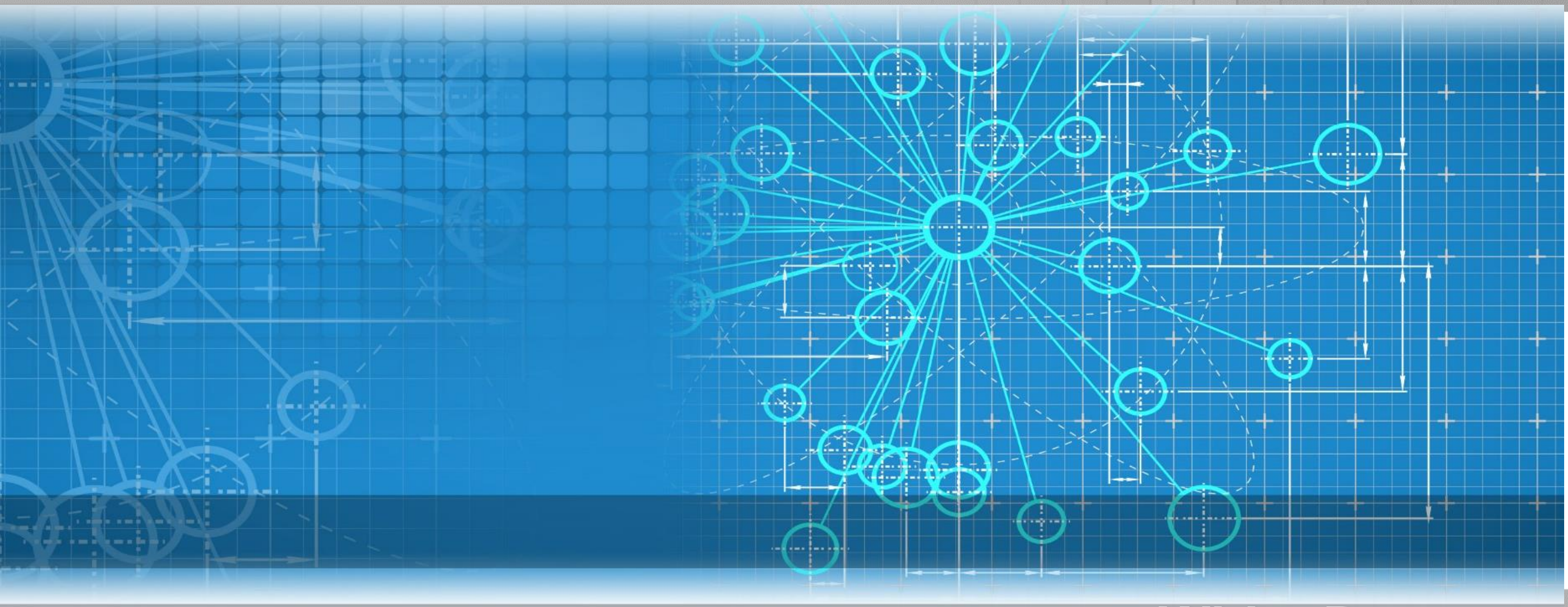


White Paper

October 2015 WP-24

A Manufacturing Network Fabric Maturity Model

Simplify planning for an IoT information
enabled manufacturing environment

PANDUIT®

Introduction

The Internet of Things (IoT) is expected to connect an astonishing 50 billion devices by 2020.[i] In the manufacturing world, this increase of devices is providing deeper insights into operations and new opportunities to improve quality, productivity, efficiency, and security.

> *According to a recent IHS Global and IMS Research study, an estimated 160,000 industrial Ethernet nodes are connected every day.*

Along with the new opportunities are new challenges. The demand to collect and analyze production information in real time is driving the need for manufacturers to converge their historically disparate industrial and enterprise networks into a single network architecture. A well-designed and reliable physical layer, known as the “network fabric”, serves as a critical foundation and strategic business advantage for forward-thinking manufacturers seeking to differentiate themselves from the competition.

