-T1L applications use the PHY's ability to deliver long distance point-to-point links with optional power delivery. The SPE media required to form these links out to their maximum distance capability of 1000 meters with 18AWG STP cable. Links are connectorized on the ends using connection technologies described in the IEC 63171 series of international standards. It is generally understood that a continuous pull of 1000 meters of cable is nearly impossible; that is the reason the IEEE 802.cg standard permits up to ten (10) intermediate connectors within the 10BASE-T1L link.

10BASE-T1S PHY designs permit multidrop topologies to be designed and implemented, delivering data connectivity to multiple nodes over a span 25 meters of cable. Note that the 25-meter span is the sum of all trunk and drop segments. ODVA recently published a very unique 10BASE-T1S system in Volume 2, "EtherNet/P Adaptation of CIP, Chapter 8: Physical Layer" that is intended for the interconnection of In-Cabinet devices. Typical devices include contactors, motor starters, overload protectors, pushbuttons, indicators, and related devices.

This in-cabinet system replaces the hardwiring between devices with composite network cabling, taking the form of a 7-conductor ribbon cable. This system of automation panel construction brings rapid assembly, programmable alteration of function, and enabling intelligence in the connected devices to provide greater information for maintenance and process optimization.

The system achieves a reduction in device complexity by using a Single Pair Ethernet bus to reduce the device interface complexity and to reduce the average number of interfaces per device. Cabling is simplified by bundling of network power and switched power (for actuation) into a single multi-conductor cable. Assembly is simplified by utilization of insulation displacement/piercing connectors

that can be *applied* (i.e., mechanically attached and contacting the signals) without cable preparation. A technique to locate the relative position of the devices on the bus cable reduces the need for manual selector switches or direct configuration tool attachment to each device – reducing device and installation complexity.

SPE Benefits for OT Networks

- **Seamless single physical layer from application edge to the enterprise**. SPE simplifies network design and operation, eliminating the support and translation of legacy networks used in OT networks.

- **Tighter integration with CPwE validated reference architectures**. SPE being Ethernet, if supported by the IACS application, allows much more effective integration and control over the edge network versus legacy networks.

- **SPE is Ethernet designed to support the way you build OT networks**. SPE PHYs allow the network edge to function like legacy networks, doing so with Ethernet.

- **Greatly enhancing security versus "cyber-vulnerable" legacy networks**. Since SPE is Ethernet, edge networks incorporate the suite of robust security measures found in IP and OT SDO networks, such as CIPSecurity.

- **Optional power delivery can transform OT network control power infrastructure**. Many edge devices are reliant on local control power sources. 10BASE-T1L SPE links allow a single connection with control power and communications transforming the network edge control power infrastructure.

SPE Powering

OT devices require both data and power to perform their designed functions. Power is not always conveniently available at the device installed location. Power over data line (PoDL), like traditional PoE solves these problems by providing power alongside data connectivity on a single cable.

Figure 2-9   Power over data line architecture
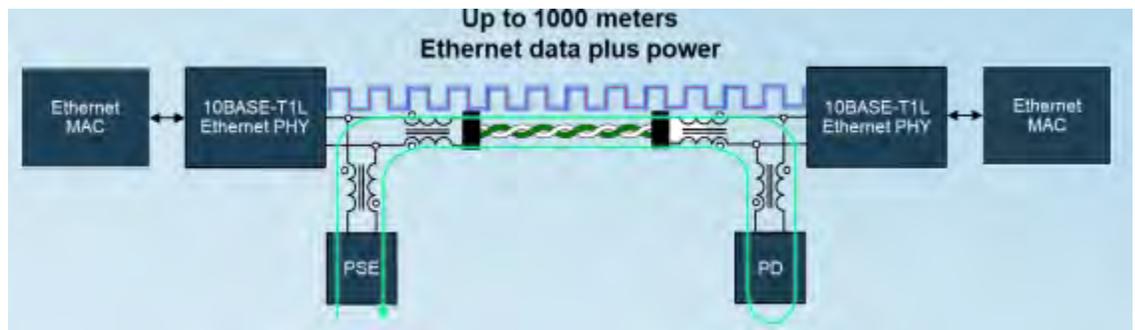
IEEE 802.3 standardized over a single pair of conductors at 100 Mbps and 1000 Mbps in the IEEE 802.3bu standard, "Physical Layer and Management Parameters for Power over Data Lines (PoDL) of Single Balanced Twisted-Pair Ethernet." The publication of IEEE 802.3cg extended the specification to include SPE applications at 10 Mbps for OT networks.

All single pair powering traces back to the PoDL standard and in that regard, all SPE powering is technically PoDL. PoDL provides very broad powering capabilities, encompassing multiple voltage levels and power delivery categories. To simplify discussion of SPE powering, industry experts speak about two variants of single-pair powering, SPoE and PoDL. SPoE is used to describe classification-based implementation used in OT networks; "plug & play" SPE powering applications that functionally mirror the user experience of 4-pair PoE installations. Experts use the term PoDL to reflect use of capabilities where control engineers design powering to function as required by their individual applications.

SPoE	• Classifies end device prior to application of power
	• Can measure cable resistance
	• 24V, 55V ranges available (common in OT networks)
	• Can deliver power up to 1 kilometer
	• Increased power levels possible at shorter distances
PoDL	• Extremely fast detection of end device prior to power application
	• No classification of end devices, appropriate for engineering systems
	• 12V, 24V, or 48V ranges
	• 15- and 40-meter cable reaches

Today, OT deployments often use a 24V DC supply voltage. However, power delivery on long cables at this voltage is subject to significant losses due to cable resistance. Power delivery efficiency is maximized when the voltage is raised near the SELV maximum, 60V DC. As shown below, SPoE provides two distinct operating voltages: 24V and 55V DC.

Class	10	11	12	13	14	15
V_{PSE} (V, min/typ/max)	20 / 24 / 30			50 / 55 / 58		
I_{CABLE} (mA, max)	92	240	632	231	600	1579
P_{PD} (W, max)	1.23	3.2	8.4	7.7	20	52
R_{CABLE} (Ohms, max)	65	25	9.5	6.5	25	9.5

Six unique classes are defined for OT networks. Classes 10, 11 and 12 enable 24 VDC power delivery over long, medium, and short cables respectively. Likewise, Classes 13, 14 and 15 enable 55VDC power delivery over long, medium, and short cables respectively.

SPE Physical Layer

Generally, installed SPE network links should conform to IEC 60950-1, IEC 62368-1, and IEC 61010-1. All equipment and cabled infrastructure should additionally conform to applicable local, state, or national standards.
All SPE equipment is expected to conform to the potential environmental stresses with respect to their mounting location, as defined in the following specifications, where applicable.
- Environmental stresses: IEC 60529 and ISO 4892
- Mechanical stresses: IEC 60068-2-6 and IEC 60068-2-31
- Climatic stresses: IEC 60068-2-1, IEC 60068-2-2, IEC 60068-2-14, IEC 60068-2-27, IEC 60068-2-30, IEC 60068-2-38, IEC 60068-2-52, and IEC 60068-2-78

SPE cable is readily routed by conventional means used for 4-pair Ethernet cables.

SPE Media

IEEE 802.3cg, like most IEEE 802.3 standards, does not prescribe physical media. Rather the standard defines electrical characteristics that must be present in the chosen media for the PHYs to perform correctly. 10BASE-T1L is designed to operate over a single balanced pair of conductors that meet the requirements specified in subclause 146.7 of IEEE 802.3cg. All SPE cabling and equipment is expected to be mechanically and electrically secure in a professional manner. All SPE cable is expected to be routed according to any applicable local, state, or national standards considering all relevant safety standards.

A 10BASE-T1L link segment supports up to ten (10) in-line connectors using a single balanced pair of conductors for up to at least 1000 meters. SPE links can be made using shielded or unshielded cables, depending upon the EMC environment encountered in the application. Transmission distance of

10BASE-T1L links is limited primarily on the DCR (direct current resistance) value of the single pair cable, e.g., smaller gauge cable limits the transmission distance.

SPE point-to-point links may be built using a variety of gauge sizes of balanced single pair cable. However, it's worth noting that link segment electrical performance is predicated on a reference 18AWG SPE cable with a characteristic impedance of 100 ohms. Larger or smaller conductor sizes generally provide longer or shorter link lengths. From the chart below, 18AWG cable delivers 1000-meter length at the insertion loss limit. Substituting 14AWG cable delivers a length over 1500 meters. Conversely, dropping conductor size to 26AWG results in a link length of only 395 meters. Note: the largest conductor size accommodated by SPE connectors is 18 AWG.

By design, SPE links can accommodate the added insertion loss of inline connectors; up to ten (10) connectors in a 1000-meter link. This design feature is intended to permit SPE users significant implementation flexibility and in some cases, enable cable reuse.

Conductor Diameter *mm (AWG)*	Resistance per Meter *ohms*	Length at IL limit *meters*	Conductor Resistance at IL limit *ohms*	Loop Resistance at IL limit *ohms*	10 Connector DCR *ohms*	Link Segment Resistance at IL limit *ohms*
1.63 (14)	0.0092	1589	14.67	29.33	1	30.33
14.5 (15)	0.0116	1415	16.47	32.94	1	33.94
1.29 (16)	0.0147	1261	18.50	37.00	1	38.00
1.14 (17)	0.0185	1123	20.78	41.55	1	42.55
1.02 (18)	**0.0233**	**1000**	**23.33**	**46.66**	**1**	**47.66**
0.91 (19)	0.0294	891	26.20	52.40	1	53.40
0.81 (20)	0.0371	793	29.42	58.84	1	59.84
0.72 (21)	0.0468	706	33.04	66.07	1	67.07
0.64 (22)	0.0590	629	37.10	74.19	1	75.19
0.57 (23)	0.0744	560	41.66	83.31	1	84.31
0.51 (24)	0.0938	499	46.78	93.55	1	94.55
0.40 (26)	0.1492	395	58.98	117.96	1	118.96

For 10BASE-T1L applications where the 1000-meter link length is desired, a balanced-pair 18AWG cable is required. Suitable cable has a characteristic impedance of 100 ohms. A word of caution. Many fieldbus cables in use today have characteristic impedance of 100 ohms but this impedance value is based on typical data rates of 31.2 kbps not the 10 Mbps rate provided by SPE. At 10 Mbps transmission rates, cables carry frequencies as high as 20 MHz which shift the characteristic impedance value, significantly in some fieldbus cables.

Cable reuse is possible given conspicuous caution. The prospect of reusing installed fieldbus cable is certainly enticing and arguably would lower the cost of deploying SPE or Ethernet-APL. Given specification-compliant media that is electrically healthy, the practice of fieldbus cable reuse can be very rewarding. There are risks that must be addressed in contemplating reuse.

- Fieldbus Cable Specification – Examine the specifications of the cable planned for reuse. Generally, a nominal impedance of 100 ohms is essential.
- Consider the link lengths needed in the application. Is the cable conductor size adequate?
- Cable topology – Determine that the installed cable topology works with SPE.
- Also, count inline connectors in each link. Are there 10 or less connectors?

Instrument Measurement of Link Performance – Analyzers are available to measure the electrical performance of links targeted for reuse. These analyzers compare actual measured performance against the accepted norms for SPE links.

Finally, bear in mind that environmental conditions that degrade cable performance – elevated and/or extremely low temperatures, high humidity, chemical contact, UV exposure and mechanical stress like shock and vibration, are available in abundance in plants and factories. These environmental stresses, combined with cable age, may push fieldbus cable beyond successful reuse parameters.

Ethernet-APL

Figure 2-10   Ethernet APL Trunk and Spur Technology
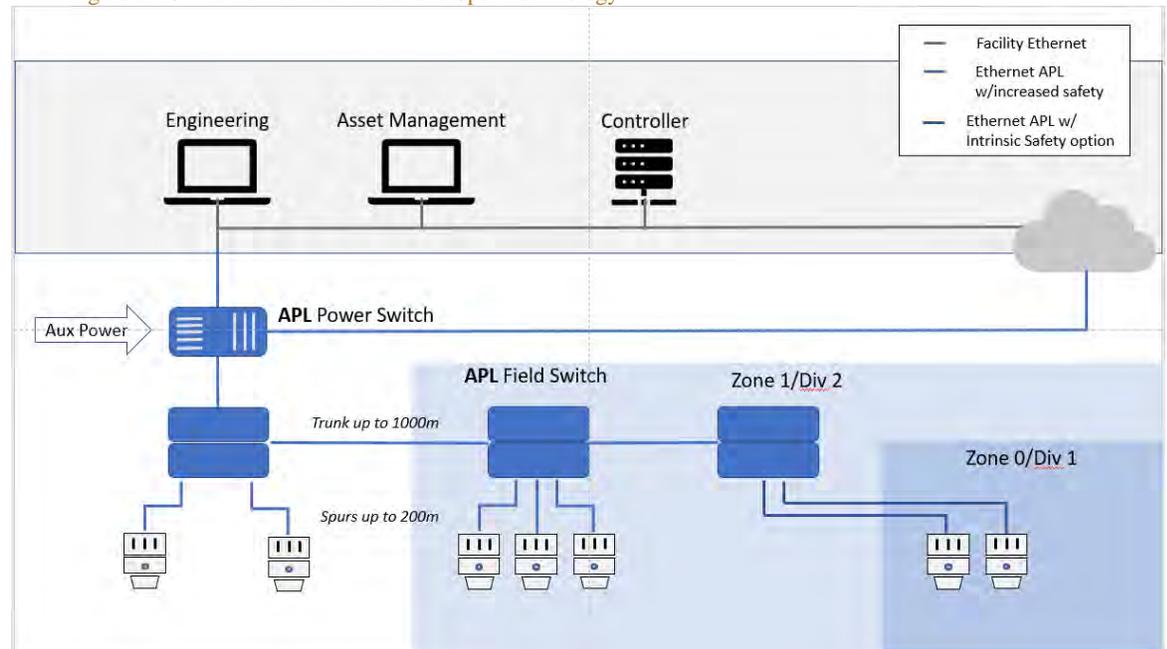
Ethernet-APL (advanced physical layer) is a ruggedized, two-wire, loop-powered Ethernet physical layer that uses 10BASE-T1L plus IEC extensions for installation within the demanding operating conditions and hazardous areas of process plants. It enables a direct connection of field instrumentation to plant-wide Ethernet networks in a way that process plants can benefit from a convergence of their OT and IT systems.

Ethernet-APL enables long cable lengths, loop power and explosion protection via intrinsic safety techniques. Based on IEEE 802.3cg and several IEC standards, Ethernet-APL physical layer supports any industrial Ethernet protocol, such as EtherNet/IP. These capabilities create a long-term stable infrastructure for the process automation community.

Ethernet-APL adopts technologies and options already established in the field of process automation. This includes the proven trunk-and-spur topology shown in the figure above with the ability to power up to 50 field devices with up to 500 mW each. Widely used and established cable infrastructures are specified to support the migration in brownfield installations to Ethernet-APL.

For more information on Ethernet-APL, visit https://www.ethernet-apl.org or https://www.odva.org/technology-standards/market-drivers/process-automation

Additional attributes beyond those of SPE are required by process automation applications.

2-WISE	2-WISE stands for 2-Wire Intrinsically Safe Ethernet. IEC Technical Specification TS 60079-47 defines intrinsic safety protection for all hazardous environment Zones and Divisions. 2-WISE includes simple steps for verifying intrinsic safety without calculations.
Ethernet-APL Port Profiles	Ethernet-APL defines port profiles for multiple power levels with and without explosion hazardous area protection. Markings on devices and instrumentation indicate power level and function as sourcing or sinking. This simple framework provides for interoperability from engineering to operation and maintenance.
Support for terminals	Ethernet-APL allows wiring to screw-type or spring-clamp terminals, thus supporting cable entry through glands. Additionally, well-defined connector technology ensures simplicity during installation work

Ethernet-APL Approved Connectors

Because Ethernet-APL focuses on process automation applications, its physical layer components must be appropriate for these applications. Therefore, the Ethernet-APL project has approved connection methods commonly encountered in this environment. These connection methods include:

- Spring-clamp terminals
- Screw-type terminals
- M8 and M12 connectors

When selecting these connection methods for use in Ethernet-APL, the connectors must also meet the following requirements.

Specification	Minimum	Maximum
Current per contact	4 amperes	
Rated voltage, contact to contact	50 VDC	
Isolation voltage, contact to shield	1500 VAC	
Insertion Loss (IL)		$0.04 \; for \; 0.1 MHz \leq f < 4 \, MHz$ $0.02 \, x \, \sqrt{(f \, / \, MHz)} \; for \; 4 \, MHz \leq f \leq 20 \, MHz$
Return Loss (RL)		$28 + 8 \, x \, f \; dB \; for \; 0.1 MHz \leq f < 0.5 \, MHz$ $32 dB \; for \; 0.5 \, MHz \leq f \leq 20 \, MHz$
PSANEXT		$73 \, dB \; for \; 0.1 \, MHz \leq f < 0.95 \, MHz,$ $50.5 \, dB - 17 log 10 (f \, / \, 20)$ for 0.95MHz ≤ f < 3.68 MHz $63 dB \; for \; 3.68 MHz \leq f \leq 20 \, MHz$
DC resistance per contact		0.025 ohms

NOTE 1: The values specified in this table shall be maintained across the full environmental temperature range of the device with which the terminal block or connector is used.

NOTE 2: The parameters given in this table are required for connector and terminal block selection. For practical reasons, for connectors built into an APL port implementation, no specific connector performance tests are required, as it is expected that the connector performance is validated during the port specific APL conformance tests (e.g. MDI return loss).

Ethernet-APL Media

Ethernet-APL specifies fieldbus Type A cable, IEC 61158-2, as reference cable. Type A cable is nominally 100 ohms, +/- 20 ohms tolerance and 18 AWG. The intent in specifying this reference cable is cable reuse. Ethernet-APL, which is based on IEEE 802.3cg, includes the ten (10) inline connector allowance, again done in anticipation of cable reuse.

Ethernet-APL is specifically designed to accommodate the requirements of intrinsic safety and hazardous environments. These applications have specific environmental requirements for the physical infrastructure to operate safely. These requirements, in addition to the electrical requirements for SPE 10BASE-T1L links, drive the specifications of the Ethernet-APL physical layer.

Cable reuse is possible given conspicuous caution. The prospect of reusing installed fieldbus cable is certainly enticing and arguably would lower the cost of deploying SPE or Ethernet-APL. Given specification-compliant media that is electrically healthy, the practice of fieldbus cable reuse can be very rewarding. There are risks that must be addressed in contemplating reuse.

- Fieldbus cable specification – Examine the specifications of the cable planned for reuse.
    - Generally, a nominal impedance of 100 ohms is essential.
- Consider the link lengths needed in the application.
    - Is the cable conductor size adequate?
- Cable topology – Determine that the installed cable topology works with Ethernet-APL.
- Count inline connectors in each link.
    - Are there 10 or less connectors?
    - Can these connectors meet the IL, RL and PSANEXT performance listed in the table above?
- Instrument Measurement of Link Performance – Analyzers are available to measure the electrical performance of links targeted for reuse.
    - These analyzers compare actual measured performance against the accepted norms for SPE and Ethernet-APL links.

Finally, bear in mind that environmental conditions that degrade cable performance – elevated and/or extremely low temperatures, high humidity, chemical contact, UV exposure and mechanical stress like shock and vibration, are available in abundance in plants and factories. These environmental stresses, combined with cable age, may push fieldbus cable beyond successful reuse parameters. Therefore, be cautious and verify the condition on any cable you plan to reuse.

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.

- **Network Mapping system** – Using pre-labeled patch cables in conjunction with an automated mapping system reduces the time and cost of network cable documentation. Scanning codes from the cables and storing the information in a database allows engineers and technicians to quickly and easily place and trace cables. Documenting the full system upon installation reduces downtime during troubleshooting of a network issue.

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. The following figure describes some of these options.

Figure 2-8 Pathway Considerations

Installation Consideration	J-Hook	Wire Basket	FiberRunner®
Cable Protection Environment	Mild	Moderate	Moderate to harsh
Cable Density	Light to medium	Medium to heavy	Light to heavy
Applicable in Constrained Spaces	Yes	No	No
Installation Complexity	Simple	Moderate	Moderate to strong
Ease of Moves, Adds, Changes	Simple	Moderate	Moderate

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. A fiber cable with a self-supporting jacket construction is preferred when routing in J-Hooks or ladder rack to protect fibers from potential pinches, kinks, or attenuation. Standard fiber distribution cable is not suitable for J-Hooks unless supported by corrugated loom tube. Maximum spacing for J-Hook installations is between four feet (4') and five feet (5') requirement from TIA-569.

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.

A fiber cable with a self-supporting jacket construction is preferred when routing in J-Hooks or ladder rack to protect fibers from potential pinches, kinks, or attenuation. Standard fiber distribution cable is not suitable for J-Hooks unless supported by corrugated loom tube. In this case, TIA-569 requires the maximum spacing for J-hook installation to be between four feet (4') and five feet (5').

Pathways are an essential component of physical infrastructure management. As the cables reach their destination point there are several methods for routing the cables in/out of the pathway. Most commonly a traditional cable gland or cord grip is used for a control panel enclosure but the method used depends on the application requirements.

Cable Entry Systems

In addition to traditional cable gland or cord grip type products, there are also cable entry systems that can be used for unterminated and terminated cables. Cable entry systems offer safe, organized cable entry into enclosures and electrical equipment. They provide cable strain relief while maintaining enclosure IP/NEMA ratings protecting against ingress of liquids and solids. These designs are used in a wide array of applications and comply with the stringent requirements of UL 508A and meet strict UV and flammability ratings.

Compared to cable glands or cord grips, cable entry systems only require one punch (based on industry-standard sizes) to mount a frame that can manage multiple cables in a dense space. This simplicity saves 60% on installation time and the high-density hole configurations provide up to 70% space savings which is critical for machine applications that require several cables with limited space on the equipment. Cable entry systems can provide extra hole locations in the same dense design for future cabling moves, adds, and changes.

Cable entry system advantages compared to traditional cable glands/cord grips:

Less installation time

Space savings

Extra hole locations for moves, adds, and changes

Designed for both unterminated and terminated cables

Unterminated cables

Unterminated cables are simply pushed through the ports of the cable entry system as they enter or exit the enclosure. These ports feature a polymer membrane that gives a high-

quality fit around cables and a high degree of strain relief. Basic membrane plate designs are also available giving good strain relief. These designs meet different levels of IP and NEMA ratings up to IP66 and NEMA Type 4X.

Figure 2-9   Unterminated cable entry system

Terminated cables

Applications that have a connector terminated on the cable require a different cable entry system design using cable grommets that fit a wide range of cable diameters and types such as USB, LAN and ASI cables. These designs also meet different levels of IP and NEMA ratings up to IP65 and NEMA Type 4X.

Figure 2-10   Terminated cable entry system

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

Figure 2-11   Earthing, Grounding, and Bonding

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 electrical shock that causes injury and/or equipment damage. A dedicated grounding conductor safely directs the hazardous stray electrical current to ground.

Ground Loop

A ground loop is an unwanted circulating current in a conductor (or shield) connecting two points that should be at the same potential. Ground loops result from multiple ground connections to earth at different potentials, creating a potential difference that causes current to flow.

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 immunity. Shielded Twisted Pair (STP) cable is more effective because it has a metallic sheath that is designed to dissipate the electrical noise when properly bonded. Ideally the shield connection of the STP cable is bonded on the extreme ends of the channel. The challenge is to maintain equipotential when measured between the ends of the channel. An equalizing potential conductor (EPC) may be necessary to eliminate any potential difference and avoid a ground loop. This STP cable bonding method provides the most protection from noise interference, avoids potential reflection from a single bonded end, and optimizes the effect of using Resistor-Capacitor (RC) circuits on end devices.

The use of an RC device termination (aka hybrid bonding or RC filter/ground/network) allows high frequency noise to pass through the loop and blocks the lower frequencies that may be present because of ground potential differences. To properly dissipate the noise many of today's industrial control system devices, such as Rockwell Automation PAC/PLC, include an RC device termination. RC device termination helps to open ground loops by providing a low impedance path at high frequencies and high impedance path at low frequencies for the shield termination, which reduces ground noise currents. Figure 2-12 is taken from ANSI/TIA-1005-A.

Figure 2-12   Example Implementation of RC Grounding
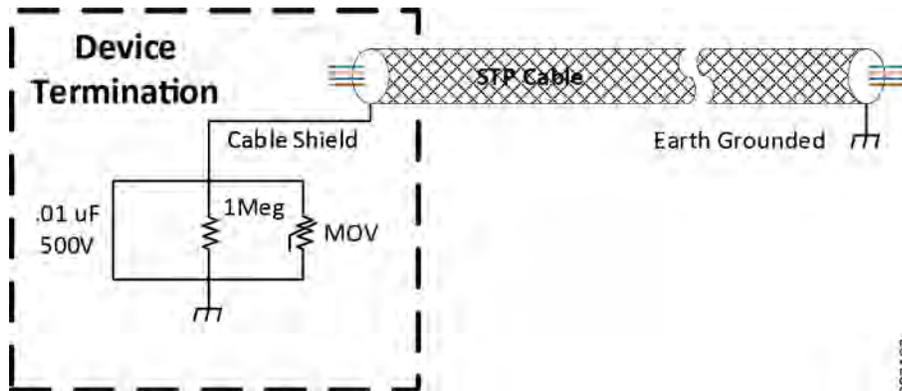
Network cable protected by a grounded noise shield or shielded duct is designed to dissipate electrical noise in an enclosure. Both noise shields and shielded duct provide an equivalent of 6 inches of air space therefore allowing a more efficient use of space in a control panel. Also, a flat, wide bonding strap bonded to the enclosure door and side panels dissipates noise more effectively than standard wire and the braided bonding strap provide a low impedance path to ground (its construction is less susceptible to 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. These types of grounds are common in an Equipotential/Mesh Grounding System. (See Figure 2-13).

