building a smarter, unified business foundation

Connect. Manage. Automate.

Worldwide

VERSION 1.0

DESIGN+ IMPLEMENTATION GUIDE

Panduit Industrial Ethernet Physical Infrastructure Reference Architecture Design Guide

Panduit
17301 S. Ridgeland Ave.
Tinley Park Illinois 60477 USA
www.panduit.com
Phone: 800-777-3300
Fax: 708-532-1811

Unified Physical Infrastructure™

About PANDUIT

PANDUIT is a world-class developer and provider of leading-edge solutions that help customers optimize the physical infrastructure through simplification, agility and operational efficiency. PANDUIT's Unified Physical Infrastructure (UPI) -based solutions give enterprises the capabilities to connect, manage and automate communications, computing, power, control and security systems for a smarter, more unified business foundation. Strong relationships with technology leaders complemented with its global staff and unmatched service and support, make PANDUIT a valuable and trusted partner.

Copyright Information

Trademark Information

- Cisco is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.
- ODVA and EtherNet/IP are trademarks owned and used by ODVA.
- Rockwell Automation and FactoryTalk are registered trademarks of Rockwell Automation in the United States and/or other jurisdictions.
- Stratix 8000™, Stratix 6000™, and Stratix 2000™ are trademarks owned and used by Rockwell Automation and its various subsidiary entities.

Disclaimer

THE INFORMATION CONTAINED HEREIN IS INTENDED AS A GUIDE FOR USE BY PERSONS HAVING TECHNICAL SKILL AT THEIR OWN DISCRETION AND RISK, AND IS PROVIDED "AS IS." PANDUIT DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT, AND FURTHER NO WARRANTIES ARE CREATED WITH RESPECT TO ANY COURSE OF DEALING, USAGE, OR TRADE PRACTICE, IN CONNECTION WITH INFORMATION CONTAINED HEREIN OR ITS IMPLEMENTATION. PANDUIT AND ROCKWELL AUTOMATION DISCLAIM ANY LIABILITY ARISING FROM ANY USE OF THIS DOCUMENT OR THE INFORMATION CONTAINED HEREIN, OR FOR THE ABSENCE OF SAME. INFORMATION CONTAINED IN THIS DOCUMENT DOES NOT CONSTITUTE THE TECHNICAL OR OTHER ADVICE OF PANDUIT.

Authorship Team

The Industrial Ethernet Physical Infrastructure Reference Architecture Design Guide is a direct result of an intensive, collaborative effort from numerous dedicated Panduit professionals. This diverse group consists of research engineers, product engineers, application engineers, control engineers, installers, technicians, product marketing specialist, technical writers, graphic designers and editors.

Panduit is fortunate to be able to tap into these individuals for their insights, creativity and experiences. This document also leveraged expertise of actual implementations, best practices and hard fought lessons from our own global manufacturing community.

Finally this Design Guide must also recognize the ongoing support and guidance from our corporate leadership team.

PANDUIT wishes to thank and recognize the Rockwell Automation Network & Security Services team for their significant contribution to this guide.

Rockwell Automation Network & Security Business
Rockwell Automation Networks Business
The Network & Security Services team is truly a converged organization made up of manufacturing engineers and IT professionals. They provide a family of services to assess, design, implement, audit, and manage new and existing industrial control and information networks and security technology, policies and procedures for those networks and the personnel that use them.

Section 1: Introduction

Section 2: Organization of Control System Networks

Section 3: Physical Infrastructure Project Phases

Section 4: Physical Infrastructure Implementation

Section 5: Network & Security Services

Appendix A: PANDUIT Copper Cabling System Technical Information

Appendix B: PANDUIT Fiber Optic Cabling System Technical Information

Appendix C: PANDUIT Grounding/Bonding System Technical Information

Figures

Section 1
Introduction

Manufacturing convergence helps companies reach their goals for productivity, globalization, innovation and sustainability by merging manufacturing and office systems with environments. The deployment of standard Ethernet-based Local Area Networks (LAN) enables businesses to utilize real-time manufacturing information to make product, material, purchasing, and resource decisions. The use of unmodified Ethernet for industrial protocols, such as EtherNet/IP, improves communications between the manufacturing floor and enterprise systems to achieve workflow efficiencies and a converged environment.

Deployment complexities associated with industrial Ethernet such as environment, noise mitigation and logical segmentation must be overcome to achieve high availability and maintain data integrity in the manufacturing cell/area zones. Poor decisions can result from a lack of understanding of both enterprise IT and manufacturing requirements and their differences. Without a strong, Unified Physical Infrastructure (UPI)-based design strategy in place, organizations take on unnecessary risk. These risks include overfilled network closets, cabinets that are difficult to service, disorganized industrial enclosures, costly re-work, and increased machine downtime.

In order to address these issues, PANDUIT has collaborated with Rockwell Automation, Cisco and other industry leaders to develop this *Physical Infrastructure Reference Architecture Guide* for designing, deploying and managing the physical infrastructure for an Industrial Ethernet network.

1.1 Goals of this Guide

The following are goals for this guide:

- With criticality of infrastructure in plant operations, Rockwell Automation and PANDUIT are joining to ensure consistent practices are applied in the Physical Infrastructure design of Industrial Networks

- By applying proven, standards-based design approaches, the organizations will deliver industrial networks with a desired state of transparency. The network, applications and controls hardware will operate in a choreographed manner.

- By delivering optimum performance and verifiable, traceable schematics that enable expedient maintenance and repair, the organizations deliver unprecedented business value to plant operations.

1.2 Related Documents

This document builds upon the work by Rockwell Automation and Cisco on *Reference Architectures for Manufacturing. Reference Architectures for Manufacturing* provides education, design guidance, recommendations and best practices to help establish a robust and secure network infrastructure that facilitates manufacturing and enterprise network convergence. *Reference Architectures for Manufacturing* incorporates the Rockwell Automation *Integrated Architecture* and Cisco *Ethernet-to-the-Factory. Reference Architectures for Manufacturing* are built on technology and manufacturing standards common between IT and manufacturing, establishing a Manufacturing Framework of network segmentation for traffic management and policy enforcement, such as security, remote access, and Quality of Service (QoS). Other documents which support and inform this Guide in the specification, deployment, and testing of Industrial Ethernet physical infrastructures include the following:

- ANSI/TIA-1005: Telecommunications Infrastructure Standard for Industrial Premises (forthcoming, 2009)

- TIA/EIA-568-B: Commercial Building Telecommunications Standard (2001)

- TIA-569A: Commercial Building Standard for Telecommunications Pathways and Spaces

- ANSI/TIA/EIA-606-A: Administration Standard for the Telecommunications Infrastructure of Commercial Buildings

- ANSI-J-STD-607: Grounding and Bonding Requirements for Telecommunications in Commercial Buildings

- ANSI/TIA/EIA-942: Telecommunications Infrastructure Standard for Data Centers

- *Network Infrastructure for EtherNet/IP*: *Introduction and Considerations* (ODVA, 2007)

- *Industrial Ethernet on the Plant Floor: A Planning and Installation Guide,* by Robert Lounsbury (ISA, 2008)

1.3 What is Industrial Ethernet?

Ethernet is the network transmission protocol, developed in 1973, that has evolved into the adopted standard for the overwhelming majority of office communication systems. While Ethernet was evolving, so were the networks for automation control. The development and growth of these two types of networks were based on significantly different demands. Over the years many protocols, both open and proprietary, have evolved for factory automation. This is problematic as industrial protocols are not interoperable, either between each other or the Ethernet in the front offices.

Industrial Ethernet solves this problem. Industrial Ethernet was developed to provide a common platform to improve Computer Integrated Manufacturing (CIM) processes among the various processing equipment manufacturers, as well as to offer a seamless cross-transfer of critical data between the plant floor and support offices. Within manufacturing, Ethernet solutions ease the deployment of industrial networks and automation control systems that enable expansion of operations as well as increased collaboration and productivity. On the factory floor, factors such as safety, security, and compliance also become an important part of physical infrastructure design (see Figure 1-1).

By integrating production, data acquisition, purchasing, quality, logistics, sales, and building automation systems onto a single common infrastructure, customers can improve network efficiency, reduce operational costs, and increase manufacturing productivity across several areas:

- Monitoring the manufacturing operations and processes
- Controlling the manufacturing operation and processes locally and remotely
- Data acquisition for Enterprise Resource Planning (ERP), production, purchasing, quality, logistics and sales
- Transfer of design files or engineering parameters

1.4 What is Reference Architecture"?

In their 2007 ODVA white paper "The Importance of Reference Architectures in Manufacturing Networks," Brian Batke (Rockwell Automation) and Paul Didier (Cisco) make a compelling case for the utility of reference designs that can be used to standardize the deployment of industrial networks:

A Reference Architecture is a fundamental organization of a system, the relationship between its components and the environment, and the principles governing its design and evolution. Architectures provide customers with a framework for optimizing their technical resources in support of business and technical requirements. … Reference Architectures provide a way to deliver knowledge and expertise in standard networking in an Automation and Control context to increase confidence, spur take-up and drive consistency in the Industrial Ethernet market.

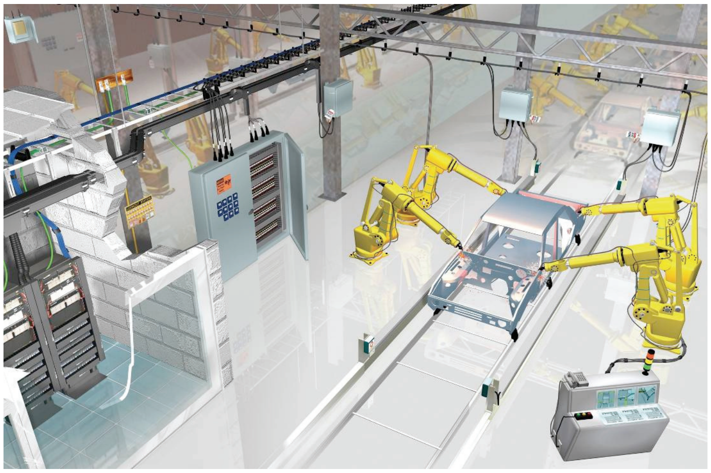


Figure 1.1-1. Industrial Ethernet continues to move forward towards the factory floor and occupies a solid position at the control level.

With a Reference Architecture, all involved stakeholders can increasingly focus on a common solution which reduces risk of deployment by relying on known and tested solutions; simplifies decision-making; enables more re-use; provides consistent models, capabilities, and equipment; improves service and support; and helps customers deploy solutions that meet their specific business issues.

According to Batke and Didier, the key attributes of a Reference Architecture are:

- Compatibility with unique industrial protocols and the communication models they incorporate
- Performance (latency, jitter, minimal packet loss) and availability requirements of automation and control applications
- Logical segmentation of production and enterprise networks, allowing networks to safely and securely share data, services, and access from the production floor without introducing security risks of the Internet and enterprise network to the control system
- Physical requirements of the production floor
- Automation and control network solutions must be manageable by people who may not be trained experts in network technologies or administration
- Scalability to meet widely varying sizes of production facilities and future growth.

1.5 Purpose of this Reference Guide

The PANDUIT *Physical Layer Reference Architecture Guide* approaches manufacturing challenges as they relate to the physical infrastructure from a broad system-level view, one that promotes manufacturing convergence. It also covers how enterprise IT and manufacturing systems stakeholders can properly connect, manage, identify, and secure cabling throughout the physical infrastructure for an end-to-end physical implementation of the reference architectures recommended by Rockwell Automation and Cisco (see Figure 1.1-2).

Like the Cisco-Rockwell Automation logical *Reference Architectures for Manufacturing* before it, the purpose of this Guide is to accelerate the convergence of standard networking technologies with the industrial automation and control environment. Specifically, this *Guide* focuses on identifying physical layer reference solutions that reflect new realities in the industrial space.

These realities include:

1. The development of hardened switches for deployment outside of a static control room environment and onto the factory floor, requiring new cabling techniques to mitigate the effects of heat, humidity, and noise over a multi-connector cabling channel
2. The use of distributed cabling topologies and patching technologies, which enhances the flexibility and scalability of Industrial Ethernet networks to achieve greater operational efficiencies
3. The critical role played by a robust, testable grounding and bonding system to ensure system uptime and availability by mitigating noise issues that can disrupt communications and control.

A converged Industrial Ethernet physical infrastructure requires deploying control rooms with a greater level of IT technology to leverage the intelligence built into today's control systems for greater productivity and reliability. This convergence with IT technology necessitates greater deployment of servers, firewalls and switching technology to deliver the productivity benefits with a robust architecture as described in the Rockwell, Cisco's reference architecture.

1.6 Best Practice for Each Area and Application

Today's automation systems depend on industrial Ethernet for real-time control, device configuration, data collection, and even safety sub-systems. The productivity of the manufacturing plant is built on layers of hardware and software that comprise the automation system with the physical layer being the lowest, but most critical, layer. This physical layer, comprised of the network media, connectivity, enclosures, pathways, grounding/bonding, identification, and port locking devices provides the critical channels for communication to exist.

This document provides guidance on selecting, planning, installing and testing a physical layer that ensures performance. The physical architecture for a typical manufacturing enterprise is physically located in multiple areas that have unique environmental, security and performance considerations. This document will describe the physical infrastructure architectures recommended for each of the following areas:

- Industrial Data Center / Control Room
- Network Distribution
- Zone Cabling Enclosure
- Control Panel
- On Machine

However, these physical locations can have differing needs based on the type of manufacturing operation. For example, a process line may have longer distances and higher security requirements than a small assembly operation.

NOTE:

Experts estimate that 50% - 90% of network disruptions are due to problems with this physical layer!

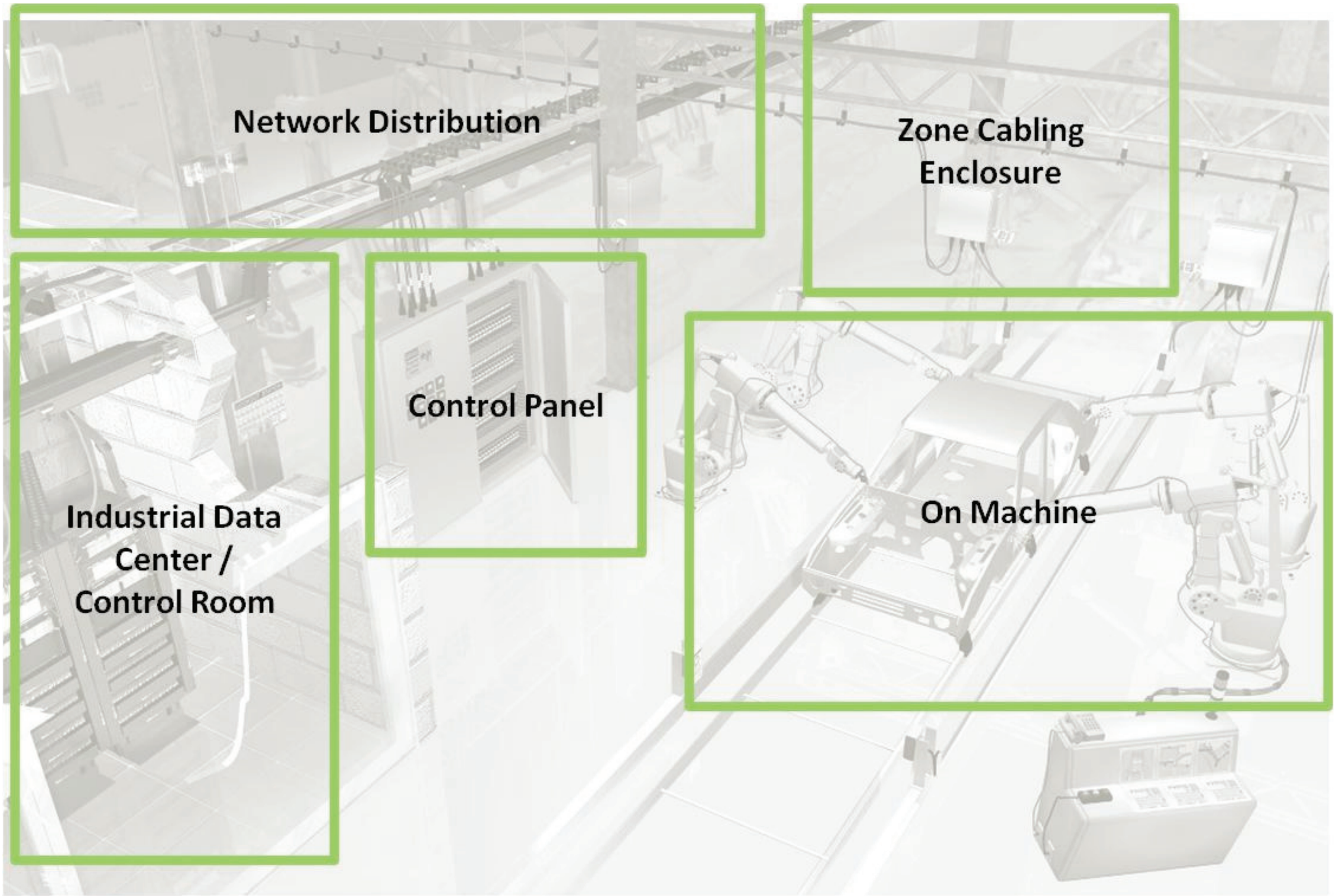


Fig. 1.1-2. Typical manufacturing infrastructure is comprised of distinct areas with differing environmental, performance, and security challenges.identified.

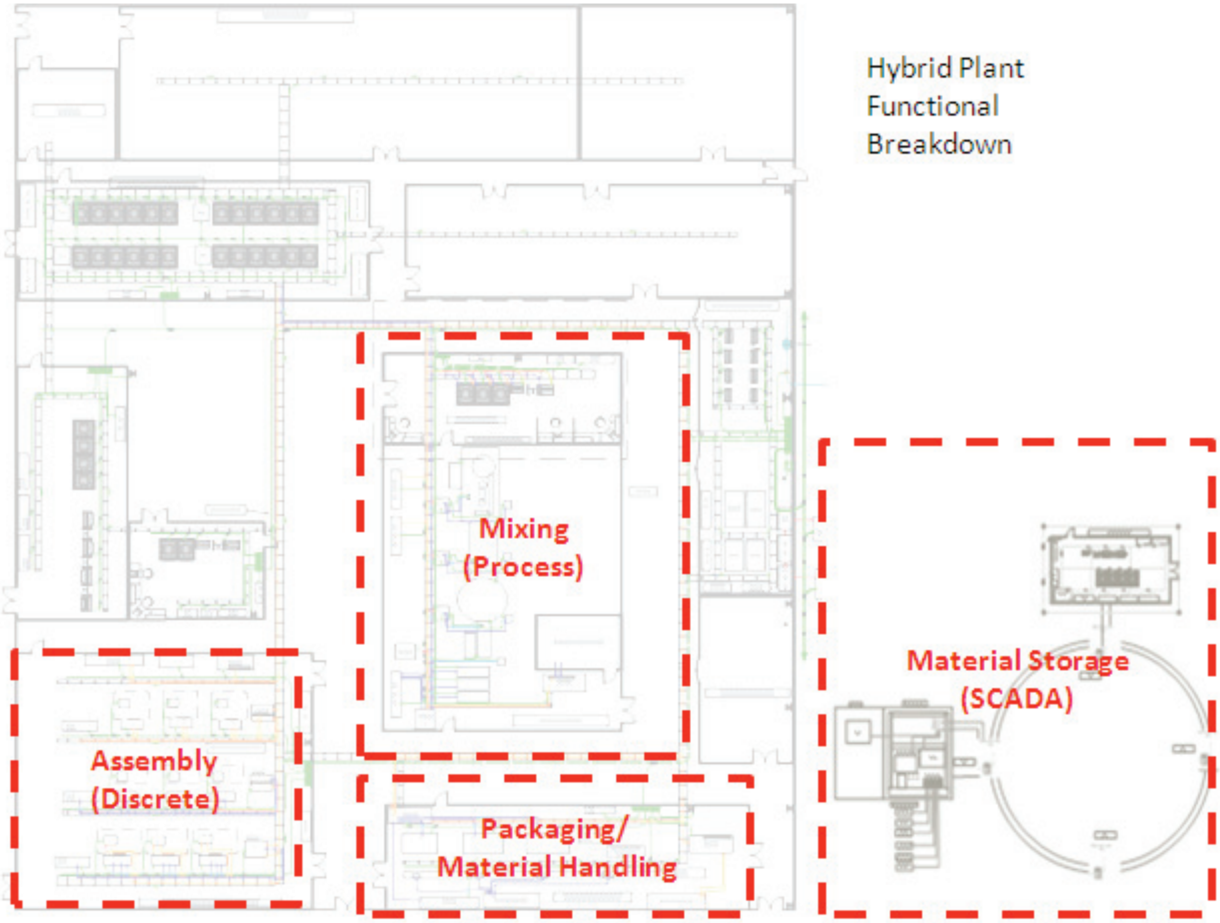


Fig. 1.1-3 Hybrid plant floor plan with example manufacturing zones identified.

The best practice recommendations for the physical infrastructure are described for a *hypothetical-hybrid-plant* that has application zones for packaging/material handling (discrete) mixing (process/batch) and material storage (SCADA) operations. The physical architecture for the networks that make this plant run overlay the factory floor plan and should be planned as a robust infrastructure based on sound Rockwell/Cisco logical architectures that are designed for performance, scalability, security, and maintainability. Each of the following application zones of this hybrid plant will be analyzed and described in this document:

- Discrete (e.g. Assembly and Packaging/Material Handling)
- Process (e.g. Mixing)
- SCADA (e.g. Material Storage)

The initial part of the plan starts with a floor plan to evaluate the building layout and to determine the location of the individual network zones. These network zones and their interconnection form the backbone of the network physical infrastructure. This is sometimes referred to as “lines-and-boxes”. However lines–and-boxes are merely a logical representation of the network. This guide helps map that logical view onto the physical implementation.

This is a critical step, so it is worthwhile to understand the trade-offs that are made for zone selection.

1.7 Zone Cabling Architecture Advantages

Zone Cabling Topology provides a cost-effective alternative to deploying your network infrastructure by increasing the network's flexibility, accessibility and scalability. This concept originated in commercial wiring for offices, etc. but can offer these same advantages for industrial applications.

Benefits include:

- Reduced home-run wiring
- Ease zone adjustments or expansions
- Reduces size of central closet

1.7.1 Office Example

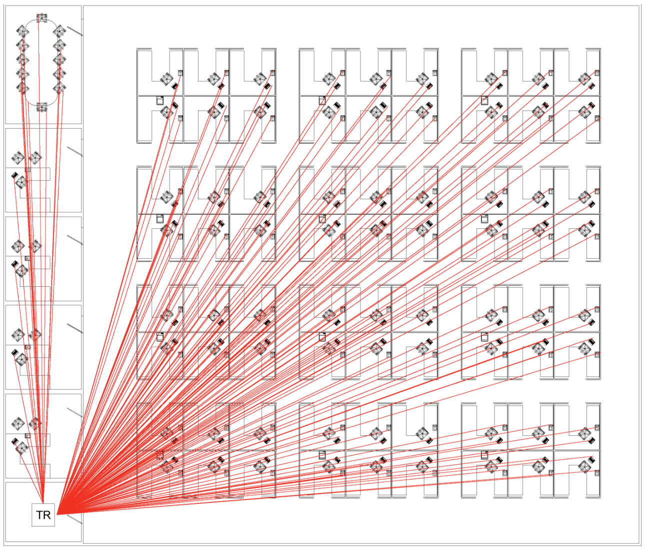


Fig. 1.1-4: Centralized Cabling: Home runs to each node back to telecommunication room in an office.

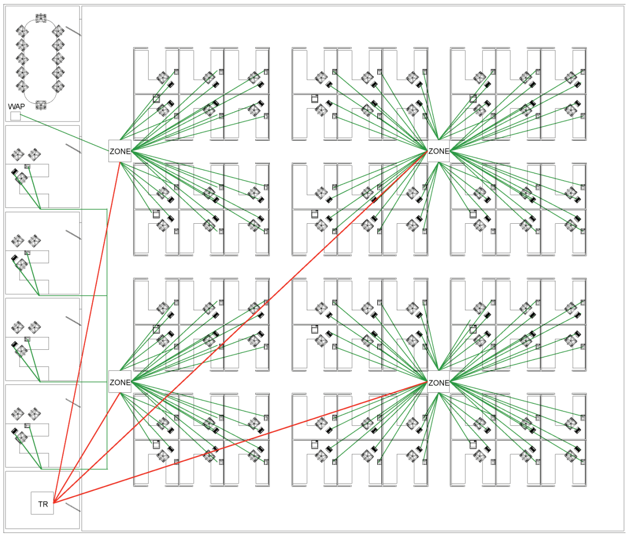
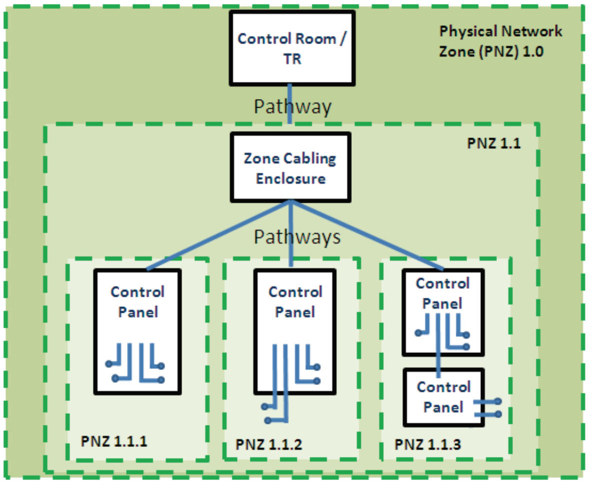
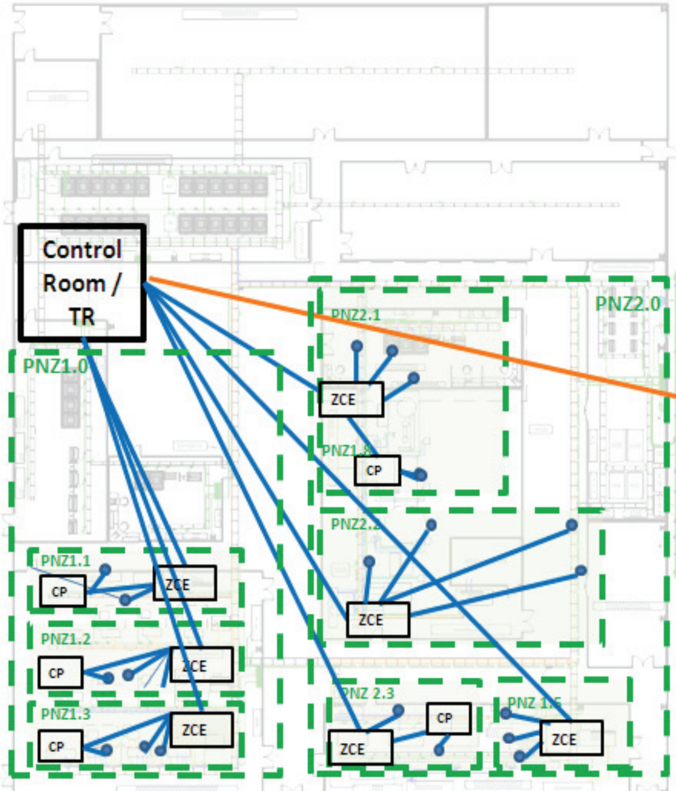


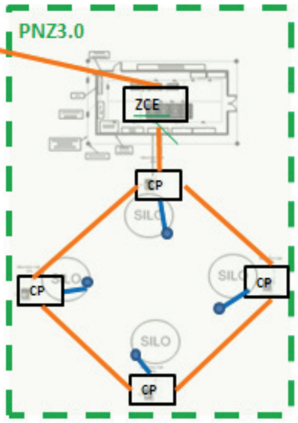
Fig. 1.1-5: Zone Cabling: Distributed zone cabling enclosures dramatically cut number of home runs.

1.7.2 Industrial Physical Network Zones

For industrial application, a zone cabling architecture can provide these same important advantages in distributing cabling to switches in control panels or on machine switches and devices.







PNZ	Physical Network Zone
ZCE	Zone Cabling Enclosure
CP	Control Panel

Fig 1.1-6: The diagram above illustrates the basic concept of mapping physical network zones to your physical infrastructure. The following describes useful terms and rules for layout of an industrial automation network into physical zones.

1. Physical Zone Network Key terms
   a. A Network is a collection of two or more end-points connected via a pathway.
   b. An end-point is a uniquely addressable device as defined by the Network.
   c. A pathway is the unbroken media that data is broken when it is changes type or connector.
   d. A Physical Network Zone (PNZ) is a collection of one or more end-points that share a common pathway.

2. Physical Zone Network Design rules
   a. A PNZ may only wholly include other PNZ . And a PNZ can only be inherited into one other PNZ. A PNZ may include multiple PNZ.
   b. Use dashed lines to represent logical collection and solid line to mean a physical location (panel, floor area, machine)
   c. The naming reference for zones shall follow [level1].[level2].[level3]…[Leveln]

This physical network zone cabling approach can be employed for our hybrid factory example for great reduction in home run cabling and improve manageability benefits.

1.8 Standards-based End-to-End Environmental Considerations

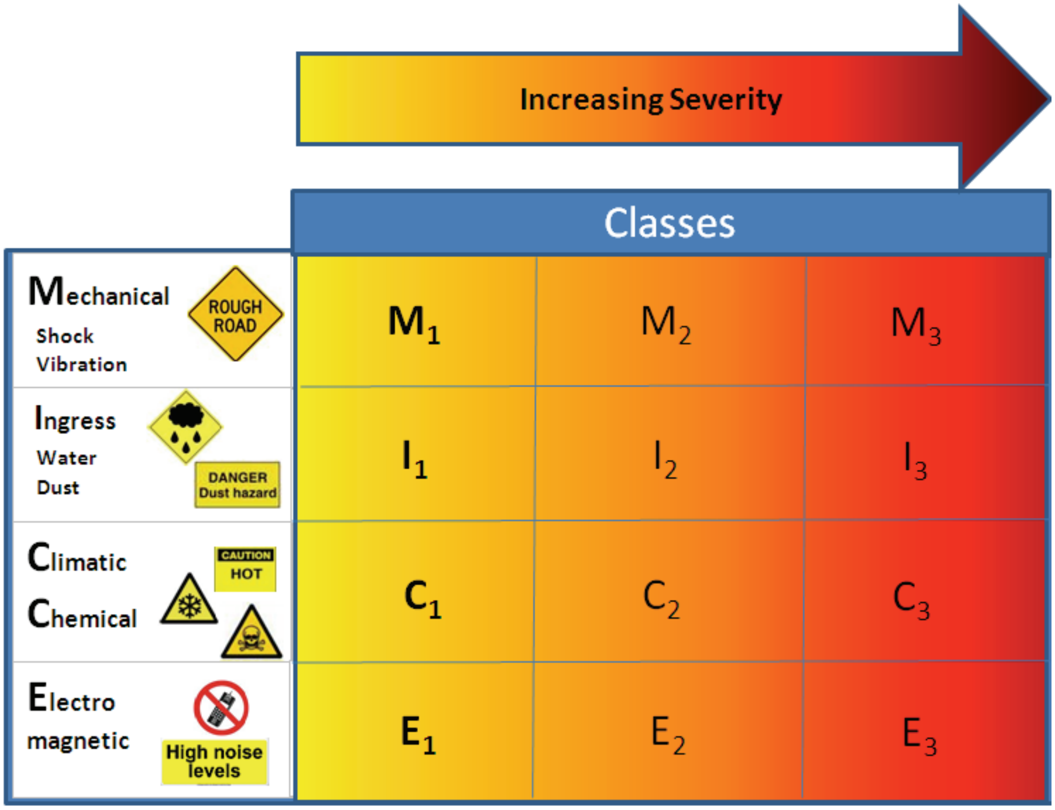
Effective integration of Industrial Ethernet into an existing or new manufacturing or processing facility can be challenging. Along with environmental protection, network stakeholders need to factor variables such as interoperability, deployment, security, reliability, electrical performance and cost into network design and deployment.

To help stakeholders throughout the decision-making process, the ISO/IEC 24702 and TIA-1005 standards recommend use of the MICE (Mechanical, Ingress Rating, Climatic, Electromagnetic) classification system. The MICE concept is based on the assumption that cabling, even under the worst conditions of an environmental class, is still protected and guarantees reliable network operation (see Figure 1-7):

- $M_1I_1C_1E_1$ describes a worst-case environment according to ISO/IEC 11801
- $M_2I_2C_2E_2$ describes a worst-case light industrial environment
- $M_3I_3C_3E_3$ describes a worst-case industrial environment

This system provides a method of categorizing the environmental classes for decision-making on the level of hardening required the network media, connectors, pathways and enclosures. A higher MICE level means that your physical infrastructure may need to be:

- Ruggedized for vibration
- Sealed for wash down
- Fabricated with materials that can withstand extreme temperatures
- Shielded for rejecting EMI noise.



	Classes		
Mechanical Shock Vibration	M_1	M_2	M_3
Ingress Water Dust	I_1	I_2	I_3
Climatic Chemical	C_1	C_2	C_3
Electro magnetic	E_1	E_2	E_3

Figure 1.1-7. The MICE matrix defines environmental classes in three levels and four parameters.

TIA-1005 defines terminology for the various levels of the physical infrastructure so that the MICE levels required can be analyzed and specified for each area. Industrial environment conditions can vary greatly depending on the type of manufacturing, location of equipment, ambient conditions, installation standards, and building construction so there are no hard rules about level of protection required for each zone. In many cases, telecommunication rooms, factory floor, and work area levels can safely use commercial grade physical infrastructure if the MICE ratings show that there are no significant hazards present. For harsh environments though, specifying connectivitywith appropriate ratings to withstand wash down or shielded solutions in high EMI environments make sense.

An end-to-end channel solution often cuts across several MICE environments, ranging from environmentally controlled control rooms or enclosures where commercial grade solutions and best practices can offer best value and performance to more rugged environments where IP67 rated connectivity offers advantages (see Figure(s) 1-8 / 1-9).