This white paper discusses the importance of the network fabric in today’s information-enabled manufacturing environments, outlines the steps that proactive manufacturers can take to capture its full value for years to come and describes a four-stage methodology for improving an existing network to a higher maturity level.

Manufacturing in the Information Age

The IoT is reshaping the plant floor. A rapid influx of smart equipment and connected devices that can communicate on an industrial Ethernet network is enabling manufacturers to understand the performance of their machines and processes like never before.

> *80 percent of network downtime is attributed to physical layer connections, Sage Research estimates.*

Equally important to ‘*what’* is being connected is ‘*how’* it is being connected. Innovative technologies are enabling manufacturers to manage their infrastructure, deploy devices, and share information in new ways. Some examples include:

- Cloud computing can remotely monitor – in real-time and from a centralized location – equipment that is dispersed across multiple sites, and can provide expanded processing power and storage capacity as operational needs change
- Virtualization de-couples software from hardware, enabling improved application uptime, increased deployment flexibility, and faster upgrades
- Wireless technology can reduce cabling costs and allow easier sharing of data, such as to mobile devices on the plant floor

The end result of this abundance of information and seamless connectivity is faster decision making, improved collaboration, and new opportunities to improve productivity.

It also represents a major turning point in how manufacturers design, install, and maintain industrial networks. The traditional approach of using separate information technology (IT) and operations technology (OT) networks impedes seamless connectivity, and is too limiting and insecure to be a valid option. Instead, manufacturers require a single unified network architecture, built on a single physical network fabric leveraging the full power of internet protocol and security defense-in-depth.

The drive for seamless connectivity and the sharing of vast amounts of data throughout the plant floor to enterprise represents a major turning point in how manufacturers design, install, and maintain industrial networks.

The Unified Network Fabric

The unified network fabric serves as the physical foundation on which a manufacturer's networked operations exist and operate. It includes all cabling, wireless, switching, computing, and storage systems, and uses standard, unmodified Internet Protocol (IP) connectivity to help ensure secure and open communications.

Network fabric is an industry term that describes a network topology in which devices pass data to each other through interconnecting switches. Industrial plant automation systems are evolving from point-to-point, dedicated connections to a more switch-centric design where traffic now can be seamlessly passed with much greater flexibility and enhanced throughput. Instead of inflexible direct connections between devices, switches and a converged plant architecture allow data to be switched and routed with security across the plant automation system as well as upstream for higher value creation.

> *Commercial, off-the-shelf cables may not meet industry performance requirements. Cable jackets and conductor insulation may be easily damaged at extreme temperature ranges.*
>
> *ODVA Media Planning and Installation Manual*

In addition to serving as a necessary backbone for a manufacturer's information architecture, the network fabric can be the deciding factor in a manufacturer's success. Similar to a "fabric unraveling", poor planning and reactive decision making can result in a network becoming a large tangle of connections and switches that can result in plant downtime, security breaches, and safety issues.

Leading manufacturers are purposely and proactively designing their network fabric to support their performance goals. An Aberdeen Group study found that best-in-class manufacturers are more likely to build reliability into the physical layer of the network, use network management apps and devices, and use a cabling strategy that is aligned with industrial networking architecture than average performers and those that lag behind.[ii]

To achieve a strong result, system integrators should consider the following five key areas when designing and deploying a network fabric.

Scalability: Plant systems growth, new technology adoption, or changing bandwidth requirements in the years to come can be difficult to predict. Ensuring infrastructure growth and scalability to meet future needs can help avoid "rip-and-replace" upgrades, reduce reliability risks, and shorten deployment times.

Reliability: Network downtime is becoming intertwined with machine downtime as more of the automated production process is brought onto the network. Base the network fabric on a robust architecture, follow industry standards, and use IT/OT collaboration to help achieve high reliability across the industrial plant because every second matters on the plant floor.