Equipotential/Mesh Grounding System

The basis of this grounding system is to provide a low impedance path to ground (earth) between all the devices in the system. This method minimizes the electrical potential difference between the devices and therefore reduce the risk of ground loops. This system requires the use of properly sized equalization conductors. The purpose of an equalization conductor is to provide a path between devices for noise currents to flow so that current does not flow on the shield of the shielded communication cable. Sizing of these conductors is illustrated in chart form in ANSI/TIA-1005-A. A matrix of bonding and equalization conductors, "mesh grounding", will properly carry the currents so that it does not interfere with other devices.

Figure 2-13   Industrial Grounding Network
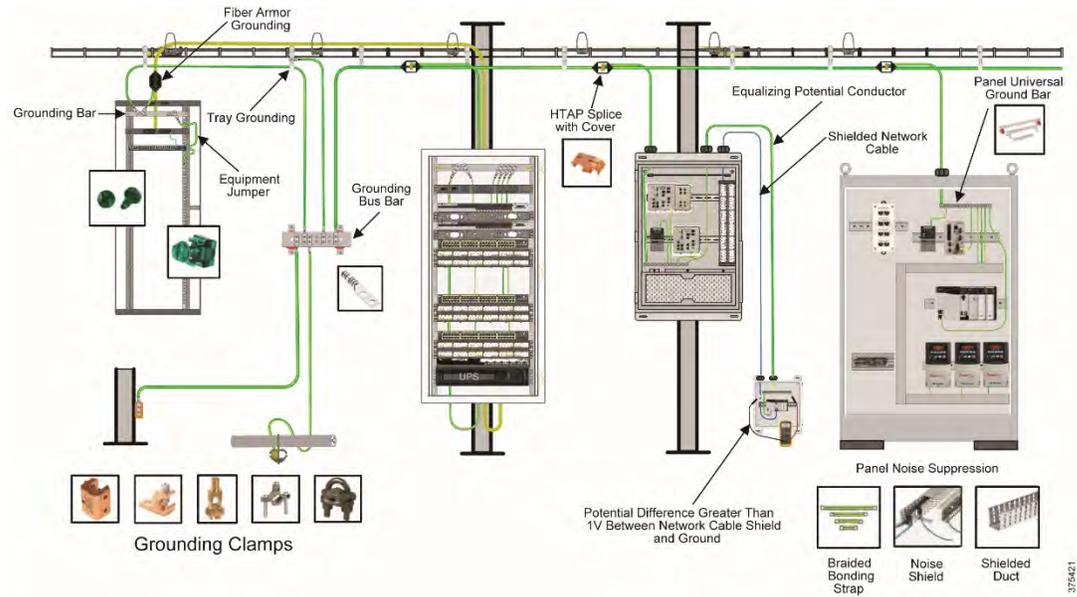
Star Grounding System

The basis of this system is to create a separate bonding system for communication commons. This setup can be utilized to mitigate ground loops in systems where equal grounding potential is not practical. Implementing this type of system will require isolation of grounds and therefore the design may include different types of ground bars that are isolated from a back panel or enclosure. This type of grounding system allows the use of RC (Resistor Capacitor) device terminations. Star grounding image below taken from ANSI/TIA-1005-A.

Figure 2-14   TIA-1005 Star Grounding System
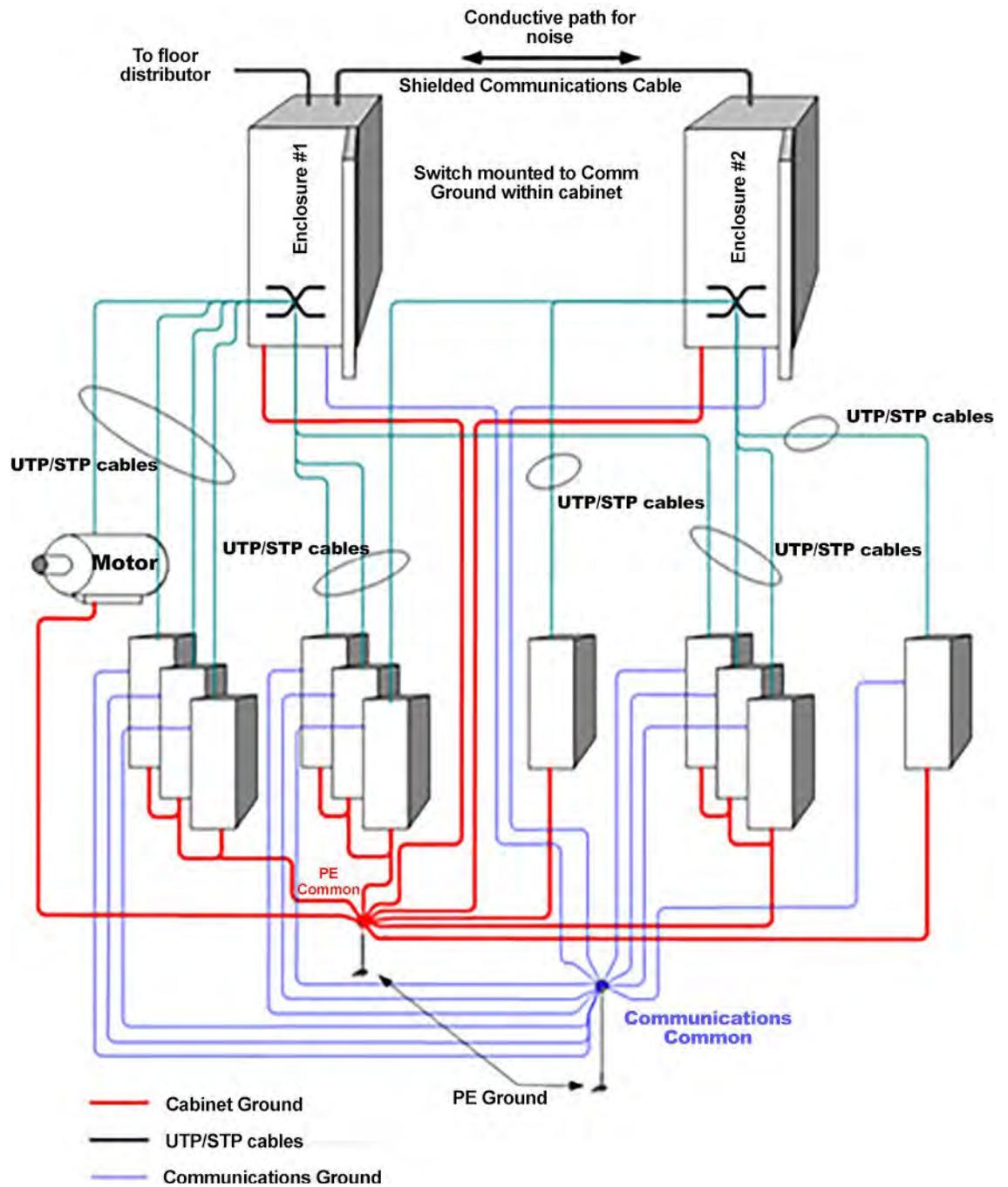
Applicable Grounding and Bonding Standards

o   NEC (NFPA-70) Article 250 and 645.15

o   TIA 607-B and ANSI/TIA-1005-A

o   BICSI

o   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 2-15) involves test instrumentation attached to each link.

Figure 2-15   TIA568 Static Link Testing Set Up
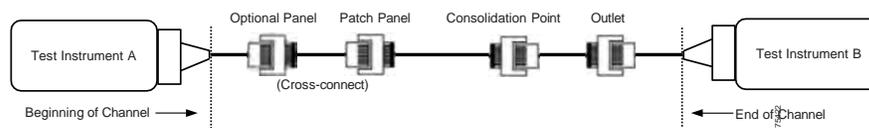
This step is important at installation and commissioning of the network to confirm that any challenges relating   to media installation are uncovered before the network moves into the operational phase. Performance measurements are made and recorded for each link. This baseline performance information 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.

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.

Many businesses are considering the deployment of augmented reality applications to aid in equipment maintenance and to facilitate remote expert interactions. AR requires low latency and significant bandwidth to function correctly. Because this high-performance connectivity must be widespread and nearly ubiquitous, these requirements motivate the use of high capacity wireless. Suitable forms of high-capacity wireless include Wi-Fi 6 / Wi-Fi 6E and 5G cellular networks. Each provides needed base functionality to support AR. Selection of which wireless infrastructure is a function of which method best suits business needs.

Most businesses considering 5G cellular networks deploy a private 5G network. A private 5G network is a cellular network dedicated to the business or organization. It includes cell sites and core network servers, eliminating reliance on public cellular networks.

Wi-Fi 6 or Wi-Fi 6E are deployed like the wireless networks in businesses today to provide employees with internet access within the facility. Traditionally, many wireless networks in businesses are architected and operated by the business IT staff, though

some opt for wireless delivered by managed service organizations like Cisco's Meraki group.

In the traditional installation, wireless access points, cabled infrastructure and network switches dedicated to the wireless network are purchased, commissioned, and maintained by business IT staff.

Managed service organizations operate like cellular providers in that they deploy, operate, and maintain the network, delivering connectivity in accordance with a mutually agreed SLA and collecting fees for their services.

Given the criticality of the applications supported by this new wireless service, the first concern of the business IT staff should be the level of wireless domain expertise they have on staff to deploy and operate such a network. Of almost equal importance is the resource available to maintain the network over its useful life.

Consider this comparison of Wi-Fi Standards in the table below.

Table 2-2   Comparison of Wi-Fi Standards

	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6	Wi-Fi 7*
IEEE Standard	802.11n	802.11ac	802.11ax	802.11be
Access Point Density	Low	Medium	High	Very High
Data Rates	450 Mbps	1.2 Gbps	2.5 Gbps	10+ Gbps
Cable	Cat 6	Cat 6a	Cat 6a	2x Cat 6a

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 transmission, like Wi-Fi or 5G cellular, carry information wirelessly through the electromagnetic spectrum, specifically the radio spectrum.

5G cellular service uses specific frequency ranges, called spectrum, to deliver connectivity. Not all service providers use the same frequency spectrum for 5G service. 5G spectrum is licensed (through auction), shared or unshared. The ITU (International Telecommunications Union) regulates the use of radio frequency spectrum around the world. Domestic use of spectrum is further controlled by different regulatory bodies, such as the FCC (Federal Communications Commission) in the United States.

Wi-Fi 6 is defined by an IEEE standard, IEEE 802.11ax. The name Wi-Fi 6 comes from the Wi-Fi Alliance and identifies 802.11ax as the 6th generation of Wi-Fi, therefore, Wi-Fi 6. Wi-Fi 6 is designed to operate in the license exempt frequency bands between 1 and 7.125 GHz. This operating spectrum includes the 2.4 GHz and 5 GHz bands used in earlier Wi-Fi generations, as well as the much wider 6 GHz band. Wi-Fi installations operating in the 6 GHz band are called Wi-Fi 6E.

Spectrum is important because frequency affects wireless speed and power. All radio waves travel at the speed of light. But not all waves react with the environment in the same way or behave the same as other waves. Generally, frequency has the following impact on wireless transmission.

Higher Frequency	Lower Frequency
Faster Speeds	Slower Speeds
Shorter Distances	Longer Distances

How does frequency affect distance? Wavelength is inversely proportional to frequency (e.g., high frequencies have shorter wavelengths). When a wavelength is short, such as the frequencies at the higher end of the wireless spectrum, the waveform is so tiny that it can easily become distorted. Therefore, high frequencies don't travel as far as the shorter ones.

Speed is the second factor impacted by frequency. Bandwidth is measured by the difference between the highest and lowest frequency of the signal. Therefore, moving up the frequency spectrum provides a higher range of frequencies and greatly improved throughput. Wi-Fi 6 or 5G technologies both bring a higher frequency range and commensurately higher bandwidth. However, higher speeds also mean the wireless signal travels shorter distances. The distance limitation imposed by higher frequencies increases the wireless access point density needed to achieve target coverage at these speeds.

Generally, frequency bands are used to support 5G cellular, low-band (sub GHz), mid-band (1-7 GHz) and high-band (24+ GHz).

Millimeter wave (mmWave) is a term often associated with 5G cellular which has a high frequency range between 24 GHz and 300 GHz. This range of frequencies is often called millimeter band, so called because its wavelengths range from 1 to 10 millimeters.

Given the influence of frequency on bandwidth, it's easy to conclude that high throughput applications need millimeter wave wireless. Millimeter wave wireless delivers staggering levels of wireless throughput. However, because of the very short wavelength in this frequency range, distances are very short compared to low-band and mid-band. The lack of coverage and penetration from millimeter wave wireless must be supplemented by increasing the wireless access point density in each area requiring its performance.

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.

Industrial environments further complicate the use of wireless. Complication arises because of the machinery, objects, people, and material handling equipment in the environment. Many of these items either reflect or absorb wireless transmissions which impacts reliable transmission. Absorption and/or reflections can cause coverage gaps – holes in the coverage if you prefer – or cause the need for signal retransmission to ensure successful communications. Further, some of these wireless disruptors are in motion, creating a literal "moving target." Therefore, carefully surveying the area is necessary to ensure a capable wireless deployment.

If 5G (public or private) cellular is chosen and your company operates over a global footprint, carrier choice is *vital* as not all carriers operate over the same frequency bands. Different frequency bands make the job of replicating your wireless deployment globally more difficult.

If a private 5G cellular network is the choice for your business, cabled infrastructure is installed by the service provider or their delegate. Be certain when planning the installation to point out any extreme environmental conditions so that proper cabling and enclosures can be chosen for the installation. Also, it is important to determine a proper demarcation point where the 5G network connects to the Enterprise network. Careful examination of security practices and policies is vitally important in this exercise. Be certain your corporate IT staff is engaged and fully satisfied with the cyber security measures undertaken by both parties.

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:

- http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.html
- http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf

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 using 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-162bases 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, 802.11na and 802.11ac, the most recent standard to be released is IEEE 802.11ax, also known as Wi-Fi 6. 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, Generation 2 APs and IEEE 802.11ax (Wi-Fi 6) the backhaul rate is increased 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.

A well-designed and installed physical layer is needed to support the wireless access points. It's important to plan current and future wireless coverage needs so the cabled infrastructure doesn't need a lot of attention over its useful lifespan.

When Wi-Fi is the chosen form of wireless for your business, bear in the mind that wireless access points are typically powered using PoE (Power over Ethernet). The network switches serving the wireless access points act as PSEs (Power Sourcing Equipment), delivering PoE to the access points which are PDs (Powered Devices). When planning AC power capacity for the network switches, remember that PoE places power supplies onboard the network switch which draw considerably more power than the switch itself.

Most known wireless application requirements indicate Wi-Fi 6 / 6E supplies satisfactory bandwidth for high capacity / low latency needs. Supplying cabled connections to the wireless access points is most often accomplished with Category 6A cable. Category 6A cable provides 10 Gb/s transmission speeds, making it the ideal choice when cabling Wi-Fi 6 / 6E access points. Current best practices recommend pulling two cables per access point.

It is important to note that the cost to install cabling is always lowest during the initial buildout. Laying cable at later stages is often substantially more expensive and difficult. When designed a cabling infrastructure, it is vital to understand where Wi-Fi standards are headed.

	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6	Wi-Fi 7*
IEEE Standard	802.11n	802.11ac	802.11ax	802.11be
Access Point Density	Low	Medium	High	Very High
Data Rates	450 Mbps	1.2 Gbps	2.5 Gbps	10+ Gbps
Cable	Cat 6	Cat 6a	Cat 6a	2x Cat 6a

The proposed IEEE 802.11be standard recommends two Category 6A cables per access point in some cases. The Wi-Fi7 name is speculative as it has not been announced by the Wi-Fi Alliance.

Hence, the requirements for cabling infrastructure should:

● Support the Wi-Fi data rates of today and of the future

● Support easy moves, adds, and changes that enable increased density

● Support the Wi-Fi data rates of the future when more than one multigigabit AP ports might be needed.

Therefore, you should consider running two to four Category 6A cables per wireless access point where high density is required.

● Today: One cable can be used today to support a Wi-Fi 6 access point

● Near future: Two cables are used to support two Wi-Fi 6 access points for increased density

● Future: Two to four cables will be needed to support two Wi-Fi 7 access points (potentially two cables to each access point)

What's next for Wi-Fi and PoE?

Several of the exciting new elements coming with Wi-Fi and PoE. While Wi-Fi 6 is the best Wi-Fi standard currently available, the IEEE 802.11be standard (we've assumed that it will be called Wi-Fi 7) is under development and the standard is expected to publish in the 2023 and 2024 timeframe.

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 four versions exist:

• IEEE 802.3af, Type 1, delivering up to 12.95 watts at the end of a maximum-length channel

• IEEE 802.3at, Type 2, delivering up to 25.5 watts at the end of a maximum-length channel.

• IEEE 802.3bt, Type 3, delivering up to 51 watts at the end of a maximum-length channel.

• IEEE 802.3bt, Type 4, delivering up to 71 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.

The next-generation IEEE 802.3bt PoE standard has been ratified, and products using this standard are being deployed. This new standard is ideal for technologies such as next-generation wireless access points that are assumed to have a higher power draw and higher data rate needs that the new PoE standard can supply. This standard is also expected to see a lot of new devices come onto the network due to its higher power capabilities.

Access Points in Harsh Environments

APs used in plant/site deployments are frequently located in harsh, or even outdoor, environments. There are some options for deploying AP's that are natively rated for this environment but if they are not then 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.

Physical Infrastructure Design for the Cell/Area Zone

Successful deployment of a Converged Plantwide Ethernet (CPwE) logical architecture depends on a robust network infrastructure design, starting with a solid physical layer that addresses the environmental, performance, and security challenges with best practices from both Operational Technology (OT) and Information Technology (IT). Through collaboration on technology and physical network infrastructure, Panduit teams work with Rockwell Automation and Cisco to help customers develop a scalable, robust, secure, future-ready plant-wide industrial automation and control system (IACS) physical network infrastructure. The rapid growth in both IACS devices that leverage EtherNet/IP, and non-IACS devices that leverage IP for security, mobility, and so forth, requires a structured, physical layer deployment.

This chapter addresses key recommendations and best practices to simplify design and deployment of a robust industrial Ethernet physical layer focused on the Cell/Area Zone - Levels 0-2 of the CPwE reference architecture.

Logical to Physical Mapping

A Cell/Area Zone consists of machines, skids, and equipment to be monitored, managed, and controlled. A Cell/Area Zone consists of Level 0 sensors and actuators, Level 1 controllers, and Level 2 local supervisory function (see the following figure). This chapter discusses aspects of the physical infrastructure deployment in the Cell/Area Zone.

Figure 3-1 CPwE Logical Architecture to Physical Plant/Site
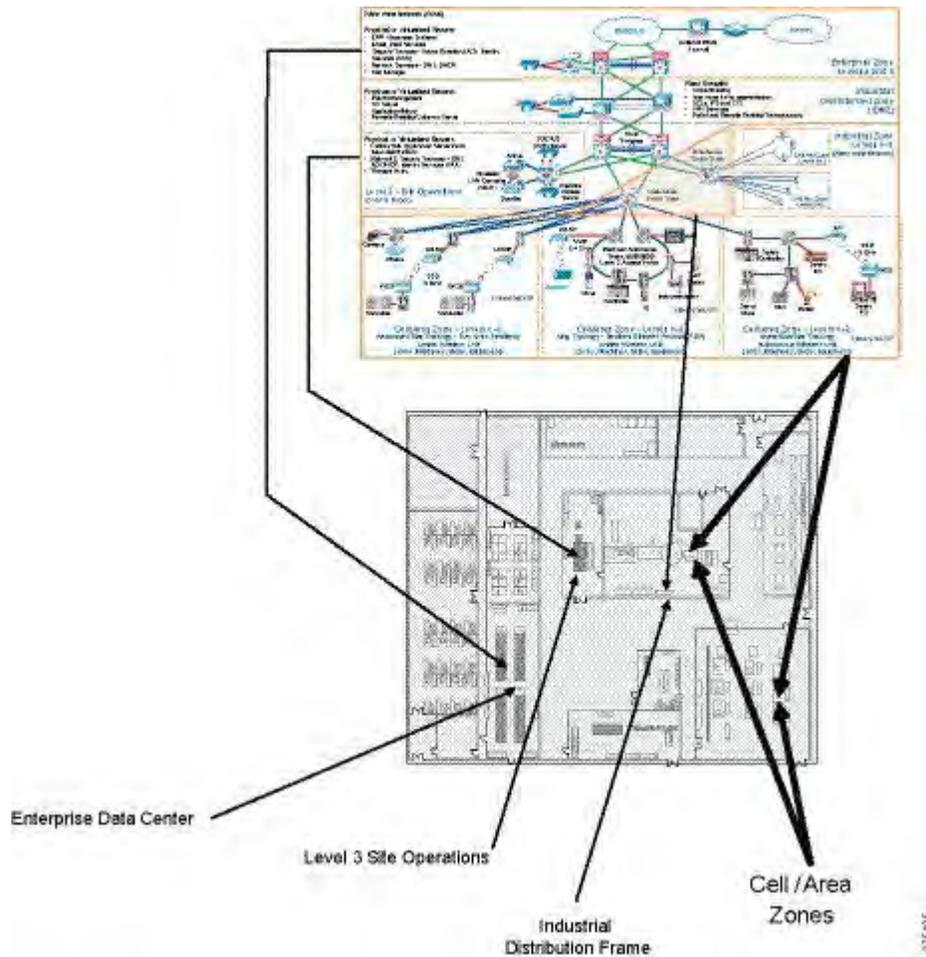
The Cell/Area Zone differs from much of the upper-level network in several important areas. Cell/Area Zone requirements affect both the equipment and media deployed in these areas as follows:

- Being directly adjacent to the process, the environment encountered by both equipment and cabling is usually at its most harsh, therefore network cables, connectors, and equipment must withstand these conditions.

- Local cabling architectures in the Cell/Area Zone can take on different forms. For example, the three types shown include Redundant Star, Ring and Linear/Bus topologies.

- Although standards-based structured cabling is almost exclusively used at higher levels within the plant and enterprise networks, frequently in Cell/Area Zone Levels 0 - 2 a point-to-point cabling method is often encountered. Although variations can exist, this cabling most typically involves the use of stranded Ethernet copper cabling field terminated with RJ45 or M12 plugs. This allows direct connections between pieces of equipment.

- Physical Cisco and Allen-Bradley Stratix IES deployment can range from switches located inside a dedicated PNZS or control panels to machine-mounted IP67-rated switches.

- Wireless deployments in plant/site environments may be subject to various factors in the environment that cause reflection or signal attenuation and competition for frequency spectrum. A thorough site survey and spectrum analysis are required.

Figure 3-2: Cell/AreaZone Logical to Physical Mapping
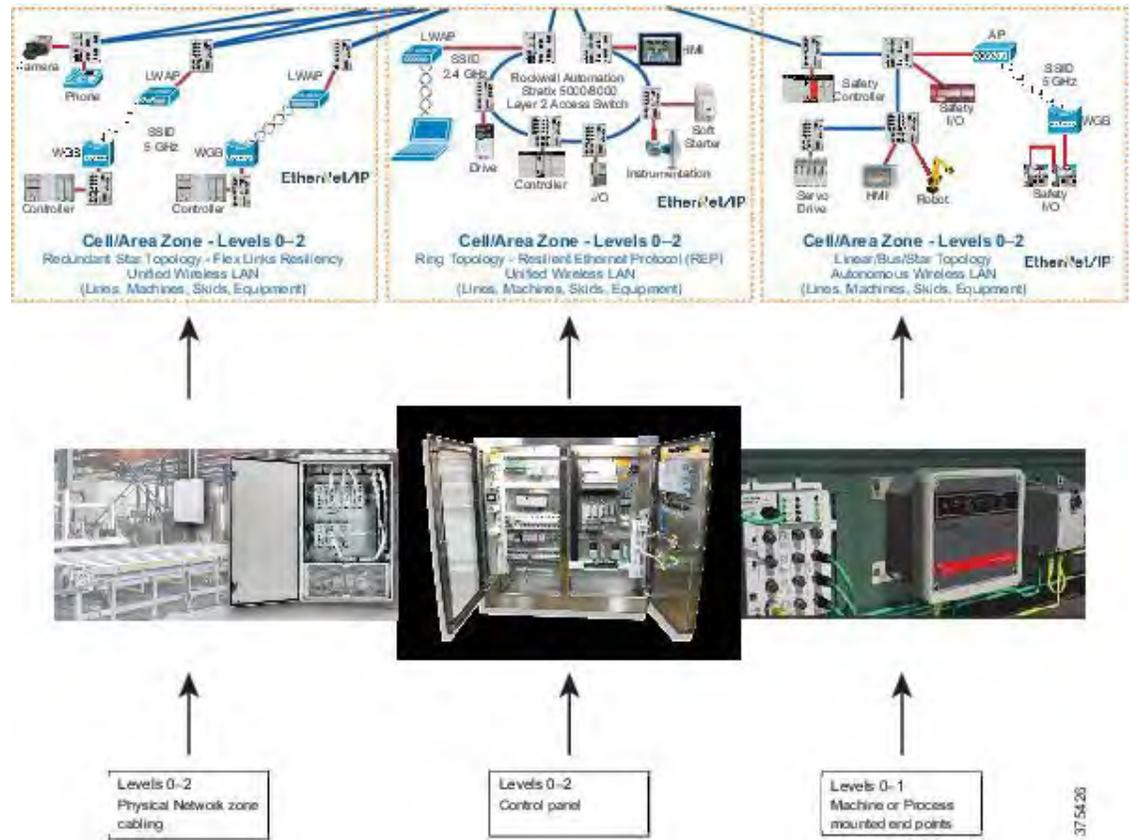
Key Requirements and Considerations

Many aspects of the Cell/Area Zone serve an important role and must be considered in the design and implementation of the network:

- **Availability**—The design of a robust and reliable infrastructure achieves service levels demanded of current and future networks. The use of standards-based cabling together with measured, validated
performance confirms reliable data throughput. Use of redundant logical and physical networks assures highest availability.

- **Reliability**—The harshest environments are often encountered in the Cell/Area Zone. In addition to
extreme mechanical and environmental exposure, network cabling is often subject to excessive levels of EMI. Solution choices must be made between unshielded, balanced twisted-pair cabling or shielded, balanced twisted-pair cabling, with appropriate attention paid to grounding and bonding. In situations where satisfactory performance cannot be achieved, fiber-optic solutions can provide an option for highly reliable, error-free communications.