Reference architectures for physical infrastructure provide a roadmap for specifying, installing, testing, and documenting the connectivity that spans from the enterprise connection down to the machine level. The physical infrastructure provides the means to ensure performance, security, reliability and maintainability of the switches, servers, and

Fig. 1.1-8:

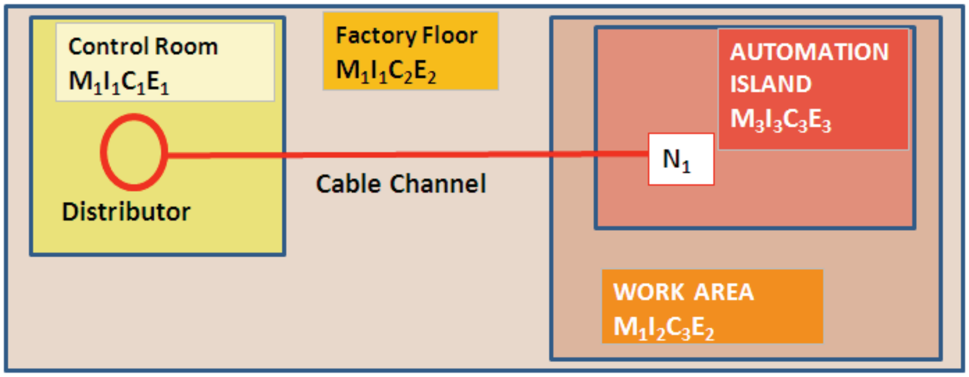
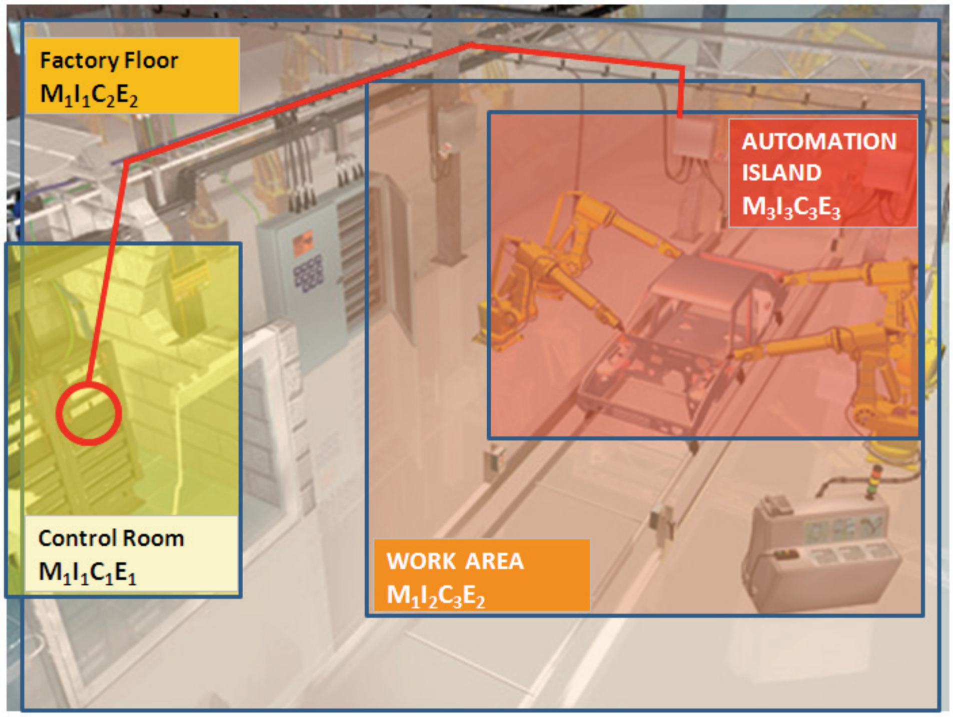


Fig. 1.1-9:



Figures 1-8 and 1-9. An end-to-end channel solution often cuts across several MICE environments, ranging from environmentally controlled control rooms to more rugged environments control devices that constitute a complete architecture. This infrastructure guidance requires a systems level view of grounding/bonding considerations, best practices for mitigating noise concerns, security defense in depth, as well as proven media and connectivity that can be installed and tested effectively.

Reference architectures also provide roadmap for IT and Controls engineers to plan the infrastructure in light of the environmental issues exposed by MICE analysis selecting appropriate hardening and form factors for the particular level of the architecture (see Table 1-1). The reference architecture provides guidance on:

- Building out control rooms that leverage best practices proven in data center applications worldwide

- Network distribution that delivers top performance with security, scalability and flexibility

- Control panel solutions engineered to mitigate noise concerns and provide testability of these critical links

- Distributed 'On-Machine' network installations requiring sealed connectors and other environmental measures.

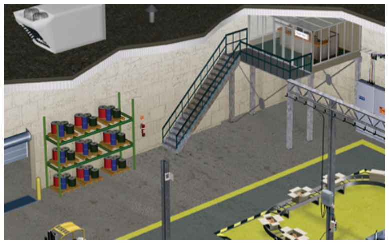
Telecommunications Room Control Room Increasing severity Typical MICE Range 1 (commercial grade)		Enclosures Racks, Pathways, Grounding/Bonding Physical Security	
Factory Floor Network Distribution Increasing severity Typical MICE Ranges 1-2 from commercial grade to light industrial		Fiber Copper Connectivity Pathways	
Work Area Consolidation points Increasing severity Typical MICE Ranges 1-2 from commercial grade to light industrial		Zone Enclosures MUTOA Physical Security	
Automation island Control Panels,On Machine (distributed) Increasing severity MICE Ranges 1-3 from commercial grade to harsh environment rated		Copper Fiber Patching Wire management Grounding/Bonding Identification Physical Security	

Table 1.1-9. Correspondence of MICE Environments, Control Network Areas, and Physical Infrastructure Elements

1.9 Organization of this Guide

Benefiting both enterprise IT and manufacturing system stakeholders, this document describes project phasing considerations, application scenarios, and service options associated with the design, testing, and maintenance of the physical infrastructure.

Section 1 introduces the goals and purpose of the Guide, and describes the basic components of an end-to-end UPI-based Industrial Ethernet physical infrastructure solution (see sidebar for a summary of the UPI vision).

Section 2 presents a series of Reference Architectures for industrial networks, which are divided into two types:

- Areas (control room, cabling and connectivity, control panel, distribution [i.e. "zone"] point, and on-machine) present detailed examples of the building blocks of the Industrial Ethernet physical infrastructure

- Applications (process, SCADA, discrete manufacturing, and packaging/shipping, which illustrate how physical layer Areas can be combined to meet application-specific requirements

Section 3 reviews infrastructure project phases, recommending best practices (and identifying likely pitfalls) that are encountered, from planning and design to testing and auditing.

Section 4 organizes installation and testing information for each element of the physical infrastructure, from copper and fiber media selection to testing procedures for cabling and grounding systems. The section concludes with a review of the benefits that several innovative technologies (Power over Ethernet [PoE], wireless, and intelligent buildings) can offer industrial networks.

Section 5 is a guide to services and support.

By using a reference architecture based on UPI principles to integrate IT and manufacturing systems, organizations can improve network efficiency, reduce operational costs, and increase manufacturing productivity to *build a smarter foundation and drive successful manufacturing convergence.*

The Vision: A Three-Phase Evolution

Designs based on Unified Physical Infrastructure (UPI) principles intelligently unite physical and logical systems to help organizations manage risk within the physical infrastructure. This approach ultimately allows organizations to increase safety and security in the workplace, manage systems more effectively, minimize downtime and mean time to repair (MTTR), and satisfy regulatory compliance requirements to minimize network disruptions and maximize performance.

The degree of unification across the physical infrastructure can be defined in terms of three levels – Align, Converge, and Optimize.

- Align: The first phase involves deploying modular and scalable passive, active and intelligent products, software and tools that align and connect systems within individual areas.

- Converge: The second phase involves integrating products, software and tools into a converged physical infrastructure solution that extends across more than one enterprise area.

- Optimize: The third phase involves optimizing the entire physical infrastructure into a seamless interoperable system across all critical systems and areas.

UPI-based solutions are tailored by industry and customized by application, and span all core systems necessary to run a business from data center and facilities operations to next-generation intelligent buildings and across the factory floor. Examples include physical cable routing and management solutions designed to integrate with the reference architectures, untangle over-filled network closets and control room cabinets that are difficult to service. Similarly designed bonding and grounding measures defuse disruptive electrical "noise" before it adversely impacts control system performance, and ID and labeling solutions clearly identify system connections as well as hazardous electrical areas to protect network and worker safety.

Frequent interaction between IT and facilities management teams helps to deliver a physical infrastructure that best fits the unique business needs of each organization. This approach to designing and specifying physical infrastructure technologies enables tangible improvements in system efficiency and productivity along with a substantial reduction in operational costs.

Networks and industrial automation systems have common challenges. Consideration has to be given to how products connect and interact together. In addition to physical attributes like cabling and connectors, the communications methods needed between products are crucial to system stability and integrity. How products exchange their data, the system throughput requirements, and the configuration, maintenance and expandability all demand careful consideration.

Data requirements vary by device and application. The amount of data that needs to be moved effects bandwidth and the optimal packet size. Another consideration for industrial automation networks is the type of data that is being moved including I/O, polled, change-of-state, cyclic, program upload/download and diagnostics to mention a few. Real time control of I/O, drives, motion control and even safety requires ensuring determinism and update frequencies to deliver the desired repeatability and system performance of the industrial automation network.

Control system networks are not new having developed from proprietary schemes to today's open systems. The explosive growth of Ethernet communications, faster microprocessors and powerful computer software applications has driven the need to architect systems that deliver on the desired efficiency and standardized connectivity enabled by networked resources while protecting the uptime and performance of critical automation systems. The following sections will examine the importance of the network infrastructure, review background on the architecture levels required for a highly   integrated manufacturing operation, review network topologies and convergence options, and finally introduce Cisco/Rockwell Automation Reference Architectures for Manufacturing which provide a framework for building automation system that leverages network communications to deliver unprecedented efficiency, security, performance, and maintainability to industrial operations.

2.1 The Importance of the Network Infrastructure

The network infrastructure is a path for information flow; it provides connectivity between automation components and its users. Network infrastructure includes the transmission media (to include fiber, copper and wireless), the hardware to control the transmission paths (to include switches, routers and access points), and the software that sends, receives and manages traffic.

Strong, Transparent Network Structure

The network infrastructure can be compared to the steel structure of a factory or plant. This skeleton is built to weather the conditions by following established standards and a design based on the requirements for the use of the structure. Regular inspections insure the structure is sound and identify any areas in need of repair. This assures the user they can go in their respective factories and plants without considering the state of the structure. Essentially, the structure becomes transparent to its users. The original design is referenced during moves, adds and changes to the structure.

The network infrastructure should also be transparent to its users. Like our example, this can be accomplished through the use of standards and a design based on the requirements from the users. Monitoring of the network ensures the transmission media, its paths and the software are operating at optimal performance. Network monitoring provides insight turning reactions into predictions when infrastructure upsets occur. The network design, after implemented and audited, becomes a living document during moves, adds and changes to the infrastructure. A clear view of the network goes a long way in intelligent decision making during troubleshooting or performance analysis. Conversely, a poorly designed, installed and documented network will cause confusion and hamper vision of those troubleshooting or analyzing a system's performance. A transparent network like a clean windshield provides your best view of the road ahead and reduces risks of problems.

Evolution from Segregation to Convergence

Commonly, automation assets were purposefully segregated on proprietary or open networks that could effectively perform data collection or control tasks but not capable of further integration. Islands of automation were isolated and constrained by networks with limited bandwidth, number of nodes and overall length. Asset owners grew confident with these networks mainly because of their relative simplicity and well documented parameters. Information exchange between the manufacturing and the enterprise zones though required expensive, customized hardware and software interfaces, if available. For many though, disjointed systems were created that relied on a user's reproduction of data stored on clipboards or transcribed from operator interfaces into spreadsheets. This scenario lends itself to slow business decisions, higher error rates and limited availability to manufacturing information.

Convergence is not a new concept, but used to be limited by disparate networks and technology in the manufacturing zone. What were islands of automation are now enabled by protocols such as CIP and technology that promote convergence from the manufacturing zone upwards into the enterprise zone. EtherNet/IP, a standard Ethernet technology, enabled users to unite control, communication and computation into a multidiscipline industrial network. Since Ethernet is the prevalent network in the enterprise it became the common point of convergence. Through providing visibility of all layers of the manufacturing architecture to formulate key performance indicators (KPIs), convergence enables greater business agility and opportunities for innovation. Instead of business decision being held up by manually created spreadsheet one can simply leverage technology used every day to view KPIs such as a VoIP phone or smart phone.

Ethernet networks quickly became accessible to users, both at home and work. With the promotion of COTS, commercial off the shelf, and plug-n-play mentality, users were enabled with confidence that networking automation assets would be as simplistic as a home Ethernet network. In other instances enterprise IT relied on established policies and procedures to enlighten the manufacturing zone with Ethernet. Not realized at first, but the requirements used to create enterprise policies and procedures for the enterprise zone were not applicable and actually detrimental in the manufacturing zone. For example, network policies of pushing automatic updates and patches that work well for office users can cause disruptions to critical control systems that may not be validated for use with the new update or patch.

Why Does the Networking Infrastructure Matter?

Infrastructure allows disparate components to work together on a grand scale that should be easy for user to interact with, accomplishing goals that otherwise would be impossible to achieve. With a well executed, transparent network infrastructure in place, the automation system architecture is better understood resulting in greater confidence in operating and maintaining highly integrated manufacturing systems. The network's physical infrastructure provides the foundation for the layers of automation that enable great productivity gains, improved performance, and enhanced safety.

Networking infrastructure can be thought of as a new critical utility for the manufacturing plant. Tremendous resources and planning ensure traditional critical utilities such as power, air, steam, etc. at a manufacturing site are reliable since these utilities enable nearly every phase of manufacturing. Now, the Ethernet network infrastructure is just as important since it is a critical part of each level of the manufacturing space including safety, process, and control as well as for supervisory functions, MES and enterprise integration. The network infrastructure is critical for convergence and enabling timely business decisions. The infrastructure, its design, policies and procedures, audits and automated monitoring is what enables transparency and 99.99% uptime that drives an operation to profitability in today's competitive environment.

2.2 Reference Architecture Terminology

The following section discusses the Purdue Enterprise Reference Architecture (PERA) for Control System Functions, ISA-95 and ISA-99 which provide important terminology and conceptual models for describing a networked control architecture. A thorough understanding of these application models and standards allows for selection of a physical infrastructure architecture that delivers full value for automation investments.

2.2.1 PERA Model

The *Purdue Enterprise Reference Architecture* is a common and well understood model in the industry for organizing control system functions and activities (see Figure 2A-1). The model was developed by a collection of industrial and academic representatives, and segments control devices and equipment into hierarchical functions.

This model has been incorporated into many other models and standards in the industry. The Instrumentation, Systems and Automation Society (ISA) ISA-95, Enterprise-Control System Integration and ISA-99, Manufacturing and Control Systems Security have identified the levels and framework.

The PERA model divides control system elements into five levels:

Level 0 – Process

Level 0 is comprised of a wide variety of sensors and devices to monitor and control both discrete and analog variables. They perform the basic functions of monitoring and controlling the cell/area zone. Devices can be traditional hard wired devices or more sophisticated networked devices with take advantage of advanced configuration and status information.

Level 1 – Basic Control

Level 1 consists of interfaces to the Level 0 devices (I/O, linking devices, bridges and so on) and controllers. Again, controllers may be stand-alone in single controller applications or multiple controllers on a peer-to-peer network. The controllers may be PLC, traditionally used in discrete applications as in discrete control, or a PAC which typically is for analog control found in the process applications such as continuous process or batch control. Controllers at this level not only need peer-to-peer communications but also to Level 2 and beyond for operator interfaces, engineering workstations, MES and so on. The upper levels may also initiate the communications by polling the controller for status and data about the actual application being controlled as well as take input for execution such as a batch cycle complete.

Level 2 – Area Supervisory Control

Level 2 represents the systems and functions associated with the runtime supervision and operation of a cell/area zone. Depending of the size and complexity of the application these functions may also carry over to Level 3.

Level 3 – Site Manufacturing Operations and Control

The systems that exist in Level 3 manage the plant/manufacturing wide functions. Levels 0 through 3 are considered critical to operations. These systems may communicate with controllers in Level 1, function as a staging area for changes in the cell/area zone and share data with the enterprise (Levels 4 and 5) systems and applications. Because these systems are primarily based on standard computing equipment and operating systems, they are more likely to communication with standard networking protocols.

Level 4 – Site Business Planning and Logistics Network

Level 4 is where functions and systems exist that need standard access to services provided by the enterprise network. This level is viewed as an extension of the enterprise network. The basic business administration tasks are performed here and rely on standard IT services. These functions and services include Internet access, E-mail, Enterprise applications, and non-critical production systems such as manufacturing execution systems and overall plant reporting (for example, inventory, performance, and so on). Although important, these services are not considered as critical to the manufacturing zone. Because of the more open nature of the systems and applications within the enterprise network, this level is often viewed as a source of threats and disruptions to the manufacturing zone.

Level 5 – Enterprise Network

Level 5 is where the centralized IT systems and functions exist. Enterprise resource management, business-to-business, and business-to-customer services are typically located here.

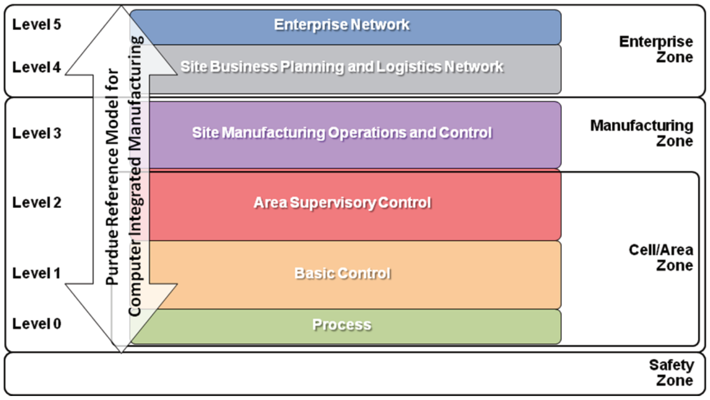


Figure 2.2-1. The Purdue Enterprise Reference Architecture (PERA) Model for Industrial Control Systems

2.2.2 ISA-95

Purpose

To create a standard that will define the interface between control functions and other enterprise functions based upon the Purdue Reference Model for CIM (hierarchical form) as published by ISA. The interface initially considered is the interface between levels 3 and 4 of that model (see Figure 2-2). Additional interfaces will be considered, as appropriate. The goal is to reduce the risk, cost, and errors associated with implementing these interfaces. The standard must define information exchange that is robust, safe, and cost effective. The exchange mechanism must preserve the integrity of each system's information and span of control.

Scope

- Multi-part effort
- Define in detail an abstract model of the enterprise, tions, and its information exchange.
- Establish common terminology for the description and understanding of enterprise, including manufacturing control functions and business process functions, and its information exchange.

- Define electronic information exchange between the manufacturing control functions and other enterprise functions including data models and exchange definitions.

Publications

The ISA-95 committee has published the first three standards in a series that define the interfaces between enterprise activities and control activities:

- ANSI/ISA-95.00.01-2000, *Enterprise-Control System Integration, Part 1: Models and Terminology*, provides standard terminology and a consistent set of concepts and models for integrating control systems with enterprise systems that will improve communications between all parties involved. The models and terminology emphasize good integration practices of control systems with enterprise systems during the entire life cycle of the systems.

- ANSI/ISA-95.00.02-2001, *Enterprise-Control System Integration, Part 2: Object Model Attributes*, contains additional details and examples to help explain and illustrate the Part 1 objects.

- ANSI/ISA-95.00.03-2005, *Enterprise-Control System Integration, Part 3: Activity Models of Manufacturing Operations Management*, presents models and terminology for defining the activities of manufacturing operations management.

For information on obtaining these published standards, click here.

Current Work

ISA-SP95 is currently developing additional standards in the series, including *Part 4: Activity Models of Manufacturing Operations Management*; and has recently completed *Part 5: Business-to-Manufacturing Transactions*. ISA-95 does much of its work electronically, but also holds periodic face-to-face meetings.

For more information on ISA-95, contact Charley Robinson, ISA Standards.

Reference: http://www.isa.org/MSTemplate.cfm?MicrositeID=285&CommitteeID=4747

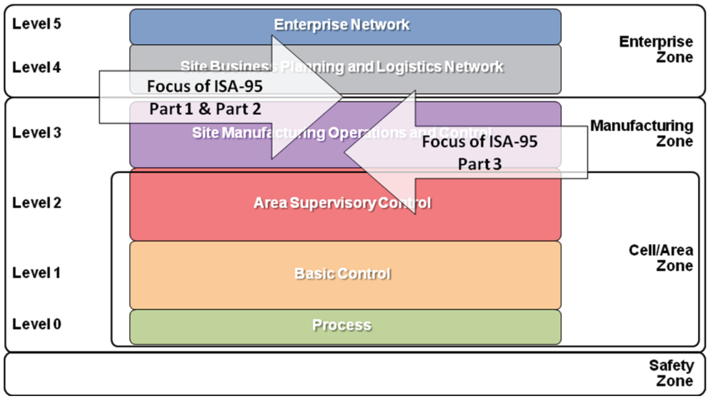


Figure 2.2-2. ISA-95 addresses the interface between levels 3 and 4 of the PERA model.

2.2.3 ISA-99

Purpose

The concept of manufacturing and control systems electronic security is applied in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries. Manufacturing and control systems include, but are not limited to:

- Hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems
- Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Physical security is an important component in the overall integrity of any control system environment, but it is not specifically addressed in this series of documents.

The ISA-99 Committee will establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure manufacturing and control systems and security practices and assessing electronic security performance (see Figure 2-3). Guidance is directed towards those responsible for designing, implementing, or managing manufacturing and control systems and shall also apply to users, system integrators, security practitioners, and control systems manufacturers and vendors.

The Committee s focus is to improve the confidentiality, integrity, and availability of components or systems used for manufacturing or control and provide criteria for procuring and implementing secure control systems. Compliance with the Committee's guidance will improve manufacturing and control system electronic security, and will help identify vulnerabilities and address them, thereby reducing the risk of compromising confidential information or causing Manufacturing Control Systems degradation or failure.

Scope

The ISA-99 Committee addresses manufacturing and control systems whose compromise could result in any or all of the following situations:

- endangerment of public or employee safety
- loss of public confidence
- violation of regulatory requirements
- loss of proprietary or confidential information
- economic loss
- impact on national security

Publications

ISA-SP99 completed the first editions of two key ISA technical reports in 2004:

- ANSI/ISA-TR99.00.01-2004, *Security Technologies for Manufacturing and Control Systems*
- ANSI/ISA-TR99.00.02-2004, *Integrating Electronic Security into the Manufacturing and Control Systems Environment*

Current Work

Currently, ISA-SP99 is focused on completing the first two in a series of ANSI/ISA standards while, at the same time, updating ANSI/ISA-TR99.00.01-2004 to reflect new information and technology.

First ballots by the ISA-99 committee were completed on the Part 1 and Part 2 draft standards on May 30 and June 5, 2006, respectively.

Reference: http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

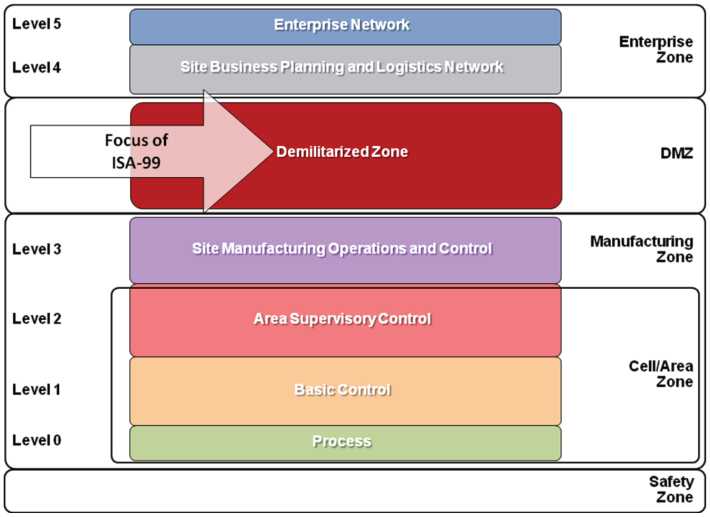


Figure 2.2-3. ISA-99 addresses manufacturing and control systems electronic security for the PERA model.

2.3 Manufacturing Zone Layers and Convergence

A thorough understanding of the manufacturing zone and convergence issues are important to selecting a physical infrastructure architecture that addresses performance, security and maintainability requirements. Based on the PERA model ISA-99, the following areas can be described for the manufacturing space which require network topologies to converge and integrate (see Figure 2-4).

Enterprise Zone. The manufacturing zone must integrate with the enterprise applications to exchange production (ex. Historical data) and resource data (ex. Recipe management). Direct access to the manufacturing zone is typically not required, with the exception of partner access (remote access). Access to data and the networks in the manufacturing zone must be managed and controlled to maintain the availability and stability of the plant or factory networks.

Demilitarized Zone (DMZ). An area for computing resources that need to be shared between the Enterprise and Manufacturing zone and that is designed with security measures to prevent direct access between the enterprise and manufacturing equipment. This area provides an important function for connecting the critical factory floor equipment to data and services from the enterprise level.

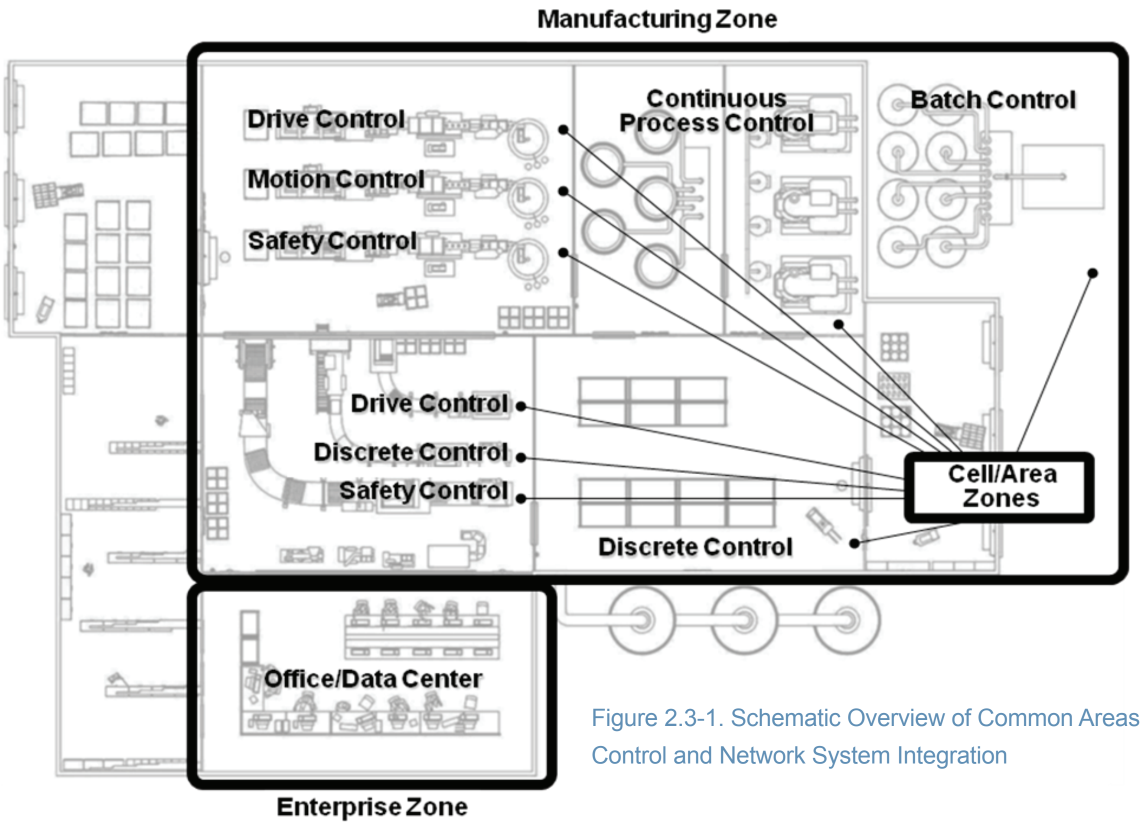


Figure 2.3-1. Schematic Overview of Common Areas of Industrial Control and Network System Integration

Manufacturing Zone. The manufacturing zone comprises the cell/area zone networks and site-level activities. It is important because all the systems critical to monitoring the plant or factory operations are in this zone.

Cell/Area Zone. The cell/area zones are the functional areas within the plant or factory. Some of the cell/area zones within a plant or factory might include raw material handling, mixing, assembly and finished goods material handling. It may be as small as a single Process Automation Controller (PAC) and its associated devices, or multiple controllers. Anything within the cell/area zones are involved in the real-time control of a functional aspect of the plant or factory.

Safety Zone. The safety zone is considered highest priority in process or manufacturing. Historically, safety systems have been hard-wired, difficult to maintain and do not accommodate change easily. Safety networks provide all the advantages of traditional distributed I/O for complex safety systems thus improving diagnostics and the ability to implement changes programmatically.

2.3.1 Layers of the Manufacturing Zone

To meet the needs of the industrial automation customer, control systems network architecture has been separated into three layers (see Figure 2-5). This three-layer architecture must be open from top to bottom. Open means that the independently managed technology is available without restriction to all, both in terms of technology access and the ability to contribute enhancements to the open standard.

This openness provides freedom of choice, allowing customers to choose the best-in-class products for their industrial automation systems. The architecture must also be based on globally accepted standards supported by a majority of companies in the control marketplace.

Taking careful consideration of communication needs of both simple and complex products, it becomes clear which layer and which network is more appropriate for that product.

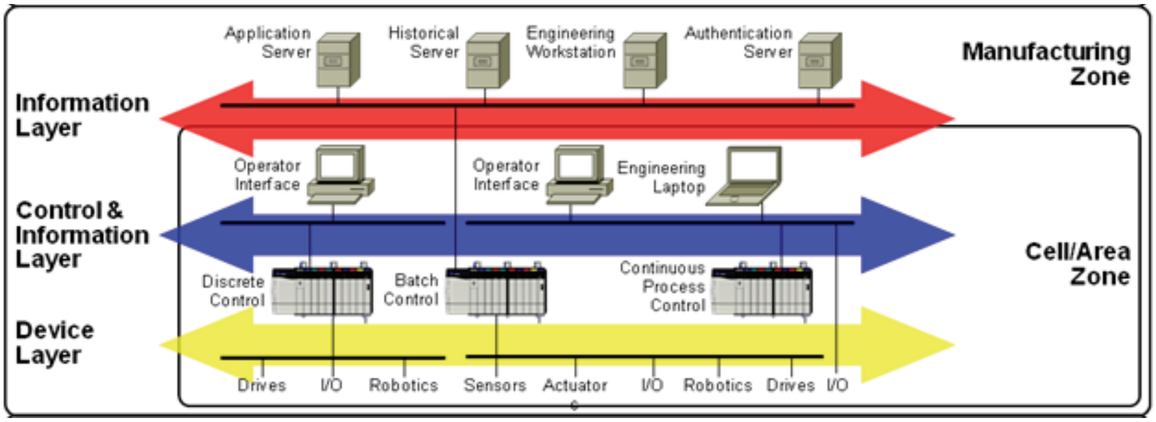
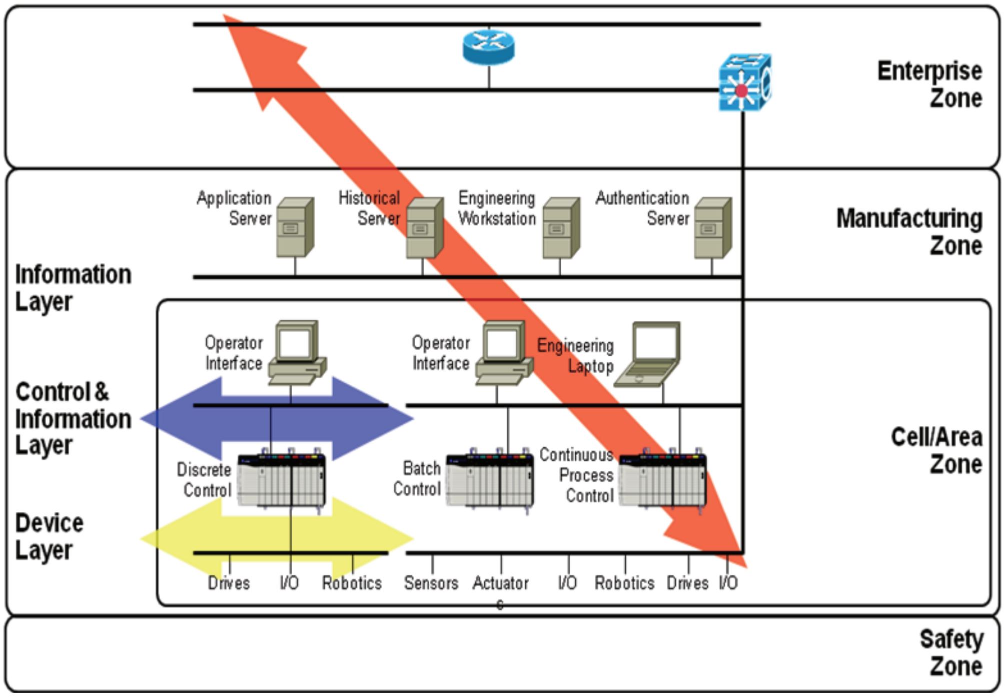


Figure 2.3-2. Manufacturing Zone Network Layers

- The Information Layer is typically a backbone and a management interface into the control system. This layer typically transfers data between supervisory devices and links into the manufacturing execution system (MES).
- The Control and Information Layer is typically used for the transmission of time-critical control data between separate manufacturing cells, where time-critical data delivery is very important. Quite often, the Control and Information Layer is used to link multiple device layer networks.
- The Device Layer network is typically used for connecting devices such as sensors and actuators, which historically have been hard wired into the Control & Information Layer. These simple sensors and actuators continue to grow in capability, and the Device Layer network makes it easier to install and use these products, taking advantage of these extended capabilities.

2.3.2 Connecting Manufacturing to Enterprise



Also, factory floor network traffic can potentially flood enterprise level.

Figure 2.3-3. Early Attempts at Control and Network System Integration Led to Unacceptable Risk

The desire to share data between manufacturing and enterprise is very strong and leads to great improvements in productivity. However, early attempts lead to problems due to failure to consider the differences between these zones and the resultant risks from connecting them together. Industrial automation networks have unique consideration from the traditional Enterprise Zone environments.

- Unique protocols and use of multicast traffic
- Determinism and real-time requirements
- Availability, security and safety considerations
- Physical requirements of the factory floor is driving unique products and topologies
- Need to provide and control vendor access

The three-layer network architectural model does not address these concerns. With significant growth in Ethernet-based industrial automation protocols driving the need for specific switching, routing, security and wireless design guidance from non-traditional IT resources are often requested.

As the need for more data increases in the Enterprise Zone from the Manufacturing Zone for systems such as MES, the Information Layer became skewed. With little or no consideration to network architecture the Manufacturing Zone was trusted into the Enterprise Zone with direct connections made from manufacturing switches and devices to existing office/enterprise networks. The results led to many problems both with manufacturing system outages as well as disruptions to office/enterprise networks.