Security: A major network transformation inevitably involves security considerations. A defense-in-depth security strategy is an industry-recommended best practice. It uses multiple layers of protection at the physical, network, computer, application, and device levels to establish several security fronts against today's ever-growing threat landscape.

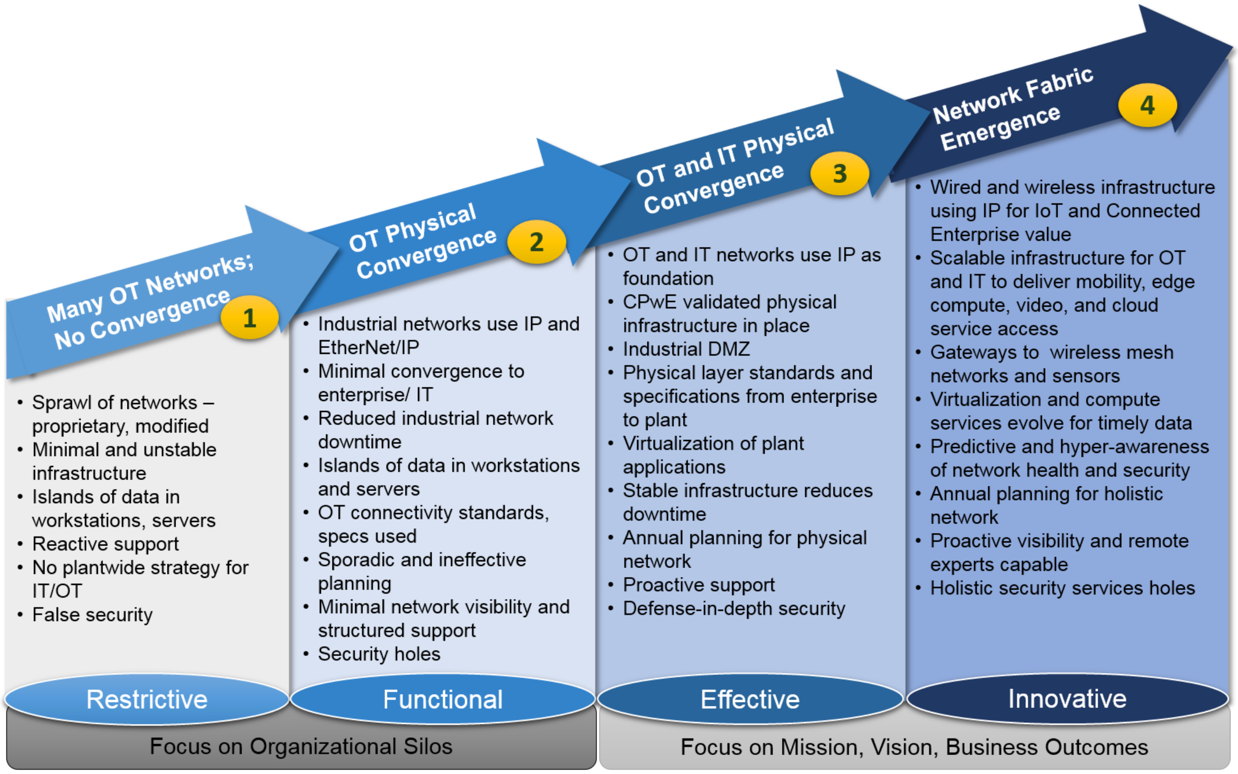
Ease of Deployment: A well-planned, thoughtful approach to the network fabric helps ease design and deployment, and reduces the likelihood of startup or operational issues. Use standards such as ISA-99 and TIA-1005 and validated architectures such as Converged Plantwide Ethernet (CPwE) to design the network fabric with greater confidence. Use structured cabling best practices and validated integrated solutions to reduce installation time and startup risks.