- **Future ready**—Consideration of higher performance cabling categories enables the data communications to fully meet current and future Cell/Area Zone requirements. Choices in media between copper and fiber cabling assure higher data rate transport requirements.

- **Security**—Network security is critical to its uptime and availability. Physical layer security products, such as jack blockouts and plug lock-ins help limit access to and help prevent inadvertent or malicious removal or installation of patch cords to help achieve service level goals.

- **Scalability**—The use of a physical zone topology with structured copper and fiber cabling chosen for high data throughput and building block type pre-configured solutions enable a network infrastructure comprised of modular components that scale to meet the increasing data communications needs of discrete and process-orientated IACS applications.

Physical Network Design Considerations

In the Cell/Area Zone, several key areas should be considered for physical network design. This section uses terminology associated with media in the Cell/Area Zone; however, these media types are described in more detail later in this chapter.

- **Physical media**—copper and fiber connectivity

- **Skid/Machine/Equipment**—Device Level

- **Cell/Area Zone Cabling**—Control Panel

- **Cell/Area Zone Cabling**—Redundant Star

- **Resilient Ethernet Protocol (REP) Ring**—Zone Deployment

PNZS for housing IES as networks scale to larger node counts.

IDF system for distribution switch infrastructure deployments for the Industrial Zone.

Physical Media

Skid/Machine/Equipment—Device-Level

Cabling on the machine is often subjected to the harshest environment in the entire network. The M.I.C.E. criteria, which are described in Chapter 2, "Physical Infrastructure Network Design for CPwE Logical Architecture," are used to characterize different environment types and guide media and connectivity selection. The following figure shows the topology often used at Level 0 and 1 where I/O devices are connected in a device-level ring topology using the ODVA Device Level Ring (DLR) protocol to provide a redundant path connecting all devices to an IES. If a cable connecting two adjacent devices fails, the ring supervisor detects this fault and forwards traffic in the other direction, maintaining the connection of all devices to the network.

Figure 3-3 Device Level Ring Topology
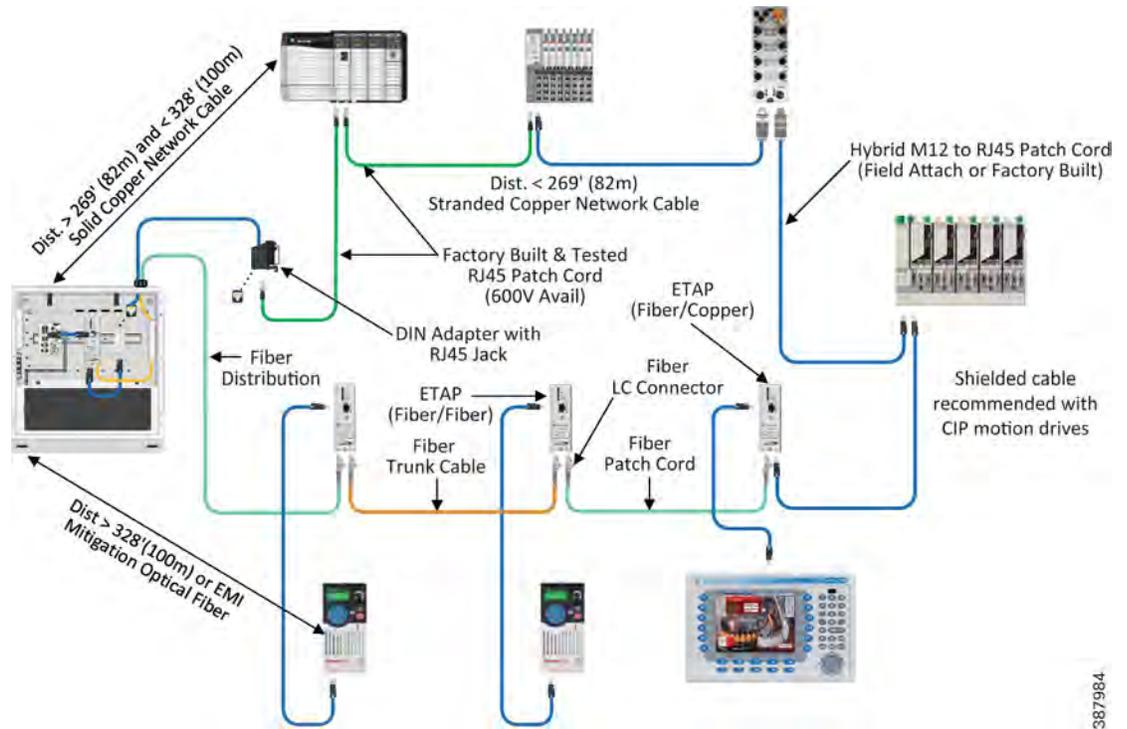
Optical fiber is also used in the Cell/Area Zone. Frequently, Cell/Area Zone installations use IP67-rated connector options. Copper cabling using M12 connectivity (see the following figures) or IP67-rated RJ45 connectivity is applicable in many environments and applications.

Figure 4: Example of M12 Connectivity - Field Terminable M12 D-code Plug

Figure 3-5 Example of M12 Connectivity - RJ45 to M12 D-code Adapter)

Cell/Area Zone Cabling—Control Panel

The control panel is typically connected to functional areas within the Cell/Area Zone. Network connections can be made from the control panel to the machine, for example, to an IES or I/O block on the machine. On the other side, network connections are made to PNZS or IDF where typically other network connections converge and consolidate before being routed to higher levels within the Converged Plantwide Ethernet architecture.

The following figure illustrates a detailed view of the Cell/Area Zone linear/bus/star topology. In this example, the control panel contains an IES (such as Stratix 5400) to connect devices such as Human Machine Interface (HMI), Programmable Automation Controller (PAC), and variable-frequency drives (VFD). The uplinks are connected to the PNZS.

Figure 3-6 Linear Connectivity Deployment Example
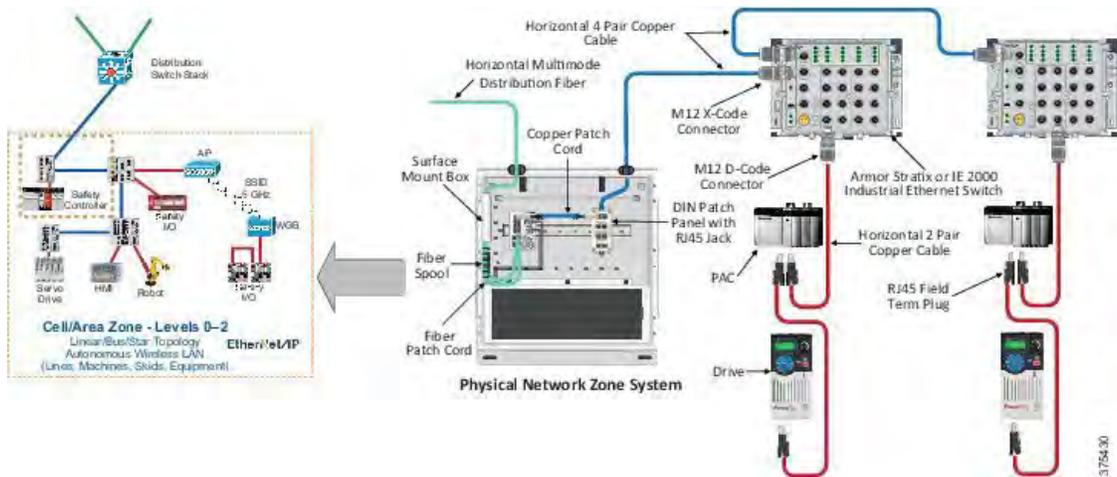
The control panel environment exposes industrial Ethernet cabling to EMI risks from VFD drives, contactors, power supplies, and other sources. The use of shielded cabling, EMI noise shields and shielded patch cords, as shown in the following figure, reduce risk of noise coupling causing equipment downtime or damage. 600V rated cabling is useful to comply with standards such as UL508A requirements for control panels with higher voltages (such as 480VAC). Consult your local standards to specify media that addresses safety guidelines in control panels.

Figure 3-7 Schematic of Control Panel
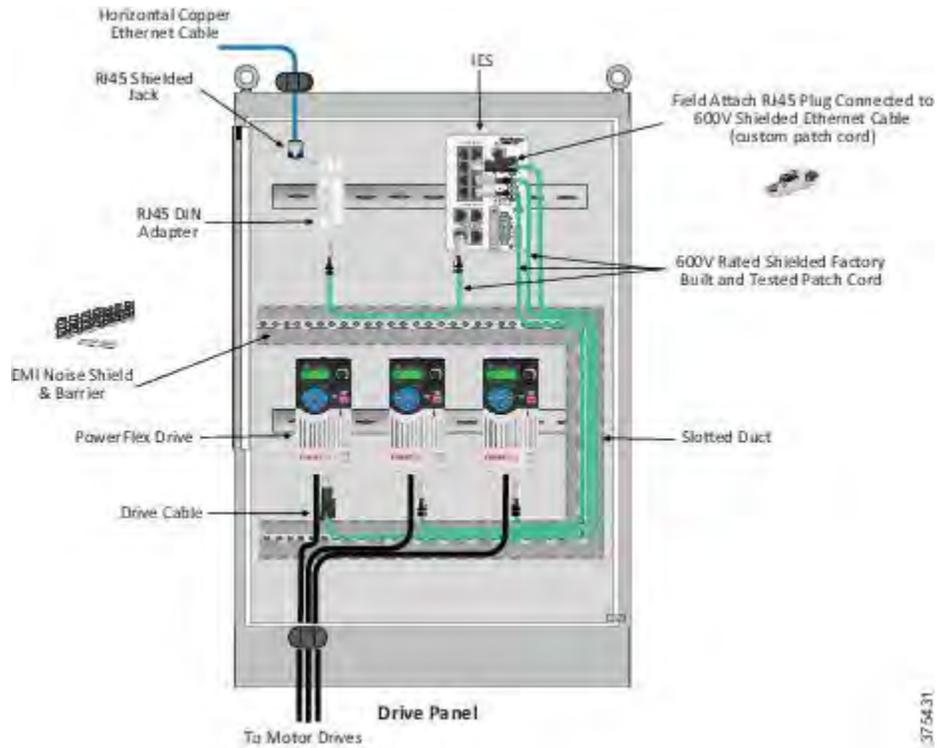
The following figure illustrates the cabling configuration for the control panel to a PNZS. In this figure, horizontal copper cable downlinks to devices are routed from the PNZS into the control panel. Entry can be made in various ways, such as through a metal conduit that is attached to the control panel enclosure by means of a conduit gland, or through a cable transit. For uplink connections, individual fibers are terminated, and the connectors installed into adapters contained in the fiber DIN patch panel. The fiber DIN patch panel
enables use of fiber adapter panels, or fiber cassettes for ideal fiber termination, slack provisioning, and protection within the DIN rail mountable housing. Fiber patch cords are used to connect from the front face of the adapters in the fiber DIN patch panel to the IES. The IES uplinks typically use SFP pluggable transceivers that in turn are provisioned with duplex LC type connections.

Figure3- 8 Fiber DIN Patch Panel, Fiber Panel, Fiber Cassette examples

Figure 3- 9: Redundant Star Topology
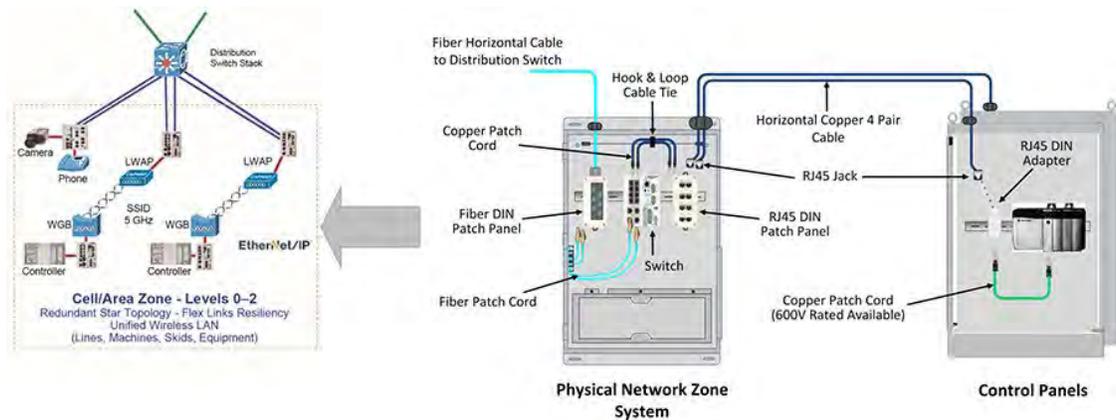
Cell/Area Zone Cabling—Redundant Star Switch-level Topology

The IES shown in the following figure provides network connections to individual applications. A number of individual applications can be connected to the IES (for example, video surveillance camera, voice over IP phone) and then connected to the higher level network. This connection to the network from the IES switch is critical because damage to the connection causes failure to multiple applications. For this reason, it is often necessary to create multiple redundant uplink paths to support traffic, if the primary connection fails.

The IES, depending on the model, is provisioned with redundant uplink ports. Two cable runs can be made to a higher level, such as distribution switching. The connection route from the IES to the distribution switch should be different for the main cable and redundant cable runs. If this is not accomplished, the level of redundancy is compromised. For example, if both runs are routed in the same pathway, then catastrophic damage to the pathway would likely sever both cable runs.

A PNZS provides environmental protection for the IES and serves as a consolidation point for multiple network connections. The PNZS contains physical infrastructure that is required to make network connections to the switch and can be pre-configured; that is, supplied with all the required physical infrastructure components assembled into the PNZS or integrated where the active IES is supplied along with the physical infrastructure to constitute a ready to go building block system. The PNZS solution is described in more detail later in this chapter.

Cell/Area Zone Cabling—Switch-Level Ring Topology

The implementation of the switch-level ring topology within the Cell/Area Zone is like the linear/ star topology described previously. However, for the switch-level ring topology, a further industrial Ethernet cable is added that connects the last IES in the linear network back to the distribution switch, which closes the ring to form redundant path topology. If one industrial Ethernet cable or IES fails, communication is converged in the other direction around the ring to make sure that all other switches are still connected to the network. The switch-level ring topology is highlighted in the following figure.

Figure 3-10 Switch-level Ring Topology in the Cell/Area Zone
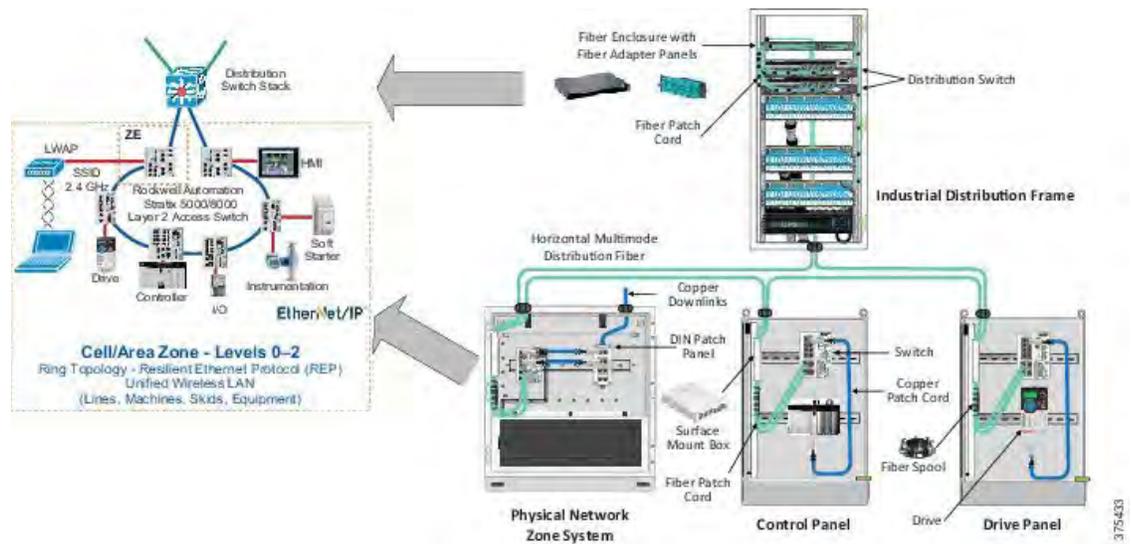
Cabling Jacketing Materials

Communications and control networks are expected to operate consistently and reliably in all types of environments that are characterized by the M.I.C.E. criteria that are described in Chapter 2, "Physical Infrastructure Network Design for CPwE Logical Architecture." In harsh environments, industrial networked communications systems are required to be extremely durable. If exposed to harsh environments, physical deterioration in cabling infrastructure can occur and failure in mission critical data transmission components can lead to defective network performance and safety issues, ultimately leading to loss of data transfer, costly downtime, or catastrophic failure. Cable jackets that are used in industrial environments, and guidance for the choice of jacketing material are indicated in the following figure.

Figure 3-11 Cable Jacket Materials

Function	PVC	TPE	PUR
Oil Resistance	Good	Very Good	Very Good
Abrasion Resistance	Good	Very Good	Excellent
High Flex Applications	Good	Excellent	Excellent
Smoke Rating	CM	CM CMX Outdoor	Zero Halogen (IEC 60332-1)
Relative Cost	$	$$$	$$$

Cable and Connector Ingress Protection

IEC 60529A specifies the degree to which an item can withstand the effects of particle or liquid entry. Ingress Protection, IP rating, is the rating that is based on these tests for the component. In the case of particle ingress, 0 represents the lowest level of ingress and 6 represents the highest level. In the case of liquid ingress, 0 represents the lowest level of ingress and 8 represents the highest level.

The IP69K rating is for applications where high pressure and high temperature washdown is used to sanitize equipment such as food and beverage. The IP69K test specification was initially developed for road vehicles, especially those that need regular intensive cleaning, but has been widely adopted in the food and beverage industries as a test of product ability to withstand sanitary washdown.

Ethernet Copper Cable Types—Unshielded and Shielded

When choosing a shielded cable type, several options should be considered. The following figure shows the three major categories of shielded cables. The difference between these 3 categories is the amount of shielding and the type of shielding utilized. For example, shielding the individual pairs provides another degree of protection from cross-talk between the pairs. Typically foil shielding is less expensive and great for
high-frequency applications whereas braided has excellent mechanical strength, great for low to medium frequency but is often more expensive than foil. The best fit depends on the specific application.

- Screened UTP cable includes an overall foil around the pairs

- a STP cable includes shield around each individual pair

- Screened STP cable includes an overall shield, or braid, around all pairs with an additional foil around each individual shield

Figure 3-12: Cross Section of Shielded Twisted Pair Cabling Type
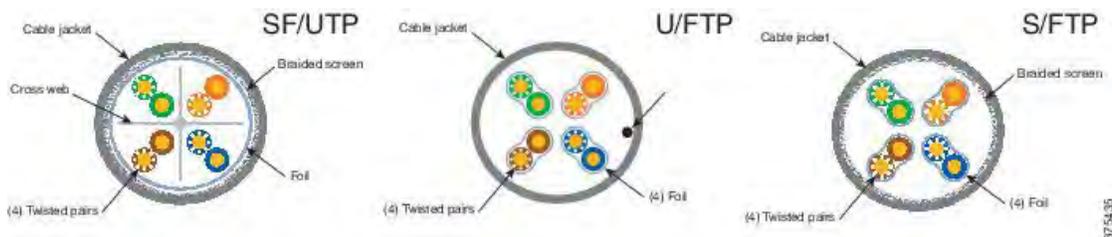
Connector Types

Ethernet connectivity makes almost exclusive use of the 4-pin or 8-pin version of the RJ45 connector. When using 4 pins, pins 1, 2, 3 and 6 two-way data traffic is supported up to and including data rates of 100 Mbps. Four-pair twisted pair cable that is connected to all eight pins of the connector supports higher data rates (such as 1 Gbps) when the channel is rated to Category 5e or higher.

The RJ45 used in Enterprise type environments, such as in the office or data center areas, is rated as being suitable to meet the requirements of IP20. An external housing is required to be fitted around the RJ45 plug and jack if the connector system is to meet higher IP ratings. Various housing types exist, defined in IEC standard 61076-3-106. Variant 1 is the type of standard that is adopted by the ODVA for EtherNet/IP
connectivity. An example of Variant 1 is shown in the following figure.

Figure 3-13 Quick Connect Variant 1 Example
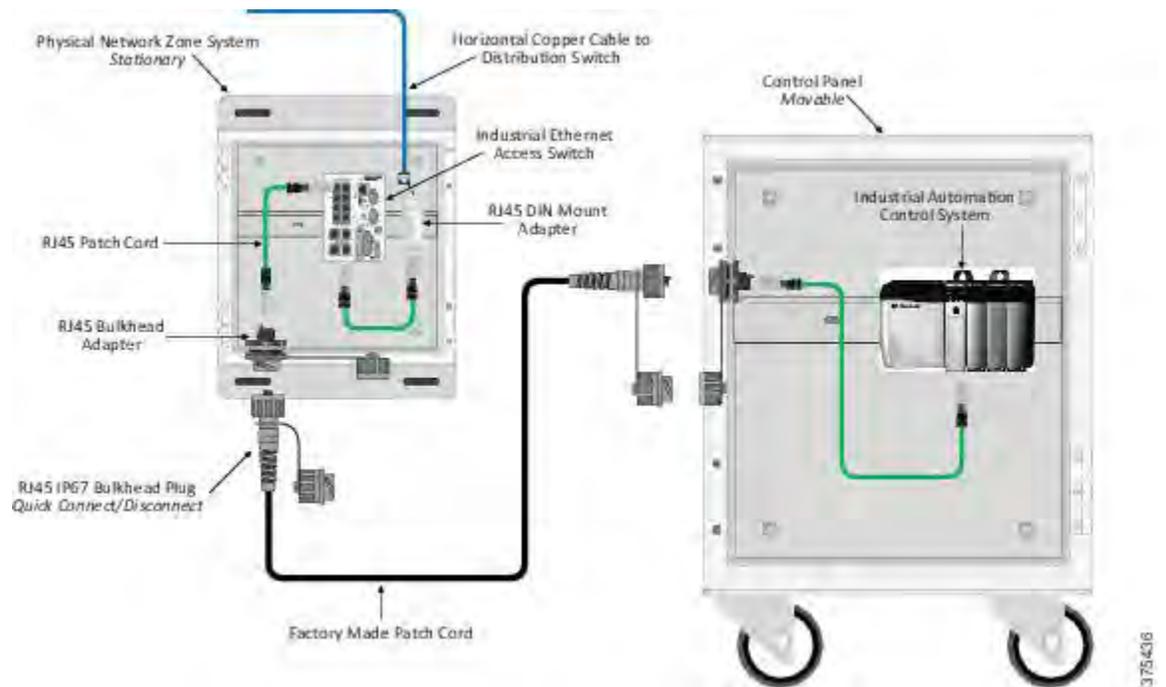
In addition to the preceding RJ45 connection types described, other connector form factors that provide IP65/IP67 ingress protection that are used for twisted-pair cabling. Figure 3-12 shows the M12 form factor. ODVA adopted four and eight pin versions in support of EtherNet/IP. Different pin and keying arrangements are possible with these connector types. Specifically, EtherNet/IP uses the D-code for the 4-pin and X-code for the 8-pin connector types. The M12 D-code connector system conforms to IEC 61076-2-101; the M12 X-code connector system conforms to IEC 61076-2-106.
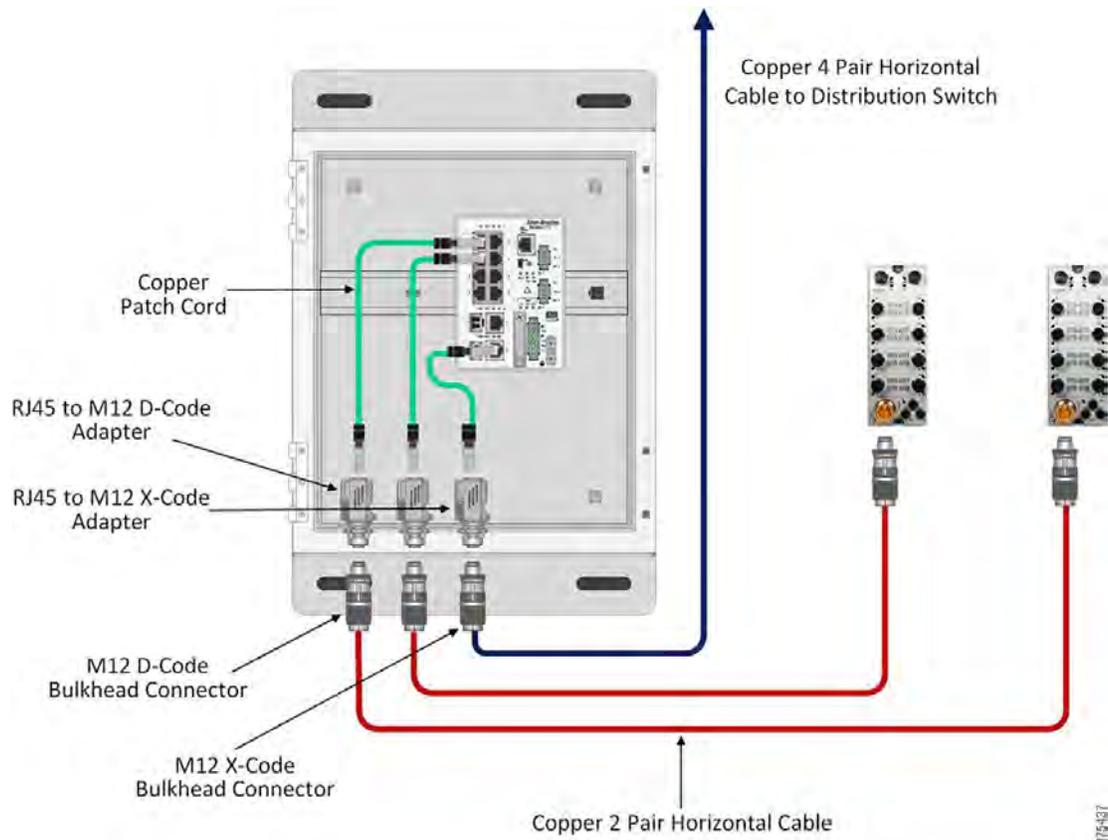
Fiber Options for the Plant/Site—Cell/Area Zone

Chapter 5,"Physical Infrastructure Deployment for Level 3 Site Operations" describes the OS and OM fiber types that are used to connect from the Industrial Zone through to the PNZS in detail. Fiber that is used in the Cell/Area Zone is often required to be easy to install. Electrical contractors are frequently employed to connect control panels to and in the vicinity of the machine using field termination methods. Although these connections generally center on copper cabling, electrician-friendly fiber-optic media does exist for use in the Cell/Area Zone.