Early attempts at enterprise integration as shown in Figure 2-6 left control cell/areas too exposed to enterprise risks. Several risks of directly connecting the manufacturing zone to the enterprise zone include:

- Security: Risk of unauthorized changes
- Malware: virus, worm disruptions
- Management: Patching or network updates not appropriate for control devices
- Traffic: Control network messages flooding enterprise causing disruption

2.3.3 Enterprise Connectivity Options

The following tables and figures clearly articulate the pros and cons for various approaches to factory integration from totally isolated to fully secure connectivity:

A. Isolated
No connection to the enterprise

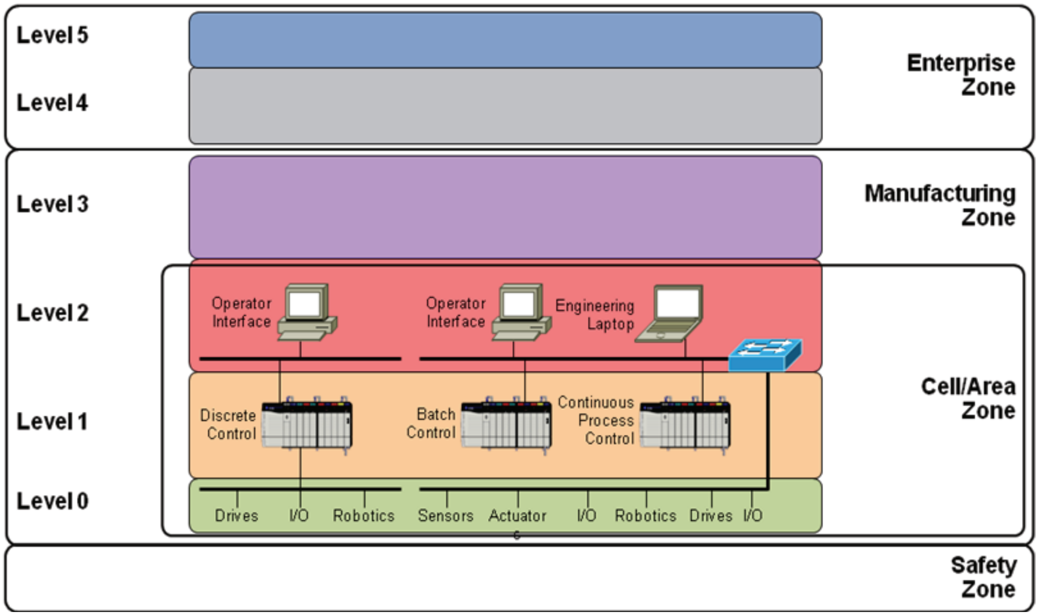
B. Integrated
Direct connection to enterprise without DMZ or VLAN

C. VLAN
Virtual LAN approach to segment and secure network

D. Firewall
Demilitarized Zone leveraging Hardware/software to separate and secure levels

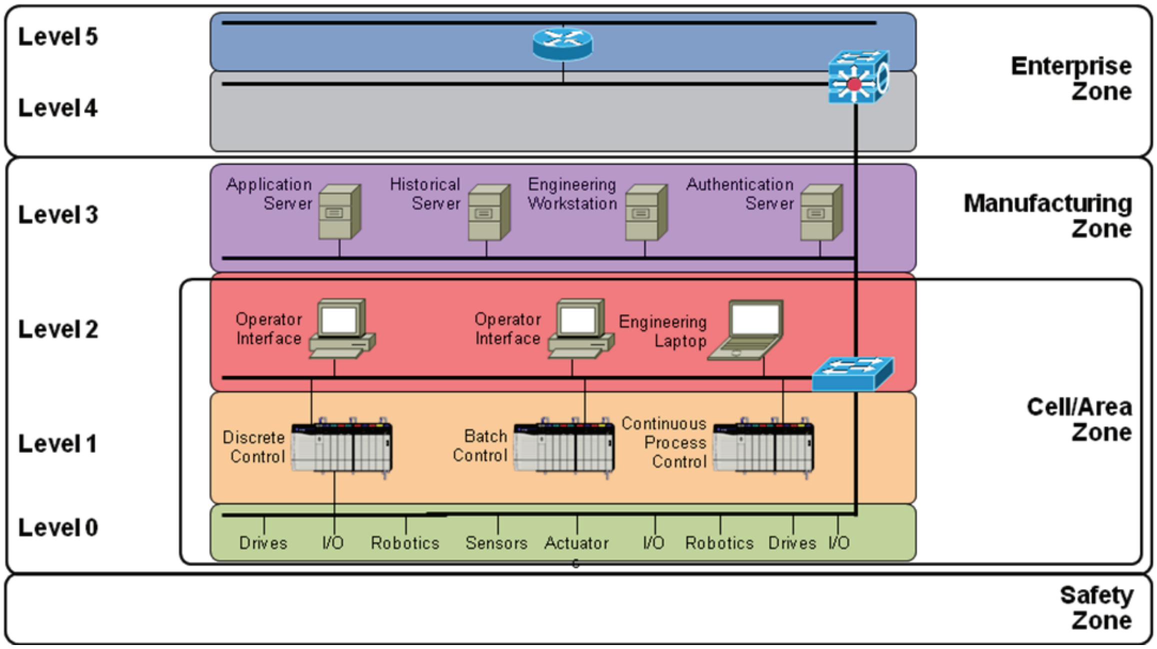
(See separate charts on subsequent pages)

A. Isolated *No connection to the enterprise*



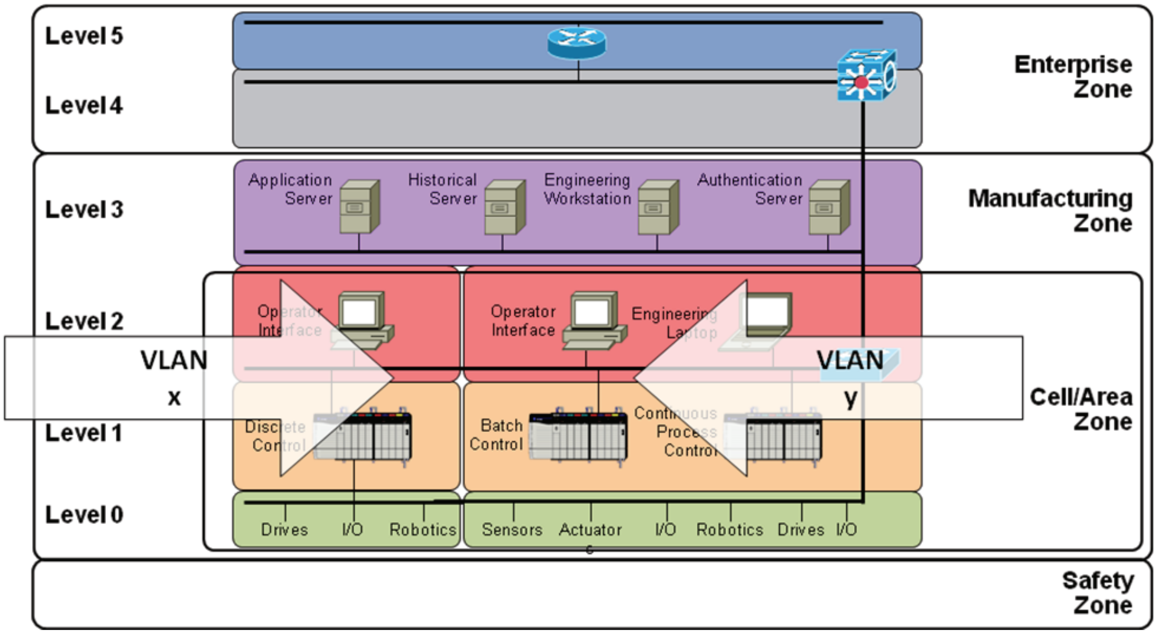
Pro	Con
100% isolation	No real time data transfer or remote access
most secure (if done properly)	Difficult (additional time) and substantial cost to: • Administer • Patch • Update Virus Definitions • Update/Install Software
	No visibility to network operations (and security issues)

B. Integrated *Direct connection to enterprise without DMZ or VLAN*



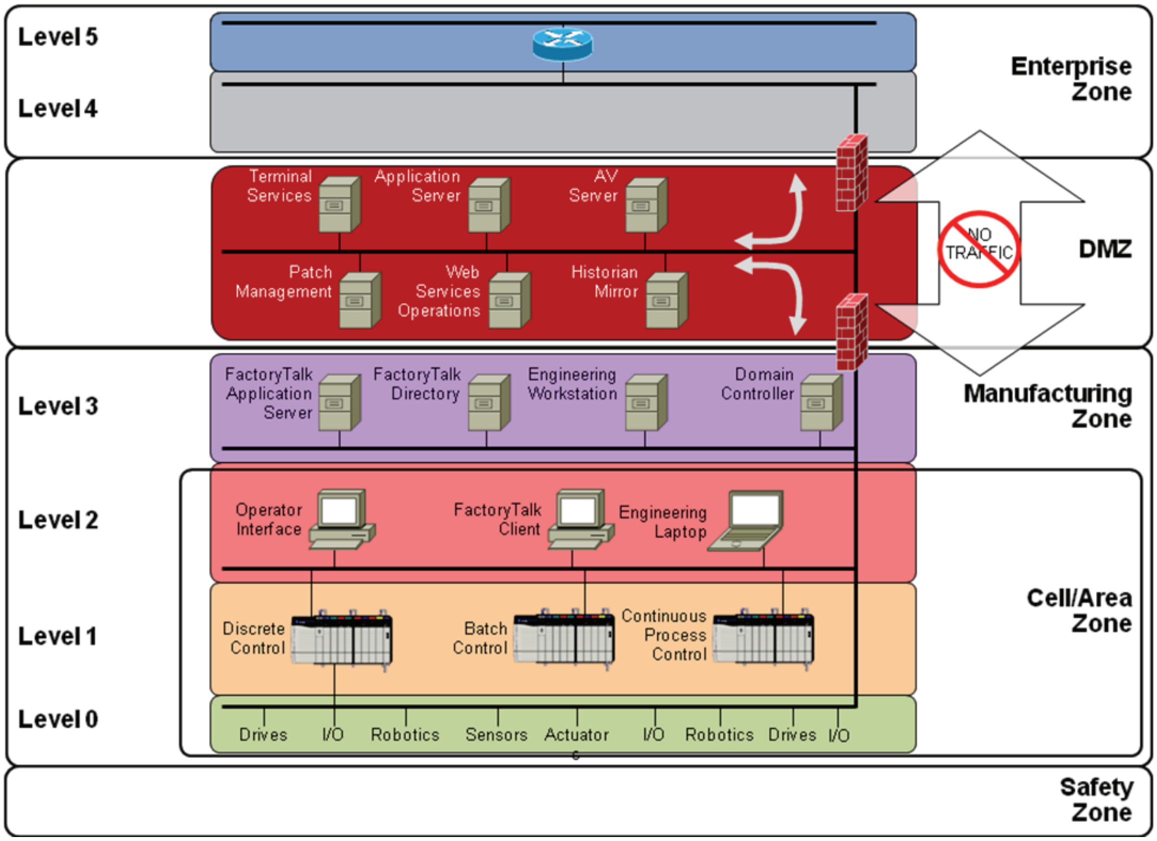
Pro	Con
Connectivity is provided for data cess/visibility	No isolation - events from one network ac- impact the other
	Administration is difficult without effecting other networks/uptime
	Control system exposed to the business networks, corporate network and internet
	Insecure - least secure

C. VLAN *Virtual LAN approach to segment and secure network*



Pro	Con
Connectivity is scalable	Difficult to secure - very high cost of ownership (from security perspective)
Better isolation	Excessive ingress and egress points
Current state	Difficult to isolate in response to network events
	Scalability with security is very difficult

D. Firewall *Demilitarized Zone leveraging Hardware/software to separate and secure levels*



Pro	Con
Best security/access trade off	Expensive - drives additional costs in networking hw and servers
Single ingress/egress point between networks	Complexity (required special skill set)
Easy to isolate in response to network events	

2.3.4 Topologies

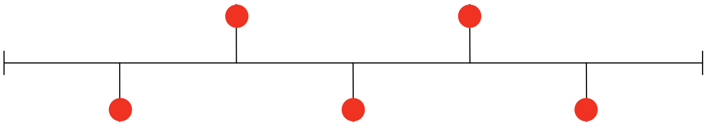
Topology refers to the network physical structure rather than the layer or zone of the architecture. A wide variety of topologies have been developed over the history of networking that address tradeoffs in cost, flexibility, robustness, and complexity. The advent of low cost embedded switch technology and wireless has allowed for a greater range of topologies for Ethernet than ever before. This section discusses the pros and cons of common topology options:

a. Bus
b. Linear or Daisy Chain
c. Star, Extended Star, Redundant Star
d. Ring, Dual Ring
e. Mesh, Partial Mesh

a. Bus

Commonly used for Level 0 and Level 1 for legacy networks but not used in today's switched Ethernet.

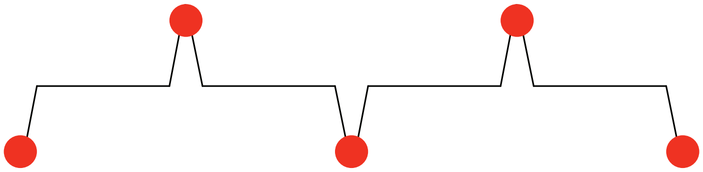
Pro	Con
	• Limited to half duplex • Collisions are unavoidable • Multiple single points of failure • No redundancy

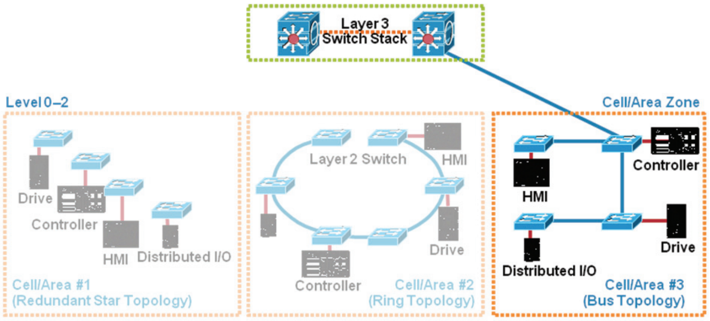


b. Linear or Daisy Chain

Commonly used for Level 0 and Level 1

Pro	Con
	• Traffic subject to the "weakest link" • Multiple single points of failure • No redundancy

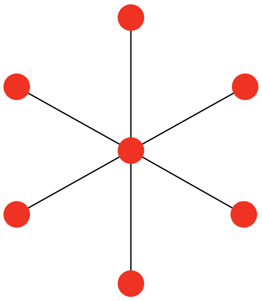




c1. Star *(i.e., Hub and Spoke)*

Commonly used for Level 0 through Level 5

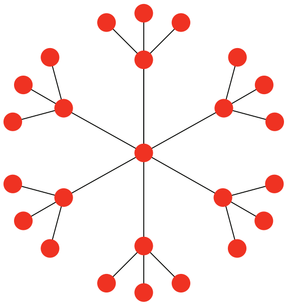
Pro	Con
	• All traffic between segments must past through a central point • Single point of failure, the "hub" • No redundancy



c.2 Extended-Star *(i.e., Hub and Spoke)*

Commonly used for Level 0 through Level 3

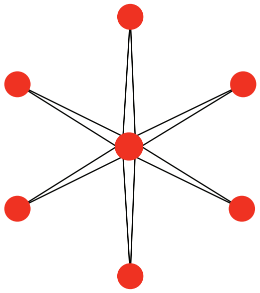
Pro	Con
	• More resilient than a star • No redundancy

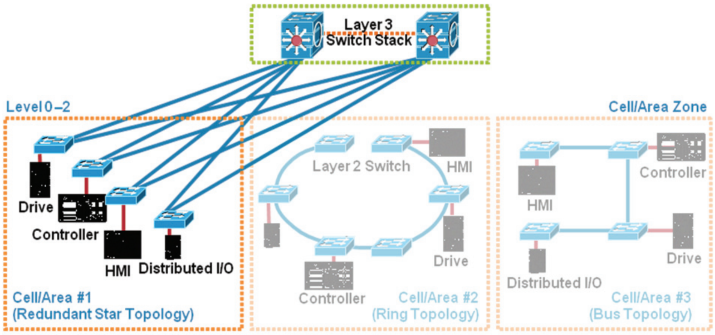


c3. Redundant Star

Commonly used for Level 0 through Level 5

Pro	Con
• Redundancy • No single point of failure when the central point uses redundant hardware	• All traffic between segments must past through a central point

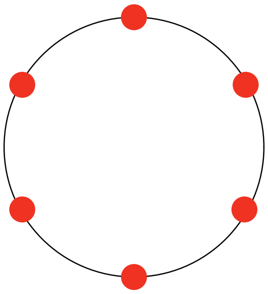


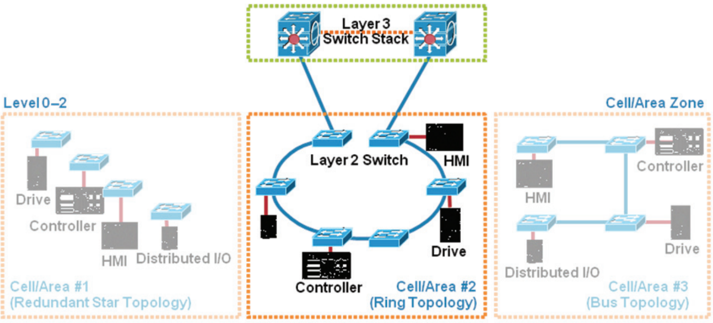


d1. Ring

Commonly used for Level 0 through Level 3

Pro	Con
• Redundancy • No single point of failure	• Possibly, convergence time depending on technology • Ring can tolerate only one failure at a time

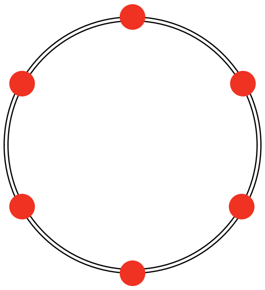




d2. Dual-Ring

Commonly used for Level 0 through Level 3

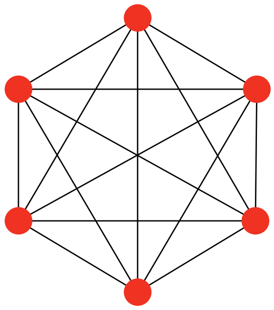
Pro	Con
• Redundancy • No single point of failure	• Possibly, convergence time depending on technology • Ring can tolerate only one failure at a time, depending on failure



e1. Full-Mesh

Commonly used for Level 3 and Level 5

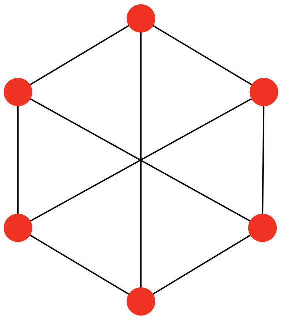
Pro	Con
• Redundancy • High availability • No single point of failure	• Expensive; N(N-1)/2 where N is the number of devices, in this case switches where the result is the number of links needed



e2. Partial-Mesh

Commonly used for Level 3 and Level 5

Pro	Con
• Redundancy • High availability • No single point of failure	• Compromise fault tolerance for cost



2.4 Rockwell Automation and Cisco Systems® Reference Architectures for Manufacturing

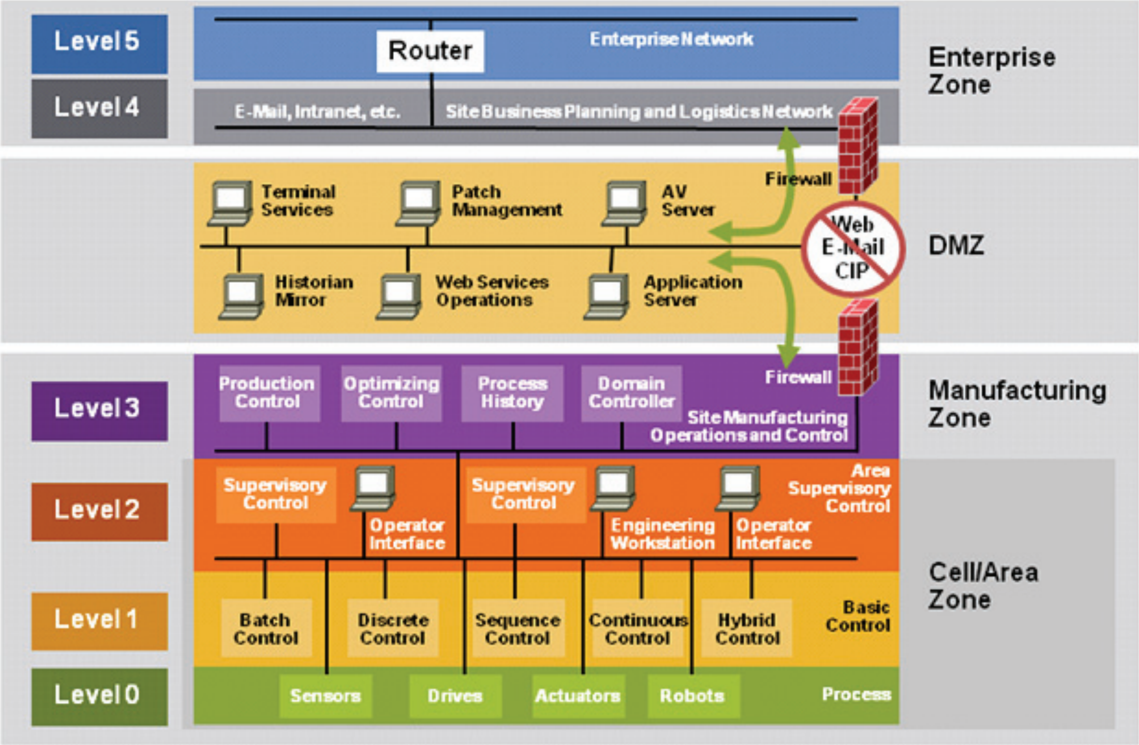
The *Rockwell Automation and Cisco Systems® Reference Architectures for Manufacturing* provide a framework for implementing automation systems that leverage network communications to deliver unprecedented efficiency, security, performance, and maintainability to industrial operations. The following diagrams show this network from a logical and switching perspective. Key concepts for this logical architecture include setup of a Demilitarized Zone (DMZ) for a secure connection of the factory floor to the enterprise through firewalls, and segmenting zones for each cell/area. Redundant star topologies are the preferred solution but there are cases where ring or bus approaches make sense.

The full explanation of the *Rockwell Automation and Cisco Systems® Reference Architectures for Manufacturing* can be found at:

http://www.ab.com/networks/architectures.html

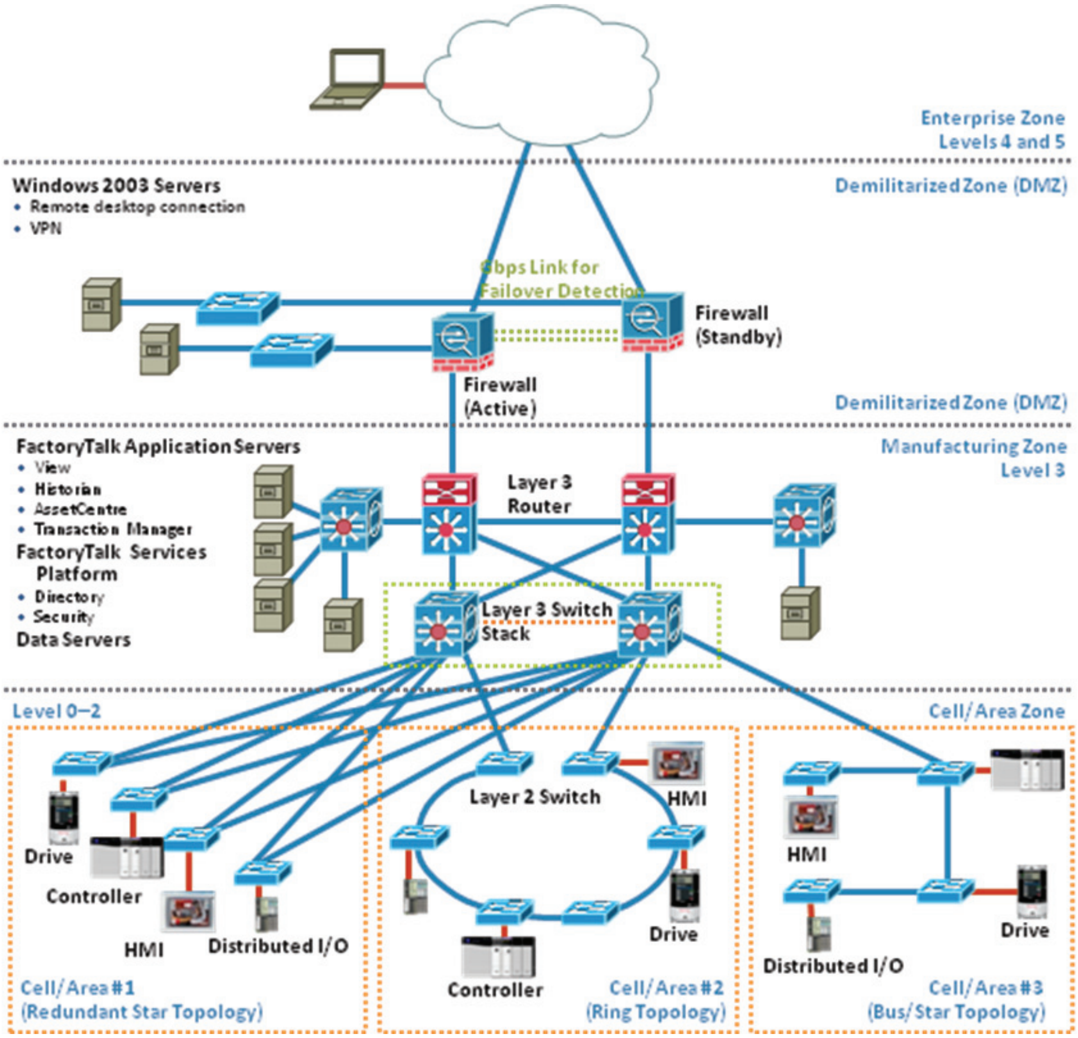
- EtherNet/IP™ Guidance for Selecting Cables [PDF] – (ODVA)
- Techniques for Infrastructure Deployment: Reference Architectures in Manufacturing Networks [PDF] – (ODVA)
- Ethernet Network Design for IT and Manufacturing Automation – (Automation Fair 2008) Learn the Guidelines for designing Ethernet infrastructures, including topology design, protocol selection, and media-switch router technology. Both IT and manufacturing automation considerations are included.

Rockwell Automation and Cisco Systems® Reference Architectures for Manufacturing offers many suggested best practices which impact availability, security, and performance. A solid understanding of this advice will lead to intelligent choices for the physical infrastructure.



Robust and Secure Network Infrastructure

- Enterprise Zone for IT networks
- DMZ as a buffer zone to securely share data and services
- Manufacturing zone where critical production floor systems exist
- Cell/Area zone where devices and controllers reside



Developed against tested and validated architectures

- Hierarchical approach to segment key network functions
- Multiple topologies
- Security built-in
- High-availability options
- Cisco Validated Design I
- Network infrastructure services
- Standard Ethernet, Standard IP, and EtherNet/IP (Standard)
- Expandable for future functions

Industrial Ethernet Reference Architecture Best Practices

Manufacturing Zone best practices

- Replicate critical services in the manufacturing zone, consider the following:
  - Domain Services e.g. LDAP or Active Directory
  - Naming services e.g. DNS & WINS
  - IP Address services e.g. DHCP
  - Time services e.g. NTP or PTP
- Availability: apply redundant network routers/switches and links to maintain overall network availability
- Scalability: small sites use combined core and distribution switches; larger or growing sites should separate to avoid oversubscription on uplinks.
- Deploy Security and Network Management
- Routing: Use link-state routing protocols or EIGRP for Layer 3 load balancing and convergence
  - Use EIGRP to simplify configuration
  - If standard protocols are required, use OSPF or IS-IS

No overlapping IP addresses with enterprise network. No redundant IP addresses (Network Address Translation is maintenance overhead).

Cell/Area Zone Design best practices

- Design small Cell/Area zones in a VLAN to better manage and shape the traffic – devices that need to talk to each other in one VLAN.
- Use Managed Switches
- Connect in Full-duplex mode to avoid collisions
- Use Gigabit Ethernet ports for trunks/uplinks for lower latency & jitter
- Use IGMP Snooping/Querier functions to control CIP multicast traffic volume
- Use resilient network topologies, Ring or preferably Redundant Star. Use RSTP to manage loops, recover from connectivity loss for network convergence.
- Apply port security to limit use of open ports.
- Enable Layer 2 security features to protect Cell/Area zone.

Security best practices

Implement network-wide security that is fully embedded into the network infrastructure, to protect against and prevent who has network access and what they can do.

- Rockwell Automation Network & Security Services – e.g. consulting and audits
- Device Hardening
- Threat defense
  - Defending the edge
  - Protecting the interior
  - Guarding the endpoints
- Manufacturing and Enterprise Zone barrier with Demilitarized zone (DMZ)

DMZ best practices

- Only path to the Manufacturing zone
- No Traffic traverses the DMZ.
  - No common protocols in each logical firewall
- Set-up functional sub-zones in the DMZ to segment access to data and services (e.g. Partner zone)
- Be prepared to “turn-off” access via the firewall
- No Control Traffic into the DMZ (or at a minimum not out of the DMZ)
- Limit outbound connections from the DMZ

2.5 Control Room Area

A highly competitive process industry is driving manufacturers to improve efficiency, productivity, and safety. At the forefront is the control room - the nerve center that links and orchestrates manufacturing processes. Greater demands are being placed on control room architectures to replace outdated controls and labor-intensive manual processes. The goal? Increased output, less waste, higher availability, and improved safety.

A robust and adaptive industrial Ethernet network infrastructure is critical to the success of this implementation. There are several key issues for control room architectures with industrial Ethernet at the core, including:

- Installation
- Security
- Performance
- Maintainability.

Reference Architectures

Rockwell and Cisco have mapped out reference architectures that meet the specialized needs for a control room to deliver process automation excellence. These architectures describe the strategy for a structured arrangement of servers, software, network switches, and control level devices that meet the needs for performance and reliability from software and device levels. In addition to this reference architecture level, the physical layer reference architecture is also crucial. The physical layer architecture refers to the infrastructure required to connect, manage, secure, and optimize the physical plant connectivity and installation. A structured, engineered approach is essential for the physical layer to ensure that investments in a control room deliver optimum output.

Physical Layout Considerations

When designing the physical layer for a control room, the key engineering considerations include the wiring back to the control room and wire management in the control room. Understanding the size of the operation, plant and control room layout, environment, plant expansion potential, and network topologies will help establish the physical layer infrastructure back to the control room. The control room may pre-exist, constraining size and lacking features like a raised floor. In addition, there may need to be coexistence with legacy wiring and devices while transitioning and during the long term. Inside the control room, there is a complex synergy of servers, monitors, printers, control devices, communication gear, etc. In fact, a modern control room is similar in architecture to a data center room. Over the years, control rooms and data centers have been converging on networks, servers, and switches driven by the need to integrate to the enterprise. Consequently, the best practices from data center rooms can be leveraged for enclosures, wire management, grounding/bonding, physical security, power distribution, and thermal dissipation. The following solution matrix explores this in more detail.

Network Schematic Analysis

Since the control room is the hub between manufacturing and the enterprise systems, both the IT and control world must be served equally. This leads to an opportunity to leverage best practices from the IT world in conjunction with process control system knowledge. Ideally, a partnership between IT and controls groups will emerge. One approach is to develop ‘hybrid’ IT and engineering resources with skills to be able to make key decisions on network architectures and physical infrastructure component selection. The ‘hybrid’ resource can come from either the IT or control groups. One of the primary tasks is to review a schematic layout of the process system’s switches and control devices. This allows the groups to make decisions on physical infrastructure components to ensure security, performance and testability for each layer of the design.

This guide provides a reference schematic layout showing a typical topology with call outs indicating where physical security for ports can be applied, where performance decisions on media and connectivity need to be made, and where it’s recommended to install patching for testability of critical fiber or copper links. For industries commonly featuring redundant networks and possibilities for sub networks from several vendors, it is crucial to identify and secure these physical links to avoid configuration mistakes and to prevent problems during startups and maintenance. Selection of appropriate fiber and copper media that can perform over the distances and environmental factors is key for robust operation. Diverse pathway planning for redundancy across the plant, as well as in control plans, should be considered. In order to reduce risks associated with installation and long term performance, select fiber and copper connectivity solutions that are engineered for high performance exceeding standard margins. A careful plan for deploying test points will insure that the network distribution meets performance targets before critical startups of equipment where delays can be costly as well as on a periodic basis during preventative maintenance to avoid loss of control during operation.

End to End Solution

In summary, perform a thorough analysis and develop a plan for the physical infrastructure for control room out to field devices. This will meet the critical needs for high availability, security and performance. Use of reference architectures that leverage best practice physical infrastructure approaches for control room hardware, network distribution, network connectivity, control panels and on-machine wiring will result in process control systems that enable the full benefit of the investments made in advanced process control systems. This guide provides information on selecting, installing, testing, and documenting this critical physical infrastructure for all levels of this architecture.

Control Room Physical Infrastructure

This section defines the sequence of actions involved with deploying a physical infrastructure for a Control Room. Necessary steps include:

1. Define the logical architecture governing the layout of industrial systems and active devices. The logical architecture should be based on logical layer reference architectures developed by Rockwell Automation and Cisco, as well as on applicable topology diagrams.

2. Map out the physical locations of servers, switches, enclosures, rack systems and control panels. The following diagram shows recommended best practices for 'in plant' distribution.

This step provides the opportunity to identify distributed zone cabling topologies and plan out required patching, test point, and security considerations.