Innovation: The network fabric provides a platform for taking advantage of new innovations. For example, Power over Ethernet (PoE) uses a single cable to deliver power and data, which can reduce wiring complexity, and lower installation and maintenance costs. A structured network of wired and wireless connectivity creates opportunities for deploying new services such as remote monitoring and edge intelligence for condition monitoring and predictive analytics.

A Maturity Model that Assesses Network Fabric

Panduit developed the Network Fabric Maturity Model (Figure 1) to help manufacturers map out their journey to a unified network fabric. This model outlines the four levels of a network fabric – from multiple unmanaged plant floor networks to a fully unified network fabric. The model can help manufacturers understand where they stand today, and provides guidance to help them progress through each level toward the end goal. This model is about shifting industrial networks from focusing solely on the organizational silos of the plant automation system to a more holistic focus on mission, vision, and overall business outcomes.

Panduit Network Fabric Maturity Model



Many OT Networks; No Convergence 1

- Sprawl of networks – proprietary, modified
- Minimal and unstable infrastructure
- Islands of data in workstations, servers
- Reactive support
- No plantwide strategy for IT/OT
- False security

Restrictive

OT Physical Convergence 2

- Industrial networks use IP and EtherNet/IP
- Minimal convergence to enterprise/ IT
- Reduced industrial network downtime
- Islands of data in workstations and servers
- OT connectivity standards, specs used
- Sporadic and ineffective planning
- Minimal network visibility and structured support
- Security holes

Functional

OT and IT Physical Convergence 3

- OT and IT networks use IP as foundation
- CPwE validated physical infrastructure in place
- Industrial DMZ
- Physical layer standards and specifications from enterprise to plant
- Virtualization of plant applications
- Stable infrastructure reduces downtime
- Annual planning for physical network
- Proactive support
- Defense-in-depth security

Effective

Network Fabric Emergence 4

- Wired and wireless infrastructure using IP for IoT and Connected Enterprise value
- Scalable infrastructure for OT and IT to deliver mobility, edge compute, video, and cloud service access
- Gateways to wireless mesh networks and sensors
- Virtualization and compute services evolve for timely data
- Predictive and hyper-awareness of network health and security
- Annual planning for holistic network
- Proactive visibility and remote experts capable
- Holistic security services holes

Innovative

Focus on Organizational Silos

Focus on Mission, Vision, Business Outcomes

Figure 1. Network Fabric Maturity Model.

Level 1: Restrictive

Situation: Multiple industrial networks that have been established over a series of years to support both new and legacy equipment at the device and control layers can result in network sprawl. Beyond machine and process control, little opportunity exists for connections across these proprietary and unmanaged networks without using specialized gateways and added software complexity.

Implication: Overgrown networks can be unstable and result in unexpected downtime events. Limited opportunities exist to leverage production data, which is largely trapped in workstations and servers. Specialized proprietary networks also create support challenges for IT staffs not familiar with proprietary industrial networks.

Level 2: Functional

Situation: Control, safety, motion, and energy data are converged into a single OT network technology, such as EtherNet/IP, which uses standard, unmodified IP. The industrial network has limited connectivity to the enterprise IT network.

Implication: A converged plant floor network using IP reduces the sprawl of proprietary networks and enables use of standard tools and troubleshooting, resulting in improved network uptime potential. At the same time, many manufacturers at this stage still use fieldbus-style architectures and do not fully utilize the power of managed switches and structured cabling best practices, leaving them with isolated subnets and data bottlenecks.

Level 3: Effective

Situation: Industrial and enterprise networks are converged into a unified network architecture that is IP-centric and uses validated design guidelines, such as CPwE. Physical layer standards are applied from the plant floor to the enterprise and a more robust defense-in-depth security approach is implemented, including the use of an industrial demilitarized zone (IDMZ) or other strong segmentation methods.