Physical Layer Design for WLAN

Wireless networks are increasingly being used for critical IACS applications in the Cell/Area Zone. The physical layer provides wired connections to wireless APs that are in the plant. Wired connections can be made from APs to switch ports that are in any of the pre-configured building blocks that are used throughout the plant. Wired connections also can be made to either of the WLAN architectures. Typically, wireless APs or WGBs are connected to the PNZS. In some plant deployments, connections for the APs may be direct to the IDF, as is typical in a Level 0-3 deployment, or directly to the IDC. The industrial WLC is commonly located in Level 3 Site Operations.

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:

- https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.htm

- https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf

The following figure shows a cabling configuration for an AP (or other device such as PoE camera) where power is supplied to the AP via PoE.

Figure 3-15 Cabling Configuration for Wireless Access Point and Other Devices
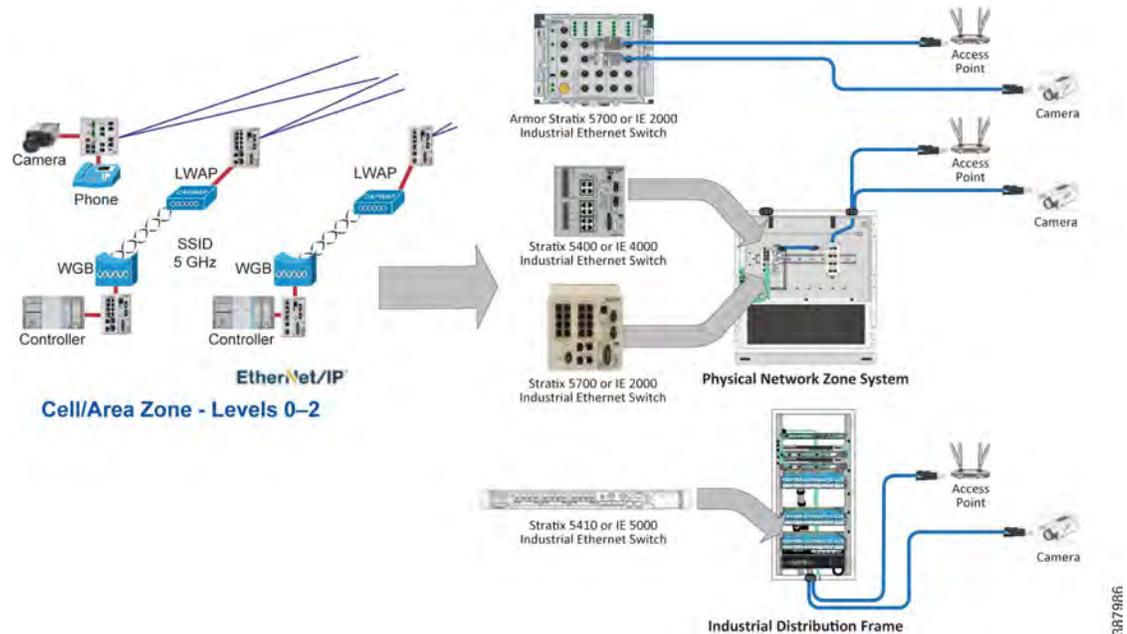
Uplink fiber termination into the control panel is made into a fiber adapter that is mounted in the surface mount box and connected to the switch by a fiber patch cord. Fiber patch cords connect both to internal devices and the Fiber DIN Rail Patching Solution. Downlink copper cables are installed, connected inside the Fiber DIN Rail Patching Solution and proceed out of the control panel to the device. Usually, but not always the cable is terminated with a plug, rather than a jack.

Deployment Points

Several topics relate to the physical layer and deployment of WAPs and are listed below:

- **Location of Wireless Access Points**

    Industrial environments are highly dynamic with RF reflectors and absorbers present in abundance. The location of WAPs is determined using wireless coverage and performance modeling software, which is then validated during the commissioning phase. Thorough initial testing of the WLAN during the commissioning phase revealed that on occasion the location of the AP has to be moved slightly to accommodate building layouts, obstacles, and so on that were not considered or changed after software modeling. The structured cabling to connect the AP to the IES can be designed to accommodate some installation variability. Use patch cords to connect APs to fixed Equipment Outlets (EO) that in turn connect to the horizontal cable run. This concept is introduced in the TIA Technical Services Bulletin (TSB): *TSB-162 Telecommunications Cabling Guidelines for Wireless Access Points*.

    The above referenced TSB bases initial design deployment of APs on a square grid model. It emphasizes software performance prediction and then determines any deviation of AP locations from this grid. Frequently, in larger plant wireless deployments, vertical structural beams that support the roof are used to support APs. These beams form an array of support locations for APs. These beams can also provide convenient support locations for the PNZS (containing IES) found in the Cell/Area Zone area.

- **Cabling Used for Wireless Access Points**

The original release of IEEE 802.11 standards for WLAN, IEEE 802.11-1997, supported data rates of up to 2 Mbps. From that starting point, IEEE have developed technology that pushes WLAN systems to ever higher data rates. The most recent standard is IEEE 802.11ax and is now referred to as Wi-Fi 6.
Through progression of 802.11b, 802.11g, 802.11a, 802.11n, backhaul data rates were less than 1 Gbps meaning that Category 5e or 6 cabling could be used. With the advent of IEEE 802.11ac, however, Generation 2 APs (the Second Wave) have backhaul rates over 1 Gbps. This wireless performance increase makes it necessary to use Category 6A cabling for 802.11ac backhaul connections. Category 6A supports data rates of up to 10 Gbps, therefore providing the ability to support Wi-Fi 5 and Wi-Fi 6 deployments. Category 6A cabling is recommended for new deployments. Some references have been made for two Category 6A cables to be used for each AP, increasing reliability and availability if channel failure occurs. Utilizing at least two cables will provide future proofing for the next generation of Wi-Fi, which is projected to have speeds over 10 Gbps. Installing the appropriate cable during the initial installation is significantly less expensive than the cost of adding or changing cables in the future.

- **Direct connection (point-to-point)**

Good use cases exist for direct connect cabling (point-to-point connectivity) for individual device connections on the network, such as short single-connection runs found when connecting field devices. Direct connect cabling provides a cost-effective and reliable way to connect devices such as wireless access points, cameras, sensors and other devices becoming more common in industrial facilities.

The easiest way to deploy direct connect cabling is to attach a field-installable plug at the end of the horizontal cable link where it is inserted into the network device. Field cord connections are also available providing a small form factor patch cord in combination with a field terminable connector.

Figure 3-16 Structured Cabling for Ethernet Networks
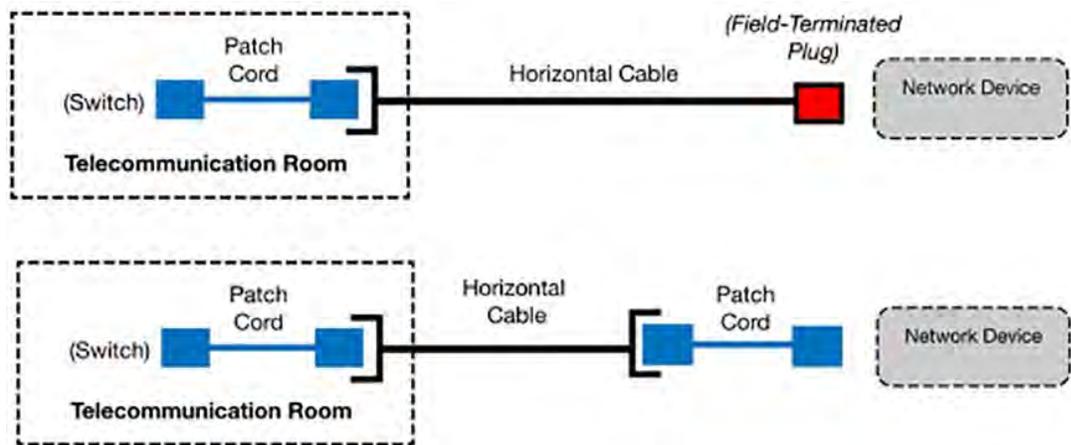
Figure 3-17 Field terminable plug, Field cord

Figure 3-18 Comparison of Standards Development for Wi-Fi and Enterprise Structured Cabling
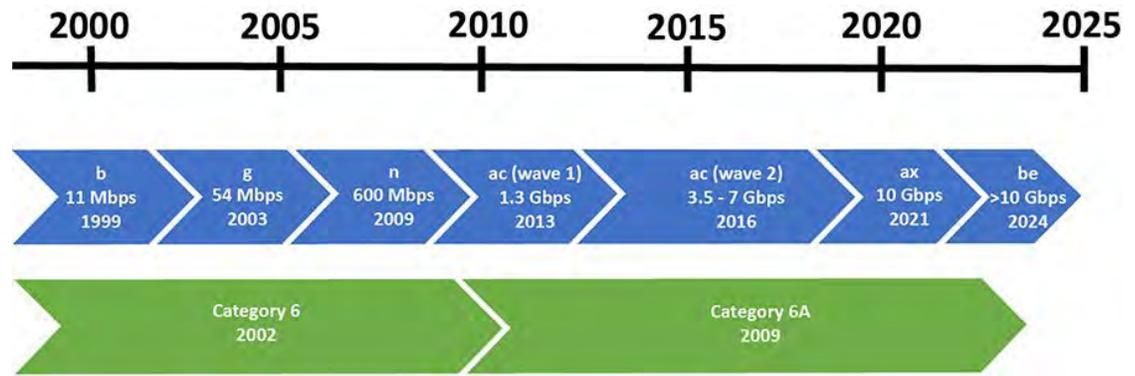
PNZS

The PNZS is a network building block of the IACS industrial Ethernet network following a physical zone topology. The PNZS, contrasted against the control panel, has relatively low power versus control panels, though it may still involve single-phase utility voltages, such as 120 Vac or 240 Vac. The supplied power is used, with a step-down transformer, DC power supply, etc., to power an IES. The PNZS serves as a consolidation point in the CPwE architecture, providing communications to a localized group of control panels in the Cell/Area Zone. An example of a PNZS is shown in the following figure.

Figure 3-19 PNZS

Control Panel Network Infrastructure Considerations

Today's control panels are more connected into the network than in years past. Control panels involve the proximity of power cabling with low voltage data cabling. Electrical noise that is generated by power cabling can be radiated or conducted to data cables. Power cable interference effects such as transients and cabling imbalance can corrupt data, leading to less reliable operation or even cause shutdown of motion control machinery. Another distinguishing factor is that space within the control panel is at a premium. Therefore, connections between active equipment present severe location and routing difficulties. In some situations,
increasing the distance between the two cable types reduces the level of radiation noise picked up by the data cable. However, increasing distance to decrease noise is diametrically opposite to the trend within the control panel industry to reduce the envelope size as much as possible.

Control Panel Network Infrastructure Considerations

Some of the factors and components arrangements adopted into the control panel industry are described in more detail in M.I.C.E. Assessment for Industrial Characteristics in Chapter 2, "Physical Infrastructure Network Design for CPwE Logical Architecture."

- **Spatial and Noise Optimization**—Considerations for cable segregation, thermal management, cable entry, EMI, cable bend radius and space for future expansion must be addressed when attempting to
- reduce the size of control panels.

- **Noise Shield and Shielded Duct**—Noise Shield and Shielded Duct can be used to separate noisy motors or drive cables from sensitive Ethernet or control cables. Both products are effective EMI barriers and provide an equivalent of six inches of air space.

- **600V-Rated Cable and Patch Cords**—Typical enterprise-rated cables are rated up to 300V. For higher voltage applications, 600V-rated cables and patch cords are available.

- **Physical Security Products**—Block-out devices help prevent unauthorized access to existing network infrastructure from the data center to the plant/site.

Panduit List of Materials

The following table is a sample bill of materials for best-in-class physical layer solutions for the Cell/Area Zone from Panduit.

Figure 3-20 Panduit List of Materials

Part Number	Description
Z23U-S15	Universal Network Zone System; 24" x 36"; mild steel enclosure; for one industrial switch; includes (16) Cat6 UTP copper patch cords and jacks, (2) MM LC fiber uplink patch cords and (6) adapters, redundant power supplies and maintenance-free UPS
FSJD912	12 Fiber OS2 9µm Dielectric Double Jacketed Fiber Cable, build up kit may be required
FSPR912Y	12 Fiber Cable, OS2, Indoor Armored TB, Riser, 900um Buffered
FLCDMCXAQY	LC Opticam® OM3/OM4 fiber-optic connector
FDPPSIG	IndustrialNet Fiber DIN Rail Patch Panel, Standard for use with FAPs, IG color
FDPPEIG	IndustrialNet Fiber DIN Rail Patch Panel, Extended for use with FAPs and Cassettes, IG color
Control Panel	
IFC6C04BBL-CEG	Shielded Cat6 stranded cable, PVC jacket, CM
CADIN1IG	DIN rail mount adapter, international gray
CADIN1IG-S	Shielded DIN shielded rail mount adapter
ISTPHCH1MBL	600 volt rated, Cat5e patch cord, 1 meter long
ICAM12DRJS	Bulkhead mounted RJ45 to M12 adapter
FPS6X88MTG	IndustrialNet™ Field attached shielded RJ45 plug
IAEBH6	Bulkhead Jack Cat6 UTP RJ45 with cap
DAP3BC-S0-6	Data Access Port, 3 inch Base, Simplex Outlet, Cat6 coupler
Machine or Skid	
ISFCH5C02ATL-XG	Industrial Copper Cable, Cat5e, 2-pair, 24/7 AWG stranded, SF/UTP, CM, 600V, Teal, 1000ft/305m reel, High Flex, Sun and Oil Resistant
ISFCH5C04ATL-XG	Industrial Copper Cable, Cat5e, 4-pair, 24/7 AWG stranded, SF/UTP, CM, 600V, Teal, 1000ft/305m reel, High Flex, Sun and Oil Resistant
ISPS5E44MFA	Field attached shielded M12 plug
JP2SBC50-L20	J Hook with screw-on beam clamp for use with flanges up to ½"
PWB2X12BL	12" wide x 10' long pathway section used to carry cables horizontally throughout the system
IUTP6X3MBL	Industrial Patch Cord, IP65/IP67, Cat6A UTP, RJ45 with caps, 3 meters
ISX6004AYL-LED	Industrial Copper Cable, Cat6, 4-pair, 24/7 AWG Stranded, S/FTP, PUR, Yellow, 500m RL
Field Deployment Points	
FP6X88MTG	UTP Field Term Plug, RJ45, Cat6A
FC-ICCP0.5MBU	Cat6A UTP FieldCord, 0.5 meter length, 23 AWG cable, Blue
FC-OCCO1MBL	Cat6A Shielded/Outdoor FieldCord, 6A STP Connector, CMX/CMR 26AWG cable, and a compact IP67-rated field-terminable connector, 1M, Black

388017

Physical Infrastructure Design for the Industrial Zone

This chapter provides recommendations and best practices to simplify industrial network physical infrastructure design and deployment for the CPwE Industrial Zone, switching infrastructure, and industrial compute. The CPwE Industrial Zone consists of the Distribution Layer that converges Level 3 Site Operations, with one or more Cell/Area Zones consisting of IACS controllers, and connections to the edge IACS devices. This portion of the network encompasses Levels 0-3 of the CPwE architecture below the Core Switches.

Level 3 Site Operations is discussed in Chapter 5, "Physical Infrastructure Deployment for Level 3 Site Operations." Levels 0-2 or the Cell/Area Zone is addressed in Chapter 3, "Physical Infrastructure Design for the Cell/Area Zone." This chapter primarily focuses on the plant/site backbone network distribution and network cabling that ties all the levels together. Five main elements are essential to consider for deployment:

In addition, this chapter provides:

Logical to Physical Mapping

The Industrial Zone forms the connectivity between Level 3 Site Operations, the Cell/Area Zones (Levels 0-2), and the space in between (see Figure 4-1). This zone covers all plant-wide networking below the IDMZ to the IACS edge devices.

Figure 4-1   Mapping CPwE Logical to Physical
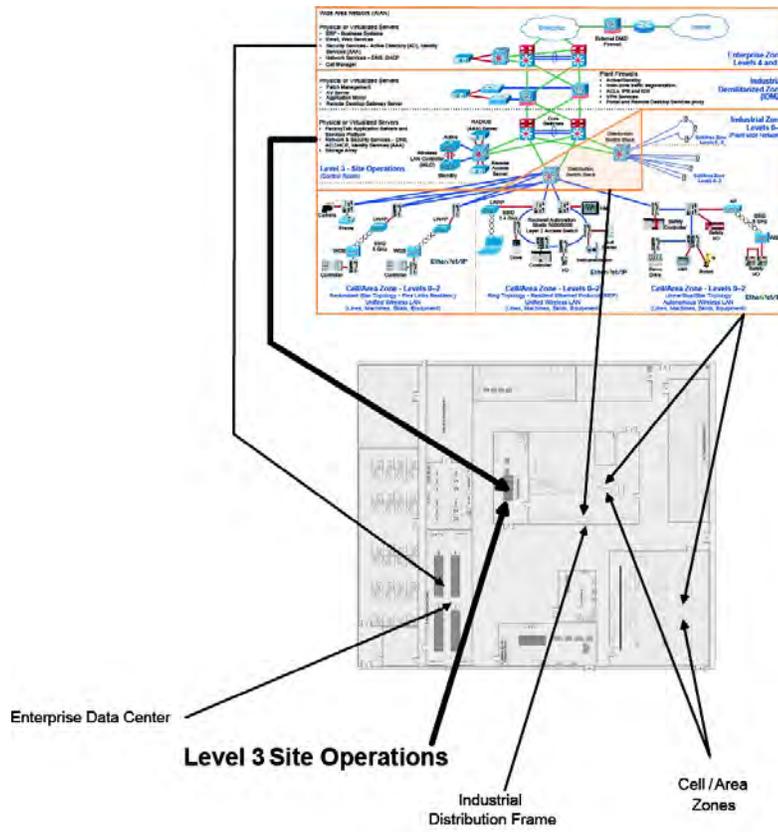
Industrial Plant Network Backbone and Distribution Switching Overview

In the CPwE architecture, Levels 0-3 are tied together with an Industrial Zone network backbone and distribution switches. The physical network routes critical traffic to coordinate IACS controllers, collect production data and connect to the IDMZ. With the high growth of EtherNet/IP devices for IACS, video, security, and so on, the importance of a structured, hardened physical layer has increased. Longevity and scalability are achieved using proven, validated designs for enclosures, media, connectivity, grounding, pathways and identification. Although machines/lines/skids may produce independently, IACS-critical functions are often tied together at the network distribution layer. Poor design and implementation of the distribution layer can impede decision-making and affect the IACS application. These operational functions include inventory transactions, material issues, regulatory data and machine control.

Network distribution switches in the Industrial Zone can be rack mount or DIN mount. Though environmentally hardened switches are available, most switches that are used for this function are protected by an industrial enclosure. Selecting industrial Ethernet switches as part of a pre-configured or integrated solution that includes the

proper enclosure and accompanying cabling infrastructure achieves rapid, low-cost deployment. These pre-configured or integrated solutions are known as physical network building block systems. One type of physical network building block system is an IDF, which is a 19-inch rack-style system. Another type is a PNZS with a DIN mount switch that can either be an Allen-Bradley Stratix 5400 or Cisco IE-4000 IESs.

The cabling for distribution switch uplink and downlink ports is typically fiber to allow for longer reach required from the Level 3 Site Operations and to IES in PNZS or control panels. The topology depends on availability requirements. Special considerations exist for hardening and bandwidth that are specific to harsh environments (for example, cable jacket design, stranded vs. solid conductor, connector protection, enclosure liquid ingress, and EMI).

Key Requirements and Considerations

Key requirements cover the physical deployment of the Industrial Zone backbone and distribution switching. This section includes requirements for housing network gear, cabling, pathways, cable management, and security. In addition to the common key requirements and considerations that are addressed in Chapter 3, "Physical Infrastructure Design for the Cell/Area Zone," the network distribution layer has these unique requirements and challenges:

- **Reach**—Cable reach is challenging for the distribution network, especially for large plants/sites.

- **Industrial Characteristics**—Environmental impacts, as assessed by M.I.C.E. (see Chapter 2, "Physical Infrastructure Network Design for CPwE Logical Architecture") are varied because the distribution layer has network connectivity to different types of environments.

- **Physical Network Infrastructure Life Span**—The physical infrastructure for the distribution layer has a longer life span compared to other parts of the industrial network, often up to 20 years. Therefore, cabling, connectivity, and enclosures must survive the expected life span.

- **Maintainability**—MACs in the distribution layer have dependencies, and a change affects many Cell/Area Zones. Changes must be planned and executed correctly because an error can disrupt or halt IACS applications. Therefore, proper cable management, like bundling, identification, and access is vital to the network distribution layer.

- **Scalability**—Major changes lower in the architecture have significant impact on the distribution layer because the distribution layer aggregates and routes traffic. Designs must account for traffic growth and additional cabling for equipment.

- **Designing for High Availability**—A key aspect of high availability is redundancy. Redundancy can be implemented in many ways, with varying degrees of protection. Different strategies at the distribution layer exist to handle redundancy. Another key element is continuous switch power to support network communication after a power outage or short power bump.

- **Network Compatibility and Performance**—Network compatibility and optimal performance are essential from port to port. This includes port data rates and cabling bandwidth. Network performance is governed by the poorest performing element. As distribution switches are upgraded, the cabling should meet increased performance requirements.

- **Grounding and Bonding**—The distribution layer travels long distances (for example, between buildings). Therefore, there may be ground voltage differences between locations. A single, verifiable grounding network is essential to avoid ground loops that can degrade data.

- **Security**—A security threat at the distribution layer can cause a widespread outage, leading to high downtime costs. The distribution network requires security hardening to help prevent unauthorized access to ports and gear.

- **Reliability Considerations**—Cabling, connectivity, and enclosure selection are essential for reliability. Network reliability must be considered for the lifecycle, starting with the installation/commissioning phase through the operational phase to help prevent or minimize failures.

- **Ease of Deployment/Cost**—A building block system approach can facilitate ease of deployment and lower cost. Ease of deployment and cost are impacted by part selection and topology. In addition, part selection can impact required skill level and expertise, affecting ease of deployment for parts such as the RJ45 jack, LC fiber connector or M12 connector.

- **PoE and Wireless**—Specialized functions such as PoE and wireless have additional requirements that impact the physical layer.

Industrial Network Building Block Systems

Industrial network building block systems, such as the IDF and PNZS, are purpose-built for various CPwE needs. The building block system approach speeds deployment and reduces deployment risk because this design is pre-engineered and validated for thermal, cable management, identification, and grounding. For the IACS plant/site backbone, which is part of the Industrial Zone, specific physical network building block systems include the PNZS and the IDF. These building block systems are described below. For more information about building block systems, see Chapter 3, "Physical Infrastructure Design for the Cell/Area Zone."

Industrial Distribution Frame

A cabinet with a Rack Unit (RU) frame is preferred when network designs include rack-mount gear. Deployment of Enterprise-grade computer or network cabinets leads to premature network switch failure because cabinets are typically open to the environment, accumulating dusts, liquids, and other contaminants over time. The predominant enclosure choice is a double-hinged 26 RU design (see Figure 4-2) and is commonly referred to as an IDF. An IDF is designed for 19-inch RU style switches and other gear, such as a UPS, and is typically wall or column mounted. An IDF may come pre-configured with cabling, duct, cable ties, and so on, leading to consistent equipment deployment, minimizing engineering effort and reducing installation time. The advantage of a pre-configured IDF is best-in-class cable management, thermal performance, and proven installation.

Often, an IDF has both access and distribution switching. Combining access and distribution switches consolidates sensitive network equipment in a protective and cooled enclosure in a cost-effective manner, controlling security access and simplifying mounting. An IDF contains many switches but is usually sized for two Cisco distribution switches (for example, 9300 fiber-based) and up to three Cisco access switches (for example, 2960-X copper-based) along with a UPS.

This section addresses the distribution switch considerations of an IDF. The details for an IDF with access switching are covered in this chapter.

Figure 4-2   Pre-configured Industrial Distribution Frame

An IDF may contain multiple distribution switches to aggregate IES from PNZSs or control panels. Distribution switches in an IDF facilitate VLANs and optimize traffic routing. The distribution switch connects to Level 3 Site Operations, a master distribution frame (MDF), or a core switch in an IDC. The distribution switch uplink cabling is a fiber-optic cable to handle the longer distances from the Industrial Zone   to the IDMZ. By-products of this media choice are faster switch convergence after a network drop-out and higher bandwidth. In addition, the downlinks from the IDF to the PNZSs or control panel are best served with fiber, primarily for faster IES convergence if there is a network drop-out to help to minimize production downtime and to help protect against EMI.

The following are specific key requirements and considerations for an IDF:

- **Reach**—An IDF can significantly increase cable reach, especially when deploying fiber uplinks and downlinks.

- **Industrial Characteristics**—A properly designed IDF mitigates M.I.C.E. hazards because IDF enclosures are IP67-rated with cooling capabilities. IDFs are isolated from Industrial Zone hazards, like vehicle traffic, and are frequently located on outside walls, at a safe elevation on building columns, in mezzanines or a telecommunication room. IDF horizontal cabling, on the other hand, traverses harsh areas to reach its destination. The cabling must survive the harshest regions while maintaining end-to-end continuity. Cabling routed in underground troughs or tunnels must be hardened to withstand severe conditions and rodent damage. In these applications, close attention must be paid to cabling the outer jacket, and an armor exterior such as aluminum clad or dielectric double jacketed. Since fiber-optic cable is inherently noise immune, fiber deployments remove EMI impacts.