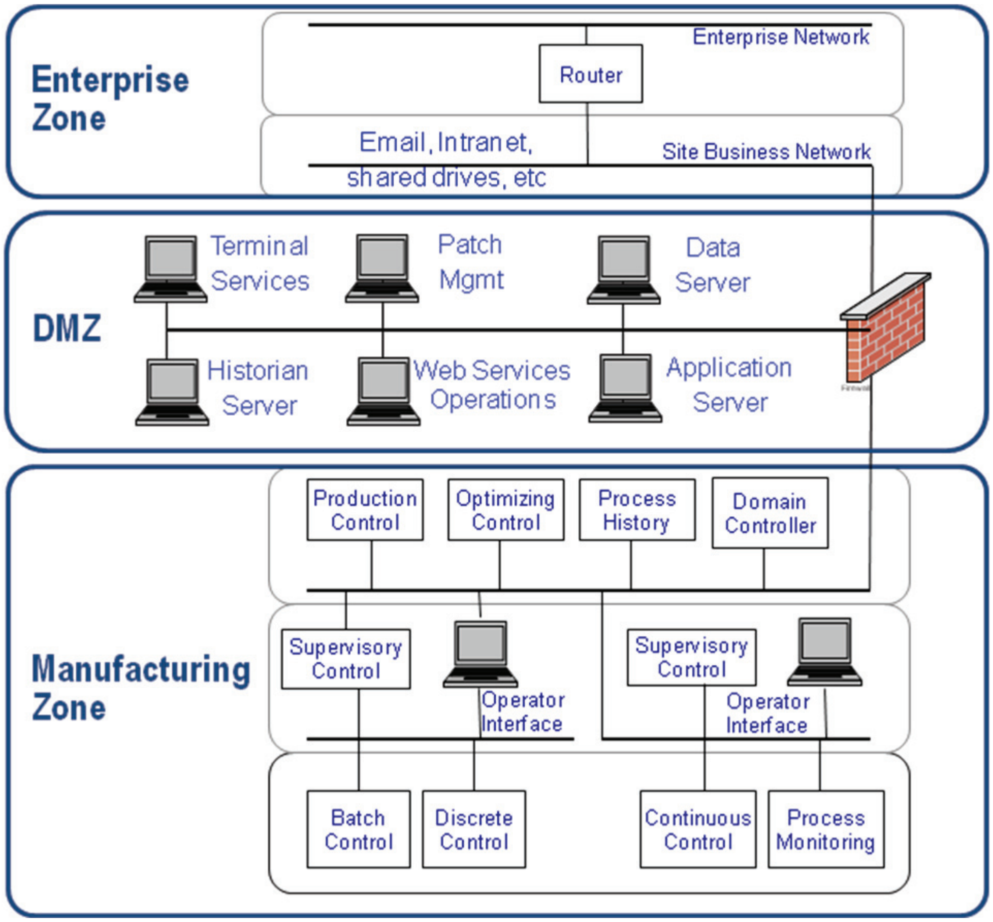
3. Develop a network-level schematic diagram (or use a reference diagram) to identify the exact physical layer components required to deploy the Ethernet network. These components include number of patch cords and horizontal links, patching fields, bonding and grounding elements, labeling and identification schemes, cable management tools, and safety and security tools.

NOTE: Steps 2 and 3 are often done concurrently.

4. Discuss the levels of the architecture in the diagram and identify solutions to address your system needs.

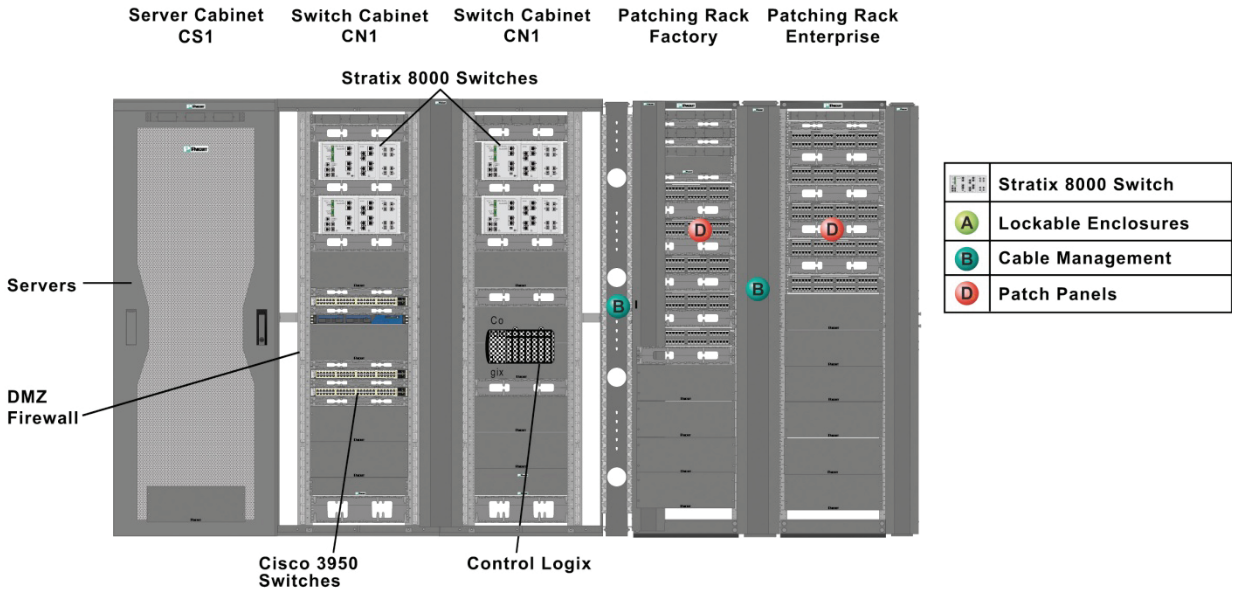
5. Review the recommended solution component List of Materials and specify your infrastructure.

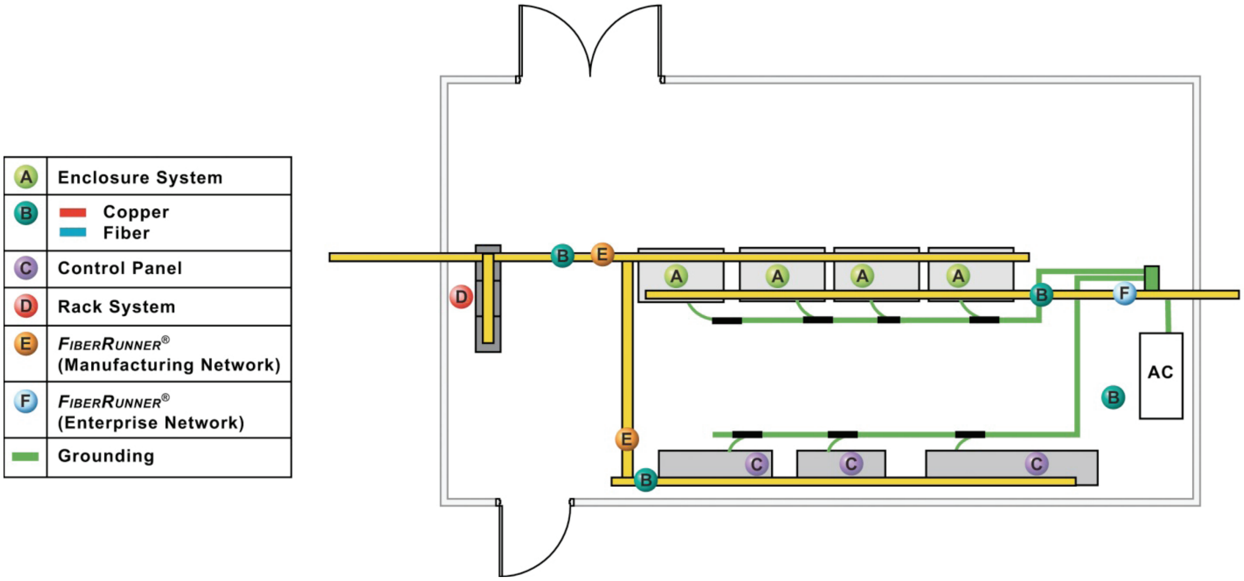
1. Define the Logical Architecture



2. Map Device Locations to Identify Physical Infrastructure Reach, Noise, Bonding/Grounding Requirements

Control Room Cabinet Layout





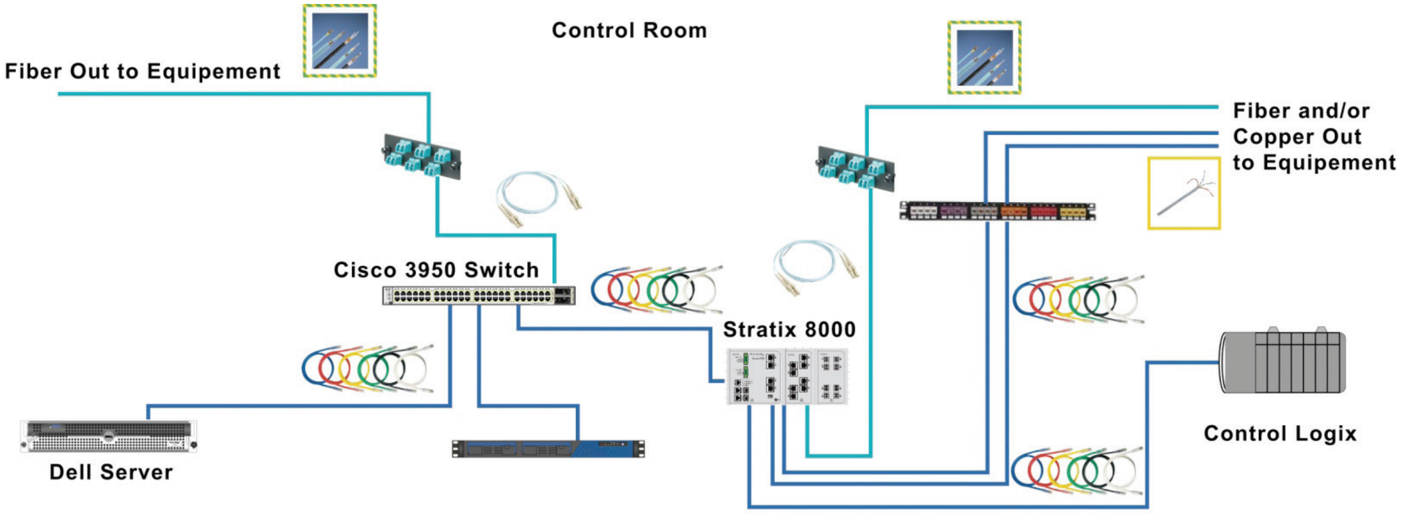
- Enclosure systems designed for optimum cable management for fiber and copper connectivity while allowing for proper thermal management of critical servers and switches

- Color coded and keyed solutions to segregate and control patching to avoid inadvertent patching mistakes that bypass DMZ firewalls that separate office and control networks

- Grounding and bonding to equipment to mitigate risks to communication disruptions

- Enhanced security with keyed jacks, lock in and block out connectivity

3. Develop Network-Level Schematic Diagram Identify Exact Physical Infrastructure Components



SECURITY

- LC Lock-in/ Block Out
- RJ45 Lock-in/ Block Out
- LC Keyed Adapter
- Keyed Fiber Patch Cord

PERFORMANCE

- Fiber Optic Cabling
- Copper Cabling
- Fiber Patch Cord
- Copper Patch Cord
- Fiber MINI-COM® Adapter Module
- Copper MINI-COM® Jack Module

TESTABILITY

- Surface Mount Enclosure with MINI-COM® Modules
- Copper MINI-COM® Jack Module
- Fiber MINI-COM® Adapter Module
- MINI-COM® Patch Panel

4. Discuss the Levels of the Architecture in the Diagram and Identify Solutions to Address Your System Needs

Zone Area Physical Infrastructure	Control Room Issues	Panduit Solution
Enterprise Zone (Level 1,2)		
Enterprise Data Center connectivity	Future proof, High Availability, high performance connectivity	Fiber and 10GB copper connectivity solutions
DMZ		
Shared enclosure, rack areas	Security: Control and Management of connections, patching	Color coded, keyed jacks can prevent crossing channels inadvertently. Lock-in connectors can secure connections in switches or patching to control who can make changes
		Lockable enclosure systems, cross connect patch panels
Manufacturing Zone (Level 3)		
Control Room	Performance: Noise issues	Grounding/Bonding solutions for under raised floor, cabinet systems
	Performance: Cable/Connector performance	Copper and Fiber solutions, installation tools, and testing guidance for end-to-end connectivity performance that exceeds standards
	Performance: Thermal management	Enclosure systems and wire management solutions that efficiently direct cooling to critical servers and switches improving robustness
	High Availability: Redundant networks	Color coded, keyed jacks can prevent crossing channels inadvertently. Lock-in connectors can secure connections in switches or patching to control who can make changes
	Maintainability: Cable management	Fiber runner, enclosure and rack systems, wire management and identification products. PanView infrastructure management
	Reliability: Power	Superior termination with Panduit terminals
Wireless implementation	Deploying wireless access points securely without expensive power runs	Utilize lockable, environmentally rated enclosures designed for Cisco Wireless Access Points and antenna systems and Power Over Ethernet (POE) to distribute power

6. **Review the Recommended Solution Component List of Materials and Specify your Infrastructure:**

Server Cabinets and accessories

Panduit Part #	Description
CS1	Server cabinet frame with top panel. Single hinge perforated front door. Two sets of cage nut equipment mounting rails. 45 RU cable management on rear of rear posts. One set of POU mounting brackets. Dimensions: 84.0"H x 31.5"W x 41.1"D (2134mm x 800mm x 1044mm)
CN1	Switch cabinet frame with top panel. Dual hinge perforated front door. Two sets of #12-24 tapped equipment mounting rails. 45 RU cable management on rear of rear posts. Dimensions: 84.0"H x 31.5"W x 41.1"D (2134mm x 800mm x 1044mm)
CMR19X84	2 Post Patching Rack with space identification Double-sided #12-24 EIA universal mounting hole spacing. 24 #12-24 mounting screws included. Paint piercing washers included.
DPFP4	4RU filler panels. Direct airflow in cabinet applications. Mount to standard EIA 19" racks or cabinets. #12-24 and M6 mounting screws included
NM1	Front and rear 1RU horizontal cable manager. Mount to 19" EIA racks and cabinets. Covers, #12-24 and M6 mounting screws included. Design fits flush to the front of the NetRunner™ High Capacity WMPVHCF45E and WMPVHC45E Vertical Managers
NMF2	Front only 2RU horizontal cable manager. Mount to 19" EIA racks and cabinets. Covers, #12-24 and M6 mounting screws included. Design fits flush to the front of the NetRunner™ High Capacity WMPVHCF45E and WMPVHC45E Vertical Managers
NMF4	Front only 4RU horizontal cable manager. Mount to 19" EIA racks and cabinets. Covers, #12-24 and M6 mounting screws included. Design fits flush to the front of the NetRunner™ High Capacity WMPVHCF45E and WMPVHC45E Vertical Managers
PRV8	8 inch wide vertical cable manager, includes four PRSP7 slack spools. Dimensions: 83.9"H x 8.0"W x 16.4"D(2131mm x 203mm x 417mm)
PRV6	6 inch wide vertical cable manager, spools are not included. Dimensions: 84"H x 6"W x 16.4"D. (2133.6mm x 152.4mm x 416.6mm)
PRD8	8 inch wide dual hinged metal door. Dimensions: 82.8"H x 8.1"W x 1.6"D(2104mm x 206mm x 40mm)
PRD6	6 inch wide dual hinged metal door. Dimensions: 82.8"H x 6.1"W x 1.6"D(2104mm x 206mm x 40mm)

Copper Cables/Connectors/Outlet Boxes

Panduit Part#	Description
CBXD6BL-AY	Surface mount box accepts six Mini-Com® Modules. Provides slots that accept cable ties for strain relief. Provides bend radius control. Supplied with label holder/screw cover. Dimensions: 1.04"H x 4.95"W x 3.79"L (26.42mm x 125.73mm x 96.27mm)
CPP24FMWBLY	1RU 24-Port flush mount modular patch panel supplied with rear mounted faceplates: For use with CJ688TG* Category 6 Jack Modules
CWPP12WBL	Alternate 12-Port patch panel supplied with three factory installed CFFP4 snap-in faceplates with integrated wall mount bracket
CJ688TG*	Category 6, RJ45, 8-position, 8-wire universal jack module. * add suffix IW (Off White, EI (Electric Ivory), WH (White), IG (International Gray), BL (Black), OR (Orange), RD (Red, BU (Blue), GR (Green), YL (Yellow) or VL (Violet)
UTPSP*M**Y	1m Category 6 UTP Patch Cord with TX6 Plus Modular Plugs on each end. * for lengths 1 to 20 feet (Increments of one foot) and 25, 30, 35, 40 foot lengths ** add suffix BL (BLACK), BU (BLUE), GR (Green), RD (RED), YL (Yellow), OR (Orange), or VL (Violet)
Optional Keyed Jack Module CJK688TG*	Keyed Category 6, RJ45, 8-position, 8-wire universal jack module
Optional Keyed Patch Cord for use with Keyed Jack Module UTPKSP*^	Keyed Category 6 UTP Patch Cord for use with matching Keyed Copper Jack Module. Patch cords contain one keyed RJ45 Plug on one and to a Standard RJ45 Plug on the other.

Copper Jacks, Cable, Patch, Assemblies

Jacks

Panduit Part#	Description
CJ6X88TGI*	Mini-Com® TX6™ 10Gig™ UTP Jack Module
CJK6X88TG*	Keyed Mini-Com® TX6™ 10Gig™ UTP Jack Module
CJ688TG*	Mini-Com® Category 6, RJ45, 8-position, 8-wire universal jack module.
CJK688TG*	Keyed Mini-Com® Category 6 UTP Jack Module
	* add suffix IW (Off White, EI (Electric Ivory), WH (White), IG (International Gray), BL (Black), OR (Orange), RD (Red, BU (Blue), GR (Green), YL (Yellow) or VL (Violet). STP Shielded Jacks also available.

Horizontal Cable

Panduit Part#	Description
PUR6X04**	TX6™ 10Gig™ CMR UTP Copper Cable
PUP6X04**	TX6™ 10Gig™ CMP UTP Copper Cable
PUR6004BU-UY	TX6™ Cat6 CMR UTP Copper Cable
PUP6004BU-UY	TX6™ Cat6 CMP UTP Copper Cable
PSR6004**	TX6™ 10Gig™ CMR U/FTP Copper Cable
PSP6004**	TX6™ 10Gig™ CMP U/FTP Copper Cable

** add suffix BL (BLACK), BU (BLUE), GR (Green), RD (RED), YL (Yellow), OR (Orange), or VL (Violet) STP Shielded Cable also available.

Patch Cords

Panduit Part#	Description
UTP6X^**	TX6™ 10Gig™ UTP Patch Cords
UTPK6X^**	Keyed TX6™ 10Gig™ UTP Patch Cords
UTPSP*M**Y	1m Category 6 UTP Patch Cord with TX6 Plus Modular Plugs on each end.
UTPKSP*^	Keyed Category 6 UTP Patch Cord for use with matching Keyed Copper Jack Module. Patch cords contain one keyed RJ45 Plug on one and to a Standard RJ45 Plug on the other.
	** add suffix BL (BLACK), BU (BLUE), GR (Green), RD (RED), YL (Yellow), OR (Orange), or VL (Violet). * for lengths 1 to 20 feet (Increments of one foot) and 25, 30, 35, 40 foot lengths STP Shielded Patch Cable also available

Patch Panels

Panduit Part#	Description
DP**6X88TGY	DP6™ 10Gig™ Modular Punchdown Patch Panel
DPA**6X88TGY	DP6™ 10Gig™ Angled Modular Punchdown Patch Panel
DP**688TGY	DP6™ Category 6 Modular Punchdown Patch Panel
DPA**688TGY	DP6™ Category 6 Angled Modular Punchdown Patch Panel
CPP**FMWBLY	Mini-Com® 1RU 24-Port flush mount modular patch panel supplied with rear mounted faceplates: For use with CJ688TG* Category 6 Jack Modules
CPPA48HDWBLY	48-Port angled high density patch panel supplied with rear mounted faceplates (space not available for component labels)
CBXD6BL-AY	Surface mount box accepts six Mini-Com® Modules. Provides slots that accept cable ties for strain relief. Provides bend radius control. Supplied with label holder/screw cover.

** = Number of Jack Ports 24 or 48

24 = 1RU Rack Space

48 = 2RU Rack Space

QuickNet

Panduit Part#	Description
QAPBCBCBXX**	QuickNet Pre-Terminated Cable Assembly construted of Category 6A, UTP, plenum cable (blue) with pre-terminated cassette (blue jacks installed) on each end. ** available in one foot increments in lengths from 10 feet to 295 feet (also available in Category 6 version)
QPP24BL	24-Port patch panel which accepts QuickNet Pre-Terminated Cassettes and Patch Panel Adapters (48 port also available)
QPPACBAB07	QuickNet Plug Pack Cable Assembly made with Category 6A, CM Blue Cable with a 6-pack blue plug pack on one end to modular plugs on the other end (also available in Category 6 version)

Punchdown System

Panduit Part#	Description
GPKBW**Y	GP6™ PLUS Punchdown System

** = either 144-Pair (36-Port) or 432-Pair (108-Port)

Fiber Products

Panduit Part#	Description
F^E10-10M*Y	Opticom® Multimode Duplex Patch Cord (various lengths). Replace ^ with X for 10Gig, 5 for 50/125um (OM2), 6 for 62.5/125um (OM1) or 9 for 9/125um (OS1). Replace the numbers for specific connector type 10 = LC, 2 = ST, 3 = SC. * implies length. Can be ordered in any hybrid configuration.
FAP*WAQ^^Z	Opticom® Fiber Adapter Panels (FAPs). Replace * with number of ports required (4, 6, 8, 12). AQ designates 10G Aqua color, also available in other colors to designate fiber type and keying solutions. Available in ST, SC, LC, and Keyed LC. Available with zirconia ceramic or phosphorous bronze split sleeves.
CFAPPBL*	Fiber Patch Panel. Replace * with one or two depending on how many FAPs or cassettes are necessary
CM*^^ZBL	MiniCom® Fiber adapter modules. Replace * with a D or S for single or duplex, ^^ with color (dependent on fiber type) and delete the Z for phosphorous bronze sleeves.
F^^MC*	Opticam Connectors. Fiber optic connectors. Replace ^^ with connector type (LC, Keyed LC, SC, or ST). Replace * with color (AQ, BL, EI)
FODR*^^Y	Fiber Optic Distribution Cable. Replace * with X-10Gig, 5 for MM (OM2), 6 for MM (OM1) and 9 for SM. Replace ^^ with fiber count (6,12,24,36,48,72,96,144,216,288)
FCXO-12-Y	QuickNet™ 10Gig™ MTP* Fiber Optic Cassettes, 50/125µm (OM3). Available in MM (OM2), MM (OM1) and SM (OS1) and in 6, 12 or 24 fiber options
FX12D5-5M1Y	QuickNet™ 10Gig™ MTP* Interconnect Cable Assemblies, 50/125µm (OM3). Replace X with, 5 for MM (OM2), 6 for MM (OM1) and 9 for SM (OS1). Replace 5-5 (LC - LC) with connectors required: 2-ST, 3-SC
FSPX*55F*A	QuickNet™ 10Gig™ MTP* Trunk Cable Assemblies, 50/125µm (OM3), various lengths. Replace X with, 5 for MM (OM2), 6 for MM (OM1) and 9 for SM (OS1)
FAP*WAQ^^Z	Opticom® Fiber Adapter Panels (FAPs). Replace * with number of ports required (4, 6, 8, 12). AQ designates 10G Aqua color, also available in other colors to designate fiber type and keying solutions. Available in ST, SC, LC, and Keyed LC. Available with zirconia ceramic or phosphorous bronze split sleeves.
CM*^^ZBL	MiniCom® Fiber adapter modules. Replace * with a D or S for single or duplex, ^^ with color (dependent on fiber type) and delete the Z for phosphorous bronze sleeves.
F^^MC*	Opticam Connectors. Fiber optic connectors. Replace ^^ with connector type (LC, Keyed LC, SC, or ST). Replace * with color (AQ, BL, EI)

Fiber Raceway Parts

Panduit Part#	Description
FR4X4**6	FIBERRUNNER 4x4 Solid Wall Channel.
FRHC4**6	FIBERRUNNER 4x4 Snap-On Hinged Cover.
FRBC4X4**	FIBERRUNNER 4x4 QuikLock Coupler.
FRT4X4**	FIBERRUNNER 4x4 Horizontal Tee Fitting.
FRTSC4**	FIBERRUNNER 4x4 Horizontal Tee Cover.
FRFWC4X4**	FIBERRUNNER 4x4 Four Way Cross Fitting.
FRFWCSC4**	FIBERRUNNER 4x4 Four Way Cross Cover.
FRRA4X4**	FIBERRUNNER 4x4 Horizontal Right Angle Fitting.
FRRASC4**	FIBERRUNNER 4x4 Horizontal Right Angle Cover.
FREC4X4**	FIBERRUNNER 4x4 End Cap.
FRSP**	FIBERRUNNER Spill-Over Fitting with 2x2 Exit.
FRSP4C**	FIBERRUNNER Spill-Over Fitting with 2x2 Exit Cover for 4x4 Channel.
FBC2X2**	FIBERRUNNER 2x2 QuikLock Coupler.
FIDT2X2**	Single Port Spill-Out t 1.5” ID Split Corrugated Loom Tubing.
FR6TRBN58	FIBERRUNNER QuikLock New Threaded Rod for 5/8” Threaded Rod
FR6TB12	FIBERRUNNER QuikLock Trapeze Bracket

*** Replace with desired color, YL for yellow, BL for Black or OR for Orange*

Gridrunner Wireway Parts

Panduit Part#	Description
GR21X4X24PG	GRIDRUNNER 21”W x 4”D x 24”L Wire Basket Section
GR21X4X48PG	GRIDRUNNER 21”W x 4”D x 48”L Wire Basket Section
GR12X4X24PG	GRIDRUNNER 12”W x 4”D x 24”L Wire Basket Section
GR12X4X48PG	GRIDRUNNER 12”W x 4”D x 48”L Wire Basket Section
GRFWC21PG	GRIDRUNNER Universal Intersection
GRPBPG	GRIDRUNNER Pedestal Bracket
GRCLAMPPG-X	GRIDRUNNER Pedestal Clamp
GRBR4PG	GRIDRUNNER Bend Radius Control Corner

Cable Routing/Management

Panduit Part#	Description
CCH50-S10-C	Heavy-Duty Fixed Diameter Clamps
CCS25-S8-C	Standard Fixed Diameter Clamps
CH105-A-C14	Cable Holder
CLT100-C20	Corrugated Loom Tubing
CSH-D20	Cable Spacers
JP131W-L20	J-PRO™ Cable Support System

Cable Ties

Panduit Part#	Description
HLM-15R0 *	HLM Series 15 Ft. Roll x .330" Width, Black
HLS-75R0 *	HLS Series 75 Ft. Roll x .75" Width, Black
HLB2S-C0 *	100 Pc TAK-TY Stacked Strips, 7" Strip Tie, 0.75" Width, Black
HLS3S-X0 *	HLS Series 12" Strip Tie, Black
HLT2I-X0 *	HLT Series 8" Loop Tie, Black
HLT3I-X0 *	HLT Series 12" Loop Tie, Black
HLTP2I-X12 *	HLTP Series 8" Loop Tie, UL, Plenum UL94V-2 - Maroon
HLSP3S-X12 *	HLSP Series 12" Strip Tie, UL, Plenum UL94V-2 - Maroon
CBOT24K	Cable Bundle Organizing Tool
PRPC13-69 PRPC13-60	Power Outlet Unit Plug Retention Device - Only used with select Panduit Power Outlet Units (Natural and BLK color)
ERT2M-C20	8.5" Elastomeric Cable Tie, Network Cable safe, Weather/UV Resistant, UL94V-0 Flammability Rating
ERT3M-C20	11" Elastomeric Cable Tie, Network Cable safe, Weather/UV Resistant, UL94V-0 Flammability Rating

* *Available in multiple colors*

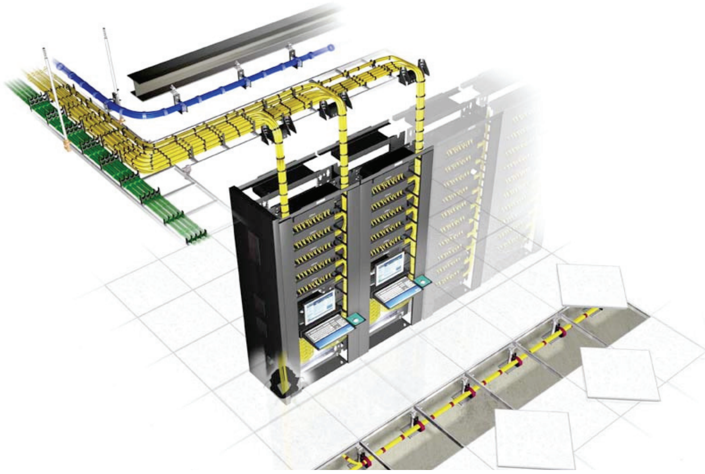
Control Room Grounding/Bonding

Panduit Part#	Description
Grounding and Bonding Infrastructure Parts	
GB2B0314TPI-1	Telecommunications Grounding Busbar (TGB) 1/4" x 2" x 24", Solid Copper, Tin Plated.
HTWC250-250-1	H-Tap w/Cover Kit: Run 250kcmil - #2 AWG, Tap 250kcmil - #2 AWG
LCC3/0-38DW	Two-hole, long barrel lug w/window, 3/0 AWG, 3/8" stud hole, 1" spacing
LCC2-38DW	Two-hole, long barrel lug w/window, 2 AWG, 3/8" stud hole, 1" spacing
LCC4-38DW	Two-hole, long barrel lug w/window, 4 AWG, 3/8" stud hole, 1" spacing
LCC4-12W	Two-hole, long barrel lug w/window, 4 AWG, 1/2' stud hole, 1 3/4" spacing
LCC6-14AW	Two-hole, long barrel lug w/window, 6 AWG, 1/4' stud hole, 5/8" spacing
GUBC500-6	Universal Beam Grounding Clamp
GLMHK	1/2" Hardware Kit for Universal Beam Grounding Clamp
HDW1/4-KT	Stainless Steel Hardware Kit, 1/4", (2) bolts, (2) nuts, (4) flat washers, (2) Belleville (locking) washers
HDW3/8-KT	Stainless Steel Hardware Kit, 3/8", (2) bolts, (2) nuts, (4) flat washers, (2) Belleville (locking) washers
LTYK	Telecommunications Grounding and Bonding Label Kit
Use these Grounding Jumper Kits when go going directly from Rack/Cabinet to TMGB or TGB. Use with HDW hardware kits.	
GJ672UH	Telecommunications Equipment Bonding Conductor (TEBC), 6 AWG, 72" (6')
GJ696UH	Telecommunications Equipment Bonding Conductor (TEBC), 6 AWG, 96" (8')
GJ6120UH	Telecommunications Equipment Bonding Conductor (TEBC), 6 AWG, 120" (10')
GJ6144UH	Telecommunications Equipment Bonding Conductor (TEBC), 6 AWG, 144" (12')
GJ6168UH	Telecommunications Equipment Bonding Conductor (TEBC), 6 AWG, 168" (14')
GJ6192UH	Telecommunications Equipment Bonding Conductor (TEBC), 6 AWG, 192" (16')
GJ6216UH	Telecommunications Equipment Bonding Conductor (TEBC), 6 AWG, 216" (18')
GJ6240UH	Telecommunications Equipment Bonding Conductor (TEBC), 6 AWG, 240" (20')
GJ6264UH	Telecommunications Equipment Bonding Conductor (TEBC), 6 AWG, 264" (22')
GJ6288UH	Telecommunications Equipment Bonding Conductor (TEBC), 6 AWG, 288' " (24')
RGCBNJ660P22	Common Bonding Network Jumper Kit. 6 AWG from Rack/Cabinet to #6 AWG to #2 AWG
RGCBNJ660PY	Common Bonding Network Jumper Kit. 6 AWG from Rack/Cabinet to #2 AWG to 250 kcmil.
For hanging grounding jumpers from ladder racks and bonding ladder rack sections together.	
GACB-1	Auxiliary Cable Bracket
GACBJ68U	Auxiliary Cable Bracket Jumper Kit, 8"
Rack and Cabinet Grounding and Bonding Components	
RGS134-1Y	Vertical Grounding Strip Kit, threaded equipment mounting rails
RGS134B-1	Vertical Grounding Strip Kit, Cage Nut equipment mounting rails
RGRB19U	Horizontal Grounding Bus Bar kit, threaded equipment mounting rails
RGRB19CN	Horizontal Grounding Bus Bar Kit, Cage Nut equipment mounting rails
RGESD2-1	ESD Port, #12-24 threaded rail
RGESDB-1	ESD Port, Cage Nut Rails
RGESDWS	ESD Wrist Strap
GJS660U	Equipment Jumper Kit, 6 AWG, 60" (5'), one end factory terminated with straight two-hole compression connector.
RGTBSG-C	Green Bonding Screws, #12-24, box of 100
CNBK	Bonding Cage Nut, 50 pack
CNB4K	Bonding Cage Nut, 4 pack
For bonding and grounding armor fiber cable.	
ACG24K	Armored Fiber Cable Grounding Kit, up to 0.84 diameter
ACG24K-500	Armored Fiber Cable Grounding Kit, up to 1.03 diameter

Identification Parts - *LS8E printer items only shown*

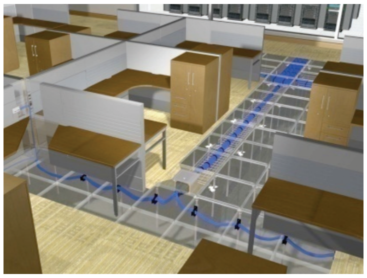
Panduit Part#	Description
C200X100YPC	Printable Label for Grounding Busbars
C200X100YPC	Printable Label for Rack Identification
C200X100YPC	Printable Label for Enclosure Identification
S100X160VAC	Printable Label for 2mm/3mm Fiber Cable Identification
S100X220VAC	Printable Label for MTP Fiber Cable Identification
NWSLC-2Y	Cable identification sleeve for 2mm fiber cable
NWSLC-3Y	Cable identification sleeve for 3mm fiber cable
NWSLC-7Y	Cable identification sleeve for MTP fiber cable
S100X150VAC	Printable Label for Cat 5/6 Copper Cable Identification
S100X225VAC	Printable Label for 10Gig Copper Cable Identification
T100X000VPC-BK	Printable Label for Fiber Port Identification
C252X030FJC	Printable Label for Copper 4 Port Identification
C379X030FJC	Printable Label for Copper 6 Port Identification
C100X000VUC-BK	Printable Label for Pathway Identification

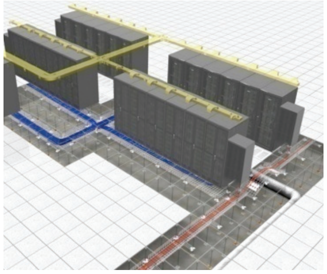
2.6 Network Distribution



There is a balancing act to connecting the manufacturing zone control room to the cell/area zone. Users must decide on architectures, physical media, and connectivity that distribute networking that is cost-effective while also possessing enough flexibility, environmental ruggedness and performance headroom to hold up to current and future manufacturing needs.