Implication: A converged network infrastructure eliminates islands of data for greater insights into manufacturing operations. The standards-based physical layer supports virtualization of plant applications and establishes a more stable infrastructure for reduced downtime. Further refinement may be necessary to support the increase in bandwidth required for emerging technologies, such as wireless and a proliferation of IoT devices.

> *Commercial, off-the-shelf cables may not meet industry performance requirements. Cable jackets and conductor insulation may be easily damaged at extreme temperature ranges.*
> *ODVA Media Planning and Installation Manual*

Level 4: Innovative

Situation: The network infrastructure now supports wired and wireless connections to link people, processes, and equipment across the industrial enterprise, and ensures scalability and security for future technology changes. The physical infrastructure network is built using modular, validated building blocks, and is based on best practices and standards for both IT and OT, ensuring the capacity and flexibility for new services.

Implication: A fully unified network fabric opens the door for innovative ways of doing business by establishing the foundation to support new and evolving technologies, such as edge computing, virtualized services, and wireless mesh device networks. At this stage, network visibility and predictive tools support greater network uptime and security, while advanced analytics and remote access offer new opportunities to capture value from the network and its connections.

Planning Ahead

A timely effort in determining the path to take can make the difference in the amount of future rework. The journey to achieving a fully unified Level 4 network fabric begins with understanding the network's current maturity level. To help, use the following characteristic sets for each Network Fabric Maturity Model level to determine precisely where the network sits on the model.

Improving From Restrictive to Functional – Level 1 to Level 2

Restrictive networks often result from disregarding OT/IT best practices in favor of taking shortcuts. This can include using proprietary fieldbus and tiered networks to save on training and learning time, or using commercial-grade unmanaged switches to save on costs. Such shortcuts can lead to network sprawl, islands of data, and security holes.

Elevating the network infrastructure to the Functional level requires a more planned, standards-based approach, gradually migrating on a priority basis.

Three Key Objectives:

1. Understand the plant floor environment

Spend the time and resources necessary to understand the plant floor environment. Identify the physical and security risks, from the environmental conditions the equipment must operate in to security holes such as open computer ports. Also, assess cell/area zone designs and apply best practices, such as using VLANs, managed switches, and resilient topologies.

2. Specify media, grounding, and connectivity solutions that satisfy plant floor requirements

With plant floor requirements defined, specify the media, grounding, and connectivity solutions that satisfy those requirements. Follow OT standards such as TIA-1005-A for harsh environment connections. Use IT best practices, such as those outlined in ANSI/TIA 568-C and TIA-1005-A for structured cabling, which can offer higher cable density, greater network longevity, and better flexibility than point-to-point cabling. It is also important to use industrialized components from only trusted providers. The Communications Cable and Connectivity Association found that 322 of the 379 offshore-produced cords it tested did not meet TIA-568-C.2 performance specifications.

3. Close security holes in the physical layer

Closing the security holes often found in Restrictive network architectures requires the implementation of a physical security foundation. This can include using physical and virtual segmentation to help limit user access to defined segments, and using lockable enclosures to secure plant connections.

Progressing from Functional to Effective – Level 2 to Level 3

Manufacturers that have converged their industrial networks into a single OT network often rely on legacy plant backbones and networking technology that lack the bandwidth to keep pace with higher data needs and new connections. Progressing to an effective network architecture requires reference architectures and best practices.

__Like-Minded Partners__
Panduit is partnering with Cisco and Rockwell Automation to turn the potential of information-enabled manufacturing into reality. Together, the companies created the Industrial IP Advantage, an educational and training resource aimed at helping manufacturers deploy a secure industrial information architecture using standard, unmodified Ethernet and the Internet Protocol.

Three Key Objectives:

1. Scale and converge the industrial network from multiple cells into an industrial zone that securely converges with the enterprise. Use reference architectures such as CPwE from Cisco and Rockwell Automation, and the Physical Infrastructure Reference Architecture Guide from Panduit to help build a more robust network that is based on industry standards.