- **Physical Network Infrastructure Life Span**—Network switches have an upgrade interval of three to five years. Cabling infrastructure should meet higher performance capabilities for future active equipment upgrades without the necessity of re-cabling the network.

- **Maintainability**—Cable management can be a challenge for an IDF. These enclosures host high port count switches and therefore must accommodate sizable cable bundles. Pre-configured solutions address these challenges by providing

patching and routing to easily handle the mass of cable. Strain relief and bundling should be applied to horizontal cables routed to the IDF due to the tight quarters and bundle articulation when the cabinet is opened. Cable slack must be kept to a minimum because excessive slack leads to entanglement and snags, especially when opening an IDF. Installers sometimes use the enclosure to store slack cable. This practice can impede proper airflow and heat dissipation and makes the enclosure door difficult to close. Fiber-optic cables should be routed through corrugated loom tube for protection. The exception to this rule is dielectric double jacketed media, for which corrugated loom protection is unnecessary. Labeling and color-coding cables facilitate MACs. Exact and shortest length patch cords can minimize cable sprawl. Small-diameter Ethernet patch cords, available in Category 5e, Category 6, and Category 6A, reduce space occupied by cabling.

- **Scalability**—An IDF is the highest-density network distribution system. Growth is usually a feature for a proper IDF design. Network ports should be scaled to serve nodes today and for the next 10 years. For cable management and cable access with some growth, the enclosure should be sized to have at least three free RUs for every RU occupied by network switches.

- **Designing for High Availability**—Redundant switch uplinks must be present along with redundant star or ring topology downlinks to the IES.

- **Network Compatibility and Performance**—As distribution switches are upgraded, the cabling infrastructure must deliver compatible performance without re-cabling.

- **Grounding and Bonding**—All active network gear must be grounded to help prevent worker injury and equipment damage. Further, laboratory tests have shown demonstrably better bit error rates when grounding and bonding practices are optimal. Typically, a network switch has a screw hole and pad for bonding. The best practice is to attach a grounding jumper to the switch grounding screw hole/pad with the opposite end connected to the enclosure grounding bar. When selecting grounding jumpers, it is important to consider that a low impedance path to ground delivers the best performance in managing EMI threats. In most cases, a braided grounding strap rather than a wire is the prudent choice. The grounding bar must be tied to the building grounding network. See Chapter 3, "Physical Infrastructure Design for the Cell/Area Zone" for more details.

- **Security**—Part of a defense-in-depth strategy, the physical security surrounding an IDF requires several layers of protection. The most effective physical layer measures include enclosure locks to help prevent unauthorized access, keyed patch cords to avoid inadvertent patches, and port

  lock-in/block-out devices to help prevent incorrect connections to unused ports.

- **Reliability Considerations**—Deploying a structured cabling approach enhances reliable communication. In a structured cabling environment, the horizontal (permanent link) cable is not touched, bundles are segregated and secured to ease handling, cable managers such as D-rings are selected to route cables with better access, power cables are secured at both device and power outlet ends to help prevent power loss, and cabling and connectivity are selected to withstand the manufacturing environment.

- **Ease of Deployment/Cost**—Design, procurement, installation, and maintenance are some of the costs to consider. When compared to designing and building enclosures for network assets, a building block system approach leads to lower total costs with faster, proven installation.

- **Smart Power** - UPS backups are essential for reducing downtime due to power issues, but they can also provide additional intelligence that can prevent issues that lead to failures. Smart-UPS systems and power distribution units (PDU) can be equipped with intelligent monitoring and network connectivity to provide additional capabilities over the network connection. With the increase in demand for data, this is a convenient and easy-to-access way to provide data points that relate to the environment. These 'Smart' capabilities include remote management and the integration of sensors directly connected to the unit. Common sensors that are connected include the following: temperature, humidity, rope water detection, magnetic door sensor, spot water sensor, and multi-purpose dry contacts. Information from these sensors is reported back to the Smart-UPS/PDU where notifications/alarms are set up or the data is sent to another server. This setup provides information to the responsible support teams for predictive and preventative maintenance.

PNZS with Distribution/Aggregation Switch

Smaller-footprint applications, where the need is to aggregate a few IES on the plant/site, can employ a DIN mount distribution/aggregation switch, such as a Stratix 5400 or Cisco IE 4000, to connect to the plant/site backbone. This can be a suitable choice for a modular line or Cell/Area Zone that potentially can be moved in whole (that is, networking is self-contained). These switches are more hardened against a hotter, harsher environment than the rack-mount Enterprise grade switches. DIN-mount IES should be protected using an appropriately specified PNZS. A DIN distribution switch can be deployed in a PNZS in the same manner as a DIN-mounted IES (see Figure 4-3). In most cases, external cooling may not be required, reducing cost and minimizing A/C maintenance when compared to an Enterprise switch deployment. Cabling and connectors are the same as those used with Enterprise switches. Cable management and connectivity include DIN mount patch panel, DIN adapter for RJ45 jacks, and slack and strain relief features mounted to backplane or DIN. In addition, a barrier may be included to separate higher voltages from the DC power to the switches.

Figure 4-3   Zone Enclosure with a DIN Mount Distribution/Aggregation Switch

Optical Fiber Overview

An optical fiber link consists of a transceiver, connector/adapter, and cable. The transceiver converts electrical data packets into light pulses that are transmitted through a glass fiber, which are converted to electrical signals by the receiving transceiver. A fiber connection usually has two fiber cables, one to transmit and the other to receive (that is, duplex). For IACS applications, optical fiber has many advantages over copper channels, such as immunity to electrical noise, faster switch

convergence after an interrupt, long reach, and higher bandwidth potential (with state-of-the-art fiber). The various considerations for selecting fiber are described below.

Physical Media

Fiber-optic cable is constructed of a core, cladding, coating, and jacket (see Figure 4-4). The geometry of each of these components determines the index grade, or Optical Multimode. The two basic types of optical fiber are single-mode (referred to as OS) and graded index multimode (referred to as OM). Single-mode optical fiber supports data communications over long distances (for example, kilometers) and requires the use of higher-cost laser transceivers. On the other hand, graded index multimode fiber supports data communications up to 550 m but makes use of lower-cost transceivers, helping to lead to a lower-cost fiber deployment.

Figure 4-4   Cross-Section of Fiber Construction Types
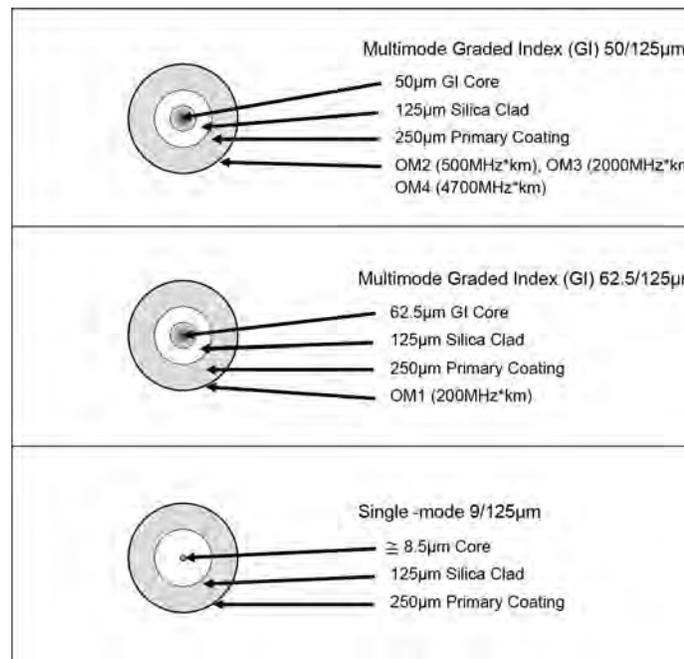
Although several transceiver types are available, most IES use a transceiver referred to as SFP. Most commonly, the connectivity is a duplex LC connector.

The term "graded index" refers to the dielectric constant of the silica material used in the core. "Graded" means that the dielectric constant is profiled as a function of radial distance from the center of the core to reduce slightly before the cladding material is reached. This parameter decreases the dispersion (a measure of the delay in time of arrival) between different modes within the fiber and helps to increase the maximum distance the fiber can support at a specified data rate.

Within multimode, two basic families of core size exist: 62.5 µm and 50 µm. They are defined as Optical Multimode (OM) and are described by five levels: OM1 through OM5. OM1 has a 62.5 µm core and is considered legacy cable. OM2, OM3,

OM4, and OM4 have a 50 µm core and are deployed more typically. Single-mode (OS) cable used in these applications typically has a core diameter of around 8.5 µm and a cladding diameter of 125µm. The designations for each are as follows:

- **OM1**—62.5/125µm graded index multimode (200 MHz·km)

- **OM2**—50/125µm graded index multimode (500 MHz·km)

- **OM3**—50/125µm graded index multimode (2,000 MHz·km)

- **OM4**—50/125µm graded index multimode (4,700 MHz·km)

- **OM5**—50/125 µm graded index multimode (6,000 MHz·km)

- **OS1**—9/125µm single-mode

The values in parentheses are referred to as the effective modal bandwidth (EMB) of the fiber. The EMB represents the capacity of the fiber to transmit a certain amount of information over a specific distance and is expressed in MHz per km.

Selecting Single-mode or Multimode Fiber

As stated above there are two different types of fiber used in connecting networks: multimode and single mode. These two types of optical media vary by glass core size and by the design/operation of the transceivers used. Multimode fiber is commonly used for shorter transmission distances due to the cost efficiency it offers. Single-mode fiber uses more precise transceivers to achieve longer transmission distances and is more expensive to implement than multimode fiber. Designers and installers need to make sure that the transceiver type and fiber type are compatible for optimal performance.

Multimode optical fiber incorporates a larger core diameter than single-mode fiber type. In addition, the core diameter used in multi-mode fiber varies depending upon the performance type used. For example, OM1 (optical multimode 1) was the first type of multimode fiber to be deployed and uses a 62.5µm core diameter with an overall cladding diameter of 125µm. This fiber type is almost never deployed in new installations but may be required for legacy installations with an installed equipment base. Multimode fiber types OM2, OM3, OM4, and OM5 are based on the use of a core diameter of 50µm (again with a cladding diameter of 125µm) and offer improved performance in terms of maximum channel length. OM4 is recommended for new installations and represents the best available compromise between total link cost (optical fiber plus transceivers) and channel length.

Single-mode fiber types used in plant network applications have a core diameter of 9µm and a cladding diameter of 125µm. The transceivers used with single-mode fiber incorporate more costly laser sources, and so the overall link cost is higher than that seen using multi-mode fiber, however longer channel lengths can be realized. There are two common designations for single-mode fiber called optical single-mode "OS", identified as OS1 and OS2. OS1 is a legacy fiber type and is not suggested to be used in any deployment, though it may be seen in legacy deployments. OS2 is the default single-mode fiber designation, though literature commonly calls this out as OS1/OS2.

Figure 4-5 Fiber cable types

Designation	Jacket Color	Core/Cladding Diameter	Fiber Type	100 Mbps Max. Distance	1 Gbps Max. Distance
OM1	Orange	62.5/125µm	Multimode	2000m	220m
OM2	Orange	50/125µm	Multimode	2000m	275m
OM3	Aqua	50/125µm	Multimode	>2000m	500m
OM4	Aqua/Violet	50/125µm	Multimode	>2000m	550m
OM5	Lime Green	50/125µm	Multimode	>2000m	550m
OS2	Yellow	9/125µm	Single-mode	>70Km	70Km

388018

Selecting the Number of Fiber Optic Cabling Strands

Multi-stranded fiber optic cabling assemblies are available with numerous strand counts. Commonly used counts include 2, 6, 12, 24, and 48 strands. The number of strands required for an optimal deployment equates to the number of pairs required for switches and devices that must be connected and includes a factor for growth. For example, connecting three access switches near a distribution switch in a different location requires six strands because each access switch requires two strands for transmit and receive. Additional strands should be included for future growth and the possibility of failed fiber strands. To determine the total number of strands, combine the required strands, future growth, and spares. For this example, a twelve-strand fiber cable is the proper choice.

Optical Fiber Cable Outer Covering

This section discusses basic optical fiber outer covering types and performance. Figure 4-6 is a M.I.C.E. chart categorizing each cable type by increasing environmental severity. The fiber type listed in the first column, Distribution, has limited protection and bend radius control but is the most cost-effective. The fiber type in the second column, Indoor/Outdoor (Dielectric), has better protection against chemical/climatic effects. The fiber type in the third column, Indoor Armored, has an aluminum clad to help protect against crush along with chemical/climatic hazards. The fiber type in the fourth column, Gel-Free Outside Plant (OSP) Armored, has robust protection for all M.I.C.E. levels. Figure 4-6 also indicates the type and designation of the compatible SFP module.

Figure 4-6   Recommended Fiber-optic Cable Types with Common SFP Modules for Plant-wide Network Applications

Increasing Severity

SFP Module	Rockwell Automation SFP Part Number	Core Diameter	Maximum Distance per Standards	Fiber Type per MICE Level				
				$M_1I_1C_1E_3$ Distribution	$M_1I_1C_2E_3$ Indoor/Outdoor (Dielectric)	$M_2I_2C_2E_3$ Indoor Armored	$M_3I_1C_3E_3$ Indoor/Outdoor Armored (Dielectric)	$M_2I_2C_2E_3$ Gel-Free Outside Plant Armored
100BASE-FX	1783-SFP100FX	62.5µm	2km		FSCR6^^Y	FSLR6^^*		FSWN6^^
		50µm	2km	FODRX^^Y	FONRX^^Y FOCRX^^Y	FOPRX^^Y	FOJDZ^^	FOWNX^^
100BASE-LX	1783-SFP100LX	9µm	10km	FSDR9^^Y	FSCR9^^Y	FSPR9^^Y	FSJD9^^	FSWN9^^
1000BASE-SX	1783-SFP1GSX	62.5µm	275m	FSDR6^^Y	FSCR6^^Y	FSLR6^^*		FSWN6^^
		10 Gig 50µm	550m	FODRX^^Y	FONRX^^Y FOCRX^^Y	FOPRX^^Y	FOJDZ^^	FOWNX^^
1000BASE-LX/LH	1783-SFP1GLX	9µm	10km	FSDR9^^Y	FSNR9^^Y FSCR9^^Y	FSPR9^^Y	FSJD9^^	FSWN9^^
1000BASE-LX/LH	GLC-ZX-SM-RGD	9µm	40km	FSDR9^^Y	FSNR9^^Y FSCR9^^Y	FSPR9^^Y	FSJD9^^	FSWN9^^

Panduit part numbers listed above for bulk cable
^^ -fiber count.
*Indoor-Outdoor armored
See https://www.panduit.com/ for additional part numbers
not listed here and more information

Fiber Connectors and Adapters

Connectors are the physical interface between the cabling media and devices. A number of connector types are used in fiber-optic physical infrastructure. This section discusses three of those connector types:

- **Lucent (LC) Connectors**—Used in data center environments and some IACS devices. They have a small footprint that allows them to be used on high port density IES and on devices, minimizing real estate. The LC connector interface presents an SFF demountable interface for connection to SFP transceivers. The standard construction of the LC connector consists of a spring-loaded, 1.25 mm diameter zirconia ceramic ferrule housed in a thermoplastic connector back shell. The dimensions for this connector are defined in both domestic (TIA-604 FOCIS-10) and international (IEC 61754-20) standards. The LC connector footprint is approximately half the size of an SC connector and has a back shell to accommodate standard 1.6 mm to 3.0 mm diameter cable designs.

- **Subscriber (SC) Connectors**—Snap-in connectors that are widely used in single-mode systems for their performance. These connectors are used in the data communication and telecommunication industries. SC connectors are losing ground to LC and other connector types due to their larger size, which is not suitable for high-density applications.

- **Straight Tip (ST) Connectors**—Bayonet-style connectors that create secure multimode connections. ST connectors are used for inline connections; however, some equipment uses this type of connector because of the stability in the connection. ST connectors were once one of the most popular types of connectors.

Of these three connector types, the LC connector is becoming the most used type due to its high performance and small size, allowing the highest connection densities to be obtained with the smallest footprint. The characteristics of the three connector types are summarized in Figure 4-7.

Note: The ODVA EtherNet/IP specification for the physical layer (Chapter 8) states that the LC connector is preferred for new installations requiring 100 Mbps data rates, though SC and ST connector types are supported. It also states that the LC connector is preferred for new installations requiring 1000 Mbps (1 Gbps) data rates, though SC connector types are allowable for legacy installations.

Figure 4-7   Fiber-optic Connector Comparison Summary

	PVC	TPE	PUR
Connector Name*	Lucanet or Little	Square or Subscriber	Straight Tip
Coupling Type	Snap	Snap (Push - Pull)	Bayonet
Connector Outside Dimensions, mm	4.5 x 4.5	9.0 x 8.3	Diameter 8.6
Ferrule Size, mm	1.25	2.5	2.5
TIA Standard	TIA-604 / FOCIS - 10	TIA-604 / FOCIS - 3	TIA-604 / FOCIS - 2
IEC Standard	IEC 61754-20	IEC 61754-4	IEC 61754-2
Duplex Type	Yes, with clip	Yes. Connector can mate	No

*Connector names vary

Horizontal Cable Fiber Connector Termination

LC, SC, and ST connectors are typically factory installed unlike horizontal fiber cables which require field terminations. Fiber cable is attached to connectors using a variety of methods. Decision criteria are ease of installation, cost, and performance. The three main methods are:

- Fusion splice onto a fiber pigtail

- Field application of epoxy and field polish

- No epoxy, no polish

Fusion Splicing

For this approach, the connector is factory terminated onto a short length of the same fiber type that is used in the field cabling, forming an assembly called a pigtail. The optical fiber to be terminated is prepared on site and along with the free end of the pigtail fiber, it is placed into a piece of equipment known as a fusion splicer, which contains a heating element. The silica is melted to fuse the fibers together and solidified to make a very reliable and high performing fiber joint. A protective splice tube is placed over the area of the joint and tube loaded into a splice tray holder that provides mechanical protection for the joint. The splice tray is frequently a 19-inch rack mounted unit that can be conveniently accessed should moves, adds, and changes (MACs) be necessary. The splice tray usually incorporates slack spools onto which the excess fiber can be routed for good cable management and protection.

Field Application of Epoxy and Polish

For this method, the fiber to be terminated in place is prepared, fed into the required connector, and extended through the front face of the connector. An epoxy is loaded into an aperture in the connector, and cured to firmly fix the fiber into the connector. Excess fiber is removed from the connector front face and field polished with a grinding puck and paste to form a reliable interface. The front end of the fiber is inspected using a small microscope called a borescope to ensure a high connection performance. The connector can be loaded into a fiber adapter that is located into a fiber enclosure. The excess buffered individual fibers are managed on slack spools in the enclosure.

No Epoxy, No Polish

More recently, termination techniques that use connectors already loaded with a short length of optical fiber and factory prepared with high accuracy faces have been introduced. The connector includes a gel to ensure lowest attenuation between the pre-loaded and installed fiber. The fiber to be terminated is prepared by stripping off the buffer and cut using a special cleaver that results in a clean fiber end. The fiber is installed into the rear of the connector and locates against the rear of the pre-installed fiber length. At the correct point in the termination procedure, a cam on the connector is rotated to lock the installed fiber into place. In modern termination tools, such as the Panduit OptiCam™ tool shown in Figure 4-8, an internal light source (the visual fault locator) shows the performance of the connection just made. An effective termination has been created if little or no light can be seen through a window in the connector.

Figure 4-8 Panduit OptiCam Tool

The terminated fiber is installed into a fiber adapter and managed in the same way as the field epoxy, field polish connector scheme described above.

Fiber Construction

The most common construction for optical fiber for indoor use is called tight buffer, where a protective coating surrounds the cladding and an additional jacket of polyvinyl chloride (PVC) brings the diameter of the individual fiber to 900μm. Multiple fibers are wrapped with a protective Aramid yarn. The entire cable assembly is coated in a durable external jacket, typically polymer material, that is riser, plenum, or otherwise rated to suit the installation environment.

Tight buffered fiber is not deployed in outdoor environments because the temperature extremes and mechanical stresses encountered in outdoor installations can cause physical degradation or even damage to the fiber. An alternate construction, loose tube, is used for fiber deployments in outdoor environments. The loose tube design consists of the individual fibers (before the PVC coating is applied), which 'float' within a polymer tube, allowing it to move yet be protected when the fiber is subject to movement. Older cable designs also use a water blocking gel inserted into the tube to help protect the fiber from both damage and moisture ingress. Newer indoor/outdoor cable types include a water absorptive tape underneath the exterior jacket that swells and forms an effective seal if the jacket is ruptured.

An example of the construction of the tight buffered and loose tube fiber types is shown in Figure 4-9.

Figure 4-9 Tight Buffered (left) and Loose Tube (right) Fiber Types
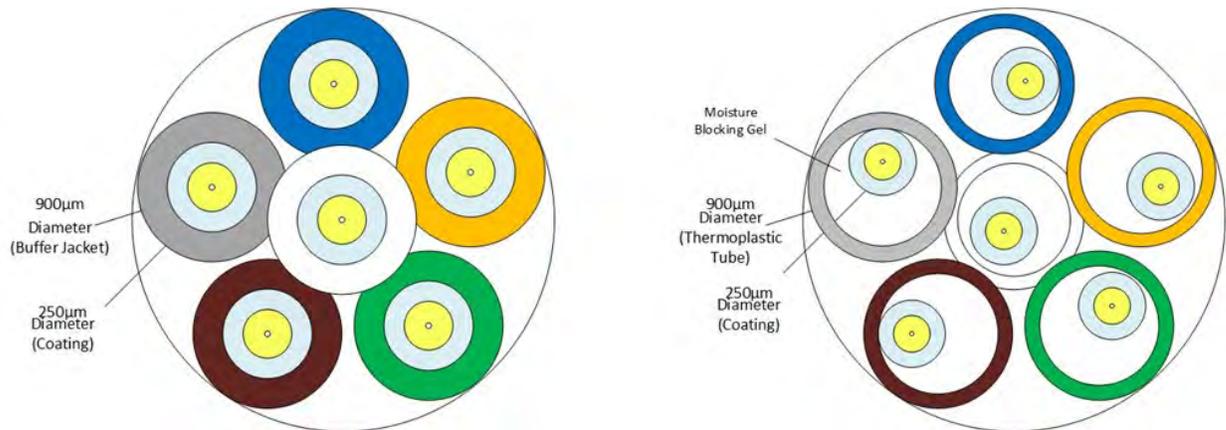
Distribution Fiber Optic Cabling (Non-armored)

Non-armored distribution fiber optic cabling (Figure 4-10) is a standard cable that runs in a cabling basket, cable ladder, or conduit in an indoor environment. Non-armored distribution fiber optic cabling requires protection, therefore, at a minimum, it should be installed in a duct or continuously supporting system depending on the environment. It may also require greater environmental hardening depending on the harshness of the environment, for example, in conduit.

This cabling type is used in intra-building backbone, building backbone, and horizontal installations for riser (OFNR), plenum (OFNP) and general-purpose environments. Riser and plenum-rated fiber optic cable are most commonly used in North America. Other regions of the world, such as Europe and Asia Pacific, require optical fiber with a low smoke zero halogen (LSZH) rated cable jacket. Always consult the local codes and standards for the plant location to be certain the proper variant is selected during the design stage. This topic is discussed in more detail in the Level 3 Site Operations Fiber Cabling Types section later in this document.

Figure 4-10 Distribution Fiber Optic Cabling (Non-Armored)
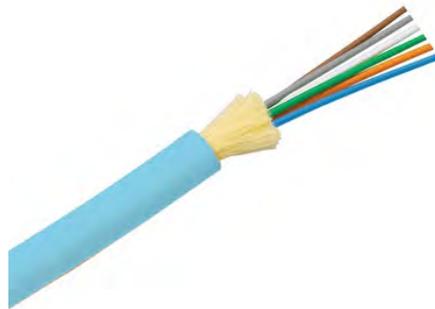
Dielectric Double Jacketed Fiber Cable for Plant Backbone

Dielectric Double Jacketed (DDJ) cable (see Figure 4-11) is a self-supporting, crush and impact resistant fiber cable. It is designed for use in horizontal installations and backbones within buildings to provide high-density connectivity and ease of

installation. Kevlar re-enforced double jacketing eliminates the need for additional conduit or pathway installation and provides a smaller crush resistant pathway for improved design flexibility and lower installed cost. All-dielectric construction eliminates the need for grounding and bonding, thereby reducing installation time and cost.

All DDJ fiber are riser rated (OFNR) and compliant with Low Smoke Zero Halogen (LSZH) specifications. DDJ can be installed using J-hooks, Wyr-Grid® Overhead Cable Tray Routing System, or ladder rack. DDJ cable is a 250µm tight buffered fiber cable with a 50µm (OM4) or 9µm (OS2) core. Typically OM4 is deployed with 6,12, or 24 fiber counts and OS2 options go up to 96 fiber counts. The fiber can be terminated following standard field polish, mechanical connector (OpticCam® Fiber Optic Connectors) or pigtail fusion splice termination methods.

Figure 4-11 Dielectric Double Jacketed Fiber Cable (DDJ)
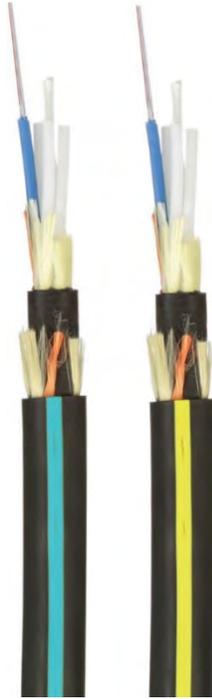
Outside Plant/indoor and outdoor

Outside plant/indoor and outdoor optical fiber cables are rated for high temperatures, are chemically resistant, and can be used in harsh environments. These fiber cables incorporate loose tube construction, making them suitable for aerial, duct, and direct burial applications. There are two types of ingress protection: gel and gel-free. Although the gel helps protect the fibers and prevents moisture ingress, it becomes sticky and messy upon handling. Gel-free designs are easier to handle and have tape that swells in contact with water to provide dry water blocking.