With the rapid pace of technological developments, specifying network distribution can be confusing as there are multiple categories of copper cabling and modes of fiber media that address varying channel lengths, performance targets, and EMI noise levels. A growing move to wireless approaches also factor into decisions for connecting far flung operations or those with challenging environmental issues. Power over Ethernet technology distributes networking and AC power sufficient for video cameras, sensors, and wireless access points.





The selection of media and connectivity for network infrastructure is best analyzed as a system design encompassing the media, connectors, security, and installation products that will perform as a solution long term. Certified designers and installers can ensure that this technology is deployed appropriately and support the underlying reference architecture for the application. Key issues for network distribution architectures with industrial Ethernet at the core include installation, reliability, security, production growth, and performance.

Reference Architectures

Rockwell Automation and Cisco have mapped out reference architectures that meet the specialized needs for network distribution to deliver automation excellence. These architectures describe the connectivity between the Cell and Manufacturing zones at a logical level. In addition to this reference architecture level, the physical layer reference architecture is also crucial. The physical layer architecture refers to the infrastructure required to achieve the connectivity considering data throughput, environment, wiring distances, and availability. A structured, engineered approach is essential for the physical layer to ensure that investments in network distribution deliver optimum output.

Physical Layout Considerations

Key engineering considerations when designing the physical layer for network distribution include data through-put, distance, reliability, and environment. Understanding the size of the operation, plant layout, harsh conditions, plant expansion potential, and network topologies will help establish the physical layer infrastructure requirements. In addition, there may need to be coexistence with legacy wiring and devices while transitioning and long term. State-of-the-art technologies like fiber, deliver superior performance by handling high traffic volume, immunity to noise, and long distances. Reliable termination is essential to achieve excellent performance and reliability. Some possibilities include pre-terminated fiber connectors, or copper bulk head connectors like IP67 or M12. Redundant networks pose different challenges such as cross connection or incorrect port connections. Color coded connectors and Lock-in connectors can mitigate this risk.

Cable routing poses other challenges. Cables may be exposed to harsh environments such as extreme weather or vibration. Insulation and abrasion protection products shield cables such as spiral wrap or heat shrink tubing. Securing cabling may require weather-resistant cable ties and, in extreme cases, rugged stainless steel wire management products.

Network Schematic Analysis

Industrial Ethernet implementations can leverage the experience of traditional office Ethernet by partnering with IT. This leads to an opportunity to apply best practices from the IT world in conjunction with process control system knowledge. The ideal is a partnering between IT and controls groups. One approach is development of ‘hybrid’ IT and engineering resources with skills to be able to make key decisions on network architectures and physical infrastructure component selection. The ‘hybrid’ resource can come from either the IT or control groups. One of the primary tasks is to review a schematic layout of the network distribution to ensure security, performance and testability for each layer of the design.

This Guide provides a reference schematic layout showing a typical topology with callouts that show where physical security for ports can be applied, where performance decisions on media and connectivity need to be made, and where it’s recommended to install patching for testability of critical fiber or copper links. For industries where redundant networks are common and also have possibilities for sub networks from several vendors, it is crucial to identify and secure these physical links to avoid configuration mistakes and to prevent problems during startups and maintenance. Selection of appropriate fiber and copper media that can perform over the distances and environmental factors is key for robust operation. Diverse pathway planning for redundancy across the plant as well as in control plans should be considered. Selecting fiber and copper connectivity solutions engineered for high performance exceeding standard margins reduces risks associated with installation and long term performance. A careful plan for deploying test points will insure that the network distribution meets performance targets before critical startups of equipment where delays can be costly as well as on a periodic basis during preventative maintenance to avoid loss of control during operation.

End-to-End Solution

In summary, a thorough analysis and plan developed for the physical infrastructure for control room out to field devices will meet the critical needs for high availability, security and performance. Use of reference architectures that leverage best practice physical infrastructure approaches for control room hardware, network distribution, network connectivity, control panels and on-machine wiring will result in process control systems that enable the full benefit of the investments made in advanced process control systems. This guide provides information on selecting, installing, testing, and documenting this critical physical infrastructure for all levels of this architecture.

Network Distribution Physical Infrastructure

This section defines the sequence of actions involved with deploying a physical infrastructure for network distribution.

1. Logical Design

Define the Logical Architecture

Define the logical architecture governing the layout of industrial systems and active devices. The logical architecture should be based on logical layer reference architectures developed by Rockwell Automation and Cisco, as well as on applicable topology diagrams.

2. Physical Design

Map Device Locations to Identify Physical Infrastructure Reach, Noise, Bonding/Grounding Requirements

Map out the physical locations of servers, switches, enclosures, rack systems and control panels. The following diagram shows how cable reach factors dictate whether to use copper, single mode or multi-mode cabling. Zone cabling approaches can also distribute cabling though passive patch panels or active patch panels with switches.

This step provides the opportunity to identify distributed zone cabling topologies and plan out required patching, test point, and security considerations.

3. Detail Design

Develop Network-Level Schematic Diagram Identify Exact Physical Infrastructure Components

Develop a network-level schematic diagram (or use a reference diagram) to identify the exact physical layer components required to deploy the Ethernet network. These components include number of patch cords and horizontal links, patching fields, bonding and grounding elements, labeling and identification schemes, cable management tools, and safety and security tools.

NOTE: Steps 2 and 3 are often done concurrently.

4. Review the levels of the architecture in the diagram and identify solutions to address your system needs.

5. Review the recommended solution component List of Materials and specify your infrastructure.

1. Logical Design

Define the Logical Architecture

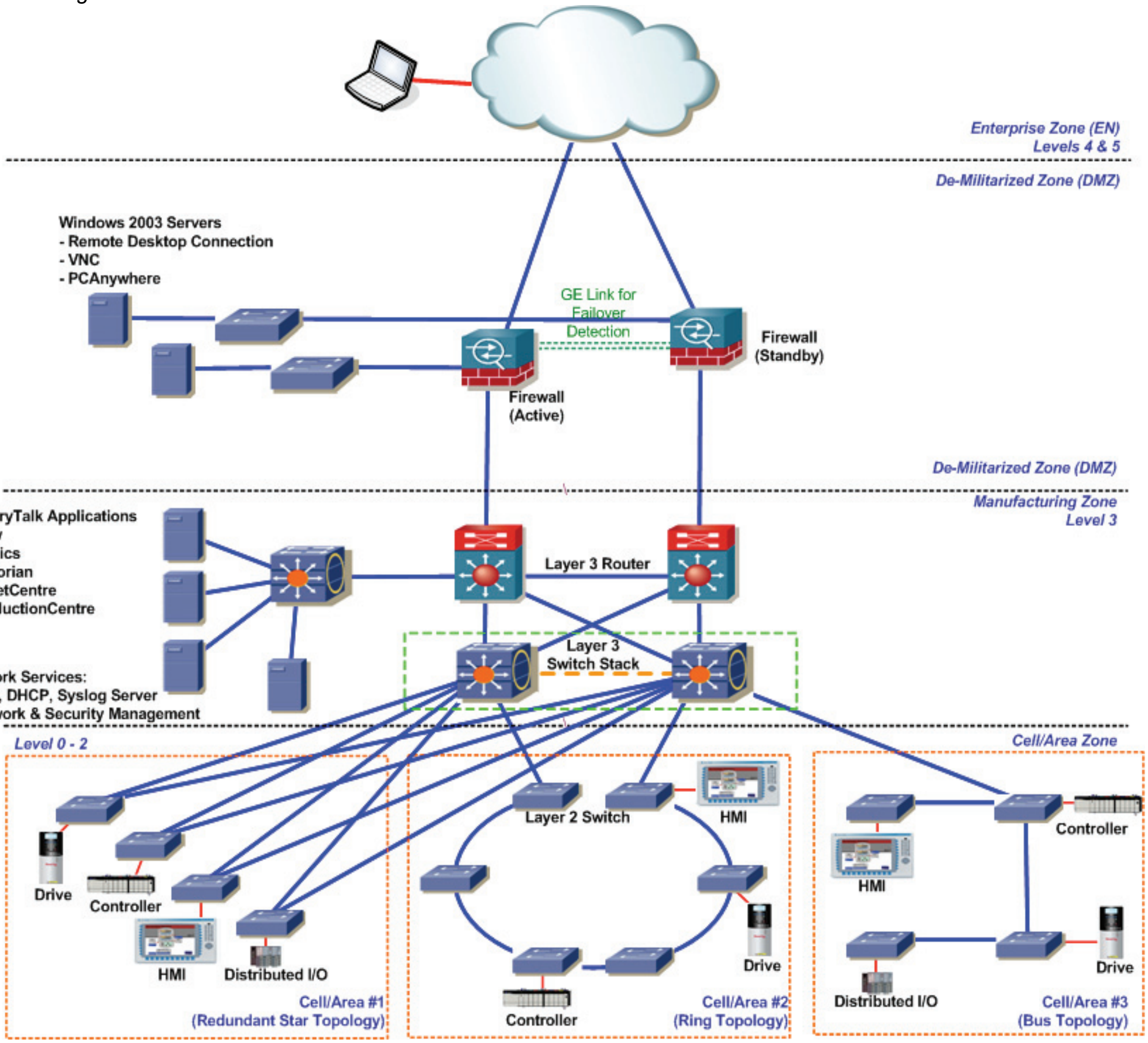


Fig 2.6-1 Logical Diagram for network distribution

2. Physical Design

Map Device Locations to Identify Physical Infrastructure

Reach, Noise, Bonding/Grounding Requirements

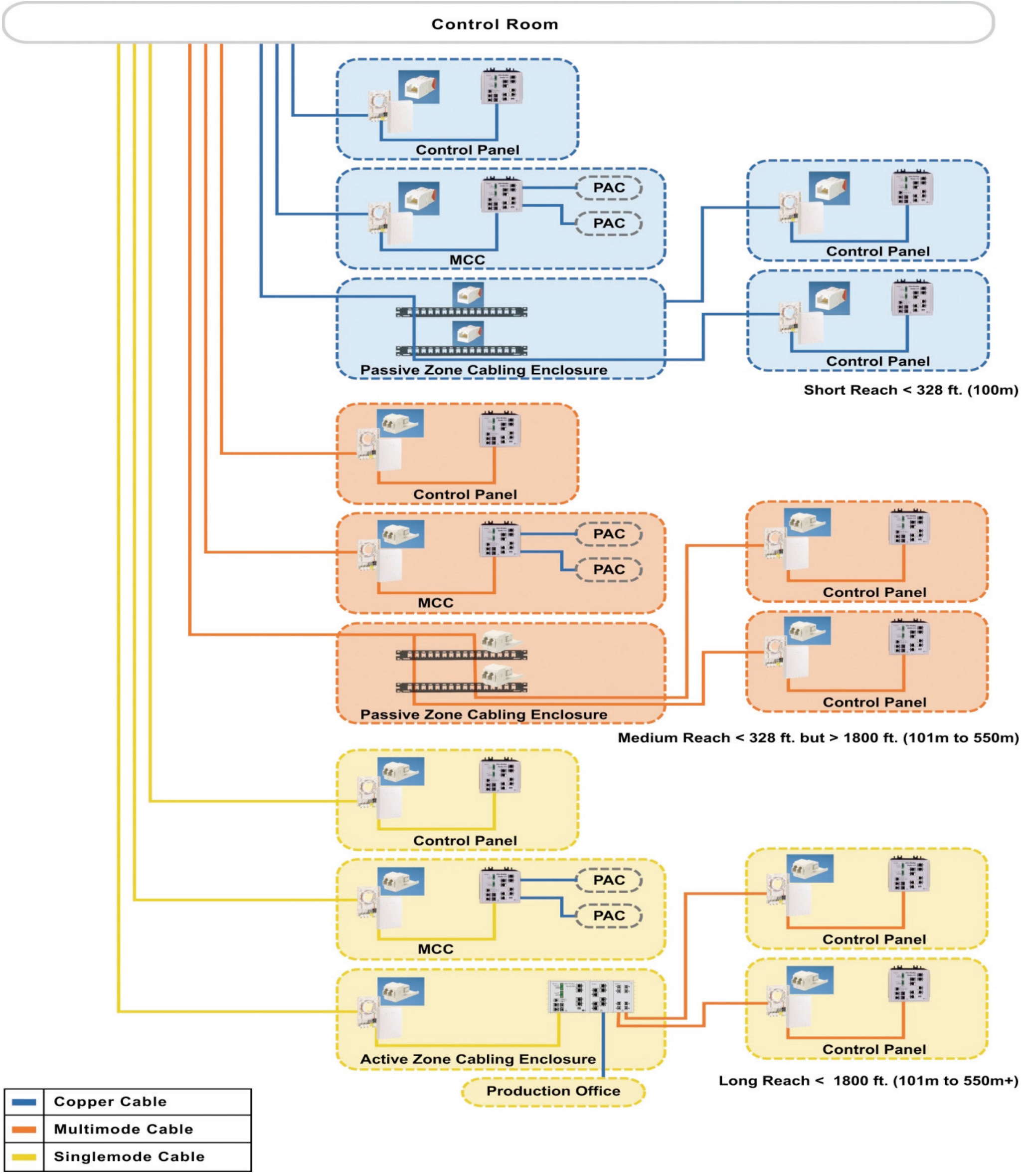


Fig 2.6-2 Physical Diagram for network distribution

- Copper Layer: Use for short reach (less than 328 ft, 100m).
    - Choose Category 6 cable and connectors for 10/100/1000Mb performance.
- Fiber Layer:
    - For Medium reach (328 to 1800 ft, 101m to 550m) use Multimode fiber cable.
    - For Long reach (Greater than 1800 ft) use Single mode fiber

3. Detail Design

Develop Network-Level Schematic Diagram Identify Exact Physical Infrastructure Components

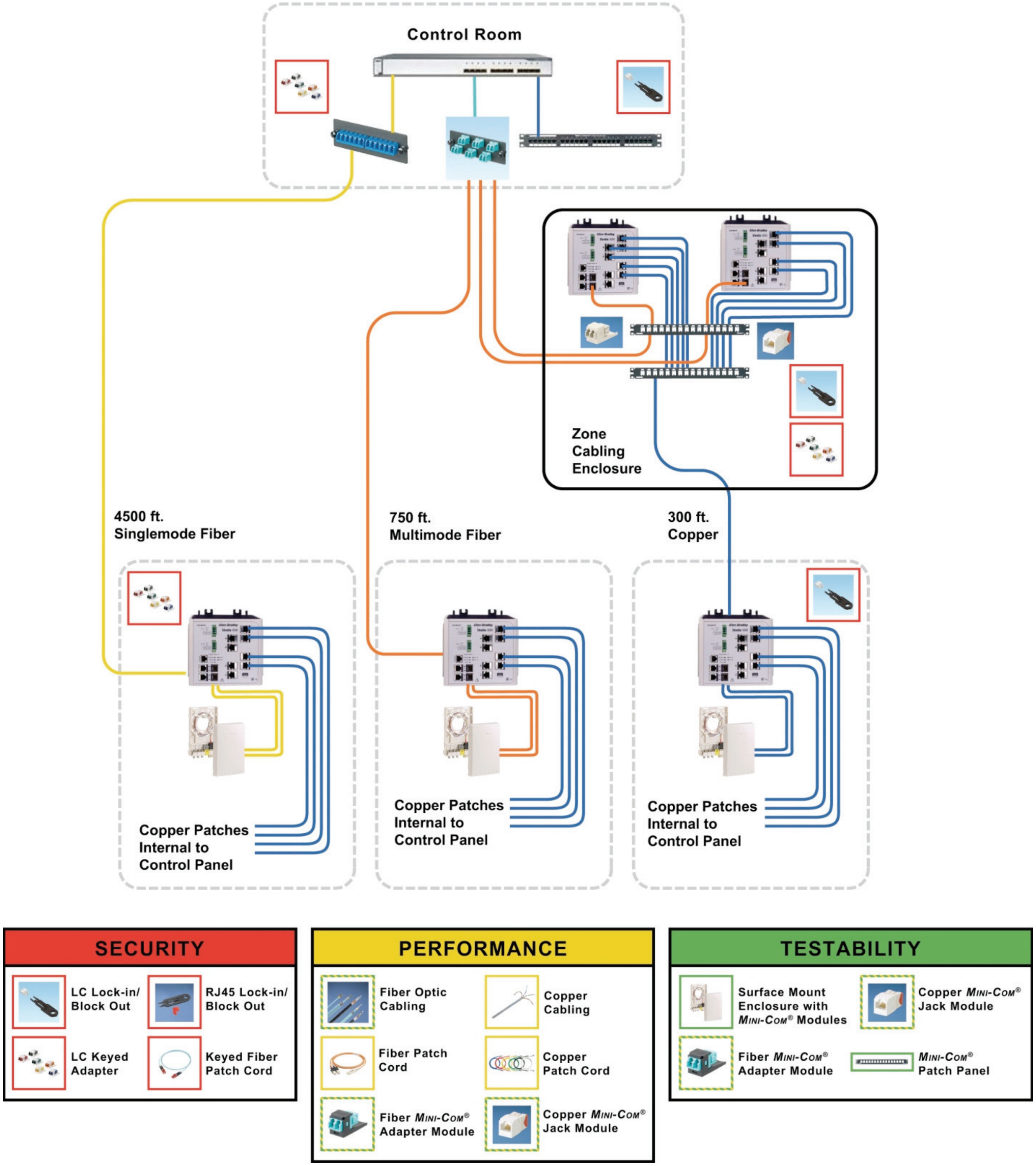


Fig 2.6-3 Detail diagram for network distribution physical infrastructure

4. *Discuss the Levels of the Architecture in the Diagram and Identify Solutions to Address Your System Needs.*

Zone Area Physical Infrastructure	Network Distribution Issues	Panduit Solution
Enterprise Zone (Level 1,2)		
Enterprise Data Center connectivity	Futureproof, High Availability, high performance connectivity	Fiber and 10GB copper connectivity solutions
DMZ		
Shared enclosure, rack areas	Security: Control and Management of connections, patching	Color coded, keyed jacks can prevent crossing channels inadvertently. Lock-in connectors can secure connections in switches or patching to control who can make changes
		Lockable enclosure systems, cross connect patch panels
		PanView infrastructure management
Manufacturing Zone (Level 3)		
Control Room	Performance: Noise issues	Grounding/Bonding solutions for under raised floor, cabinet systems
	Performance: Cable/Connector performance	Copper and Fiber solutions, installation tools, and testing guidance for end-to-end connectivity performance that exceeds standards
	High Availability: Redundant networks	Color coded, keyed jacks can prevent crossing channels inadvertently. Lock-in connectors can secure connections in switches or patching to control who can make changes
	Maintainability: Cable management	Fiber runner, enclosure and rack systems, wire management and identification products. PanView infrastructure management

5. *Review the Recommended Solution Component List of Materials and Specify your Infrastructure:*

Copper Jacks, Cable, Cable Assemblies

Jack Modules

Panduit Part#	Description
CJ6X88TG*	Mini-Com® TX6™ 10Gig™ UTP Jack Module
CJK6X88TG*	Keyed Mini-Com® TX6™ 10Gig™ UTP Jack Module
CJ688TG*	Mini-Com® Category 6, RJ45, 8-position, 8-wire universal jack module.
CJK688TG*	Keyed Mini-Com® Category 6 UTP Jack Module
	* add suffix IW (Off White, EI (Electric Ivory), WH (White), IG (International Gray), BL (Black), OR (Orange), RD (Red, BU (Blue), GR (Green), YL (Yellow) or VL (Violet). STP Shielded Jacks also available.

Horizontal Cable

Panduit Part#	Description
PUR6X04**	TX6™ 10Gig™ CMR UTP Copper Cable
PUP6X04**	TX6™ 10Gig™ CMP UTP Copper Cable
PUR6004BU-UY	TX6™ 10Gig™ CMR UTP Copper Cable
PUP6004BU-UY	TX6™ 10Gig™ CMP UTP Copper Cable
PSR6004**	TX6™ 10Gig™ CMR U/FTP Copper Cable
PSP6004**	TX6™ 10Gig™ CMP U/FTP Copper Cable
PUR6X04BU-UY	High Performance Category 6A riser (CMR) 4-pair UTP copper cable.
PSR6004BU-UGY	Category 6A riser (CMR) 4-Pair U/FTP shielded copper cable.
PUR6004BU-UY	High Performance Category 6 riser (CMR) cable 4-pair UTP copper cable.
PUR5504BU-W	Category 5e riser (CMR) cable 4 pair UTP copper cable.

STP Shielded cable also available.

QuickNet

Panduit Part#	Description
QAPBCBCBXX**	QuickNet Pre-Terminated Cable Assembly construted of Category 6A, UTP, plenum cable (blue) with pre-terminated cassette (blue jacks installed) on each end. ** available in one foot increments in lenghts from 10 feet to 295 feet (Category 6 also available)
QPP24BL	24-Port patch panel which accepts QuickNet Pre-Terminated Cassettes and Patch Panel Adapters

Punchdown System

Panduit Part#	Description
GPKBW**Y	GP6™ PLUS Punchdown System

*** = either 144-Pair (36-Port) or 432-Pair (108-Port)*

Plug to Plug, Plug to Jack Cable Assemblies

Panduit Part#	Description
UAPPBU25	Category 6A UTP solid plenum cable with TX6 PLUS modular Plugs on each end
UAPRBU25	Category 6A UTP solid riser cable with TX6 PLUS modular Plugs on each end
UPPBU25Y	Category 6 UTP solid plenum cable with TX6 PLUS modular Plugs on each end
UPRBU25Y	Category 6 UTP solid riser cable with TX6 PLUS modular Plugs on each end
UAJPBU25BL	Category 6A UTP solid plenum cable with TX6A 10Gig modular plug on one end and a black Mini-Com TX6A 10Gig UTP Jack Module on the other.
UAJRBU25BL	Category 6A UTP solid riser cable with TX6A 10Gig modular plug on one end and a black Mini-Com TX6A 10Gig UTP Jack Module on the other.
UJPBU25BLY	Category 6 UTP solid plenum cable with TX6 PLUS Modular Plugs on one end and a black Mini-Com TX6 PLUS UTP Jack Module on the other.
UJRBU25BLY	Category 6 UTP solid riser cable with TX6 PLUS Modular Plugs on one end and a black Mini-Com TX6 PLUS UTP Jack Module on the other.

Fiber Interconnection

Panduit Part #	Description
FSDR606Y	Opti-Core 6 fiber indoor multimode OFNR riser type distribution cable, 62.5/125µm (OM1)
FSDR606Y	Opti-Core 6 fiber indoor multimode OFNR riser type distribution cable, 50/125µm (OM2)
FODRX06Y	Opti-Core 10gig, 6 fiber indoor multimode OFNR riser type distribution cable, 50/125µm (OM3)
FSDR906Y	Opti-Core 6 fiber indoor singlemode OFNR riser type distribution cable, 9/125µm (OS1)
FSPR606Y	Opti-Core 6 fiber indoor armored multimode OFNR riser type distribution cable, 62.5/125µm (OM1)
FSPR506Y	Opti-Core 6 fiber indoor armored multimode OFNR riser type distribution cable, 50/125µm (OM2)
FOPRX06Y	Opti-Core 10gig, 6 fiber indoor armored multimode OFNR riser type distribution cable, 50/125µm (OM3)
FSPR906Y	Opti-Core 6 fiber indoor armored singlemode OFNR riser type distribution cable, 9/125µm (OS1)
FSCR606Y	Opti-Core 6 fiber indoor/outdoor all-dielectric multimode OFNR riser type distribution cable, 62.5/125µm (OM1)
FSCR506Y	Opti-Core 6 fiber indoor/outdoor all-dielectric multimode OFNR riser type distribution cable, 50/125µm (OM2)
FOCRX06Y	Opti-Core 10gig, 6 fiber indoor/outdoor all-dielectric multimode OFNR riser type distribution cable, 50/125µm (OM3)
FSCR906Y	Opti-Core 6 fiber indoor/outdoor all-dielectric multimode OFNR riser type distribution cable, 9/125µm (OS1)
FSGR606Y	Opti-Core 6 fiber indoor/outdoor armored multimode OFNR riser type distribution cable, 62.5/125µm (OM1)
FSGR506Y	Opti-Core 6 fiber indoor/outdoor armored multimode OFNR riser type distribution cable, 50/125µm (OM2)
FOGRX06Y	Opti-Core 10gig, 6 fiber indoor/outdoor armored multimode OFNR riser type distribution cable, 50/125µm (OM3)
FSGR906Y	Opti-Core 6 fiber indoor/outdoor armored singlemode OFNR riser type distribution cable, 9/125µm (OS1)
FSTN606	Opti-Core 6 fiber outside plant all-dielectric multimode OFNR riser type distribution cable, 62.5/125µm (OM1)
FSTN506	Opti-Core 6 fiber outside plant all-dielectric multimode OFNR riser type distribution cable, 50/125µm (OM2)

Panduit Part #	Description
FOTNX06	Opti-Core 10gig, 6 fiber outside plant all-dielectric multimode OFNR riser type distribution cable, 50/125µm (OM3)
FSTN906	Opti-Core 6 fiber outside plant all-dielectric multimode OFNR riser type distribution cable, 9/125µm (OS1)
FSWN606	Opti-Core 6 fiber outside plant armored multimode OFNR riser type distribution cable, 62.5/125µm (OM1)
FSWN506	Opti-Core 6 fiber outside plant armored multimode OFNR riser type distribution cable, 50/125µm (OM2)
FOWNX06	Opti-Core 10gig, 6 fiber outside plant armored multimode OFNR riser type distribution cable, 50/125µm (OM3)
FSWN906	Opti-Core 6 fiber outside plant armored multimode OFNR riser type distribution cable, 9/125µm (OS1)
FOGPX^^^LNF***B	10 Gig LC to pigtail armored distribution cable with pulling eye on pigtail end and grounding kit for both ends of cable (also available in SM) ^^ is fiber count to 288. *** Length in meters
FOGP9^^^LNF***B	Singlemode LC to LC armored distribution cable with grounding kit for both ends of cable (also available in 10Gig MM) *** length in meters
F^E10-10M*Y	Opticom® Multimode Duplex Patch Cord (various lengths)
FAP*WAQ^^Z	Opticom® Fiber Adapter Panels (FAPs)
CFAPPBL*	Fiber Patch Panel
CM*^^ZBL	MiniCom® Fiber adapter modules
F^^MC*	Opticam Connectors
FODR*^^Y	Fiber Optic Distribution Cable
FCXO-12-Y	QuickNet™ 10Gig™ MTP* Fiber Optic Cassettes, 50/125µm (OM3)
FX12D5-5M1Y	QuickNet™ 10Gig™ MTP* Interconnect Cable Assemblies, 50/125µm (OM3)
FSPX*55F*A	QuickNet™ 10Gig™ MTP* Trunk Cable Assemblies, 50/125µm (OM3), various lengths
FAP*WAQ^^Z	Opticom® Fiber Adapter Panels (FAPs)
CM*^^ZBL	MiniCom® Fiber adapter modules
F^^MC*	Opticam Connectors

Cable Ties

Panduit Part #	Description
HLM-15R0 *	HLM Series 15 Ft. Roll x .330" Width, Black
HLS-75R0 *	HLS Series 75 Ft. Roll x .75" Width, Black
HLB2S-C0 *	100 Pc TAK-TY Stacked Strips, 7" Strip Tie, 0.75" Width, Black
HLS3S-X0 *	HLS Series 12" Strip Tie, Black
HLT2I-X0 *	HLT Series 8" Loop Tie, Black
HLT3I-X0 *	HLT Series 12" Loop Tie, Black
HLTP2I-X12 *	HLTP Series 8" Loop Tie, UL, Plenum UL94V-2 - Maroon
HLSP3S-X12 *	HLSP Series 12" Strip Tie, UL, Plenum UL94V-2 - Maroon
CBOT24K	Cable Bundle Organizing Tool
PRPC13-69 PRPC13-60	Power Outlet Unit Plug Retention Device - Only used with select Panduit Power Outlet Units (Natural and BLK color)
ERT2M-C20	8.5" Elastomeric Cable Tie, Network Cable safe, Weather/UV Resistant, UL94V-0 Flammability Rating
ERT3M-C20	11" Elastomeric Cable Tie, Network Cable safe, Weather/UV Resistant, UL94V-0 Flammability Rating

Fiber Raceway Parts

Panduit Part #	Description
FR4X4**6	FIBERRUNNER 4x4 Solid Wall Channel.
FRHC4**6	FIBERRUNNER 4x4 Snap-On Hinged Cover.
FRBC4X4**	FIBERRUNNER 4x4 QuikLock Coupler.
FRT4X4**	FIBERRUNNER 4x4 Horizontal Tee Fitting.
FRTSC4**	FIBERRUNNER 4x4 Horizontal Tee Cover.
FRFWC4X4**	FIBERRUNNER 4x4 Four Way Cross Fitting.
FRFWCSC4**	FIBERRUNNER 4x4 Four Way Cross Cover.
FRRA4X4**	FIBERRUNNER 4x4 Horizontal Right Angle Fitting.
FRRASC4**	FBERRUNNER 4x4 Horizontal Right Angle Cover.
FREC4X4**	FIBERRUNNER 4x4 End Cap.
FRSP**	FIBERRUNNER Spill-Over Fitting with 2x2 Exit.
FRSP4C**	FIBERRUNNER Spill-Over Fitting with 2x2 Exit Cover for 4x4 Channel.
FBC2X2**	FIBERRUNNER 2x2 QuikLock Coupler.
FIDT2X2**	Single Port Spill-Out t 1.5" ID Split Corrugated Loom Tubing.
FR6TRBN58	FIBERRUNNER QuikLock New Threaded Rod for 5/8" Threaded Rod
FR6TB12	FIBERRUNNER QuikLock Trapeze Bracket
FR6ALB	FIBERRUNNER Adjustable Ladder Rack Bracket
	** Replace with desired color, YL for yellow, BL for Black or OR for Orange

Identification Parts - LS 8E printer items only shown

Panduit Part #	Description
S100X160VAC	Printable Label for 2mm/3mm Fiber Cable Identification
S100X220VAC	Printable Label for MTP Fiber Cable Identification
NWSLC-2Y	Cable identification sleeve for 2mm fiber cable
NWSLC-3Y	Cable identification sleeve for 3mm fiber cable
NWSLC-7Y	Cable identification sleeve for MTP fiber cable
S100X150VAC	Printable Label for Cat 5/6 Copper Cable Identification
S100X225VAC	Printable Label for 10Gig Copper Cable Identification
C100X000VUC-BK	Printable Label for Pathway Identification
H100X044H1C	Printable Label for 2mm/3mm Fiber Cable Identification
H100X084H1C	Printable Label for MTP Fiber Cable Identification
H100X084H1C	Printable Label for Cat 5/6 Copper Cable Identification
H100X084H1C	Printable Label for 10Gig Copper Cable Identification
C100X000VUC-BK	Printable Label for Pathway Identification

2.7 Zone Cabling Enclosure

Network architectures spread out over large areas can benefit from topologies that consolidate network infrastructure closer to the areas where network drops are located. The basic idea is to move infrastructure such as switches and patch panels that might be housed in racks or enclosures in a control room out to the manufacturing cell/area.

This approach, termed a "zone cabling" approach by the cabling industry, can help facilitate a network design that complies with Rockwell Automation and Cisco guidance for cell/area zones concerning segmenting networks for each automation cell to improve performance and robustness. This zone cabling approach has many benefits including cost savings, flexibility for machine moves/changes, and improved availability. To distribute switches, patch panels, POE equipment, and wireless requires designing enclosures with appropriate environmental ratings, security features, wire management, and identification.

The manufacturing zone and the cell/area zones that comprise it are potentially home to several layers of networking including critical automation networks linking PAC systems, FactoryTalk servers, motion control as well as networking required for PCs, displays, and printers that are tied to the business network. These enterprise application interfaces may be co-located near the machines or process line so that the distribution of both of these networks may be efficiently handled by one zone cabling enclosure. A further complication is that there may be network drops for building automation related systems such as security cameras, environmental controls, HVAC or power systems. Thus there may be 2-3 networks co-located in one area. Consolidating the network drops from these different network layers into one zone cabling enclosure can reduce floor space, enclosure costs and maintainability if properly managed. However, this converged approach can result in serious outages and security breaches if not properly secured and organized.

Reference Architectures

Rockwell Automation and Cisco have mapped out reference architectures that meet the specialized needs for network distribution to deliver automation excellence. These architectures describe the connectivity between the Cell and Manufacturing zones at a logical level. In addition to this reference architecture level, the physical layer reference architecture is also crucial. The physical layer architecture refers to the infrastructure required to achieve the connectivity considering data throughput, environment, wiring distances, and availability. A structured, engineered approach is essential for the physical layer to ensure that investments in network distribution deliver optimum output.

Reference Architectures

Rockwell Automation and Cisco have mapped out reference architectures that promote segmenting networks into cell/area zones at a logical level based on PERA models. In addition to this reference architecture level, the physical layer reference architecture for a zone cabling approach is also crucial. The physical layout and component selection for a zone cabling architecture comprised of enclosures and zone cabling is critical for ensuring the desired logical architecture performs with the desired level of performance and availability while also ensuring security and maintainability.

Physical Layout Considerations

Zone enclosures can range in complexity from small enclosures housing one Stratix switch with connectivity to a handful of devices in an area to larger 19” rack systems that consolidate wiring for dozens of control network drops as well as for business system and/or building system drops in the area.

The design principles for a small enclosure leverage control panel design principles utilizing DIN rail devices while the layout for a 19” rack system can employ rack-based patch panels for high-density network wiring management. In either case, it’s advised to design the network infrastructure with security, performance, testability, and maintainability in mind. For control panel based designs, design tools such as Bentley’s promise can enable easy standardization on best practice designs leveraging reference designs. For 19” rack designs, Visio based reference designs for layout of each RU of the rack space with the appropriate patching, POR, Cisco switch or Rockwell Automation Stratix switch can assist in providing designs that leverage best practices for wire management and connectivity.

Network Schematic Analysis

Network schematics are important tools for control engineers and IT personnel to review the physical infrastructure design and component selection. By reviewing the copper and fiber channels implemented in the zone cabling enclosure, the locations where testability, performance and security are concerns can be highlighted and addressed.

This Guide provides a reference schematic layout showing a typical topology with callouts that show where physical security for ports can be applied, where performance decisions on media and connectivity need to be made, and where it’s recommended to install patching for testability of critical fiber or copper links. For industries where redundant networks are common and also have possibilities for sub networks from several vendors, it is crucial to identify and secure these physical links to avoid configuration mistakes during startups and maintenance. Selection of appropriate fiber and copper media that can perform over the distances and environmental factors is key for robust operation. Diverse pathway planning for redundancy across the plant as well as in control plans should be considered. Selecting fiber and copper connectivity solutions engineered for high performance exceeding standard margins reduces risks associated with installation and long term performance. A careful plan for deploying test points will insure that the network distribution meets performance targets before critical startups of equipment where delays can be costly as well as on a periodic basis during preventative maintenance to avoid loss of control during operation.