2. Specify media that delivers the performance and availability for growing data and connectivity needs. Replace low-cost, plug-and-play unmanaged switches with managed switches to improve network monitoring and traffic management. Fiber and 10GB copper cables offer high-performance, high-availability connectivity, while well identified, color-coded or keyed jacks can help prevent inadvertent cross connections that can result in downtime.

3. Use pre-configured network building blocks to help reduce risks and speed up deployment times. These factory-assembled systems are validated to industry standards and factory tested to reduce startup time and risks. These solutions reduce the time and resources required to engineer and install customized solutions.

   Example turn-key solutions include:

   - The Panduit pre-configured Micro Data Center (MDC) can house a complete data center infrastructure in a single rack- or cabinet-based deployment. It can act as a standalone system to run manufacturing applications, serve as a networking or data-collection hub, or house virtual environments.

   - Combining industry-leading technology from Panduit, Cisco, and Rockwell Automation, the Industrial Data Center (IDC) is a virtualization infrastructure designed for industrial environments that includes the hardware, software, and documentation in a pre-assembled and bundled solution.

   - The Panduit Network Zone Systems rapidly deploy an EtherNet/IP* network on the plant floor with a reliable, structured approach that reduces installation time and lifecycle costs. All systems include copper/fiber connectivity, cable management, grounding and a patented voltage barrier to accelerate deployments and reduce risk by isolating hazardous voltages. Multiple levels of integration (e.g., pre-configured, switch-ready, fully integrated) are available, delivering design flexibility in demanding industrial applications and requirements.

- The Panduit Pre-configured Industrial Distribution Frame (IDF) is designed to deploy and protect industrial rack-mount Ethernet switches. It can deploy 25 percent faster than a non-pre-configured IDF and reduce the risk of downtime due to switch overheating.

Evolving from Effective to Innovative – Level 3 to Level 4

Converged IT/OT networks is the defining characteristic of an Innovative network architecture, as it provides new opportunities for collecting and using data across a manufacturing enterprise, and serves as the foundation for defense-in-depth security. Achieving a fully unified network fabric that can deliver on its full potential requires scaling the network foundation with adequate bandwidth and structure for the sudden increase of wired and wireless connections and compute resources at the edge.

Three Key Objectives:

1. Assess the network infrastructure's capability to support the extension of computing and mobile access capabilities with new IoT architectures. Designing an infrastructure to support remote-access technology, for example, can allow engineering experts to monitor and access equipment from a centralized location, or allow IT personnel to service plant floor computers from their desks. Mobile technology can deliver plant floor visibility anywhere in a facility – rather than only in a fixed location – for faster responses and decision making.

2. Collaborate with IT/OT for network visibility documentation and diagnostic tools for sustainable value throughout the network life cycle. Use of tools designed for network discovery and documentation of plant industrial Ethernet networks fills a gap for a comprehensive view of enterprise to plant convergence down to the device level. Likewise, providing plant floor and operations real-time diagnostics of network alerts speed troubleshooting and improves plant uptime. Holistic, up-to-date network monitoring greatly aids in ongoing network planning for expansion with a focus on performance and security. Advanced approaches include dashboards and predictive analytics that can help prevent emerging network problems before they cause downtime.

3. Develop test beds and pilots for IoT architectures that leverage cloud and fog computing for a broader network fabric that includes gateways and wireless mesh networks. For instance, the cloud may not be an option for manufacturers when real-time processing of manufacturing data is required. Instead, fog computing can leverage intelligent gateways and integrated services routers to provide local, real-time data processing closer to the machine. Additionally, wireless mesh solutions that connect to the network fabric provide opportunities to cost-effectively deploy wireless sensors.

Defining a Path

The journey to achieving a fully unified Level 4 network fabric begins with understanding your network's current maturity level. Check off the following characteristics for each Network Fabric Maturity Model level or take our online survey at www.panduit.com/mapyourjourney to determine where your network resides on the model.