A corrugated steel armoring over the polymer jacket protecting the fibers provides high crush resistance for increased durability in direct burial applications. A UV resistant cable sheathing is often used in these applications to protect the individual fiber cable. As in the case of the indoor cable described above, outside plant/indoor and outdoor cable is available in 6, 12, 24, 36, 48, 72, 96, and 144-fiber counts. This cable construction also supports multimode (OM5, OM4, OM3, OM2, and OM1) and single-mode (OS2) fiber types.

Figure 4-12 Outside plant non-armored cable

Interlocking Armored Fiber Optic Cabling

Interlocking armored fiber optic cabling (both indoor and outside the plant) has a protective aluminum or metal housing around the fiber cable to provide superior crush resistance and guard the cabling from animal intrusion (Figure 4-13). Aluminum interlocking armor also eliminates the need for inner duct or conduit with a smaller pathway for improved design flexibility and lower installed cost. In addition, these cables permit easy retrofit into existing industrial environments, removing the need for sophisticated and expensive pathways.

Armored fiber optic cabling types are used in intra-building backbone, building backbone, and horizontal installations for riser (OFCR), plenum (OFCP), and harsh environments. The cables are available in 6, 12, and 24-fiber counts in a "single jacket" design, and in 36, 48, 72, 96, and 144-fiber counts in a "subunit" (group) design. For higher fiber count types, depending upon the construction, subunits of fibers are housed within internal jackets inside the overall cable jacket to facilitate identification and installation. Multimode (OM4, OM3, OM2, and OM1) and single-mode (OS2) fiber are widely available.

Figure 4-13: Armored Fiber Optic Cabling

High Speed SFPs

Industrial control system switches commonly include small form-factor pluggable (SFP) interfaces, typically 100 Mbps or 1 Gbps over copper or fiber cabling, to be used as uplinks. As these uplink signals are aggregated to the Distribution level, higher speeds are required. Due to a continuing need for faster data and the connection of additional devices, the requirement for higher-speed networks results in the development of more advanced interfaces. The original SFPs have a single transmit and receive channel that typically transmits at 1 Gbps. There are two updated versions known as SFP+ and SFP28. Although they are about the same size, these modules do not plug into the same port as a standard SFP, due to the difference in technology. The SFP+ transmits up to 10 Gbps and the SFP28 up to 25 Gbps on a single channel.

A four (quad) channel system allows for even greater speeds, 4x to be precise. The QSFP, QSFP+, and QSFP28 provide four channels of the same speed as their single-channel counterparts. With the added channels 4 GB, 40 GB, and 100 GB respectively can be achieved with the quad system. This four-channel system still supports both copper and fiber but requires a different type of cable. Typically, the copper or fiber cable will contain 1 pair per channel for a total of 4 pairs. Applications for these quad transceivers are mostly seen in data centers and high-speed server/switching applications.

Figure 4-14 High speed SFPs

	SFP	SFP+	SFP28	QSFP	QSFP+	QSFP28
Typical Speed	1 Gbps	10 Gbps	25 Gbps	4 x 1 Gbps 4 Gbps total	4 x 10 Gbps 40 Gbps total	4 x 25 Gbps 100 Gbps total
	Single Channel			Quad (4) Channels		

388020

Other SFPs

Bidirectional receivers, commonly known as BiDi, use two different wavelengths allowing each strand of fiber to both send and receive, each at 20 GB bandwidth. When upgrading an existing 10 GB SFP+ network BiDi is a good option because it does not require replacement of the fiber optic cable infrastructure. BiDi operates with the same fiber optic cabling as SFP+ networks.

Fibre Channel is a way of transferring data serially over copper or optical fiber for high speed and low latency. Fibre Channel Protocol (FCP) is a SCSI interface protocol that uses underlying a fiber channel connection. When referring to the FC protocol it is often spelled *Fibre* (in the United States) to denote it is referring to the protocol.

High-Performance Cable Assemblies

Today most industrial applications use 4-pair Ethernet with a copper cable that is plugged into a standard RJ45 port. As speeds and distances increase there are more applications utilizing small form-factor pluggable (SFP) connections that allow for the use of copper or fiber media. Typically, stand-alone transceivers are purchased separately, inserted into SFP port, and the connection is made via fiber optic cable terminated with an LC style connector.

The type of SFP used is based on speed and connection requirements. However, when using SFP interfaces there are other methods of transmitting the signal. The transceiver/electronics that is required on either end can be built into the cable and the signal can be transmitted over fiber or copper cabling. Two of these methods include

Active Optical Cables (AOC) and Direct-Attached Copper (DAC) which can be passive or active. Traditionally use of AOCs and DACs have been limited to data centers and enterprises for short reach high-speed applications. As plant floor networks continue to leverage more edge and high-speed computing, new applications for cabling such as AOC and DAC are emerging.

Direct Attached Copper (DAC)

DAC cable assembly consists of a copper cable with built-in electronics on both sides. This assembly connects two SFP ports that are near each other. There are two types of DACs: passive and active. A passive assembly does not contain any electronics in the cable assembly, it simply allows the signal to pass as-is over the copper cable and is limited to a distance of 7m. The active DAC assembly includes built-in signal amplification and equalization.

These built-in features allow for a longer transmission distance, up to 15m, and ensure better transmission quality. The active DAC consumes more power and costs more to purchase than a passive DAC, although both passive and active DACs are less expensive than copper transceivers with individual cables. When properly specified, DAC cables can save cost and complexity when connecting short cable runs of high-speed devices such as switches, servers, and storage arrays.

Figure 4-15 DAC cable

Active Optical Cable (AOC)

AOC cable assembly is a multimode fiber optic cable with a built-in transceiver at each end of a fixed-length cable. Due to the assembly being a fixed length, the transceiver can be optimized for that length and therefore it is less expensive. AOC assemblies are generally used for runs up to 30 meters because when runs get up to around 100 meters the AOC is less competitive in cost comparison.

Inherent to the design of the integrated cable/transceiver the visual interface is not exposed, so there is no need for cleaning. Also, the enclosed terminations make it more durable in harsh environmental conditions and vibration. However, if there is a problem with the cable, the entire assembly must be replaced which includes replacing both transceivers that are built into the cable. Also, the ends of the AOC cables are larger which can be harder to pull through some pathways like conduit.

These connections can be 1 to 1, or 1 to many, depending on the cable assembly. AOC breakout cables allow a single high-speed port to supply multiple lower-speed connections. Since AOCs are made with fiber optic cables, they reduce the amount of space needed when compared to copper cables. AOCs can provide cost savings when properly specified for an application that would otherwise use traditional standalone transceivers and cables for each connection.

Figure 4-16 AOC cable

	Direct Attached Copper (DAC)		Active Optical Cable (DAC)
	Passive	Active	
Reach	< 7m passive	< 15m active	100m +
Cable Type	Twin-axial copper		Fiber optic
Power Consumption	< 0.15 W	0.5 – 1 W	< 1 W
Price	$	$$	$$$

388021

Physical Network Design Considerations

Figure 4-17 illustrates a simplified Industrial Zone physical deployment between Levels 0-3. Depending on the plant/site size, the Level 3 Site Operations could connect to the Cell/Area Zone(s) through Core Switches. The links between the core switches in the Level 3 Site Operations and the distribution switch in the IDF use fiber-optic cabling. The distribution layer also connects to control panels that have IES with fiber network cabling.

Figure 4-17   Physical Industrial Network Backbone
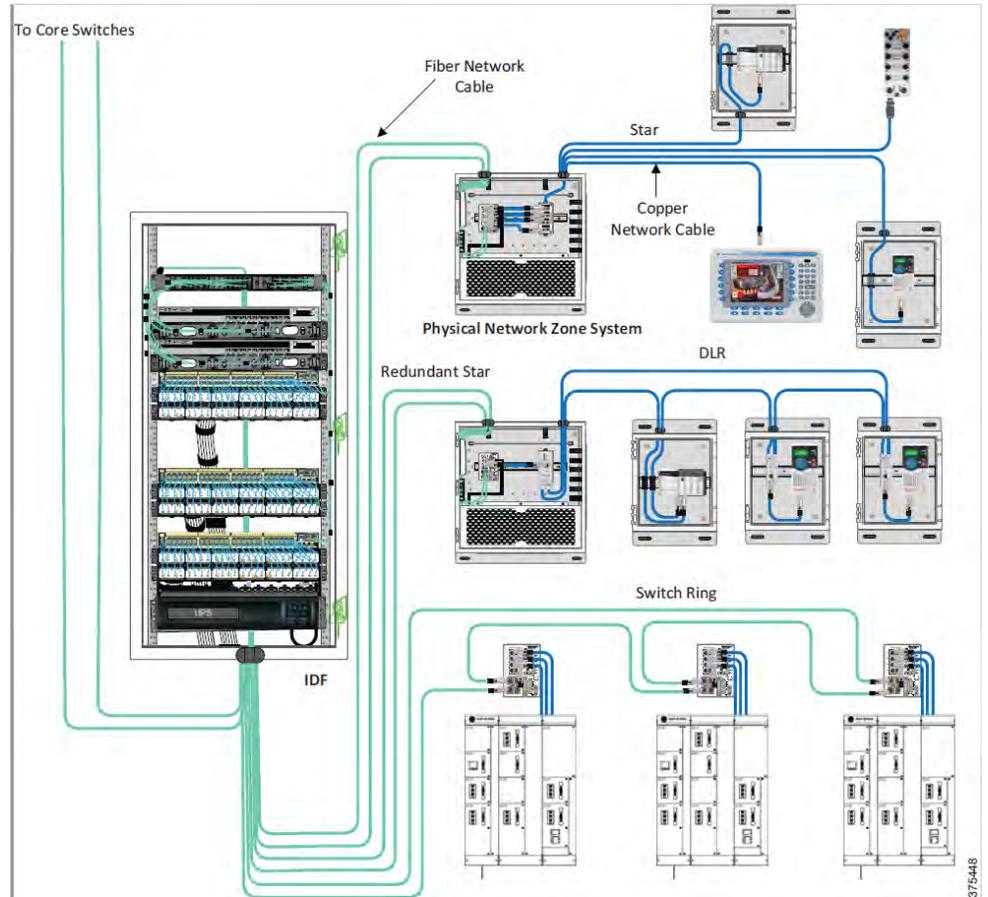
IDF Physical Deployment Details

Figure 4-18 illustrates IDF physical connectivity, detailing the enclosure cabling, jacks, patch cords, cable management, power, network switches, and cable ties. In general, an IDF is assembled in a similar manner as other RU cabinets and racks. The biggest challenge is to compensate for back articulation, thermal management, tight quarters, and cable sprawl from MACs. Following the best practices described below facilitates maintenance and long life.

Figure 4-18   Typical IDF Deployment
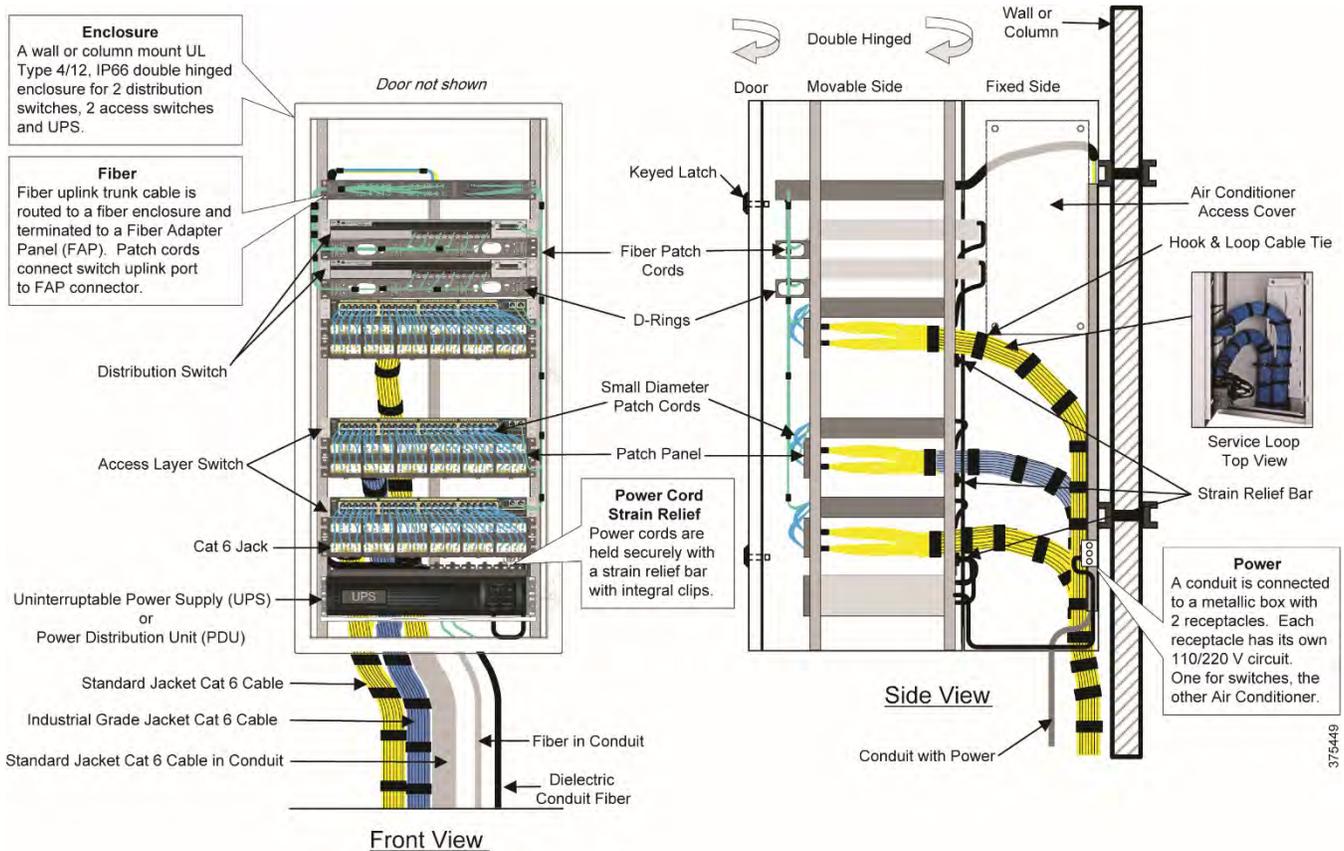
Horizontal Cable Service Loop

The horizontal cabling is extended when opening a double-hinged IDF. Therefore, a cable service loop is necessary for both fiber and copper. Planned and managed cable slack is required to fully open the enclosure. Although allowing service slack is important, too much extra cabling consumes excess space and can act as a spring when closing the enclosure. Also, the cable length increases from the first to the last copper port across the patch panel. The IDF stationary section uses hook & loop ties in the back to secure cabling. The copper cabling is also secured with hook & loop ties to strain relief bars on the movable side to minimize tugging on the jack when opening the enclosure. Fiber horizontal cable is channeled through duct and loom tube and then into a fiber enclosure for protection.

Thermal Management

The IDF can operate with an ambient temperature of up to 25º C (77º F) without air conditioning. Adding an air conditioner allows the IDF to operate up to 50º C (122º F) ambient air temperature. All cables should be neatly bundled and secured to help prevent cabling from impeding airflow.

Connectivity and Patching

The IDF may have both copper and fiber cabling. Typically, all cable enters from the bottom of an IDF to help prevent liquid ingress. The holes in the enclosure for the cabling should have a fitting or grommet to help prevent chaffing.

For fiber-optic cable, the best practice is to terminate the horizontal fiber cable into a fiber enclosure. The fiber enclosure is similar to an Enterprise enclosure, containing slack spools and strain relief to secure fiber strands, along with Fiber Adapter Panels (FAP). Patching is performed with fiber patch cords from the enclosure FAP to the switch uplink ports. Copper downlinks from the switch are connected to a patch panel via a patch cord. The best practice is to have switches next to patch panels. This helps to minimize cable sprawl, makes ports more visible, and helps to minimize entanglement. A short (8-inch) small-diameter patch cord (28 AWG) is recommended for easier handling and less space consumption.

DIN Panel Tiers for 19" Rack Mounting

As an optional deployment method, the Universal Distribution Frame Tier allows for most DIN mount industrial Ethernet switches (IES) to be deployed within 19" rack mount environments, including the Industrial Distribution Frame. The version below DINS24 is pre-configured to accept the IES and only requires additionally the field power connection.

Figure 4-19 Universal Distribution Frame Tier

IDF with Access Control

Enabling smart access control is part of a defense in depth approach to physical network security limiting access to IT equipment and extending access control profiles to equipment on the plant floor. IDF enclosures with access control are engineered to deploy and protect 19" rack mount switches along with access control and power distribution capabilities to protect and monitor critical IT equipment. Versions of the IDF are available with access control, which includes the intelligent PDU, switch handle as well a temperature and door sensor shown below.

Figure 4-20 Smart PDU

Figure 4-21 Security Handle

Figure 4-22 Temperature and Door Sensor

Panduit List of Materials

Table 4-2 is a sample list of materials for best-in-class physical layer solutions for the Industrial Zone.

Table 4-2　　　　　Sample List of Materials

Part Number	Description
ZDF48-RADA2	26RU Dual Hinge NEMA 4/12 Enclosure with Access Control. Installed (2) 48-Port Patch Panels, fiber tray, fiber spools; Installed cable management; Installed grounding hardware; Back panel with 10" Long DIN Rail Mounting Provision. Includes: SmartZone™ intelligent PDU, security handle / card reader, PDU harness, temperature and door sensor
Z23U-S21	Universal Network Zone System; 24" x 36"; mild steel enclosure; for up to two industrial switches; includes (16) Cat6 UTP copper patch cords and jacks, (4) MM LC fiber uplink patch cords and (6) adapters, redundant power supplies and maintenance-free UPS
FOJDZ12	12 Fiber OM4 Dielectric Double Jacketed Fiber Cable (OFNR-LS), build up kit may be required
FLCDMCXAQY	LC Opticam® OM3/OM4 fiber-optic connector
UTP28X8IN	28 AWG small diameter Cat6A UTP patch cord, 8" in length, 0.185 (4.7mm) in diameter, off white
ZDINS24	Expansion Tier for 2 industrial switches, (1) 48-port patch panel, (1) 4U DIN bracket, (2) power supplies AC to DC, terminal blocks, wiring for 120 V AC input
Control Panel	
IFC6C04BBL-CEG	Shielded Cat6 stranded cable, PVC jacket, CM
CADIN1IG	DIN rail mount adapter, international gray
ISTPHCH1MBL	600 volt rated, Cat5e patch cord, 1 meter long
FPS6X88MTG	IndustrialNet™ Field attached shielded RJ45 plug
IAEBH6	Bulkhead Jack Cat6 UTP RJ45 with cap
DAP3BC-S0-6	Data Access Port, 3 inch Base, Simplex Outlet, Cat6 coupler
Machine & Robot	
ISFCH5C02ATL-XG	Industrial Copper Cable, Cat5e, 2-pair, 24/7 AWG stranded, SF/UTP, CM, 600V, Teal, 1000ft/305m reel, High Flex, Sun and Oil Resistant
ISFCH5C04ATL-XG	Industrial Copper Cable, Cat5e, 4-pair, 24/7 AWG stranded, SF/UTP, CM, 600V, Teal, 1000ft/305m reel, High Flex, Sun and Oil Resistant
ISPS55E44MFA	Field attached shielded M12 plug
JP2SBC50-L20	J-Hook with screw-on beam clamp for use with flanges up to ½"
WG12BL10	12" wide x 10' long pathway section used to carry cables horizontally throughout the system
IUTP6X3MBL	Industrial Patch Cord, IP65/IP67, Cat6A, UTP, RJ45 with caps, 3 meters
ISX6004AYL-LED	Industrial Copper Cable, Cat6, 4-pair, 24/7 AWG Stranded, S/FTP, PUR, Yellow, 500m RL

388022

5

Physical Infrastructure Deployment for Level 3 Site Operations

The Level 3 Site Operations Area provides the switching, computer, and storage resources needed to efficiently operate a plant-wide IACS architecture. This area is the foundation for data collection and application hosting in the industrial setting. Level 3 equipment may be physically housed in an Industrial Data Center, in a rack in the control room, or several other locations on the premise. Level 3 Site Operations applications range from MES measures such as Overall Equipment Effectiveness (OEE), lot traceability preventive maintenance schedules, process monitoring/management, safety/security dashboards, and productivity key performance indicators (KPIs). Continuity of service is imperative as these functions are used for daily decision-making on an ever-increasing basis. Manufacturing downtime is readily measured in minutes and in thousands of dollars from missed customer commitments. Reliable and secure network support for these applications keep operations and business communication running smoothly.

The successful deployment of Level 3 Site Operations depends on a robust network infrastructure built on a rock-solid physical layer that addresses the environmental, performance, and security challenges present when deploying IT assets (servers, storage arrays, and switching) in industrial settings. The Level 3 Site Operations is a key convergence point for IT and OT. Many businesses obtain these functions in a pre-engineered package, Industrial Data Center (IDC). IDC systems include the proper IT assets housed in an appropriate cabinet with patching, power, grounding/bonding, identification, and physical security considerations already addressed a plug and play solution.

The Level 3 Site Operations Area presented in this chapter is a model for integrating a scalable, modular, logical network and computer systems into the physical infrastructure. Some benefits of this approach are listed below:

- Improves network availability, agility, scalability, and security

- Reduces operational costs, including energy costs, with improved efficiencies

- Can help to simplify resource provisioning

- Lays the foundation for consolidation and virtualization

- Helps to create a path to future technology requirements such as 10/40GbE. This chapter includes the following major topics:

    o Key Requirements and Considerations, page 5-2

    o Physical Network Design Considerations, page 5-9

    o Panduit List of Materials, page 5-18

Key Requirements and Considerations

Industrial network deployments have evolved over the years from a network gateway layout to a converged plant-wide architecture. CPwE architecture provides standard network services to the applications, devices, and equipment found in modern IACS applications and integrates them into the wider enterprise network. The CPwE architecture provides design and implementation guidance to achieve the real-time communication and deterministic requirements of the IACS and to help provide the scalability, reliability and resiliency required by those systems.

In support of industrial network performance, many physical infrastructure aspects of the Level 3 Site Operations serve an important role, and must be considered in the design and implementation of the network:

• **Industrial Characteristics**—Plant/site 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 heat dissipated by equipment and power quality considerations.

• **Physical Network Infrastructure Life Span**—IACS and plant/site backbone can be in service as long as 20 years or more. Hardware used in Level 3 Site Operations being IT gear has a much shorter life span, generally three to five years. The infrastructure used to connect and house the 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 needs of current and future data communications to be fully met. Choices between copper and fiber-optic cabling deliver higher data rate transport requirements.

• **Maintainability**—MACs at Level 3 have dependencies that affect many Cell/Area Zones. Also, changes must be planned and executed correctly to avoid bringing down the IACS process. Proper cable management such as bundling, identification and access is vital for proper Level 3 Site Operations maintenance.

• **Scalability**—The high growth of EtherNet/IP and IP connections can strain network performance and cause network sprawl that threatens uptime and security. A strong physical building block design accounts for traffic growth and management of additional cabling to support designed network growth. Use a physical zone topology with structured copper and fiber-optic cabling chosen for high data throughput. Choose building block pre-configured solutions to enable a network infrastructure comprised of modular components that scale to meet increasing industrial Ethernet communications needs in the 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 with measured, validated performance confirms reliable data throughput. Use of redundant logical and physical networks assures highest availability. Properly designed and deployed pathways should be employed to achieve resilient redundant cable paths.

• **Network Compatibility and Performance**—Cable selection is the key to optimal physical network performance. Network performance is governed by the poorest performing element in any link. Network compatibility and optimal performance are essential from port to port, including port data rate and cabling bandwidth.

• **Grounding and Bonding**—A well architected grounding/bonding system is crucial for of industrial network performance at every level whether internal to control panels, across plants/sites, or between buildings. A single, verifiable grounding network avoids ground loops that can degrade data and have equipment uptime and safety implications.

• **Security**—Network security is a critical element of network uptime and availability. Physical layer security measures, such as logical security measures, should follow a defense-in-depth hierarchy. The Level 3 Site Operations physical defense in-depth strategy could take the form of locked access to industrial data center/control room spaces and cabinet key card access to help limit access, use of 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 connectivity achieving service level goals.

- • **Wireless** - Unified operation of wireless APs requires a WLC at Level 3 Site Operations and distribution of Lightweight Wireless Access Points (LWAPs) across Industrial Zone and Cell/Area Zones. Autonomous wireless APs, typically WGBs, in Cell/Area Zones involve cabling for APs and WGBs. The Industrial Zone backbone media selection and cabling for APs using PoE are critical for future readiness and bandwidth considerations. PoE is evolving to deliver more power over copper cabling. Therefore, understanding industrial applications with scalability and environmental considerations is critical.

Industrial Characteristics

Room Environment

A sustainable cooling system design that follows industry best practices is essential to the success of modern Level 3 Site Operations deployment. Optimized cooling management and a more efficient energy system are the results, which means IT equipment is safe from unplanned downtime due to overheating and significant operational expense (OpEx) savings are realized. The Level 3 Site Operations room is divided into a hot aisle/cold aisle arrangement, to separate the cold inlet air on the front side of the cabinets and the hot exhaust air on the rear side of the cabinets. Cold air in this design is fed through the raised floor via a Computer Room Air Conditioning (CRAC) unit. Cold air can be delivered by several different means, if it maintains the hot aisle/cold aisle arrangement. Hot air in this design is exhausted through fans in the ceiling.