End-to-End Solution

In summary, a thorough analysis and plan developed for the physical infrastructure for the zone cabling enclosure is key for ensuring its value and performance. Use of reference architectures that leverage best practice physical infrastructure approaches for zone cabling enclosures and cabling will result in cost savings, flexibility and improved performance and security. This guide provides information on selecting, installing, testing, and documenting this critical physical infrastructure for all levels of this zone cabling architecture.

Network Distribution Physical Infrastructure

This section defines the sequence of actions involved with deploying a physical infrastructure for a zone cabling enclosure system.

1. Logical Design

Define the Logical Architecture

Define the logical architecture governing the layout of industrial systems and active devices. The logical architecture should be based on based on logical layer reference architectures developed by Rockwell Automation and Cisco, as well as on applicable topology diagrams.

2. Physical Design

Map Device Locations to Identify Physical Infrastructure Reach, Noise, Bonding/Grounding Requirements

Map out the physical locations of servers, switches, enclosures, rack systems and control panels. This step provides the opportunity to identify distributed (i.e., "zone cabling") topologies and plan out required patching, test point, and security considerations. Physically layout the zone cabling enclosure with switches, patching, and PoE devices, as required.

This step provides the opportunity to identify distributed zone cabling topologies and plan out required patching, test point, and security considerations.

3. Detail Design

Develop Network-Level Schematic Diagram Identify Exact Physical Infrastructure Components

Develop a network-level schematic diagram (or use a reference diagram) to identify the exact physical layer components required to deploy the Ethernet network. These components include number of patch cords and horizontal links, patching fields, bonding and grounding elements, labeling and identification schemes, cable management tools, and safety and security tools.

NOTE: Steps 2 and 3 are often done concurrently.

4. Review the levels of the architecture in the diagram and identify solutions to address your system needs.

5. Review the recommended solution component List of Materials and specify your infrastructure.

1. Logical Design

Define the Logical Architecture

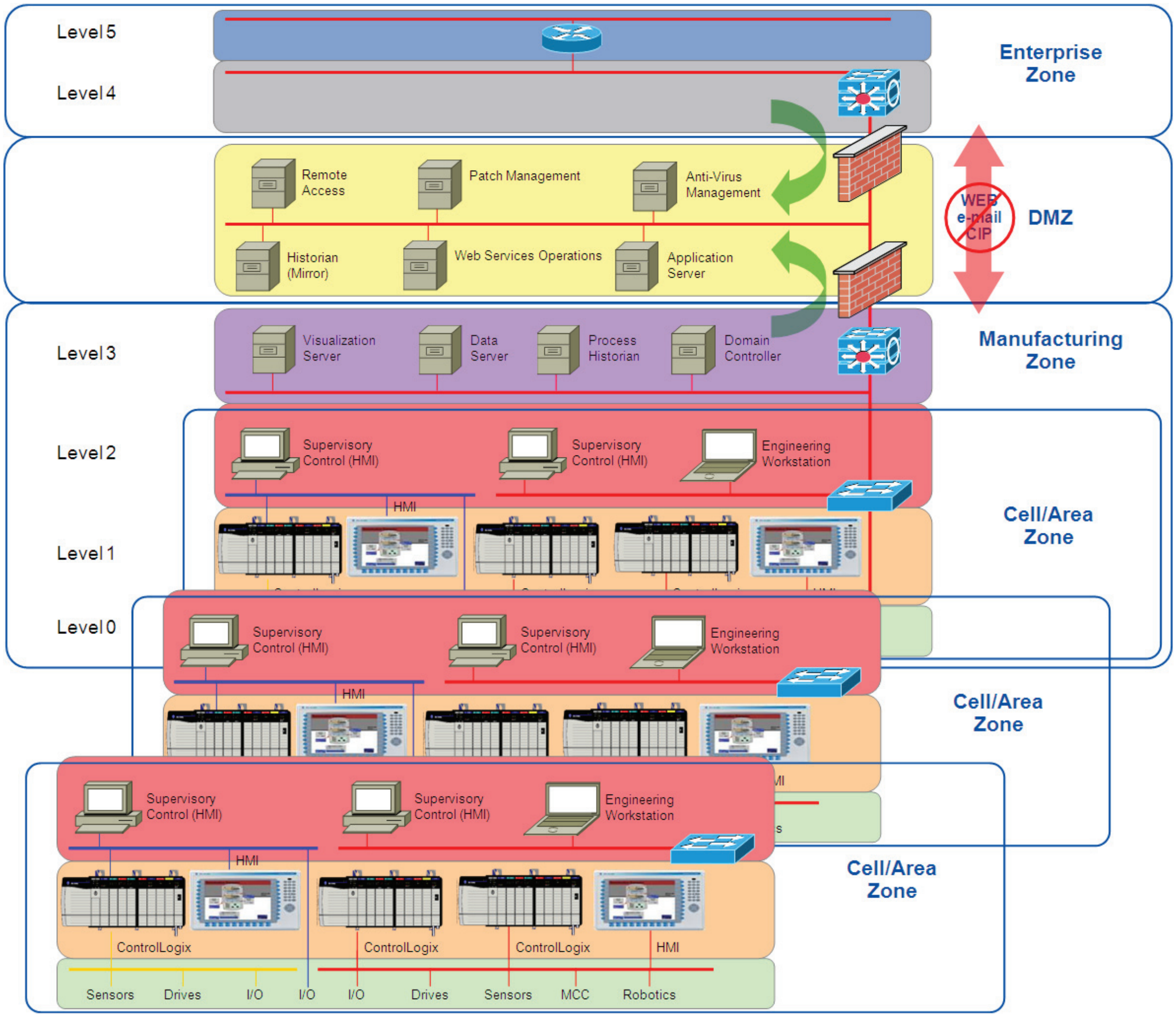


Fig 2.7-1 Logical Diagram for Network Zones

2. Physical Design

Map Device Locations to Identify Physical Infrastructure
Reach, Noise, Bonding/Grounding Requirements

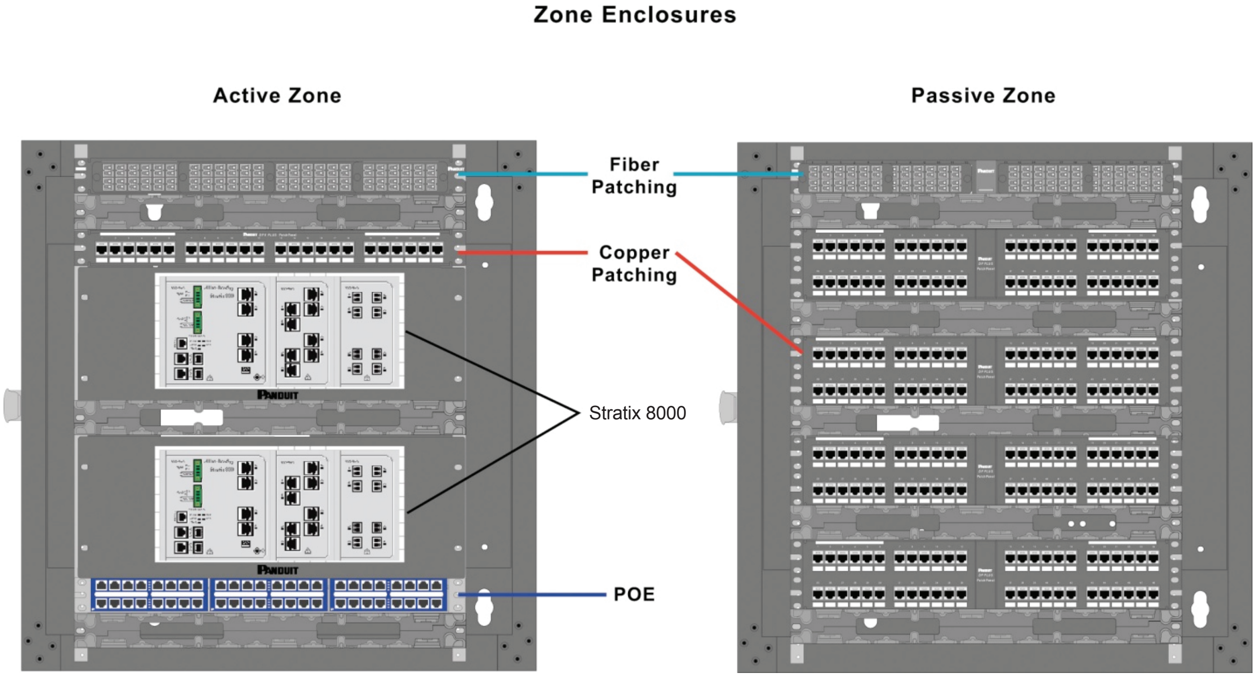


Fig 2.7-2 Physical Diagram for Zone Cabling Enclosure

- Enclosure systems designed for optimum cable management for fiber and copper connectivity while allowing for proper thermal management of critical servers and switches.

- Color coded and keyed solutions to segregate and control patching to avoid inadvertent patching mistakes that bypass DMZ firewalls that separate office and control networks.

- Grounding and bonding to equipment to mitigate risks to communication disruptions

\- Enhanced security with keyed jacks, lock in and block-connectivity

3. Detail Design

Develop Network-Level Schematic Diagram Identify Exact Physical Infrastructure Components

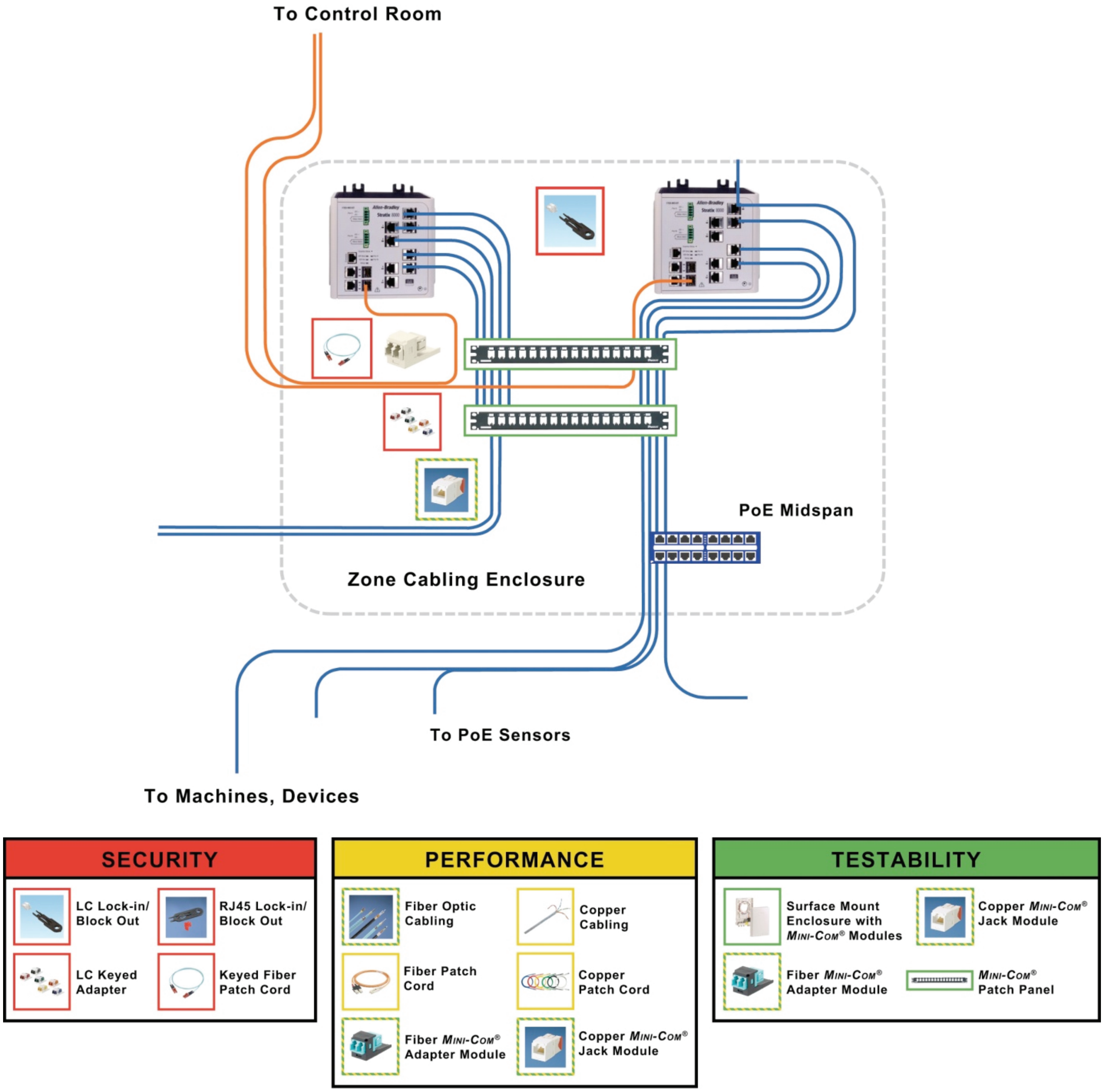


Fig 2.7-3 Detail diagram for zone cabling enclosure

4. *Review the Levels of the Architecture in the Diagram and Identify Solutions to Address Your System Needs.*

Zone Area Physical Infrastructure	Zone Issues	Panduit Solution
Zone Cabling	Security: Control of ports	Color coded fiber and copper jacks or keyed connectivity solutions can provide means to segregate critical systems
	Performance: Distance, Throughput	Fiber and 10GB copper connectivity solutions
	Performance: Throughput, Latency	Connectivity solutions that exceed standards for copper and fiber connectivity. Pre-tested patch cords deliver long term performance, reducing risk
	Maintainability: Access	Ceiling enclosures, racks, panels ideal for mainframe or array storage
	Maintainability: Cabling	Pre-terminated MTP cassettes, fiber adapter panel (FAP), or fiber optic adapter modules and their associated trunk cables, interconnect cables, connectors and patch cords
	Mixture of Office and IE network	Color coded, keyed jacks can prevent crossing networks inadvertently. Lock-in connectors can secure connections in switches or patching to control who can make changes
	Testability: Verify during startup, preventative maintenance	Patching for testing fiber, copper uplinks and critical external connections. Pre-tested copper and fiber patch cords to mitigate risks

5. *Review the Recommended Solution Component List of Materials and Specify your Infrastructure:*

Server Cabinets, Ethernet enclosures and accessories

Panduit Part#	Description
CS1	Server cabinet frame with top panel. Single hinge perforated front door. Two sets of cage nut equipment mounting rails. 45 RU cable management on rear of rear posts. One set of POU mounting brackets. Dimensions: 84.0"H x 31.5"W x 41.1"D (2134mm x 800mm x 1044mm)
CN1	Switch cabinet frame with top panel. Dual hinge perforated front door. Two sets of #12-24 tapped equipment mounting rails. 45 RU cable management on rear of rear posts. Dimensions: 84.0"H x 31.5"W x 41.1"D (2134mm x 800mm x 1044mm)
CMR19X84	2 Post Patching Rack with space identification Double-sided #12-24 EIA universal mounting hole spacing. 24 #12-24 mounting screws included. Paint piercing washers included.
DPFP4	4RU filler panels. Direct airflow in cabinet applications. Mount to standard EIA 19" racks or cabinets. #12-24 and M6 mounting screws included
NM1	Front and rear 1RU horizontal cable manager. Mount to 19" EIA racks and cabinets. Covers, #12-24 and M6 mounting screws included. Design fits flush to the front of the NetRunner™ High Capacity WMPVHCF45E and WMPVHC45E Vertical Managers
NMF2	Front only 2RU horizontal cable manager. Mount to 19" EIA racks and cabinets. Covers, #12-24 and M6 mounting screws included. Design fits flush to the front of the NetRunner™ High Capacity WMPVHCF45E and WMPVHC45E Vertical Managers
NMF4	Front only 4RU horizontal cable manager. Mount to 19" EIA racks and cabinets. Covers, #12-24 and M6 mounting screws included. Design fits flush to the front of the NetRunner™ High Capacity WMPVHCF45E and WMPVHC45E Vertical Managers
PRV8	8 inch wide vertical cable manager, includes four PRSP7 slack spools. Dimensions: 83.9"H x 8.0"W x 16.4"D(2131mm x 203mm x 417mm)
PRV6	6 inch wide vertical cable manager, spools are not included. Dimensions: 84"H x 6"W x 16.4"D. (2133.6mm x 152.4mm x 416.6mm)
PRD8	8 inch wide dual hinged metal door. Dimensions: 82.8"H x 8.1"W x 1.6"D(2104mm x 206mm x 40mm)
PRD6	6 inch wide dual hinged metal door. Dimensions: 82.8"H x 6.1"W x 1.6"D(2104mm x 206mm x 40mm)
IAEIP66	Industrial Ethernet enclosure 18.50"H x 18.50"W x 8.00"D, supplied with 115/230V to 24Vdc Power Supply. Ip 66/Nema 4x rated.
IAECGP	Industrial Ethernet gland plate, with 14 industrial ethernet bulkhead fittings and patch cords. Attaches to IAEIP66 enclosure.
IAEFKSC	Industrial Ethernet SC fiber uplink kit. Terminates 4 SC connectors to two duplex fiber uplinks.
PZAEWM3	PanZone Active wall enclosure, 38.50"H x 27.92"W x 8.61"D
PZAEGK	Structured Ground kit for PanZone enclosure.
PZC12S	PanZone Wall mount cabinet for consolidation, 25.81"H x 25" W x 22.85"D
PZWIFIN	Wireless Access Point, for Cisco Aironet, 13.75"H x 12"W x 4.75"D
PZNWE12	Wireless Access Point for Cisco Aironet, 13.56"H x 13.47"W x 6.56"D, Nema 4x/IP 66 rated.
PZNWE12S	Wireless Access Point for Cisco Aironet, 13.56"H x 13.47"W x 6.56"D, Nema 4x/IP 66 rated. Includes shielded connectivity kit for POE (power over ethernet) applications.
PRD6	6 inch wide dual hinged metal door. Dimensions: 82.8"H x 6.1"W x 1.6"D(2104mm x 206mm x 40mm)

Copper Cables/Connectors/Patch/Assemblies

Jack Modules

Panduit Part#	Description
CJ6X88TG*	Mini-Com® TX6™ 10Gig™ UTP Jack Module
CJK6X88TG*	Keyed Mini-Com® TX6™ 10Gig™ UTP Jack Module
CJ688TG*	Mini-Com® Category 6, RJ45, 8-position, 8-wire universal jack module.
CJK688TG*	Keyed Mini-Com® Category 6 UTP Jack Module
	* add suffix IW (Off White, EI (Electric Ivory), WH (White), IG (International Gray), BL (Black), OR (Orange), RD (Red, BU (Blue), GR (Green), YL (Yellow) or VL (Violet). STP Shielded Jacks also available.

Patch Cords

Panduit Part#	Description
UTP6A^**	TX6™ 10Gig™ UTP Patch Cords
UTPK6A^**	Keyed TX6™ 10Gig™ UTP Patch Cords
UTPSP*M**Y	Category 6 UTP Patch Cord with TX6 Plus Modular Plugs on each end, meter lengths.
UTPKSP*^	Keyed Category 6 UTP Patch Cord for use with matching Keyed Copper Jack Module. Patch cords contain one keyed RJ45 Plug on one and to a Standard RJ45 Plug on the other.

Patch Panels

Panduit Part#	Description
DP**6X88TGY	DP6™ 10Gig™ Modular Punchdown Patch Panel
DPA**6X88TGY	DP6™ 10Gig™ Angled Modular Punchdown Patch Panel
DP**688TGY	DP6™ Category 6 Modular Punchdown Patch Panel
DPA**688TGY	DP6™ Category 6 Angled Modular Punchdown Patch Panel
CPP**FMWBLY	Mini-Com® 1RU 24-Port flush mount modular patch panel supplied with rear mounted faceplates: For use with CJ688TG* Category 6 Jack Modules
CPPA48HDWBLY	48-Port angled high density patch panel supplied with rear mounted faceplates (space not available for component labels)
	** = Number of Jack Ports 24 or 48 24 = 1RU Rack Space 48 = 2RU Rack Space
CBXD6BL-AY	Surface mount box accepts six Mini-Com® Modules. Provides slots that accept cable ties for strain relief. Provides bend radius control. Supplied with label holder/screw cover.

QuickNet

Panduit Part#	Description
QAPBCBCBXX**	QuickNet Pre-Terminated Cable Assembly construted of Category 6A, UTP, plenum cable (blue) with pre-terminated cassette (blue jacks installed) on each end. ** available in one foot increments in lengths from 10 feet to 295 feet (also available in Category 6 version)
QPP24BL	24-Port patch panel which accepts QuickNet Pre-Terminated Cassettes and Patch Panel Adapters (48 port also available)

Plug to Plug, Plug to Jack Cable Assemblies

Panduit Part#	Description
UAPPBU25	Category 6A UTP solid plenum cable with TX6 PLUS modular Plugs on each end
UAPRBU25	Category 6A UTP solid riser cable with TX6 PLUS modular Plugs on each end
UPPBU25Y	Category 6 UTP solid plenum cable with TX6 PLUS modular Plugs on each end
UPRBU25Y	Category 6 UTP solid riser cable with TX6 PLUS modular Plugs on each end
UAJPBU25BL	Category 6A UTP solid plenum cable with TX6A 10Gig modular plug on one end and a black Mini-Com TX6A 10Gig UTP Jack Module on the other.
UAJRBU25BL	Category 6A UTP solid riser cable with TX6A 10Gig modular plug on one end and a black Mini-Com TX6A 10Gig UTP Jack Module on the other.
MPSI588T	Category 5e, RJ45 shielded industrial plug with protective cover
IUTPCH*BLY	Category 5e UTP patch cord constructed of industrial grade UTP category 5e solid cable with dust caps
ISTPCH*MBLY	Category 5e STP patch cords constructed of industrial grade STP category 5e solid cable with dust caps

IndustrialNet Products

Panduit Part#	Description
IAEBH5E	Category 5e, RJ45, 8-position, 8-wire black industrial connector with protective cover
IAEBH5ES	Category 5e, RJ45, 8-position, 8-wire shielded black industrial connector with protective cover
IAEBH6	Category 6, RJ45, 8-position, 8-wire black industrial connector with protective cover
IAEBH6S	Category 6, RJ45, 8-position, 8-wire shielded black industrial connector with protective cover
IAEBHC6	Category 6, RJ45, 8-position, 8-wire black industrial bulkhead coupler with protective cover
IEABHC5E	Category 5e, RJ45, 8-position, 8-wire black industrial bulkhead coupler with protective cover
MPI588T	Category 5e, RJ45 industrial plug with protective cover
MPSI588T	Category 5e, RJ45 shielded industrial plug with protective cover
IUTPCH*BLY	Category 5e UTP patch cord constructed of industrial grade UTP category 5e solid cable with dust caps
ISTPCH*MBLY	Category 5e STP patch cords constructed of industrial grade STP category 5e solid cable with dust caps

Fiber Products

	Zone Cabling Enclosure
Panduit Part#	**Description**
F^E10-10M*Y	Opticom® Multimode Duplex Patch Cord (various lengths). Replace ^ with X for 10Gig, 5 for 50/125um (OM2), 6 for 62.5/125um (OM1) or 9 for 9/125um (OS1). Replace the numbers for specific connector type 10 = LC, 2 = ST, 3 = SC. * implies length. Can be ordered in any hybrid configuration.
FAP*WAQ^^Z	Opticom® Fiber Adapter Panels (FAPs). Replace * with number of ports required (4, 6, 8, 12). AQ designates 10G Aqua color, also available in other colors to designate fiber type and keying solutions. Available in ST, SC, LC, and Keyed LC. Available with zirconia ceramic or phosphorous bronze split sleeves.
CFAPPBL*	Fiber Patch Panel. Replace * with one or two depending on how many FAPs or cassettes are necessary.
CM*^^ZBL	MiniCom® Fiber adapter modules. Replace * with a D or S for single or duplex, ^^ with color (dependent on fiber type) and delete the Z for phosphorous bronze sleeves.
F^^MC*	Opticam Connectors. Fiber optic connectors. Replace ^^ with connector type (LC, Keyed LC, SC, or ST). Replace * with color (AQ, BL, EI)
FODR*^^Y	Fiber Optic Distribution Cable. Replace * with X-10Gig, 5 for MM (OM2), 6 for MM (OM1) and 9 for SM. Replace ^^ with fiber count (6,12,24,36,48,72,96,144,216,288)
FCXO-12-Y	QuickNet™ 10Gig™ MTP* Fiber Optic Cassettes, 50/125µm (OM3). Available in MM (OM2), MM (OM1) and SM (OS1) and in 6, 12 or 24 fiber options
FX12D5-5M1Y	QuickNet™ 10Gig™ MTP* Interconnect Cable Assemblies, 50/125µm (OM3). Replace X with, 5 for MM (OM2), 6 for MM (OM1) and 9 for SM (OS1) . Replace 5-5 (LC - LC) with connectors required: 2-ST, 3-SC
FSPX*55F*A	QuickNet™ 10Gig™ MTP* Trunk Cable Assemblies, 50/125µm (OM3), various lengths. Replace X with, 5 for MM (OM2), 6 for MM (OM1) and 9 for SM (OS1)
FAP*WAQ^^Z	Opticom® Fiber Adapter Panels (FAPs). Replace * with number of ports required (4, 6, 8, 12). AQ designates 10G Aqua color, also available in other colors to designate fiber type and keying solutions. Available in ST, SC, LC, and Keyed LC. Available with zirconia ceramic or phosphorous bronze split sleeves.
CM*^^ZBL	MiniCom® Fiber adapter modules. Replace * with a D or S for single or duplex, ^^ with color (dependent on fiber type) and delete the Z for phosphorous bronze sleeves.
F^^MC*	Opticam Connectors. Fiber optic connectors. Replace ^^ with connector type (LC, Keyed LC, SC, or ST). Replace * with color (AQ, BL, EI)

Cable Ties

Panduit Part#	Description
HLM-15R0 *	Hook and Loop HLM Series 15 Ft. Roll x .330" Width, Black
HLS-75R0 *	Hook and Loop HLS Series 75 Ft. Roll x .75" Width, Black
HLB2S-C0 *	100 Pc TAK-TY Stacked Strips, 7" Strip Tie, **0.75" Width, Black**
HLS3S-X0 *	HLS Series 12" Strip Tie, Black
HLT2I-X0 *	HLT Series 8" Loop Tie, Black
HLT3I-X0 *	HLT Series 12" Loop Tie, Black
HLTP2I-X12 *	HLTP Series 8" Loop Tie, UL, Plenum UL94V-2 - Maroon
HLSP3S-X12 *	HLSP Series 12" Strip Tie, UL, Plenum UL94V-2 - Maroon
ERT2M-C20	8.5" Elastomeric Cable Tie, Network Cable safe, Weather/UV Resistant, UL94V-0 Flammability Rating
ERT3M-C20	11" Elastomeric Cable Tie, Network Cable safe, Weather/UV Resistant, UL94V-0 Flammability Rating

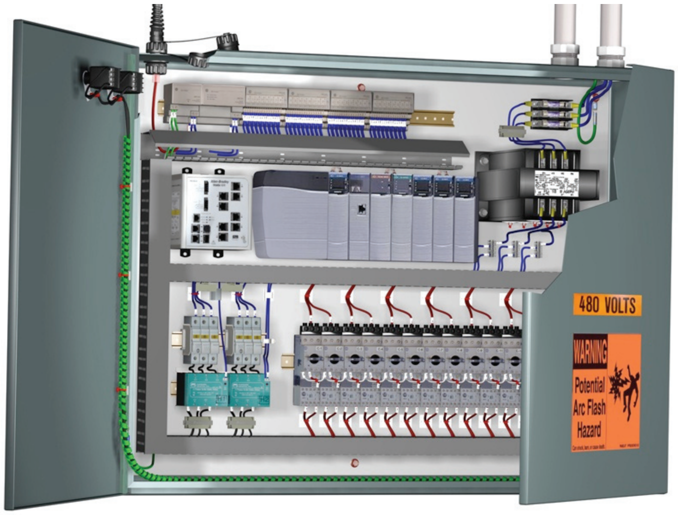
Safety/Security Parts

Panduit Part #	Description
PSL-DCPL	Package of 10 RJ45 Plug Lock-In Devices and one installation/removal tool -- for standard jacks
PSL-DCPLR	Package of 10 RJ45 Plug Lock-In Devices and one installation/removal tool -- for recessed jacks
PSL-DCJB	Package of 10 RJ45 Blockout Devices and one installation/removal tool
PSL-LCAB	Package of 10 LC Duplex Adapter Blockout Device and one installation/removal tool
FLCCLIW-X	Package of 10 LC Duplex Lock-In Clips and one removal tool

Identification Parts - LS 8E printer items only shown

Panduit Part #	Description
C200X100YPC	Printable Label for Enclosure Identification
S100X160VAC	Printable Label for 2mm/3mm Fiber Cable Identification
S100X220VAC	Printable Label for MTP Fiber Cable Identification
NWSLC-2Y	Cable identification sleeve for 2mm fiber cable
NWSLC-3Y	Cable identification sleeve for 3mm fiber cable
NWSLC-7Y	Cable identification sleeve for MTP fiber cable
S100X150VAC	Printable Label for Cat 5/6 Copper Cable Identification
S100X225VAC	Printable Label for 10Gig Copper Cable Identification
T100X000VPC-BK	Printable Label for Fiber Port Identification
C252X030FJC	Printable Label for Copper 4 Port Identification
C379X030FJC	Printable Label for Copper 6 Port Identification

2.8 Control Panel Area



Control Panels are the enclosures that protect automation components in a rugged NEMA rated enclosure specified for targeted environment. Control panels can vary greatly in size and construction depending on the size, power rating, and application requirements. However, one common control panel need that has developed is for recommended best practices for installing the critical control panel Ethernet switch and associated fiber and copper which provide connectivity to devices internal to and connected from the control panels.

This Ethernet physical infrastructure internal to the control panel is critical to the performance of the automation system as Ethernet is now used for control and device level communications as well as for information level and safety level. The control panel environment can be hostile to networking and can present very real problems with communication disruptions or device failure so it is important to follow best practices for noise mitigation in control panel designs. The design of the physical infrastructure needs to ensure the performance, security, and maintainability in an environment that can have serious EMI, thermal, and space challenges.

Key considerations for panel layout to mitigate noise issues include:

1. Grounding and Bonding

Grounding and bonding is the foundation for controlling EMI in control systems. Use of galvanized back panels and low impedance braided bonding straps provide a ‘ground plane’ that has low impedance for high frequency noise currents. This low impedance helps prevent noise from polluting network communications

2. Separation and Segregation

One of the easiest and least expensive ways to prevent noise problems is to lay out the control panel using segregation and separation techniques. Segregation and separation is the practice of physically separating noisy circuits and devices from potential victims. When creating a panel layout, it is best to identify physical areas in the panel for clean and noisy circuits. The areas are defined by how much noise is generated and the sensitivity of the devices and circuits to noise. Two to three areas are created in each panel, depending on the application:

- Very Noisy / Dirty (Right Side of the enclosure)
- Noisy/ Dirty (Right Side of the Enclosure)
- Clean / Sensitive (Left Side of the Enclosure)

Higher voltage devices should be mounted in the upper right-hand corner of the panel keeping as much distance as possible between the high voltage devices and any electronic devices such as Programmable Automation Controllers (PACs), DC power supplies, and timers that should ideally be on the opposite left side of the panel. Also maintain distance between motor power and encoder, I/O, and analog cables.

3. Filters and Suppression

Filters are used both to clean up signals or power entering the panel as well as to prevent noise from a noise source from spreading within the panel. Install close to noise source or panel entrance to minimize length of unfiltered cable in the panel. Avoid bundling line side and load of filter together so noise does not couple back from the dirty side to the clean side. Suppressors are also used to redirect unwanted energy to inhibit noise coupling to sensitive circuits. They are recommended to be used across dry contacts or inductive loads to short circuit the energy stored in relay or solenoid coils rather than allowing high voltage noise spikes to be developed. The noise spikes from opening a large coil can easily reach hundreds or thousands of volts and present a very real noise source that should be suppressed at its source.

Physical Layout Considerations for Industrial Ethernet in Control Panels

Industrial network planning for control panels requires more thought today than in the past. With the increase of industrial networking applications, special considerations are warranted to maximum protection from noise. Network cables should be carefully segregated from noisy and very noisy components, conductors, and zones.

The key considerations for layout of Ethernet switches and cabling systems in a control panel include:

- Panel space for Ethernet switch, patching, and cable management
- Media and connector selection
- Design for testability, maintainability, safety
- Use of design tools

Panel space for Ethernet switch, patching, cable management. Proper space allocation provides important benefits for noise immunity for the switch as well as for the cabling. The cabling needs to be routed away from noise sources while also following recommended bend radius control. NEC/NFPA 70 Article 800.133A recommends communication wires and cables be separated at least 50 mm (2 in.) from conductors. For fiber, provide panel space for installing fiber patching with slack management. For copper cables that need to leave panel, it is recommended to install patching so that the link can be tested.

Many cabinets can accommodate a side panel which can provide adequate spacing for a well executed industrial networking layer (see Figure 2.8-1). Use of wire management products that maximize use of panel corners can provide additional back panel or side panel space as well as improve wire management and cable segregation. Note that locating the Ethernet switch and patching well away from any power devices or live conductors can improve safety for any qualified technician working in the control panel. Inadvertent contact with high voltage is a cause of arc flash events or electrical shock events that are life threatening as well as costing industry millions a year in damages and litigation.