Level 1: Restrictive
__ Network sprawl
__ Proprietary networks
__ Unmanaged, poorly documented networks
__ Islands of data
__ Reactive support
__ Security holes

Level 2: Functional
__ Converged industrial networks
__ IP and EtherNet/IP used in industrial networks
__ Minimal convergence to IT
__ Islands of data
__ OT standards are used
__ Minimal network visibility
__ Security holes

Level 3: Effective
__ OT and IT networks converged
__ Network architecture based on IP
__ Validated physical infrastructure
__ Virtualization of plant applications
__ Proactive support
__ Defense-in-depth security
__ Industrial DMZ

Level 4: Innovative
__ Robust wired and wireless infrastructure
__ Scalable infrastructure supports mobility, edge computing, IoT
__ Gateways to non-IP wireless mesh
__ IT and OT best practices applied
__ Remote access capable
__ Holistic security service

Note that different cells or areas in your plant may be at different maturity levels and may therefore need to be assessed separately.

Summary

IHS Technology predicts the industrial automation sector will account for nearly three-fourths of all connected devices by 2025.[iii] The potential for value generated by all these industrial connections will drive new business models, transforming productivity dramatically. The future competitiveness of almost all manufacturing companies hinges on how rapidly they can embrace convergence and IP technologies. A unified network fabric based on standard IP with a strong physical infrastructure will serve as the foundation of tomorrow's information and connectivity needs, and an enabler for converging the networks to gain robustness, visibility, and reliability. The use of maturity models can help guide both the OT staff and IT staff to accelerate progress to more effective and innovative networks that will deliver on the promise of the IoT.

Resources

For more information on key design considerations, products and support services, or for help in designing and deploying a network fabric, contact a Panduit representative, visit www.panduit.com/ia, or email us at iai@panduit.com.

Training on implementing and managing networked industrial control systems is also available through the Industrial IP Advantage. For more information or to register, visit http://www.industrial-ip.org/training

- Panduit: Physical Infrastructure Reference Architecture Guide
- Cisco and Rockwell Automation: Converged Plantwide Ethernet (CPwE) Design and Implementation Guide
- Industrial IP Advantage: The Network Fabric
- ODVA: Media Planning and Installation Manual
- ISA99: Industrial Automation and Control Systems (IACS) Security
- TIA-1005: Telecommunications Infrastructure Standard for Industrial Premises
- ANSI/TIA 568-C: Generic Telecommunications Cabling for Customer Premises

About Panduit

Simplifying Robust Network Deployment

Panduit is a world-class developer and provider of physical infrastructure solutions that improve reliability, security, and safety of Industrial Automation Infrastructure systems while reducing deployment and operating costs. Working with industry leaders, Panduit helps bridge the gap between IT and Controls Engineers by providing optimized building-block architectures for connecting enterprise, industrial networks and control systems.

Panduit is simplifying robust industrial network deployments, providing our customers confidence and peace of mind through our enterprise, data center and industrial automation expertise, tools, and comprehensive offering.

Design, Deploy, Manage

Panduit collaborates with industry leaders to address deployment complexities associated with Industrial Ethernet. Our *Industrial Ethernet Physical Infrastructure Reference Architecture Design Guide* can help you design, deploy, and manage a reliable Industrial Ethernet physical infrastructure.

www.panduit.com/ia · iai@panduit.com · www.panduit.com/mapyourjourney

References

[i] *Source: Cisco, The Internet of Things, April 2011*

[ii] *Source: Aberdeen Group, Industrial Networking Real-time Foundation for Manufacturing and Enterprise, August 2012*

[iii] *Source: IHS Technology, Industrial Internet of Things, 2014 Edition*

* *EtherNet/IP is a trademark of ODVA.*

CPAT18- -WW-ENG, Rev 1, 08/2016