Thermal Ducting

Network switches deployed in data centers (for example, Catalyst 4500-X/6800) often uses side-to-side airflow cooling. This airflow design requires less vertical space and permits high switch port density. Given proper inlet air conditions, these switches are well designed to cool themselves. However, large bundles of cabling driven by high port density impede airflow. Also, hot exhaust air can recirculate to the intake, raising inlet temperatures and inhibiting the self-cooling ability of the switch. For network equipment that uses side-to-side airflow patterns, in-cabinet ducting optimizes cooling system efficiency by establishing front-to-back airflow patterns throughout the cabinet. By using Computational Fluid Dynamics (CFD) analysis and testing, ducting solutions have been developed that improve inlet air conditions for cabinet applications.

Physical Network Infrastructure Life Span

IACS and plant/site backbone technologies can have a lifespan of up to 20 years. IT hardware has a much shorter life span, generally in the 3–5-year range. While a three-year refresh cycle is commonplace for IT personnel in enterprise and data center domains, it is not routine in current OT domains. Level 3 physical infrastructure that supports IT hardware should have a much longer lifespan, usually three to four IT hardware refresh cycles. As a result, it is important to consider the structural dependability of cabinets, future proof types of cabling, and pathways optimized for capacity growth projections. It is also important to adhere to structured cabling practices and install upgraded and spare media to help protect against physical layer obsolescence. Making informed physical infrastructure decisions from the beginning affect the ability to complete future projects in a timely and cost-effective manner.

Maintainability

Patching

The best practice for patching is to land fiber cable into an enclosure or box following a structured cabling approach. When fiber is terminated, several inches of the glass strand are exposed. This part of the fiber is fragile and needs the enclosure or box to help protect the fiber from damage. Terminating directly to a connector without protection or support can lead to failures. For rack/cabinet installations, a 19" style fiber enclosure is a suitable choice. When installing fiber into a control panel, components such as the DIN Patch Panel or Surface Mount

Box provide patching. Another advantage for structured cabling is to build in spares ready for use to accommodate growth or for recovery from link failure.

Bundling

The best practice for bundling numerous standard jacket fiber cables is to use a hook and loop cable tie. This cable tie does not overtighten the bundle, which can lead to damage. However, the environmental impact on the hook and loop tie is an important consideration and for these instances, a more durable cable tie for fiber is the elastomeric tie. It can stretch to help prevent over tension and guard against weather, oil, salts, and so on. The use of nylon cable ties can potentially damage the cable and is not recommended for standard jacket fiber cable, but it is appropriate for armored or dielectric double jacketed fiber cabling.

Identification

Identification facilitates MACs and aids in troubleshooting. Fiber cabling identification includes labeling and color coding. Labeling can be applied to enclosures, ports, patch cords, horizontal cables, and so on. Since some fiber cable diameter is small, applying a label can be a challenge. A sleeve can be applied to increase the diameter to make the label readable. The text on the labeling should follow TIA-606A standards. A breakdown usually occurs from the enclosure/rack, RU, port, and so on, that is consistent throughout the facility. For example, CP1.PP1.02 could mean control panel 1, patch panel 1 and port 2. Color coding can identify VLANs, zones, functional areas, network traffic type, and so on, and can be achieved with labels, hook and loop cable ties, and color bands. Although fiber cable is color coded by cable type, additional color coding can be performed for clarity using the preceding methods.

Scalability

Pathway Decisions—Type and Sizing

Pathways for cables are critical for distributing copper and fiber cabling securely across the plant/site while helping protect from physical threats that can degrade or damage the cable. The TIA-1005 standard, ODVA Media Planning and Installation manual, and TIA resources provide recommendations on pathways including cable spacing and installation guidance to minimize risks from environmental threats. Several options exist for routing cables via pathways that simplify deployment using best practices for various environments across the plant. Figure 5-1 describes some of the options.

Figure 5-1 Pathway Options

Installation Consideration	J-Hook	Wire Basket	FiberRunner®
Cable Protection Environment	Mild	Moderate	Moderate to harsh
Cable Density	Light to medium	Medium to heavy	Light to heavy
Applicable in Constrained Spaces	Yes	No	No
Installation Complexity	Simple	Moderate	Moderate to strong
Ease of Moves, Adds, Changes	Simple	Moderate	Moderate

387980

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 often secured with a cable tie. The J-Hook maintains proper bend radius control when transitioning down. J-Hook systems should be used with cables that have rigidity to have an acceptable bend between spans

and is 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. Cable tray material should also be rated 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 highest protection with few network cables, conduit is the preferred choice. Care must be taken to maintain proper bend radius and lineal support to prevent cable sag.

Designing for High Availability

Cable Management

Proper cable management is essential for high system performance, availability, and reliability. A resilient cable management system is critical in areas such as MACs (for example, identification and color coding) to verify that the proper action is taken and to aid in troubleshooting. Care must also be taken to help protect the cabling from excessive bend, flexing, sag, rubbing, crush, and so on. A strong cable management system needs to be designed around the following key elements:

• Bend radius control

• Cable routing and protection

Bend Radius Control

It is important to have a bend radius greater than or equal to the manufacturer-specified minimum when handling fiber-optic cabling to help prevent it from excessive bending, which can cause physical damage. Two considerations for bend radius control are:

• **Dynamic**—Cable flexing (especially during installation)

• **Static**—Cable held in place

Fiber cable manufacturers specify both radiuses where the dynamic bend radius can be 20 times the Outer Cable Diameter (OD) and the static bend radius is typically 10 times the OD. Although fiber strands are very thin and made of glass, the strand is durable and can withstand some flexing. However, flexing in general can cause deformities in the fiber, leading to signal loss over time (microbend). Therefore, the stricter bend radius is dynamic. Another risk to a properly terminated and validated fiber cable is attenuation due to excessive cable bend (static). Essentially, the bend allows the light to escape the glass, reducing signal strength (macrobend).

The bend radius is based on the OD, therefore the minimum bend radius for the application can vary. For example, a fiber patch cord cable has a static bend radius of 1.1" while a 12 fiber distribution cable has 2.4" bend radius. Bend radius is maintained by spools, clips, fins, product features, and proper coiling. In a 19" data center style server or switch rack/cabinet, bend radius accessories can be installed to route fiber cable vertically and horizontally. Fiber enclosures and boxes used in data center cabinets/racks typically have built-in slack spools. Also, supplied adhesive backed clips secure the cabling and provide strain relief.

Cable Routing and Protection

Often, fiber cable is routed through conduit for protection. Although conduit is an excellent safeguard, it is designed for power cabling and has fittings, junction boxes, and so on, where fiber cable under some tension can potentially bend below the minimum bend radius. Pathways such as wire basket and J-hooks have challenges for sagging and bends that can attenuate the signal, especially for unprotected standard distribution cable.

Therefore, the cable must be supported and bends must be controlled. Draping unprotected distribution cable over J-Hooks or laying the cable over an open tray with grids can potentially lead to fiber sagging below the minimum bend radius. To avoid this risk, fiber cabling can be pulled through corrugated loom tube, providing rigidity and support. Typically, fibers in

interlocking armor or DCF do not encounter these issues because the armor provides support and restricts the bend radius.

To protect fiber cabling when routed in control panels, it must be carefully laid in duct or tubing to avoid snags and kinks, maintaining proper bend radius. Adhesive backed mounting clips can hold fiber cabling in place outside of ducts along the panel wall or top.

Smart Reliable Power Protection and Backup Power

To improve availability and reduce unplanned downtime Uninterruptible Power Supply solutions are often implemented, protecting data and critical IT equipment. Best in class systems intelligent power solutions are highly reliable, provide efficient power distribution and have secure access and manageability. These solutions support a range of applications from Data Centers and Enterprise environments to supporting Edge IT equipment, including in plant environments.

Show below, the SmartZone UPS provides excellent electrical performance, intelligent battery management, enhanced intelligent monitoring, secure network functions and long lifespan for lithium units. Additionally, they comply with ENERGY STAR 2.0, EMC and safety standards. . Output capacities can range from 1/2/3kVA, 5/6/10kVA to 10/15/20kVA with lead acid (VLRA) or Lithium-Ion battery types.

These UPS solutions are integrated for use with the SmartZone Cloud Software that combines power and environment monitoring along with cabinet access, asset tracking and connectivity management.

Figure 5-2 Smart UPS Example – SmartZone UPS

Network Compatibility and Performance

Cable Media Selection

Depending on cable construction, many considerations exist for cable media selection such as reach, industrial characteristics, life span, maintainability, compatibility, scalability, performance, and reliability. See table that follows.

Figure 5-3 Cable Media Selection Characteristics

Parameter	Copper Cable	Multimode Fiber	Single-mode Fiber
Reach (maximum)	100 m 1,000 m (SPE)	2,000 m (1 Gbps) 400 m (10 Gbps)	70 km (1 Gbps) 10 km (10 Gbps)
Noise Mitigation Option	Foil shielding	Noise immune*	Noise immune*
Data Rate (Industrial)	10 Mbps (SPE) 100 Mbps (Cat 5e) 1 Gbps (Cat 6) 10 Gbps (Cat 6a)	1 Gbps 10 Gbps	1 Gbps 10 Gbps
Cable Bundles	Typically small (SPE) Large	Small	Small
Power over Ethernet (PoE) capable	Yes	Yes, with media conversion	Yes, with media conversion

388023

*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. Traditionally, if the required cable reach exceeds 100 m (328 feet), then the cable media choice is optical fiber cable. 4-pair copper Ethernet cable is limited to maximum link length of 100 m. A new Ethernet variant, Single Pair Ethernet, exists for long reach applications. Standardized by IEEE 802.3cg – 2019, Single Pair Ethernet using 10BASE-T1L PHYs is capable of transmitting at 10 Mbps over balanced copper conductors at distances up to 1000 meters. Single Pair Ethernet (SPE) targets difficult applications at the network edge. Its design intent is bringing Ethernet to applications while supporting media and topology choices common with existing Fieldbus methods.

However, other considerations exist for distances less than 100 m such as EMI susceptibility where fiber-optic cable is chosen due to its inherent noise immunity. Another consideration is the fact that IES uplinks connected with optical fiber converge faster after an IES power interruption, lessening the duration of the network outage. When it comes to data rates, copper and fiber are similar for typical industrial applications. However, other higher performing optical fiber is available for high demand networks.

Regarding media performance, a major consideration is network lifespan. For instance, installing a network with Cat 5e cabling could be obsolete in a couple of years, especially if transporting video. If the expectation is 10 or more years of service, the fastest category cabling should be considered. Upgrading networked equipment and switches in the future may only come with higher data rate ports.

Multimode versus Single-mode

Fiber has two types, single-mode and multimode. Multimode has many glass grades from OM1 to OM5. Single-mode has two glass grades, OS1 and OS2. When selecting any optical fiber, the device port must be considered first 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, flexibility exists to select compatible transceivers and the transceiver best for the application. In addition to different media, the number of strands, mechanical protection, and outer jacket protection should be considered. Refer to chapter 4 for detailed information on fiber selection.

Cable Fire Ratings Reference

Cable fire ratings need to be considered when specifying cabling infrastructure to ensure local building codes are met. The rating guide below provides the information needed to determine which rating is appropriate for different installation environments.

Plenum Rated Cable (OFNP)

An Optical Fiber, Nonconductive, Plenum (OFNP) rating signifies cable that has passed stringent burn testing and is suitable for installation into air plenum spaces. OFNP cables have fire resistance and low smoke production characteristics. They can be installed in ducts, plenums, and other spaces used for building airflow. This is the highest fire rating fiber cable and no other cable types can be used as substitutes.

Plenum Rated Cable (OFCP)

An Optical Fiber, Conductive, Plenum (OFCP) rating differs from OFNP in that the cable contains metallic elements, typically armor, and therefore, conducts electricity. All other aspects of this rating are the same as OFNP.

Riser Rated Cable (OFNR)

An Optical Fiber, Nonconductive, Riser (OFNR) rating is commonly required when cables are run between floors through open vertical shafts. OFNR cables are used in riser areas which are building vertical shafts or runs from one floor to another floor. OFNR cables cannot be installed in plenum areas since they do not have the same required smoke rating as plenum rated cables. OFNP plenum cables can be used as a substitute for OFNR riser cables.

Riser Rated Cable (OFCR)

An Optical Fiber, Conductive, Riser (OFCR) rating differs from OFNR in that the cable contains metallic elements, such as a layer of armor, and therefore, conducts electricity. All other aspects of this rating are the same as OFNR.

Low Smoke Zero Halogen (LSZH)

A Low Smoke Zero Halogen (LSZH) rating is sometimes referred to as low toxicity cable. When burned, PVC-based cables produce a cloud of toxic smoke containing corrosive compounds such as hydrochloric acid. The LSZH cables do not contain the halogen type compounds that form these toxic substances. Smoke emitted from burning LSZH cables do not produce the toxic halogen-based gasses previously mentioned. LSZH ratings are expressed as OFN-LS or OFNR-LS if the cable also meets the requirements of a OFNR rated cable.

Grounding and Bonding

It is essential that robust and clean power is supplied to the Level 3 Site Operations to keep the IACS network running smoothly without compromises in communications and equipment performance. The incoming power feed typically includes an UPS and one or more Power Outlet Units (POUs) to distribute power for IT assets where needed. POU voltages range from 100V to 125V or 220V to 250V depending upon the region of the world, with currents ranging from 15 amp to 30 amp. Connectors may be straight blade or twist locks. Popular IEC configurations are C13 to C14 and C19 to C20. Additionally, POUs may include intelligent features such as power and environmental monitoring to aid in troubleshooting and diagnostics.

Grounding of the Level 3 Site Operations is critical to optimizing performance of all equipment located within the Level, reducing downtime due to equipment failures and reducing the risk of data loss. Exemplary grounding and bonding provide demonstrable improvement in bit error rate in data center and enterprise applications. Given the higher potential for EMI in industrial applications, the improvement stands to be remarkable. Also, Cisco and Rockwell Automation logic components require good grounding practices to maintain warranty support. The use of a single ground path at low impedance is commonly achieved through a busbar.

Bridging the grounding connection from Level 3 Site Operations to busbar can occur in several ways: First, a braided grounding strap connects the rack or cabinet to the building ground network. Second, grounding jumpers connect equipment to the housing structure. Finally, paint piercing screws and washers achieve a direct metal-to-metal connection throughout the Level 3 Site Operations. Unless a clear and deliberate effort to confirm that proper grounding has been performed, ground loops can be established that result in lost communication data and compromised equipment performance.

Security

Both physical and logical security should be important considerations when designing Level 3 Site Operations. Physical layer security measures, such as locked access to data center/control room spaces and key card access to cabinets help limit access to and help prevent inadvertent or malicious damage to equipment and connectivity to help achieve service level goals. Often overlooked basics such as labeling, color coding, and use of keyed jacks can help prevent crossing channels or inadvertently removing active links. Lock-in connectors can secure connections in switches or patching to control who can make changes and help protect against cables being unintentionally disconnected.

For more information, see the *Securely Traversing IACS Data Across the Industrial Demilitarized Zone Design and Implementation Guide* at the following URL:

https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf

Wireless

Secure wireless access in Industrial environments is a growing need. Considerations for jobs to be completed wirelessly and an idea of future growth are needed to begin planning and design. Two main applications are served wirelessly today. These are mobility and WGB communications.

Mobility helps knowledge workers and guest workers securely access data to make more timely and accurate decisions, increasing their overall productivity and effectiveness. Therefore, mobility designs must give sufficient coverage to afford access as needed. In addition, knowledge workers such as engineers and technicians employed by the business typically need to access not only the Internet but internal network resources. Guest workers such as contractors and repair personnel deployments are typically used to enable machinery communications. Often the machinery is dynamic (for example, movement through the facility) and needs to quickly reestablish wireless communications with the network once in place. WGB wireless does an excellent job for this use case.

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:

http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.html

http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf

Physical Network Design Considerations

Logical to Physical Simplified

The following figure represents a potential layout of a plant/site with enterprise office space. The CPwE logical architecture (on the top) is mapped to the locations that the different levels of operation could potentially be placed within the plant/site.

Figure 5-4 CPwE Logical to Physical Plant/Site

Enterprise Data Center

Level 3 Site Operations

Industrial Distribution Frame

Cell /Area Zones
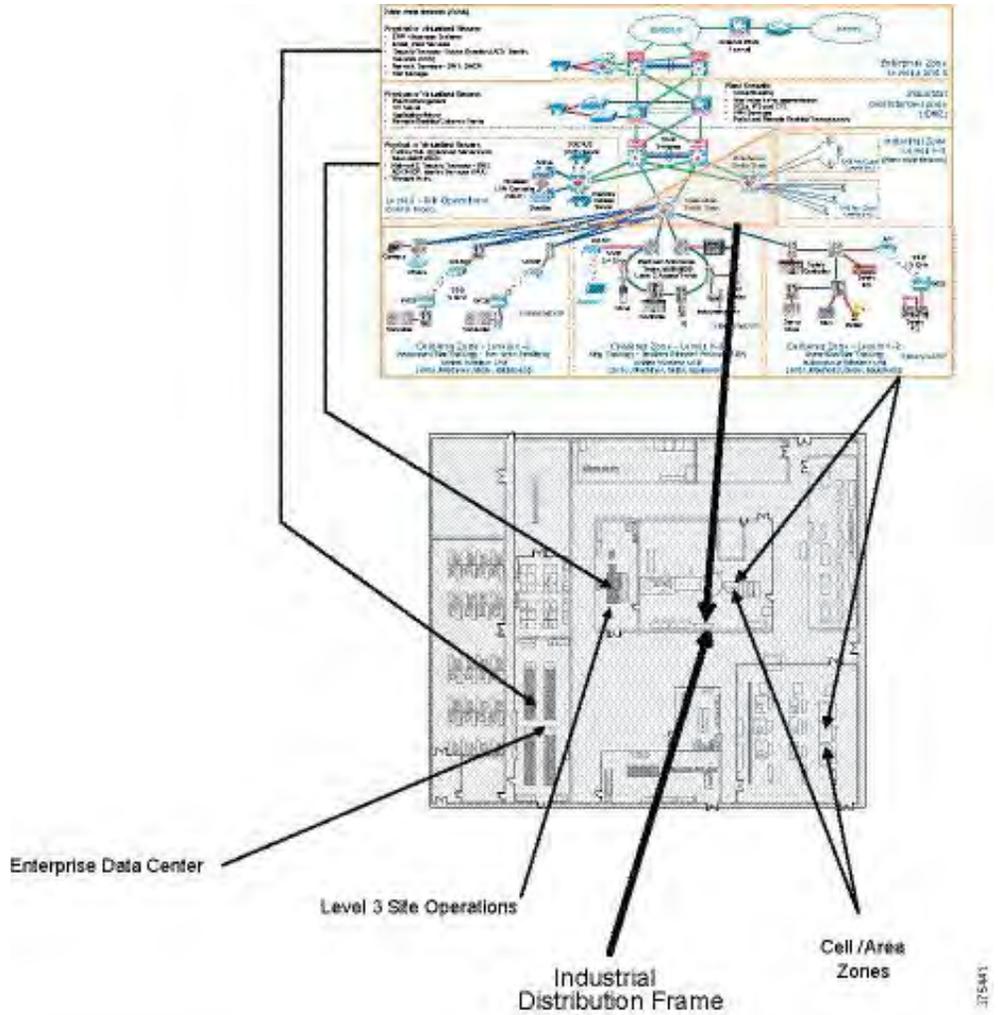
Level 3 Site Operations—Large Scale Deployment

Figure 5-5 Level 3 Site Operations Logical to Physical Deployment
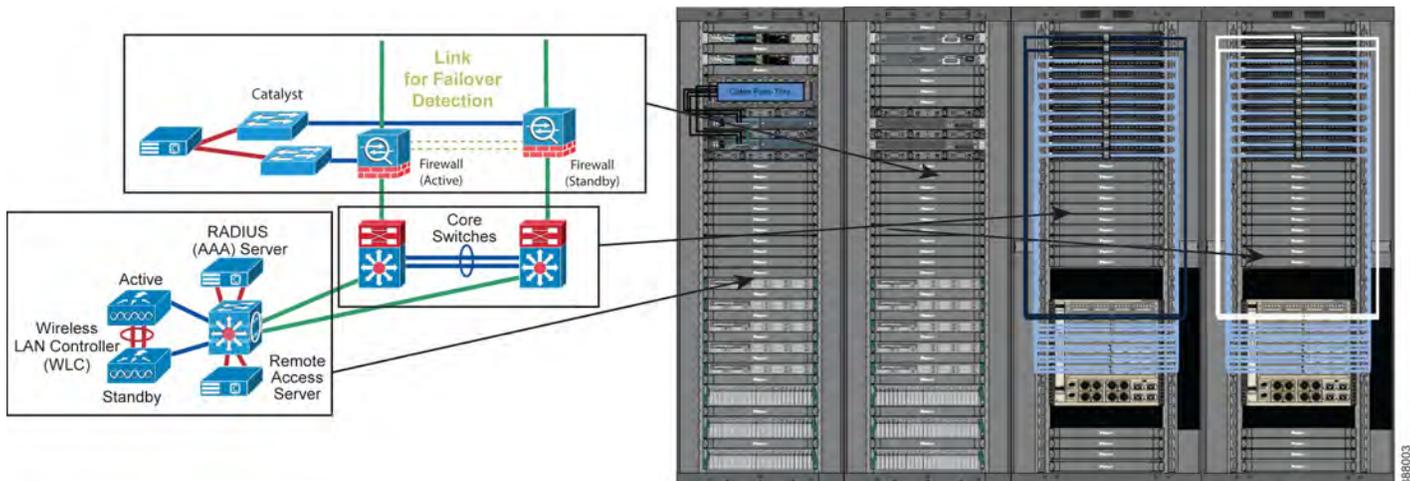
The Level 3 Site Operations can function differently in diverse environments and layouts, but generally it houses the networking to connect the plant/site to the enterprise and applications that allow the plant/site to operate efficiently. The layout described in Figure 5-5 demonstrates a larger industrial deployment. This deployment is likely much larger than most plants/sites would

require, but demonstrates how the Level 3 Site Operations infrastructure would be deployed if this scale were required. The core of the network is using two Cisco Catalyst 9000 with a full fiber distribution network. This deployment is employing virtualized servers to provide efficient and resilient compute power to the plant/site and beyond. Four distinct cabinets house equipment for three different areas of the CPwE architecture: Level 3 Site Operations or IDC, IDMZ, and Core Switching Cabinets. Each of the cabinets is detailed further below.

IDC Cabinets

The IDC cabinet (see the following figure) houses the Catalyst 9300 switches that deliver access to WLC and the virtualized servers which can provide several services and applications to the plant/site.

Figure5-6 IDC Cabinet Logical to Physical Deployment
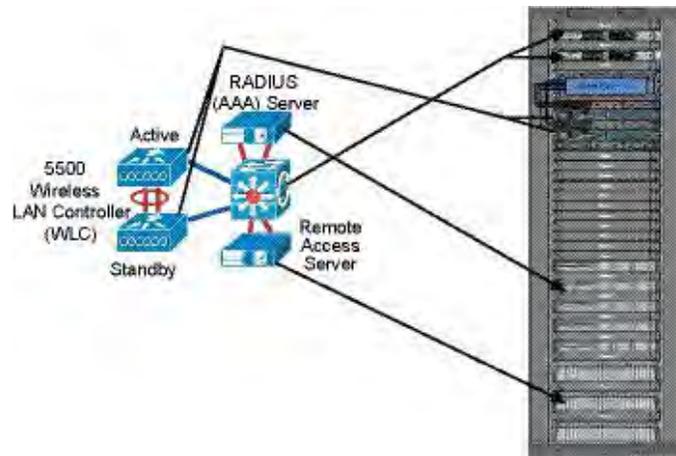
Within the cabinet, the servers are placed at the bottom of the cabinet, and switches are at or near the top. The servers are the heaviest pieces of equipment within the cabinet and are placed at the bottom to create the lowest center of gravity possible. This helps prevent the cabinet from tipping over and makes it more stable in case it needs to be moved as a unit. The Catalyst 9300 switches are placed at the top of the cabinet to allow for easy connections to the Catalyst 6800 switches. The Catalyst 9300 switches have a back to front airflow, which means that the port side of the switch is facing the hot aisle. The Cisco WLCs are placed a few RU below the Catalyst 9300 switches. The Cisco WLCs have their ports on the front side and have an airflow from front to back only. This means that to connect to the Catalyst 9300 switches, which have their ports on the back side, a cable pass-through is required to connect. The servers have their network ports on the hot aisle side (or back side), which allows them to connect easily to the Catalyst 9300 switches.

IDMZ Cabinet

The IDMZ cabinet (see the following figure) houses the equipment that logically separates the enterprise from the plant/site.

Figure 5-7 IDMZ Cabinet Logical to Physical Deployment
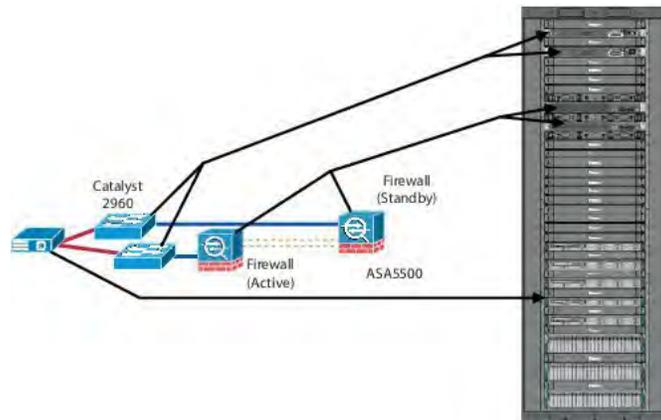
The IDMZ Cabinet has two Cisco Catalyst 9200 switches, two (active/standby) Cisco firewalls, and several virtualized servers that house applications and software, which must reside within the IDMZ. The servers are the heaviest pieces of equipment within the cabinet and are placed at the bottom to create the lowest center of gravity possible. This helps prevent the cabinet from tipping over and makes it more stable in case it needs to be moved as a unit. The Catalyst 2960 switches are placed at the top of the cabinet to allow for easy connections to the Catalyst 9500 switches. The equipment has network ports on the hot aisle (back side) that allows for easy connections between equipment.