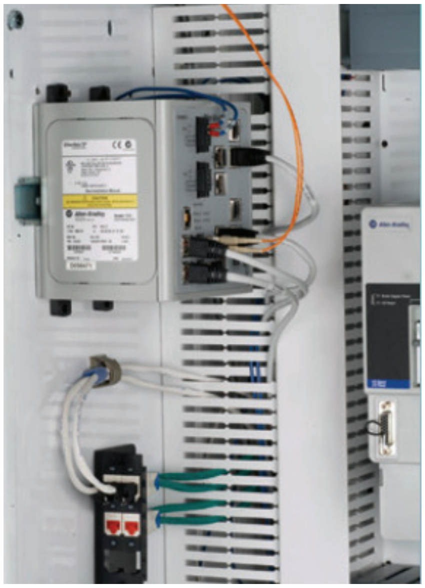
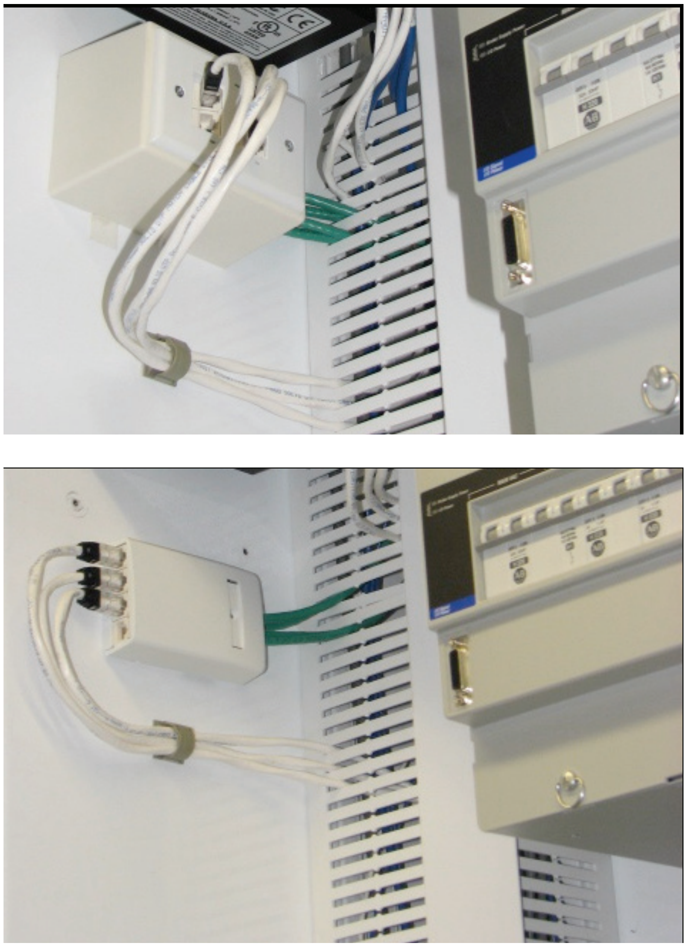


Figure 2.8-1. Ethernet Switch and Panduit Patch Panel mounted on Side Plane with PANDUIT PanelMax™ Corner Duct



Avoid deforming the Ethernet cable by cinching too tight with cable ties. Deforming the cable can cause increased return loss and unbalance in the cable resulting in more noise pick up.

Media and Connector Selection: Copper Cabling.

Installation of copper Ethernet cabling near control panel noise sources increases potential for common mode noise coupling that can result in bit errors and delays. Common-mode noise is the voltage that can develop on the entire LAN channel with respect to ground. Since Ethernet cabling system uses differential mode signaling, the voltage difference within the two wires in a twisted pair defines the signal so common mode noise should be subtracted out and not cause a problem.

Figure 2.8-2 illustrates the allowed coupled common mode noise signal in a 1000Base-T and 100Base-T system for a 100 meter channel. Note that 100Base-T cable cannot tolerate more than 0.5 volt of noise coupling near 100 MHz with the 1000BaseT tolerating much less only 0.1 V. A VFD, servo, or inductive load with spikes in hundreds of volts could easily couple in noise at these low levels leading to disrupted communications.

The balance of twisted pair cables and RJ45 connectors is key to preventing common mode noise from being converted to differential mode noise that corrupts communication (see Figure 2.8-3). If the balance is perfect, then the differential mode measurements will be equal on both conductors of the twisted pair and thereby cancel out imposed noise. Not all manufacturers design their connectors for optimized balance so it is important to review this critical specification when choosing a connector as well as patch cable vendor.

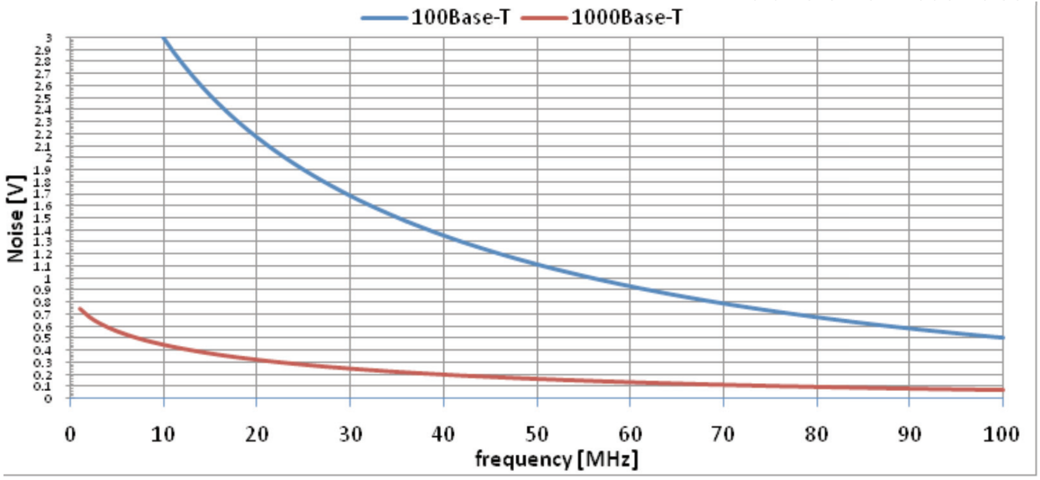


Figure 2.8-2. Coupled Noise on Ethernet

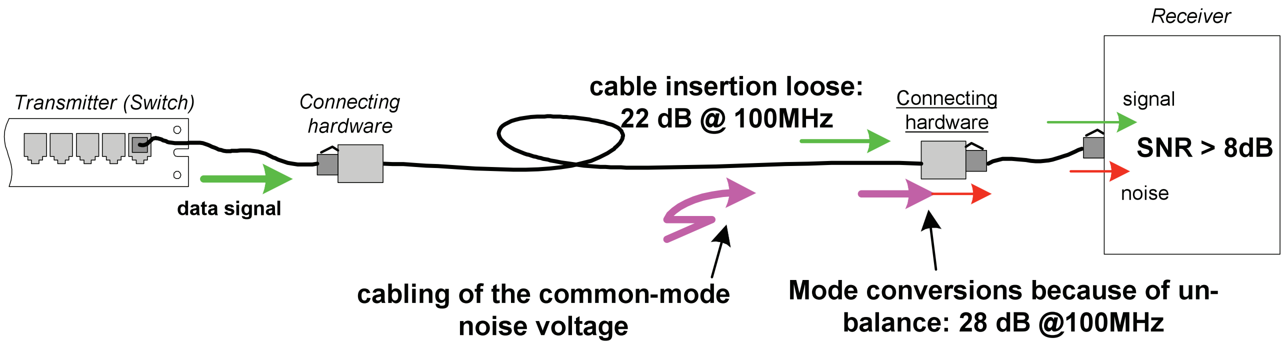

Receiver
Transmitter (Switch)
Connecting hardware
cable insertion loose: 22 dB @ 100MHz
Connecting hardware
signal
SNR > 8dB
noise
data signal
cabling of the common-mode noise voltage
Mode conversions because of un-balance: 28 dB @100MHz

Figure 2.8-3. Signal and Noise Routing Diagram.

In practice, a completely balanced system is unachievable and a level of imposed noise is observed on one of the two conductors. The CMRR (Common-Mode Rejection Ratio) of a cabling system is a ratio, articulated in dB, of common-mode noise rejected and prevented from converting to a differential mode voltage. IEEE and EIA/TIA defies the minimum requirements for CMRR in term of TCL and TCTL which are power ratio measurements characterizing unbalance from transmit and receive ends.

Infrastructure design techniques that can improve noise rejection include maintaining proper bend radius and separation distance between conductors, avoiding over-tightened cable ties, using shielded cables where possible, observing good bonding practices for shielded and motor cables, and ensuring cable and connector balance using best-in-class vendor connectivity solutions that exceed standards specifications. The key for unshielded copper performance is to select connectivity with superior balance that exceeds standard margins to minimize risks.

Tips for Industrial Ethernet

The following are key considerations that can improve noise rejection.

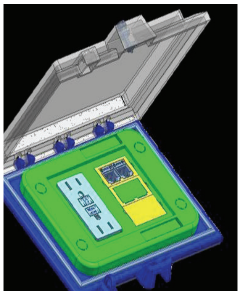
- Separation distance from conductors
- Cable balance
- Connector selection
- Maintain proper bend radius
- Avoid over tightened cable ties
- STP use where possible
- Shielding bonding for STP
- Good motor cable bonding practice
- Exceed standard connector and cabling specs

Media and Connector Selection: Copper Cabling

Fiber inherently provides noise immunity and supports longer runs than copper media. Internal to the control panel, more devices are supporting direct fiber connectivity. PANDUIT offers modular pre-tested patch cords that can transition for legacy fiber cable that may already be in your control panel area. For example, patch cords and surface mount boxes that would allow transitioning from SC to LC connectors required for the Stratix switch interface.

Pre-polished termination solutions and application tools provide the ability to terminate fiber in the field without adhesive or polishing using an easy to use tool that provides visual indication that a quality termination was made. Electricians can be easily trained to install fiber rather than relying on outside specialists.

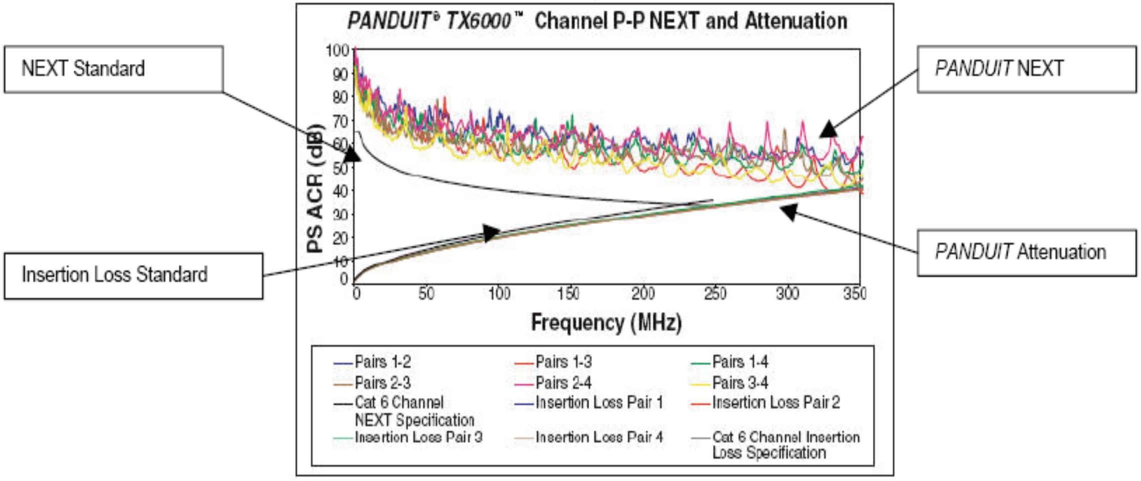
Design for Testability, Maintainability, Safety.



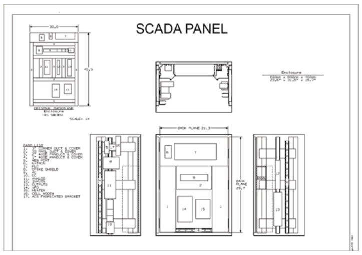
Testability refers to the ability to verify that the network links are functional and can pass tests indicating that they meet the intended category or performance margin targets. A best practice recommendation is to install patching locations in the control panel so that these critical links can be tested after installation and on periodic basis to insure performance. The identification of cables, ports, devices, and panels are key for maintainability. The identification aids in cross-referencing to documentation and in interpreting/documenting test results.

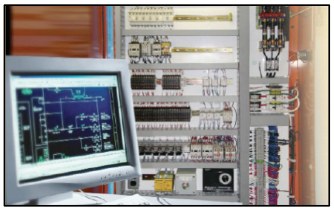
As control panels grow more sophisticated network-wise and may require collaboration from controls and IT people during troubleshooting and commissioning, it's important to not lose sight of safety. Control panels can house dangerous voltages and arc flash hazards that endanger life and limb. NFPA and OSHA regulations require that only qualified electricians are allowed access to the control panel due to these extreme hazards. An important safety tool in minimizing this risk is a data access port that provides safe access to a network port and utility outlet without opening the control panel. Due to the dynamic nature of control panel devices and network connectivity that changes over time, a data access port that is modular and can be field upgraded offers advantages in preserving its utility and safety function.

Graph 2



Use of Design Tools





Using reference designs and design tools can greatly aid the control panel designer to conform to best practices to achieve desired system life cycle cost savings. Reference designs can include preferred arrangements for devices PLCs, drives, power supplies, filters as well as for the critical physical infrastructure of the control panel. The guidance for a 'defense in depth' for noise mitigation is spelled out in these reference designs where the control vendor shows recommendations for the critical bonding, grounding scheme for the system. These reference designs detail how to lay out clean and dirty wireways in the control panel to avoid noise coupling by providing recommended spacing between different classes of conductors. There are also recommendations for shielded cable practice as well as filter location and wiring guidance.

Templates and Design tool area	Related Standards, Information
Noise mitigation layout	IEEE 1100 Chapter 10 Rockwell Automation GMC-RM001_-en-p.pdf
Industrial network practice	ODVA PUB00035R0_Infrastructure_Guide.pdf ODVA PUB00148R0_EtherNetIP_Media_Planning_and_Installation_Manual.pdf
Panel Layout Design tools	UL508A Industrial control panels http://www.bentley.com/en-US/Products/promise/Product-Resources.htm

Reference designs for industrial networking layer practice in control panels are also available to provide examples of best practice recommendations for an industrial Ethernet layer designed for performance, testability, reliability and maintainability (see Figure 2.8-4). Cisco and Rockwell have provided design guides as well as organizations such as ODVA. Design tools such as Bentley's promisE provide control panel design tools with the ability for the user to develop their own template referencing the best practices for their industry and vendor list. This layout tool includes 3 D images of devices along with ability to layout wireways and cable routing. Thus you can leverage template designs that include all factors for good noise mitigation.

Network Schematic Analysis

Industrial Ethernet implementations can leverage off of the experience of traditional office Ethernet by partnering with IT. This leads to an opportunity to apply best practices from the IT world in conjunction with process control system knowledge. The ideal is a partnering between IT and controls groups. One approach is development of 'hybrid' IT and engineering resources with skills to be able to make key decisions on network architectures and physical infrastructure component selection.   The 'hybrid' resource can come from either the IT or control groups. One of the primary tasks is to review a schematic layout of the network distribution to ensure security, performance and testability for each layer of the design.

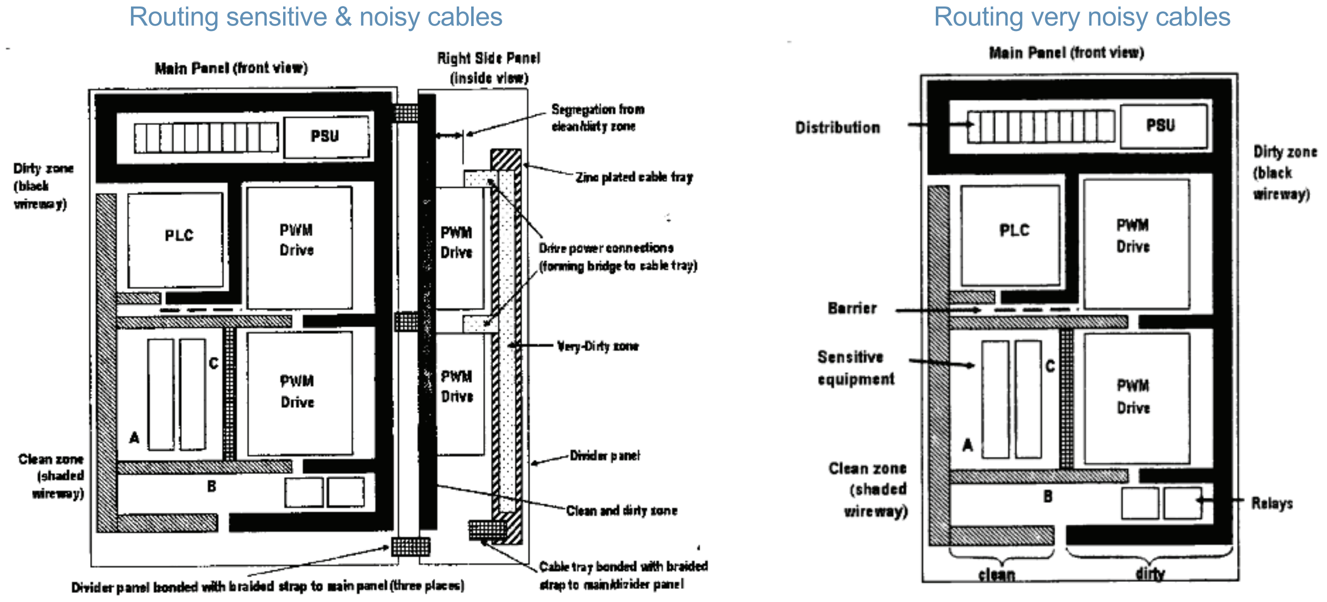

Routing sensitive & noisy cables
Main Panel (front view)
Right Side Panel (inside view)
Segregation from clean/dirty zone
Zinc plated cable tray
Dirty zone (black wireway)
PSU
PLC
PWM Drive
PWM Drive
Drive power connections (forming bridge to cable tray)
Very-Dirty zone
C
PWM Drive
PWM Drive
A
Divider panel
Clean zone (shaded wireway)
B
Clean and dirty zone
Cable tray bonded with braided strap to main/divider panel
Divider panel bonded with braided strap to main panel (three places)
Routing very noisy cables
Main Panel (front view)
Distribution
PSU
Dirty zone (black wireway)
PLC
PWM Drive
Barrier
Sensitive equipment
C
PWM Drive
A
Clean zone (shaded wireway)
B
Relays
clean
dirty

Figure 2.8-4. Examples of Reference Designs (IEEE 1100 Emerald Book)

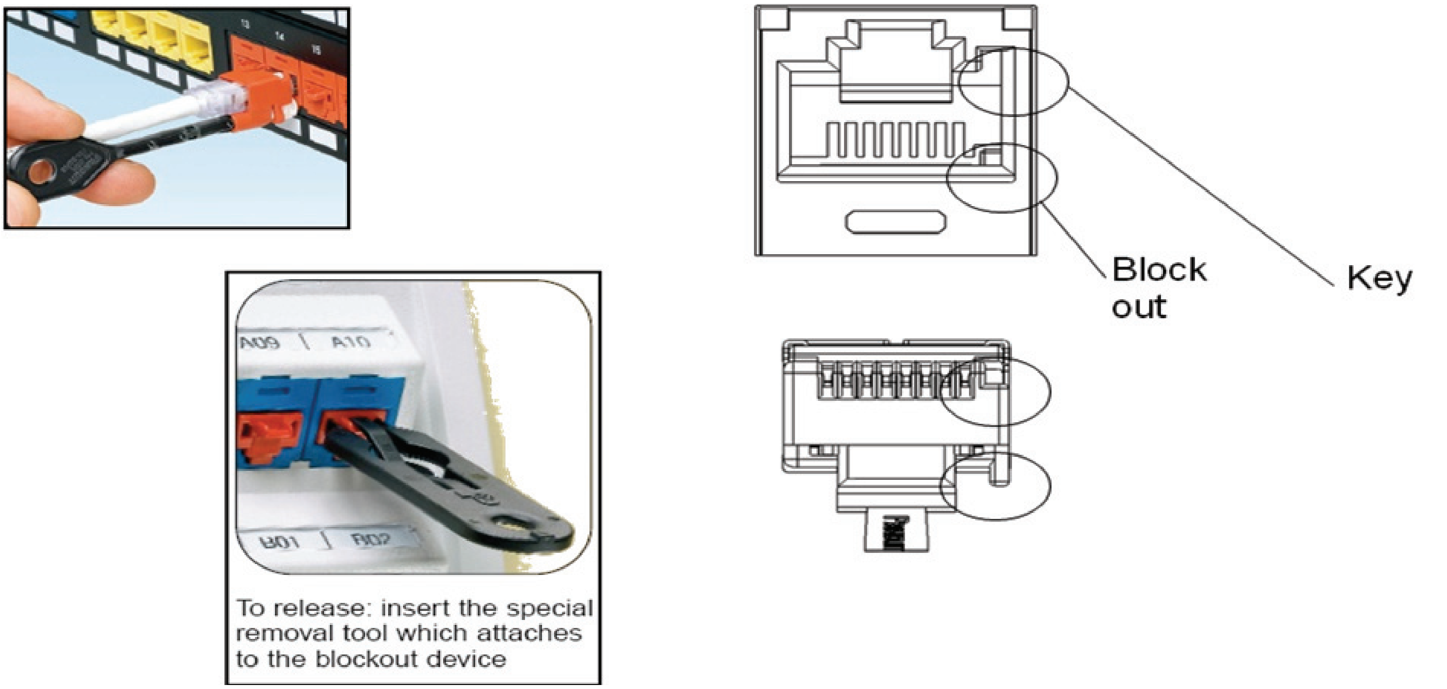
Physical Security

Physical security can prevent unauthorized devices from being plugged into a critical network risking a control disruption and downtime. Lock-in products can keep connectors plugged into a PAC or other device unless removed by an authorized user with a special tool. Blockout products conversely can keep open ports from a switch from being connected to unless the blockout device is removed with a special key (see Figure 2.8-5). Keyed copper or fiber solutions can prevent different network classes or segments from being inadvertently crossed. Uplink ports can be keyed differently than links to devices for example. Color coding can assist in making network ports for various segments more readily identifiable and keying.

Network Schematic Analysis

Network schematics are important tools for control engineers and IT personnel to review the physical infrastructure design and component selection. By reviewing the copper and fiber channels implemented in the zone cabling enclosure, the locations where testability, performance and security are concerns can be highlighted and addressed.

This Guide provides a reference schematic layout for a control showing a typical topology with callouts that show where physical security for ports can be applied, where performance decisions on media and connectivity need to be made, and where its recommended to install patching for testability of critical fiber or copper links. For industries where redundant networks are common as well as possibilities for sub networks from several vendors, it is crucial to identify and secure these physical links to avoid configuration mistakes and to prevent problems during startups and maintenance. Selection of appropriate fiber and copper media that can perform over the distances and environmental factors is key for robust operation. Diverse pathway planning for redundancy across the plant as well as in control plans should be considered. Selecting fiber and copper connectivity solutions engineered for high performance exceeding standard margins reduces risks associated with installation and long term performance. A careful plan for deploying test points will insure that the network distribution meets performance targets before critical startups of equipment where delays can be costly as well as on a periodic basis during preventative maintenance to avoid loss of control during operation.



To release: insert the special removal tool which attaches to the blockout device

Figure 2.8-5. Example Blockout Device to Support Network Security Initiatives at Control Panel Locations

End-to-End Solution

In summary, a thorough analysis and plan developed for the physical infrastructure for the control panel needs to be made to deliver on goals for high availability, security and performance. Use of reference architectures that leverage best practice approaches for noise mitigation, space optimization, grounding/bonding, safety, security, and industrial network media provide a clear path to control panel solutions that will support high performance networks and converged architectures.

Control Panel Physical Infrastructure

This section defines the sequence of actions involved with deploying a physical infrastructure for a Control Panel.

1. ***Logical Design***

Define the logical architecture governing the layout of industrial systems and active devices internal to the panel and how these connect to the cell/area and manufacturing zone. The logical architecture should be based on logical layer reference architectures developed by Rockwell Automation and Cisco, as well as on applicable topology diagrams.

2. ***Physical Design***

Map out the physical layout of the panel. This step provides the opportunity to mitigate noise risks and provide enough space for installing the Stratix switch and networking with proper bend radius, identification, and patching for testability of links. A Data Access Port is critical for safe access to the internal networks internal to the panel.

3. ***Detail Design***

Develop a network-level schematic diagram (or use a reference diagram) to identify the exact physical layer components required to deploy the Ethernet network to the control panel. These components include number of patch cords and horizontal links, patching fields, bonding and grounding elements, labeling and identification schemes, cable management tools, and safety and security tools.

NOTE: Steps 2 and 3 are often done concurrently.

4. Review the levels of the architecture in the diagram and identify solutions to address your system needs.

5. Review the recommended solution component List of Materials and specify your infrastructure.

1. Logical Design : *Define the Logical Architecture*

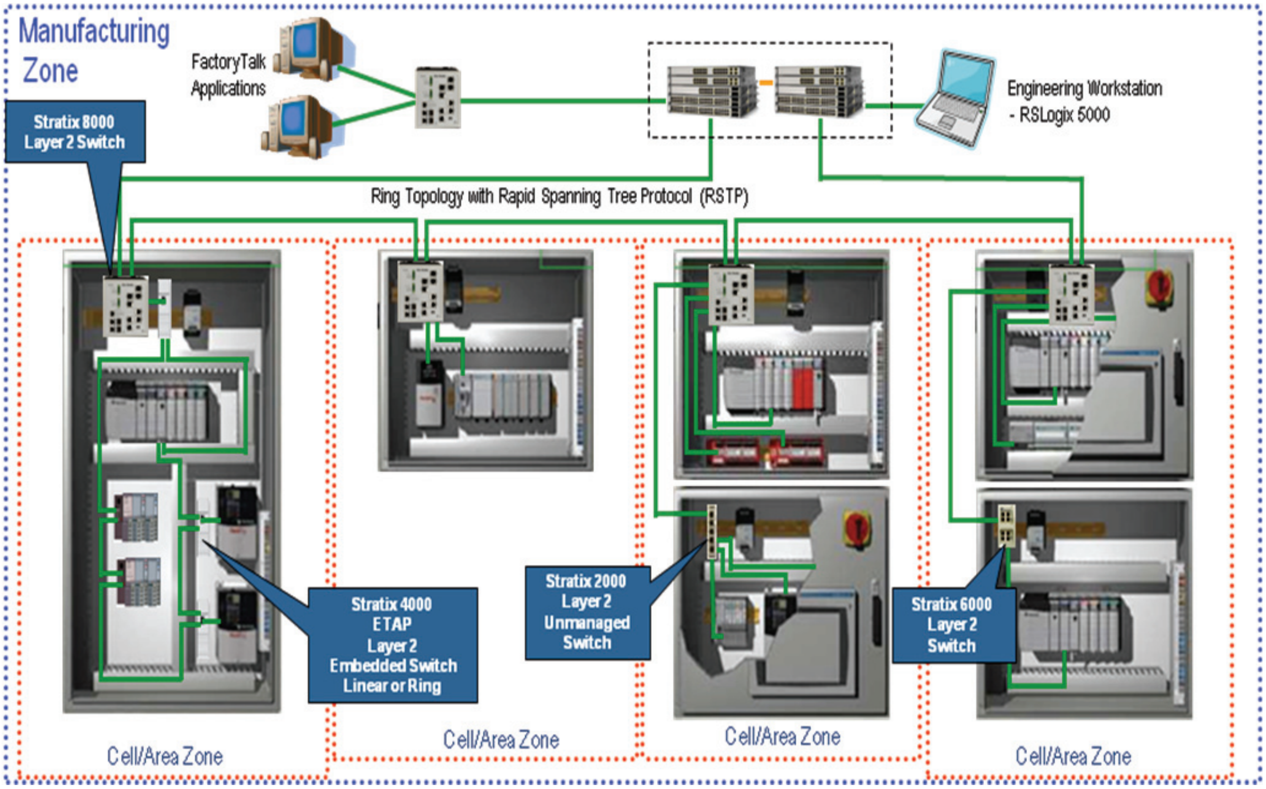

Manufacturing Zone
FactoryTalk Applications
Engineering Workstation - RSLogix 5000
Stratix 8000 Layer 2 Switch
Ring Topology with Rapid Spanning Tree Protocol (RSTP)
Stratix 4000 ETAP Layer 2 Embedded Switch Linear or Ring
Stratix 2000 Layer 2 Unmanaged Switch
Stratix 6000 Layer 2 Switch
Cell/Area Zone
Cell/Area Zone
Cell/Area Zone
Cell/Area Zone

Fig 2.8-6 Logical Diagram for control panel(s)

2. Map Device Locations to Identify Physical Infrastructure Reach, Noise, Bonding/Grounding Requirements

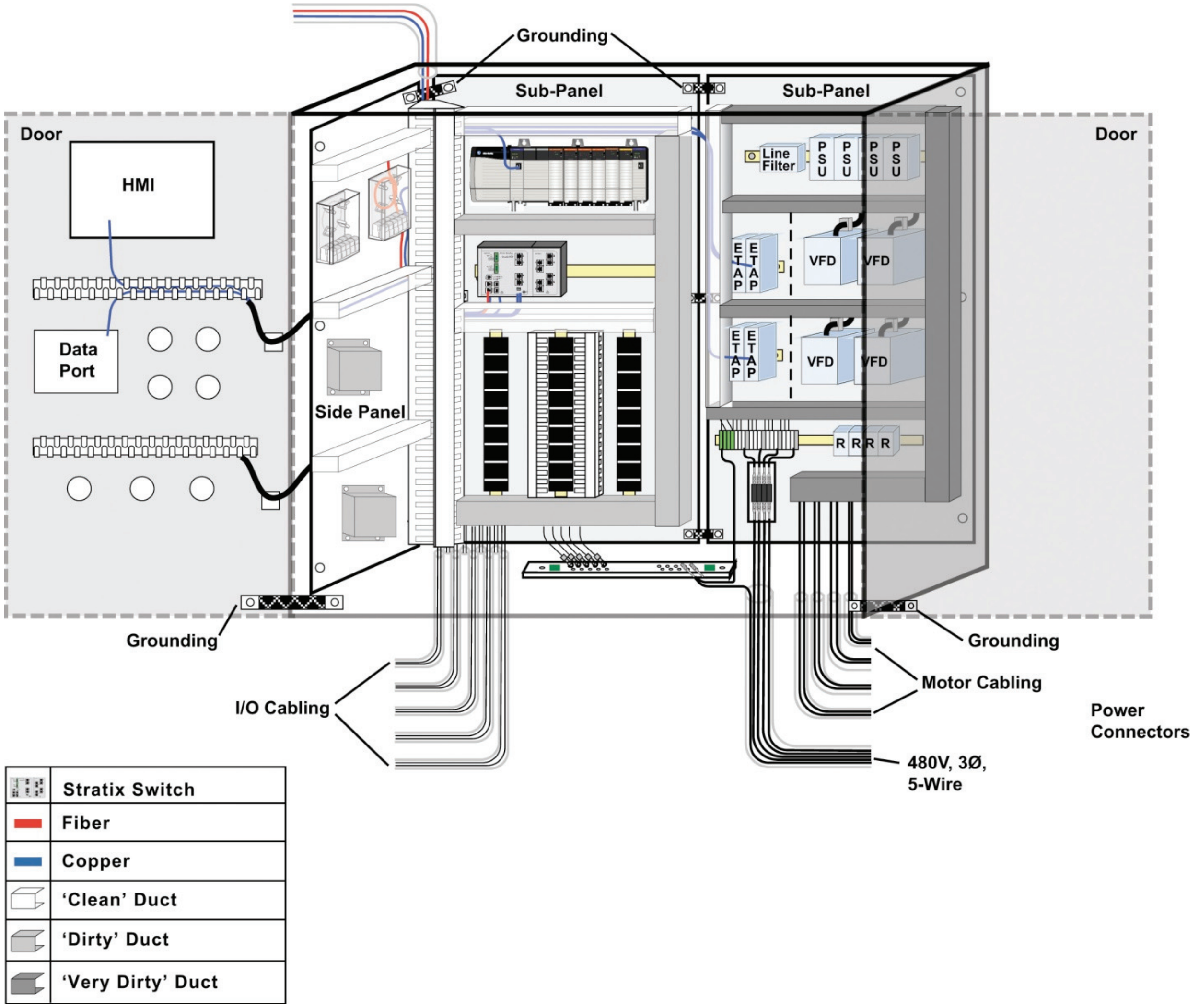


Fig 2.8-7 Physical Diagram for Control Panel overall layout

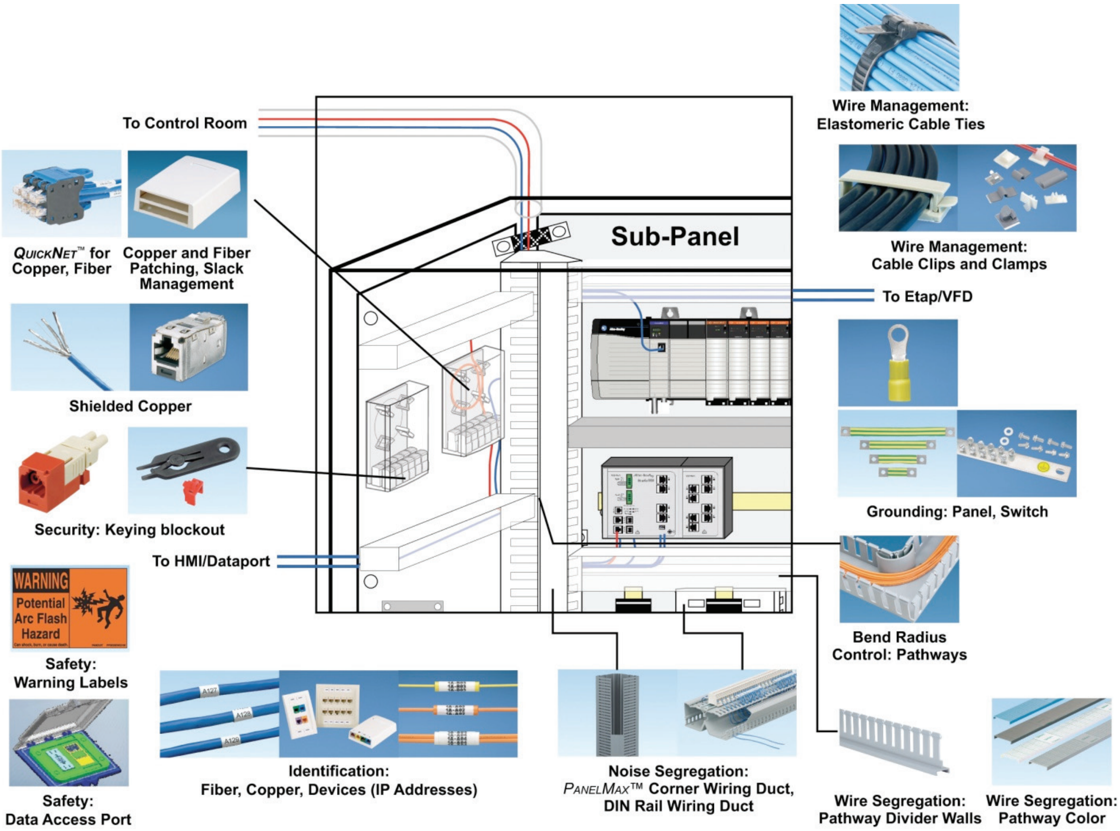


Fig. 2.8-8 Physical Diagram for control panel stratix mounting

- EMI noise considerations mitigated with grounding/ bonding and segregation of cabling to prevent noise coupling
- Surface mount boxes and patching for optimum cable management for fiber and copper connectivity and testability
- Color coded and keyed solutions to segregate and control patching to avoid inadvertent patching mistakes or unauthorized changes.
- Enhanced security with keyed jacks, lock in and block out connectivity