Server Cabinets

Server Cabinets offer several features that enhance cable and thermal management and should be used when deploying servers, such as the Cisco UCS C-series. Cabinet air seal features and integration with passive hot and cold air containment components drive efficient utilization of cooling capacity and reduce cooling energy consumption. Modular cable management systems available on server cabinets, enable simplified organization of cables and proper bend radius control. Smart cabinet features allow access to environmental, power, and security information.

Core Switching Cabinets

The core switching cabinets (see the following figure) house the redundant Cisco Catalyst 9500 switches that serve as the plant/site core switches and the gateway between the plant/site and the enterprise.

Figure 5-8 Core Switching Cabinets Logical to Physical Deployment

Network Cabinets

Network cabinets offer several features that enhance cable and thermal management and should be used when deploying large chassis-based switches, such as the Cisco Catalyst 9500 switch. An inset frame design efficiently manages large quantities of cables and provides space for access maintenance. Cabinet air seal features and integration with passive hot and cold air

containment components drive efficient utilization of cooling capacity and reduce cooling energy consumption. Dual-hinged doors reduce time needed to perform MACs. Modular cable management systems available on network cabinets, enable simplified organization of cables and proper bend radius control.

Physical to Physical Simplified

IDMZ Cabinet to Core Switching Cabinets

The IDMZ to Core Switch connections shown in the following figures can be copper or fiber depending on the model of firewall and the line card used in the Catalyst switch.

Figure 5-9 IDMZ Cabinet to Core Switches Cabinets Physical to Physical Deployment
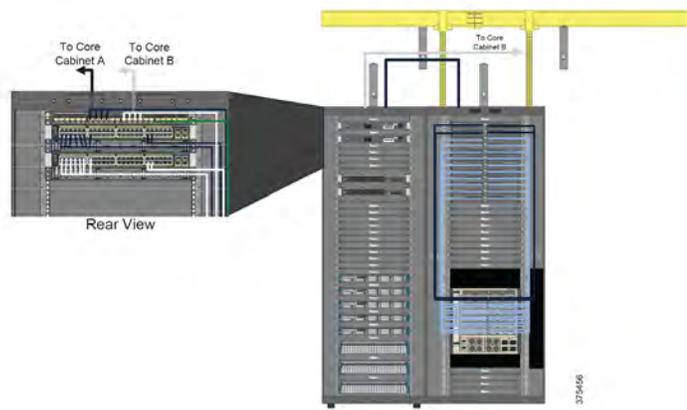
In the figure above and the figure that follows, copper connects the Cisco firewall and the Cisco Catalyst 9500 switch. Starting at the Cisco firewall, the one side of the Cat 6A patch cable plugs into the Cisco firewall port and the other side plugs into the jack module that is housed in the adapter, which is connected into the patch panel. On the back side of the jack module the Cat 6A horizontal cable is connected and runs to the core switch cabinet. When the Cat 6A horizontal cable reaches the Catalyst cabinet, it is attached to the back side of the jack module. On the front of the jack module, the Cat 6A patch cable is plugged in and on the opposite side the Cat 6A patch cable is plugged into the RJ45 port on the Cisco Catalyst 9500 line card.

Figure 5-10 Cisco Firewall to Catalyst 9500 Switch Single Line
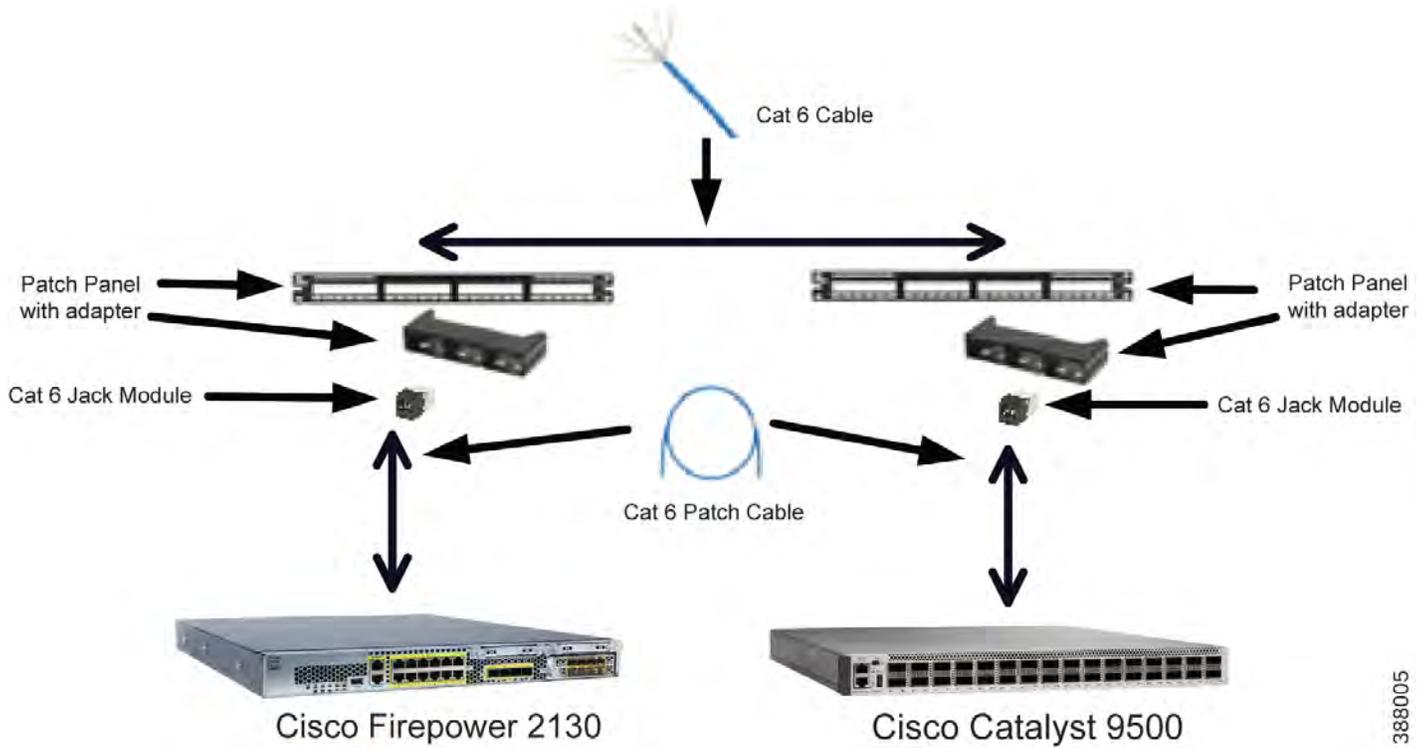
IDC Cabinet to Core Switching Cabinets

The IDC Cabinet-to-Core Cabinets connections shown in the following figures can also be copper or fiber depending on the model of switch in the IDC cabinet and the line card used in the Catalyst switch.

Figure 5-11 IDC Cabinet to Core Switching Cabinets Physical to Physical Deployment
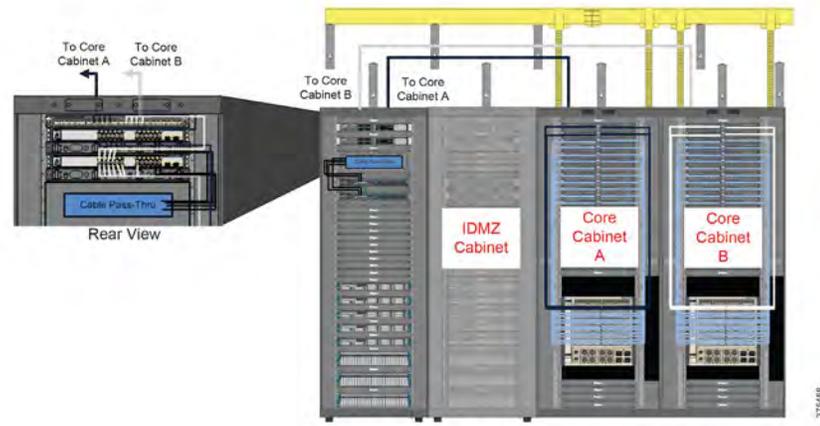
In this scenario, copper connects the Cisco Catalyst 9300 switch and the Cisco Catalyst 9500 switch. Starting at the Cisco Catalyst 9300 switch, the one side of the Cat 6A patch cable plugs into the RJ45 port on the Cisco Catalyst 9500 switch and the other side plugs into the jack module that is housed in the adapter, which is connected into the patch panel. On the back side of the jack module, the Cat 6A horizontal cable is connected and runs to the Catalyst cabinet. When the Cat 6A horizontal cable reaches the Catalyst cabinet, it is attached to the back side of the jack module. On the front of the jack module, the Cat 6A patch cable is plugged in. On the opposite side, the Cat 6A patch cable is plugged into the RJ45 port on the Cisco Catalyst 9500 line card.

Key Requirements and Considerations

Figure 5-12 IDC Cabinet to Core Switching Cabinets Physical to Physical Deployment
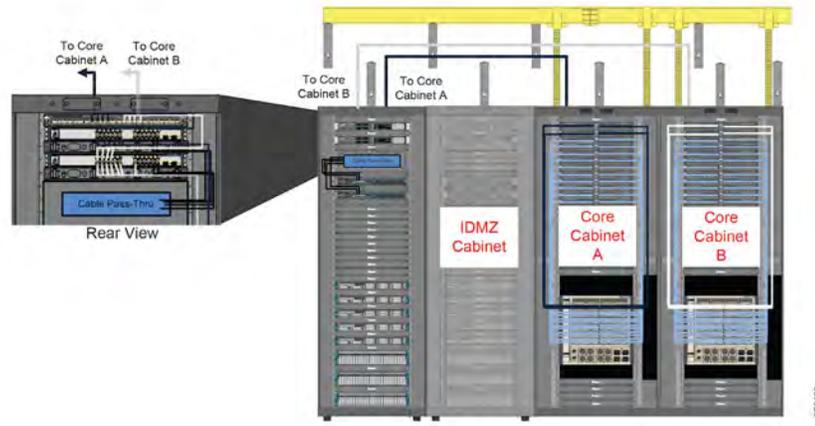
Figure 5-13 Catalyst 9300 Switch to Catalyst 9500 Switch Single Line
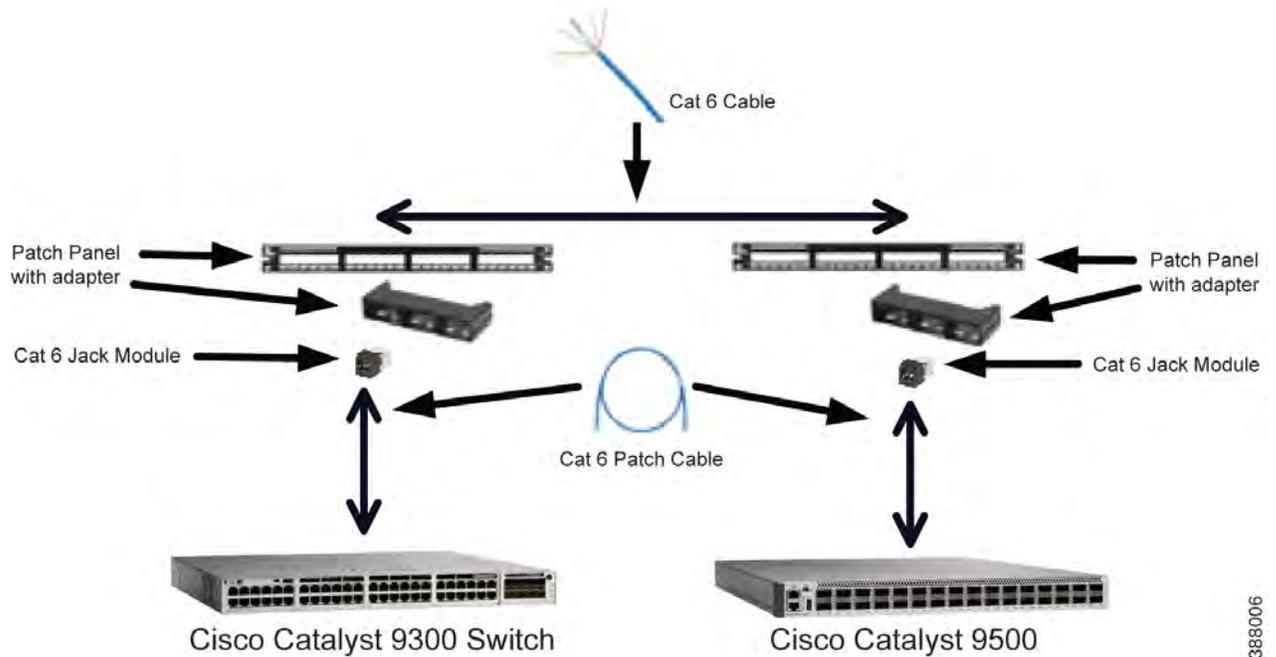
Level 3 Site Operations—The Industrial Data Center from Rockwell Automation

The IDC from Rockwell Automation (see the following figure) can help your business realize the cost savings of virtualization in a production environment through a pre-engineered, scalable infrastructure offering. The hardware you need to run multiple operating systems and multiple applications off virtualized servers are included in the cost. Industry-leading collaborators including Cisco, Panduit, Dell/EMC, and VMware work together with Rockwell Automation to help your business realize the benefits of virtualization through this integrated offering.

As a pre-engineered solution, the IDC from Rockwell Automation is designed to ease the transition to a virtualized environment for your business, saving you time and money. Instead of ordering five different pieces of equipment with five purchase orders, in addition to hiring the correct certified installation professionals to get you up and running, the IDC combines equipment from industry leaders that are pre-configured specifically for the manufacturing and production industries. All equipment is shipped pre-assembled and a Rockwell Automation professional will come to your site and commission the system.

Figure 5-14 The Industrial Data Center from Rockwell Automation—Physical Layout
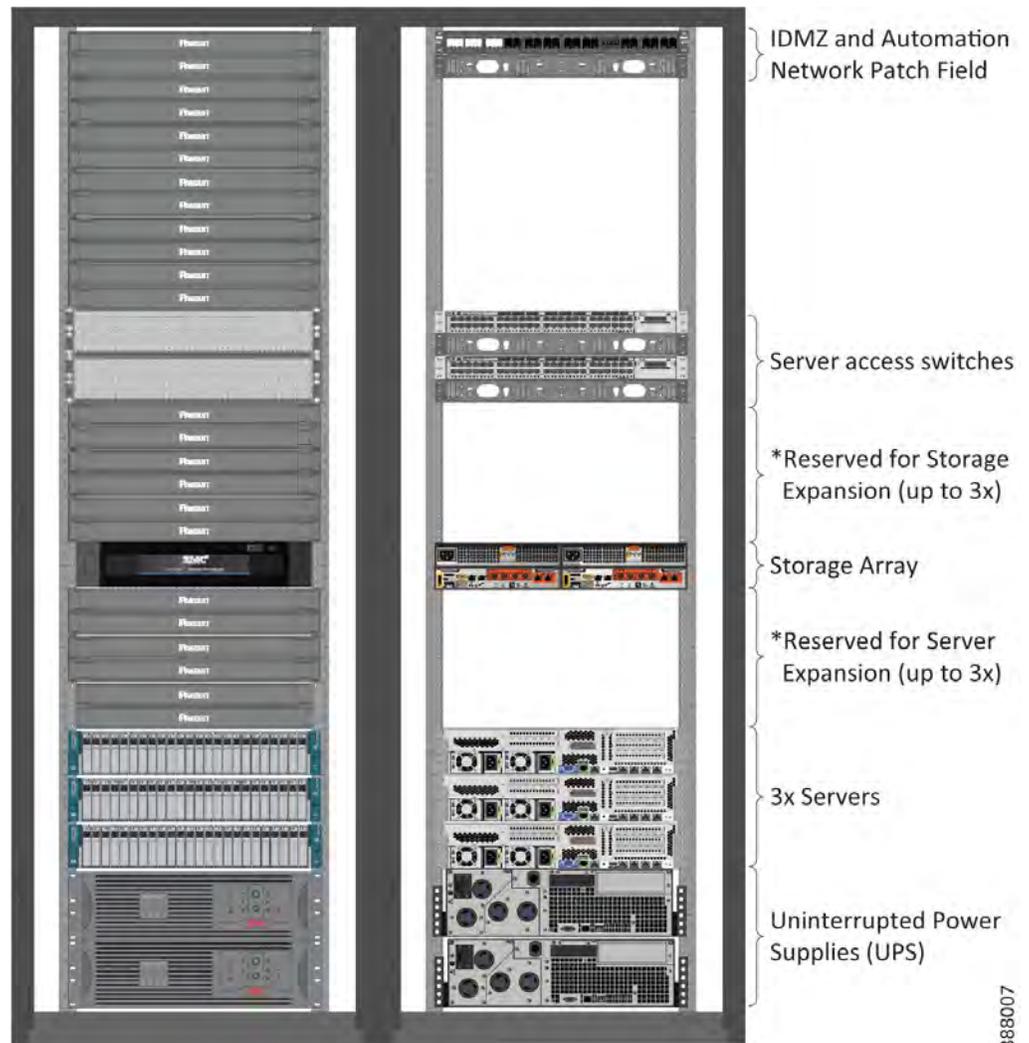
Features and Benefits:

• **Reduced Cost of Ownership**—Decrease the server footprint in your facility and realize savings over the lifetime of your assets

- **Uptime Reliability**—Deliver high availability and fault tolerance

• **Designed for Your Industry**—Engineered specifically for use in production and manufacturing environments

• **Ease of Ordering and Commissioning**—Pre-assembled solution that includes configuration service. No need to place multiple equipment orders

• **One Number for Technical Support**—Includes TechConnect™ support so you have one phone number to call. Additional support levels include 24x7 support and remote monitoring

Panduit List of Materials

The following table is a sample list of materials for best-in-class physical layer solutions for the Level 3 Site Operations from Panduit.

Figure 5-15 Sample List of Materials

Part Number	Description
N8222B	Net-Access™ N-Type Cabinets – Network Cabinet, 800mm, 42RU, 1200M Depth, Black
MDC79	Pre-configured Micro Data Center, 42U, Two Side Panels, Network Cabling, Patch Panels, Cable Management, Grounding, and Casters; Net-Access S-Type Cabinet – Server Cabinet, 700mm, 42RU, 1200M Depth, Black
UPS	
U03N11V	SMARTZONE UPS, 3kVA, 2U, 120V, VRLA, Single Phase, Double-Conversion On-Line Power Protection with Intelligent Network Card & Rail Kit
Patch Panels	
QPP24BL	QuickNet™ Patch Panel
TLBP1S-V	1RU Tool-less Cage Nut Blanking Panel
QPPABL	MiniCom® Patch Panel Adapter
CJ6X88TGBL	Cat6A RJ45 MiniCom® Jack, Black
Cable	
UTP28X7	Cat6A 28 AWG UTP Patch Cord – 7 ft, Off White
UTP28X7BU	Cat6A 28 AWG UTP Patch Cord – 7 ft, Blue
FZE10-10M2	OM4 LC-LC Duplex Fiber Patch Cable - 2M
Cable Management	
CMPHHF1	RU D-ring Cable Manager
Pathways	
Various	Wire Basket Overhead Cable Tray Routing System
Various	FiberRunner® – Fiber Cable Routing System

388024

References

This appendix includes the following major topics:

Converged Plantwide Ethernet (CPwE)

- Design Zone for Manufacturing-Converged Plantwide Ethernet
  http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

- Industrial Network Architectures-Converged Plantwide Ethernet
  https://www.rockwellautomation.com/en-us/capabilities/industrial-networks/network-architectures.html

- *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide:*
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
  - Cisco site:
    http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG.html

- *Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture:*
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf
  - Cisco site:
    http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.html

- *Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture:*
  - Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf

- – Cisco site:
  http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.html

- *OEM Networking within a Converged Plantwide Ethernet Architecture*:

  - – Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td018_-en-p.pdf

  - – Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/OEM/WP/CPwE-5-1-OEM-WP/CPwE-5-1-OEM-WP.html

- *Deploying Identity Services within a Converged Plantwide Ethernet Architecture*:

  - – Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td008_-en-p.pdf

  - – Cisco site:
    http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/ISE/DIG/CPwE_ISE_CVD.html

- *Securely Traversing IACS Data Across the Industrial Demilitarized Zone*:

  - – Rockwell Automation site:
    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td009_-en-p.pdf

  - – Cisco site:
    http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/IDMZ/DIG/CPwE_IDMZ_CVD.html

- *Cloud Connectivity to a Converged Plantwide Ethernet Architecture*:

  - – Rockwell Automation site:
    https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td017_-en-p.pdf

  - – Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Cloud/DIG/CPwE_Cloud_Connect_CVD.html

- *Deploying Network Security within a Converged Plantwide Ethernet Architecture*:

  - – Rockwell Automation site:
    https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td019_-en-p.pdf

  - – Cisco site:
    https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/5-1/Network_Security/DIG/CPwE-5-1-NetworkSecurity-DIG.html

- *Deploying CIP Security within a Converged Plantwide Ethernet Architecture*:

  - – Rockwell Automation site:
    https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td022_-en-p.pdf

- – https://www.cisco.com/c/en/us/support/switches/catalyst-9500-series-switches/products-installation-and-configuration-guides-list.html

- *Cisco Catalyst 3850 Switch Deployment Guide*:

  - – http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/deployment_guide_c07-727067.html

- *Industrial Ethernet 5000 Software Configuration Guide:*

  - – http://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie5000/software/release/15-2_2_eb/configuration/guide/scg-ie5000.html

- *Stratix Managed Switches User Manual*:

  - – http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

Access Layer Switches

- *Industrial Ethernet 4000 Software Configuration Guide*:

  - – http://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie4000/software/release/15-2_2_ea/configuration/guide/scg-ie4000.html

- *Industrial Ethernet 2000 Software Configuration Guide*:

  - – http://www.cisco.com/c/en/us/td/docs/switches/lan/cisco_ie2000/software/release/15_2_2_e/configuration/guide/scg-ie2000.html

- *Stratix Managed Switches User Manual*:

  - – http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um007_-en-p.pdf

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
ASDM	Cisco Adaptive Security Device Manager
ASIC	Application Specific Integrated Circuit
ASR	Cisco Aggregation Services Router
BYOD	Bring Your Own Device
CA	Certificate Authority
CDP	CRL Distribution Points
CIP	ODVA, Inc. Common Industrial Protocol
CLI	Command Line Interface
CoA	Change of Authorization
CoS	Class of Service
CPwE	Converged Plantwide Ethernet
CRD	Cisco Reference Design
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSSM	Cisco Smart Software Manager
CTL	Certificate Trust List
CUR	Coarse Update Rate
CVD	Cisco Validated Design

Appendix B – Acronyms and Initialisms

Table B-1   Acronyms and Initialisms (continued)

Term	Description
DACL	Downloadable Access Control List
DAN	Double Attached Node
DC	Domain Controller
DCR	Direct Current Resistance
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
EMI	Enterprise Manufacturing Intelligence
EoIP	Ethernet over IP
ERP	Enterprise Resource Planning
ESP	Encapsulating Security Protocol
ESR	Embedded Services Router
FIB	Forwarding Information Base
FIFO	First-In First-Out
FPGA	Field-Programmable Gate Array
FQDN	Fully Qualified Domain Name
FVRF	Front-door Virtual Route Forwarding
GNSS	Global Navigation Satellite Systems
GRE	Generic Routing Encapsulation
HMAC	Hash Message Authentication Code
HMI	Human-Machine Interface
HSRP	Hot Standby Router Protocol
IACS	Industrial Automation and Control System
ICS	Industrial Control System
IDMZ	Industrial Demilitarized Zones
IES	Industrial Ethernet Switch (Allen-Bradley Stratix, Cisco IE)
IGMP	Internet Group Management Protocol
IIoT	Industrial Internet of Things
IKE	Internet Key Exchange
I/O	Input/Output
IoT	Internet of Things
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

Physical Infrastructure for the Converged Plantwide Ethernet Architecture

Table B-1   Acronyms and Initialisms (continued)

Term	Description
LBS	Location Based Services
LWAP	Lightweight Access Point
MAC	Moves, Adds, and Changes, as used in the context of this application guide
MDM	Mobile Device Management
ME	FactoryTalk View Machine Edition
mGRE	Multipoint Generic Routing Encapsulation
MLS	Multilayer Switching QoS
MMC	Microsoft Management Console
MnT	Monitoring Node
MPLS	Multiprotocol Label Switching
MQC	Modular QoS CLI
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
NHRP	Next Hop Routing Protocol
NOC	Network Operation Center
NPS	Microsoft Network Policy Server
NSP	Native Supplicant Profile
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OEE	Overall Equipment Effectiveness
OEM	Original Equipment Manufacturer
OT	Operational Technology
OTA	Over-the-Air
OU	Organizational Unit
PAC	Programmable Automation Controller
PAN	Policy Administration Node
PAT	Port Address Translation
PCS	Process Control System
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PoDL	Power over Data Line (IEEE 802.3bu, SPE powering)
pps	Packet per second
PRP	Parallel Redundancy Protocol
PSK	Pre-Shared Key
PSN	Policy Service Node
PTP	Precision Time Protocol
QoS	Quality of Service
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service

Table B-1   Acronyms and Initialisms (continued)

Term	Description
RAS	Remote Access Server
RD	Route Descriptor
RDG	Remote Desktop Gateway
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
RedBox	PRP redundancy box
REP	Resilient Ethernet Protocol
RPI	Request Packet Interval
RTT	Round Trip Time
SA	Security Association
SaaS	Software-as-a-Service
SAN	Single Attached Node
SCEP	Simple Certificate Enrollment Protocol
SE	FactoryTalk View Site Edition
SHA	Secure Hash Standard
SIG	Secure Internet Gateway
SPE	Single Pair Ethernet (IEEE 802.3cg)
SPW	Software Provisioning Wizard
SSID	Service Set Identifier
STP	Spanning Tree Protocol
SYN	Synchronization
TAI	International Atomic Time
TCN	Topology Change Notification
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VDAN	Virtual Double Attached Node
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
VSS	Virtual Switching System
WAN	Wide Area Network
wIPS	wireless Intrusion Prevention Service
WLAN	Wireless LAN
WLC	Cisco Wireless LAN Controller
WSA	Cisco Web Security Appliance
ZFW	Zone-Based Policy Firewall