3. Detail Design

Develop Network-Level Schematic Diagram Identify
Exact Physical Infrastructure Components

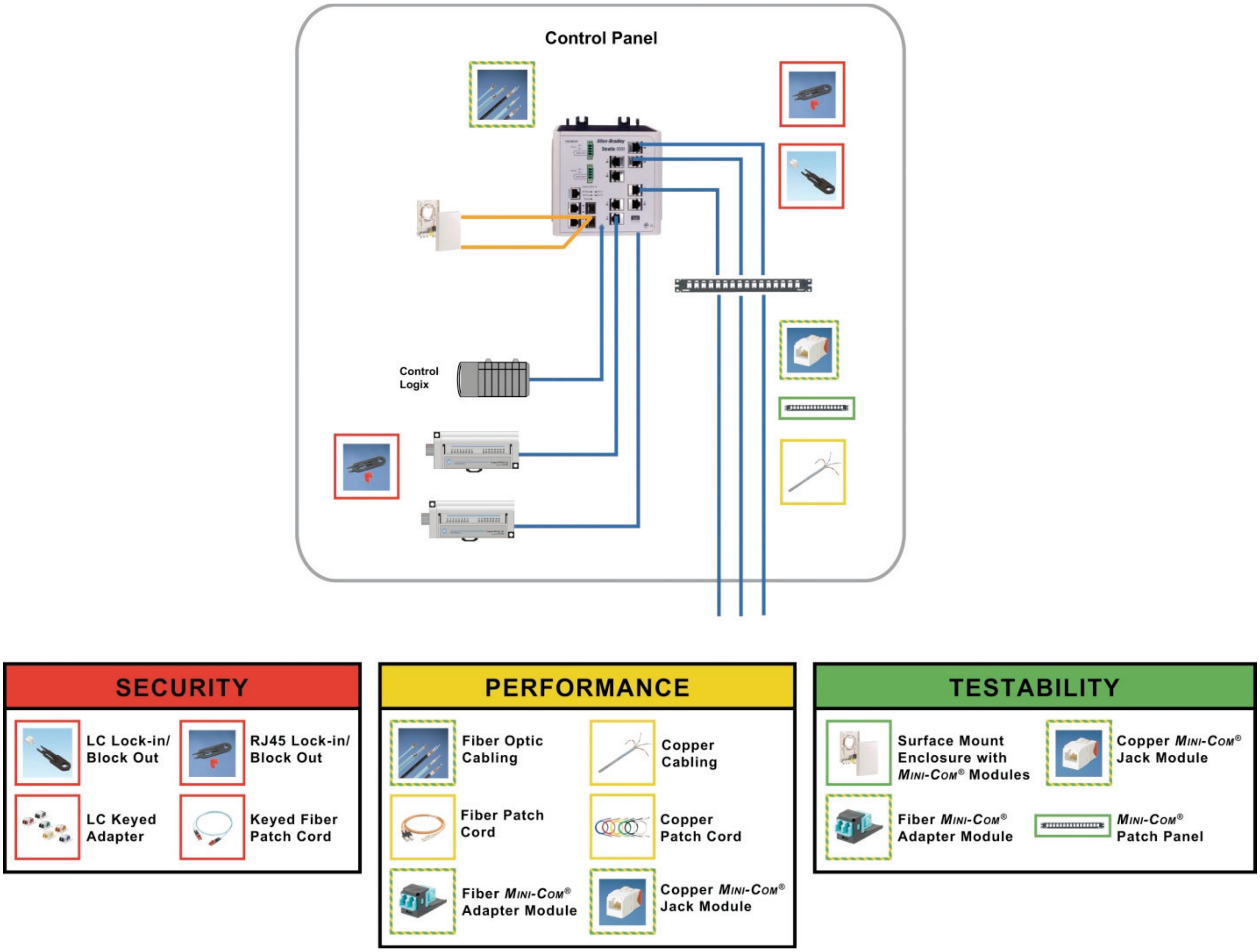


Fig 2.8-9 Network Detail diagram of control panel

4. The Levels of the Architecture in the Diagram and Identify Solutions to Address Your System Needs.

Zone Area Physical Infrastructure	Control Panel Issues	Panduit Solution
Cell/Area Zone (Level 0,1,2)		
Control panels	Security: Control of ports	Color coded fiber and copper jacks or keyed connectivity solutions can provide means to segregate critical systems
	Performance: Noise issues	Comprehensive control panel solution utilizing grounding/bonding, cable segregation and separation to reduce risks
	Performance: Throughput, Latency	Connectivity solutions that exceed standards for copper and fiber connectivity. Pre-tested patch cords deliver long term performance reducing risk
	Testability: Verify during startup, preventative maintenance	Patching for testing fiber, copper uplinks and critical external connections. Pre-tested copper and fiber patch cords to mitigate risks
	Reliability: Power	Superior termination with Panduit terminals.
	Safe access to networks without exposing to shock, arc flash	Panduit Data Access Port featuring secure modular connectivity
	Arc Flash, Voltage hazards identified	Warning labels, lock out solutions

5. the Recommended Solution Component List of Materials and Specify your Infrastructure:

Copper Cables/Connectors/Outlet boxes

Panduit Part#	Description
PUR6004BU-UY	High Performance Category 6 riser (CMR) 4-pair UTP copper cable.
PSR6004BU-UGY	Category 6A riser (CMR) 4-Pair U/FTP shielded copper cable.
CBXD6BL-AY	Surface mount termination box accepts six Mini-Com® Modules. Dimensions: 1.04"H x 4.95"W x 3.79"L (26.42mm x 125.73mm x 96.27mm)
CJ688TG*	Category 6, RJ45, 8-position, 8-wire universal jack module
CJS688TGY	Category 6, RJ45, 8-position, 8-wire universal shielded black jack module with integral shield
UTPSP1MY	1m Category 6 UTP Patch Cord with TX6 Plus Modular Plugs on each end
STP6X1MIG	1m Category 6A, 10 Gb/s STP Patch Cord with TX6 PLUS Modular Plugs on each end
Optional Keyed Jack Module CJK688TG*	Keyed Category 6, RJ45, 8-position, 8-wire universal jack module
Optional Keyed Patch Cord for use with Keyed Jack Module UTPKSP*^	Keyed Category 6 UTP Patch Cord for use with matching Keyed Copper Jack Module. Patch cords contain one keyed RJ45 Plug on one and to a Standard RJ45 Plug on the other.
IAEBH6	Category 6 RJ45 IP67/IP65 rated bulkhead connector. UTP type.
IAEBH6S	Category 6 RJ45 IP67/IP65 rated bulkhead connector. STP type.
IAEBHC6	Category 6, RJ45 bulkhead coupler, IP67/IP65 rated.
	(Required for higher MICE levels.)

Fiber Optic Parts

Panduit Part#	Description
F^E10-10M*Y	Opticom® Multimode Duplex Patch Cord (various lengths)
FAP*WAQ^^Z	Opticom® Fiber Adapter Panels (FAPs)
CMDJAQLCZBL	Fiber Optic adapter module, supplied with one LC Sr/Jr 10G fiber optic adapter.
CBX^IW-AY	MiniCom® Surface Mount Box
IAEF7JMA	Industrial LC fiber optic bulkhead adapter
IAEF617P-7PM1*	Industrial duplex multimode 62.5µm LC to LC patch cord
IAEF617P-NM1**	Industrial duplex multimode 62.5µm LC to pigtail
CM*^^ZBL	MiniCom® Fiber adapter modules
F^^MC*	Opticam Connectors (^^=LC, SC or ST)

Duct Parts

Panduit Part#	Description
DRD33WH6	PanelMax DIN Rail Wiring Duct (base, cover, rail fasteners),PVC,7.25” x 3.16”X6’,White
DRDWR3-X	3” wire retainer for PanelMax™ DIN Rail Wiring Duct.
DRDCS-X	3” corner transition strip for PanelMax™ DIN Rail Wiring Duct.
CWD3WH6	PanelMax Corner Wiring Duct Base,PVC,4.40” x 3.57”,White (use with C2WH6 cover)
C2WH6	Duct Cover, PVC, 2”W X 6’, White
F1X3WH6	Narrow slotted duct,PVC,1”X3”X6’,White
C1WH6	Duct Cover, PVC, 1”W X 6’, White
F1X3LG6	Narrow slotted duct,PVC,1”X3”X6’,White
C1LG6	Duct Cover, PVC, 1”W X 6’, White
F2X3LG6	Narrow slotted duct,PVC,2”X3”X6’,White
C2LG6	Duct Cover, PVC, 2”W X 6’, White
F3X3WH6	Narrow slotted duct,PVC,3”X3”X6’,White
C3WH6	Duct Cover, PVC, 3”W X 6’, White
F3X3LG6	Narrow slotted duct,PVC,3”X3”X6’,LGray
C3LG6	Duct Cover, PVC, 3”W X 6’, Lgray
G1X3BL6	Slotted duct,PVC,1”X3”X6’,Black
C1BL6	Duct Cover, PVC, 1”W X 6’, Black
G3X3BL6	Slotted duct,PVC,3”X3”X6’,Black
C3BL6	Duct Cover, PVC, 3”W X 6’, Black
SD3HWH6	Slotted Duct Divider Wall, PVC, 3”H X 6’, White
SD4HWH6	Slotted Duct Divider Wall, PVC, 4”H X 6’, White (for use with CWD3WH6)
DB-C	Duct Divider Wall Mounting Base, PC
NR1	Duct Nylon Push Rivet For Mounting
CSPC3LG-Q	1” bend radius corner strip pre-cut for 3” wall height
FWR-C	Duct Wire Retainer/Label, Type F or CWD
WR3-X	Duct Wire Retainer, Type G or H, 3”
FL25X25LG-A	Slotted Flexible Duct, Polypropylene,25X25X500mm,LG,Adh.

Cable Ties

Panduit Part#	Description
PLT1M-M	Pan-Ty Cable Tie - Nylon 1” Bundle, Natural, miniature
PLT1.5M-M	Pan-Ty Cable Tie - Nylon 1.5” Bundle, Natural, miniature
PLT1.5I-M	Pan-Ty Cable Tie - Nylon 1.5” Bundle, Natural, Intermediate
PLT2I-M	Pan-Ty Cable Tie - Nylon 2” Bundle, Natural, Intermediate
PLT3I-M	Pan-Ty Cable Tie - Nylon 3” Bundle, Natural, Intermediate
PLT2S-M	Pan-Ty Cable Tie - Nylon 2” Bundle, Natural, Standard
PLT3S-M	Pan-Ty Cable Tie - Nylon 3” Bundle, Natural, Standard
PLT4S-M	Pan-Ty Cable Tie - Nylon 4” Bundle, Natural, Standard
PLC2S-S10-M	Pan-Ty Clamp Tie - Nylon 2” Bundle, Natural Clamp tie, Standard
PLC2S-S10-M30	Pan-Ty Clamp Tie - Heat Stabilized Nylon, Clamp tie, Standard
PLT1M-M30	Pan-Ty Cable Tie - Heat Stabilized Nylon,1” Bundle, Black, miniature
PLT2S-M30	Pan-Ty Cable Tie - Heat Stabilized Nylon, 2” Bundle, Black, Standard
PLT4S-M30	Pan-Ty Cable Tie - Heat Stabilized Nylon, 4” Bundle, Black, Standard
PLM2S-M	Pan-Ty Marker Tie - Nylon, 2” Bundle, Natural Marker Tie
PLM2S-M30	Pan-Ty Marker Tie - Heat Stabilized Nylon, 2” Bundle, Black Marker Tie
PFX-0	Marking Pen
PLWP1M-C	Pan-Ty Push Mount Tie - Nylon, 1” bundle, Natural, Wing mount, Miniature
PLWP2S-C	Pan-Ty Push Mount Tie - Nylon, 2” Bundle, Natural, Wing mount, Standard
PLWP1M-D30	Pan-Ty Push Mount Tie - Heat Stabilized Nylon, 1” bundle, Black, Wing mount, Miniature
PLWP2S-D30	Pan-Ty Push Mount Tie - Heat Stabilized Nylon 2” Bundle, Black, Wing mount, Standard
PLT2S-M702Y	Pan-Ty Cable Tie - HALAR, Plenum Rated, Flame Retardant, 2” Bundle, Standard
PLT3S-M702Y	Pan-Ty Cable Tie - HALAR, Plenum Rated, Flame Retardant, 3” Bundle, Standard
GTS	Cable Tie Tool - Manual Install-SM,M,I,S
GTH	Cable Tie Tool - Manual Install-S,HS,LH,H
PTH	Cable Tie Tool - Pneumatic Install-S,HS,LH,H
PLT1M-M0	Pan-Ty Cable Tie - Weather Resistant Nylon
PLT1.5I-M0	Pan-Ty Cable Tie - Weather Resistant Nylon
PLT2I-M0	Pan-Ty Cable Tie - Weather Resistant Nylon
PLT3I-M0	Pan-Ty Cable Tie - Weather Resistant Nylon
PLT2S-M0	Pan-Ty Cable Tie - Weather Resistant Nylon
PLT3S-M0	Pan-Ty Cable Tie - Weather Resistant Nylon
PLT4S-M0	Pan-Ty Cable Tie - Weather Resistant Nylon
PLWP1M-D0	Pan-Ty Push Mount Tie - Weather Resistant Nylon
PLWP2S-C0	Pan-Ty Push Mount Tie - Weather Resistant Nylon
PLT1M-C186	Pan-Ty Cable Tie - Metal Detectable Polypropylene
PLT2S-C186	Pan-Ty Cable Tie - Metal Detectable Polypropylene
PLT3S-C186	Pan-Ty Cable Tie - Metal Detectable Polypropylene
PLT4S-C186	Pan-Ty Cable Tie - Metal Detectable Polypropylene

Abrasion Protection/Mounting Products

Panduit Part#	Description
CCH50-S10-C	Heavy-Duty Fixed Diameter Clamps
CCS25-S8-C	Standard Fixed Diameter Clamps
CH105-A-C14	Cable Holder
CLT100-C20	Corrugated Loom Tubing
CSH-D20	Cable Spacers
JP131W-L20	J-PRO™ Cable Support System
MTP3S-E6-C	Standard Multiple Tie Plates
MTP4H-E10-C	Heavy-Duty Multiple Tie Plates
PUM-071-2S-D30	Push Mount Assemblies
PUM100-D30	Push Mounts with Umbrellas
PW75F-C20	PAN-WRAP™ Split Harness Wrap
SE75P-CR0	Braided Sleeving
T50F-C	Spiral Wrap
TA1S10-C	Tie Anchor Mounts
TM3S8-C	Cable Tie Mounts
TM3-X2-C0Y	Swivel Mounts
ABDCM30-A-C	Dynamic Cable Manager
ABM112-A-C	Adhesive Backed Mounts
ABMQS-A-Q	Multiple Bridge Adhesive Backed Mounts
ACC38-A-C	Adhesive Cord Clip
BEC62-A-L	Beveled Edge Clip
CPM87S-C	Control Panel Mounts
LC5-A-C8	Adhesive Backed Latching Clips
LWC50-A-L	Latching Wire Clip
MACC62-A-C	Metal Adhesive Cord Clip
VCC25-A-C	Vertical Cord Clip
HSTT50-C	Heat Shrink Thin Wall
HSTT4A47-48-Q	Heat Shrink (4:1)
T50F-C	Spiral Wrap
PW75F-C20	PAN-WRAP™ Split Harness Wrap
CLT100-C20	Corrugated Loom Tubing
SE75P-CR0	Braided Sleeving
MP250-C	Marker Plates

Grounding/Bonding Parts

Panduit Part#	Description
RGRB19U	Grounding Busbar, 19”, tin plated, 20 mounting holes with #12-24 x 1/2” screws. For terminating Ground wires from various components
PV*-14RX	Ring Terminal, 1/4” stud hole, * PV14 to PV6 - 16awg-6awg. For terminating Ground wires from various components. Other sizes and styles available
BS10**45U	Braided Bonding Strap, 1” Width, #4 AWG (38,400 CMA) Tin Copper Braid, one-hole terminals, 3/8” bolt hole. For bonding multiple sub-panels together and other equipment. ** Sizes 04 - 12 in inches
BS10**45	Braided Bonding Strap, 1” Width, #4 AWG (38,400 CMA) Tin Copper Braid, one-hole terminals, 3/8” bolt hole, green/yellow insulation. For bonding of doors to enclosures and where abrasion protection is required. ** Sizes 04 - 12 in inches.
RGW-100-1Y	3/8” bolt hole, Paint Piercing Grounding Washers, pack of 100. For bonding sub-panels to enclosures at the mounting studs.
RGTBSG-C	Green Bonding Screws, #12-24 x 1/2”, box of 100. Bonds equipment with painted flanges to sub-panels.
RGTBSM6G-C	Green Bonding Screws, M6 x 15mm, box of 100. Bonds equipment with painted flanges to sub-panels.
TRBSK	Bonding Stud Kit, #12-24 fasteners, box of 25. For bonding various components to sub-panels, on-machine applications
TRBSM6K	Bonding Stud Kit, M6 fasteners, box of 25. For bonding various components to sub-panels, on-machine applications
BGN-C	Bonding Nuts, #12-24, box of 100. For bonding various components to sub-panels, on-machine applications
BGNM6-C	Bonding Nuts, M6. For bonding various components to sub-panels, on-machine applications
RGTS-CY	Thread Forming Screw, #12-24 x 1/2”
RGTSM6-C	Thread Forming Screw, M6 x 12mm

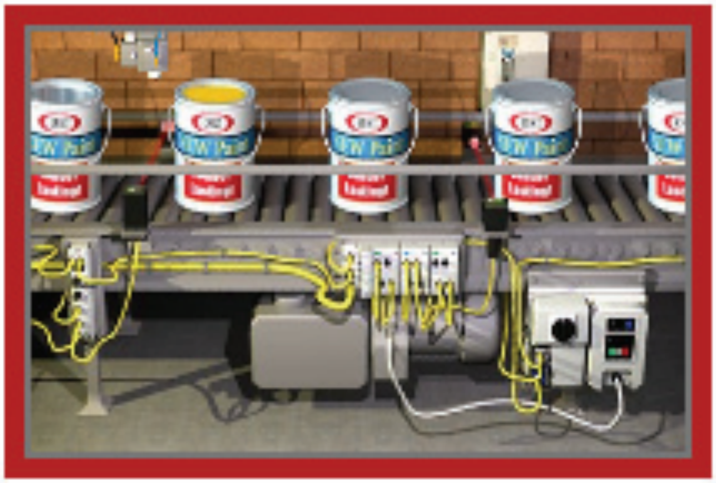
Safety/Security Parts

Panduit Part#	Description
PVS0305W2102Y	Arc Flash Label, 3”x5”
PVS0305W2201Y	Short Circuit Current Rating Label, 3”x5”
PSL-CBNT	“No” Tool Circuit Breaker Lockout Device
PSL-P	Individual Plug Lockout Device
PSL-WS	Toggle Switch Lockout Device
PSL-4RED	XENOY™ plastic body padlock with steel shackle
PSL-1	Lockout Hasp with 1” diameter jaw and overlapping tabs
PVT-41	“DO NOT OPERATE” Lockout/Tagout tag with cable tie

Identification Parts - LS 8E printer items shown only

Panduit Part#	Description
C200X100YPC	Printable Label for Enclosure Identification
S100X160VAC	Printable Label for 2mm/3mm Fiber Cable Identification
S100X220VAC	Printable Label for MTP Fiber Cable Identification
NWSLC-2Y	Cable identification sleeve for 2mm fiber cable
NWSLC-3Y	Cable identification sleeve for 3mm fiber cable
NWSLC-7Y	Cable identification sleeve for MTP fiber cable
S100X150VAC	Printable Label for Cat 5/6 Copper Cable Identification
S100X225VAC	Printable Label for 10Gig Copper Cable Identification
T100X000VPC-BK	Printable Label for Fiber Port Identification
C061X030FJC	Printable Label for Single Port Identification
C252X030FJC	Printable Label for Copper 4 Port Identification
C379X030FJC	Printable Label for Copper 6 Port Identification
C100X000VUC-BK	Printable Label for Duct Identification

2.9 On-Machine Area



The term “On-Machine” refers to automation components installed directly to the equipment so they are distributed across a machine or process rather than in a protected control panel. Mounting control devices on machinery or process equipment rather than in a panel offers many advantages compared to mounting in a control panel. However, it also requires devices and cabling systems that can take the environment as well as special considerations for wire management, identification, and maintainability. The advantages include enclosure cost savings, installation time savings, and less specialized expertise in wiring required.

However, exposure to the machine/process environment typically means that there are more issues with dust, moisture, shock, temperature, etc. than in a protected control enclosure. Thus, devices need to be sealed and ruggedized as do their network and power connections. As there are many devices and cables consolidating on a machine, there are new requirements for wire management and abrasion protection as well as rugged identification that will ensure that the on machine cabling and devices can be installed and maintained efficiently. An analysis of the MICE levels (mechanical, Ingress, Climatic/Chemical and Electromagnetic conditions) will allow for selecting media, connectivity, and wire management that performs reliably long term.

Reference Architectures

Rockwell Automation and Cisco have mapped out reference architectures that meet the specialized needs for network distribution to deliver process automation excellence. These architectures describe the connectivity between the Cell and Manufacturing zones at a logical level. In addition to this reference architecture level, the physical layer reference architecture is also crucial. The physical layer architecture refers to the infrastructure required to achieve the connectivity considering data throughput, environment, wiring distances, and availability. A structured, engineered approach is essential for the physical layer to ensure that investments in network distribution deliver optimum output. The On-Machine Device level networks typically utilize M12 connectivity rather than RJ45 connectivity because of the need for improved ruggedness. Rockwell Automation provides design tools in Integrated Architecture Builder for layout of the network and creating a bill of material for these M12 network connections and related modular power solutions.

Physical Layout Considerations

Key engineering considerations when designing the physical layer for network distribution for an On-Machine application include environmental analysis and machine or process layout. Understanding the size of the operation, plant layout, harsh conditions, plant expansion potential, and network topologies will help establish the physical layer infrastructure requirements. Zone cabling architectures and enclosures (see Section 2.7 of this Guide) can provide means to cost effectively and agilely distribute cabling for a wide area ‘on-machine’ application like a process plant. The physical layout of the machine will suggest locations for pathways and ‘on-machine’ device mounting panels. Cable routing, slack management and abrasion protection are important considerations for on machine cabling that should be considered once the machine layout is analyzed.

Cables may be exposed to harsh environments such as extreme weather or vibration. Insulation and abrasion protection products shield cables such as spiral wrap or heat shrink tubing. Securing cabling may require weather resistant cable ties and in extreme cases rugged stainless steel wire management products. Food processing lines may require metal detectable wire management products for food safety.

Network Schematic Analysis

This section provides a reference schematic layout showing a typical On-Machine topology with callouts that show where physical security for ports can be applied, where performance decisions on media and connectivity need to be made, and where its recommended to install patching for testability of critical fiber or copper links. Selection of appropriate fiber and copper media that can perform over the distances and environmental factors is key for robust operation. Diverse pathway planning for redundancy across the plant as well as in control plans should be considered. Selecting fiber and copper connectivity solutions engineered for high performance exceeding standard margins reduces risks associated with installation and long term performance. A careful plan for deploying test points will insure that the network distribution meets performance targets before critical startups of equipment - where delays can be costly - as well as on a periodic basis during preventative maintenance to avoid loss of control during operation.

End-to-End Solution

In summary, a thorough analysis and plan developed for the physical infrastructure for control room out to field devices will meet the critical needs for high availability, security and performance. Use of reference architectures that leverage best practice physical infrastructure approaches for control room hardware, network distribution, network connectivity, control panels and on machine wiring will result in automation systems that enable the full benefit of the investments made. This guide provides information on selecting, installing, testing, and documenting this critical physical infrastructure for all levels of this architecture.

On-Machine Physical Infrastructure

This section defines the sequence of actions involved with deploying a physical infrastructure for an On-Machine distributed system.

1. Logical Design
Define the logical architecture governing the layout of industrial systems and active devices. The logical architecture should be based on logical layer reference architectures developed by Rockwell Automation and Cisco, as well as on applicable topology diagrams.

2. Physical Design
Map out the physical locations of servers, switches, enclosures, rack systems and control panels. The following diagram shows recommended best practices for 'in plant' distribution.

This step provides the opportunity to identify distributed zone cabling topologies and plan out required patching, test point, and security considerations.

3. Detail Design
Develop a network-level schematic diagram (or use a reference diagram) to identify the exact physical layer components required to deploy Ethernet network. These components include number of patch cords and horizontal links, patching fields, bonding and grounding elements, labeling and identification schemes, cable management tools, and safety and security tools.

For On-Machine applications it is important to leverage Rockwell Automation's Integrated Architecture Builder tool for developing the machine connectivity bill of material for On-Machine devices, power cables, device cables and associated M12 Ethernet cabling. PANDUIT physical infrastructure solutions are available to implement the higher level zone or control panel architectures as well as products to help secure, protect, manage, and identify the wiring mounted on the machinery.

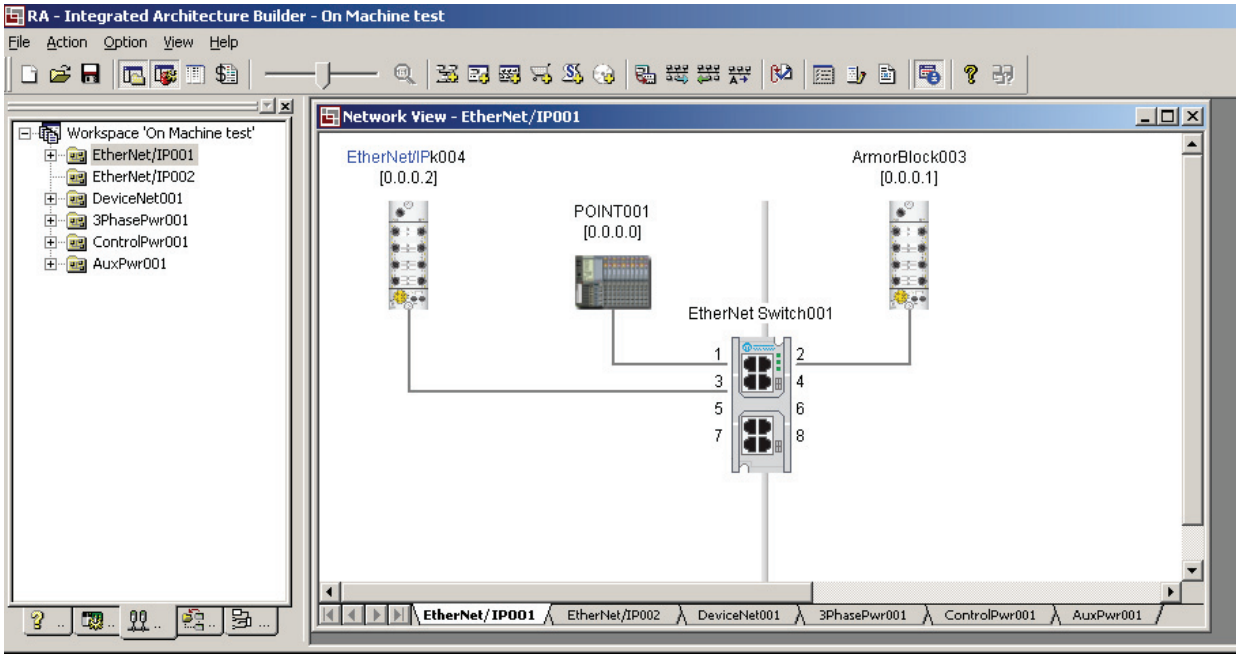
NOTE: Steps 2 and 3 are often done concurrently.

4. Review the levels of the architecture in the diagram and identify solutions to address your system needs.

5. Review the recommended solution component List of Materials and specify your infrastructure.

1. Logical Design

Define the Logical Architecture .



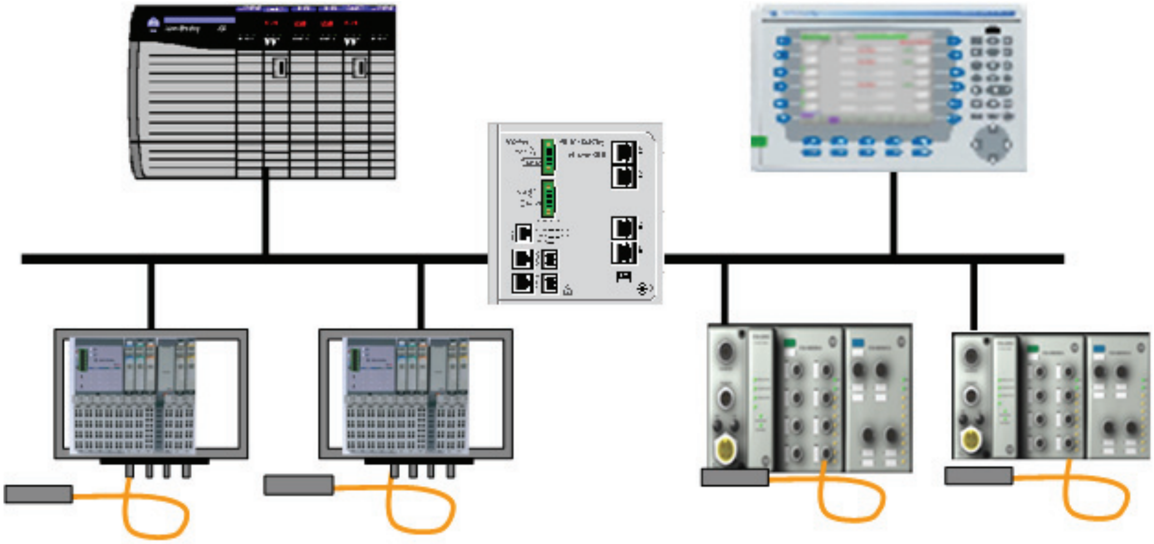


Fig 2.9-1. Logical diagrams for On Machine distributed networking

2. Physical Design

Map Device Locations to Identify Physical Infrastructure Reach, Noise, Bonding/Grounding Requirements. Consider locations to Identify, manage, secure and protect the network and associated On-Machine cabling.

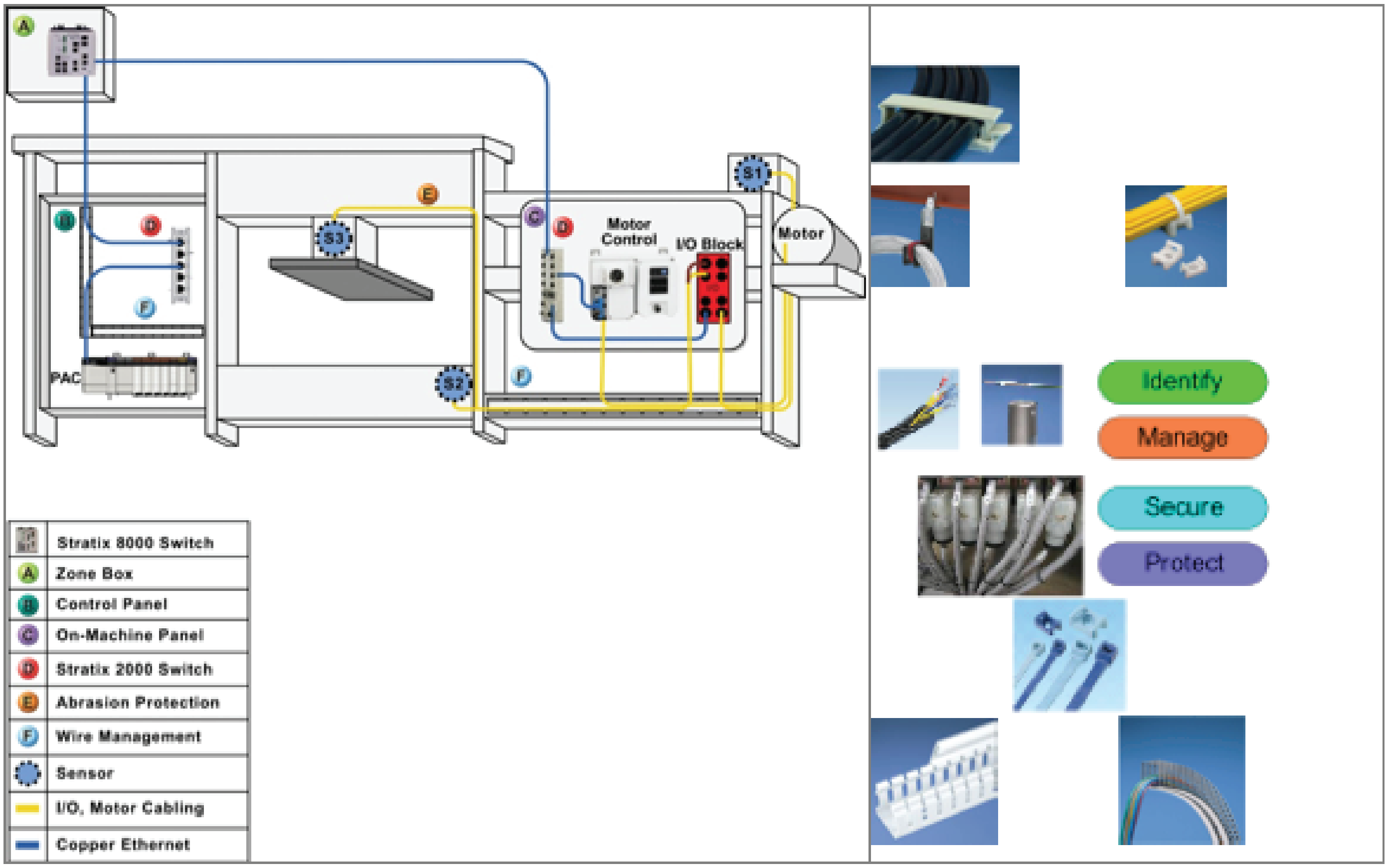


Fig 2.9-2. Physical Diagram of On-Machine network

- On-Machine wire management for slack management and protecting cabling.
- Identification products should be applied to device and network cabling
- Grounding and bonding to equipment to mitigate risks to communication disruptions
- Enhanced security with keyed jacks, lock-in and blockout connectivity in zone cabling enclosures and control panels that connect to the On-Machine wiring