White Paper

October 2013

Scaling the Plant Network

An Approach to Industrial Network Convergence

PANDUIT®
building a smarter, unified business foundation
Connect. Manage. Automate.

HESCO

Introduction

As rapid advancements in networking, computing, data storage and software capabilities increase the value potential of automation systems, controls engineers and IT organizations are pressured to update their plant network architectures with solutions that securely merge information and control data. As a result, the factory networks need to deploy connectivity to both automation devices that are critical to machine and process line systems as well as support connectivity to non-automation devices such as wireless access points, digital signage, video surveillance, energy and building automation systems nodes. To address this challenge, validated architectures and tested physical solutions that integrate information and control systems are growing in importance. This white paper describes how Panduit Industrial Network Deployment Solutions can improve reliability, security, and safety of Industrial Automation systems and *offer up to 30% reduction in deployment costs and 75% savings in deployment time*.

Trends and Challenges in the Industry

Historically, there has been little convergence between manufacturing and enterprise in the plant network. Instead, there are multiple, separate networks – one network may run fieldbus protocol at the device level, another network may run ControlNet protocol for machine-to-machine communications, while a third protocol – such as Ethernet, or a proprietary network – links the machines to data acquisition and storage units for reporting or archiving. Meanwhile, a separate network, often an extension of the office Ethernet network, is on the plant floor, enabling workstation access to work orders and task instructions. These networks, and the data moved across these networks, have typically been managed and maintained by separate groups within an organization on a separate infrastructure, with minimal communication or interaction. As a result, there is less capability for real-time manufacturing system visibility. This increases overhead and risks inconsistency associated with operations status reports, which incurs the high cost of maintaining disparate networks through the need for staffing multiple fields of expertise in the various types of data networks, the inability to standardize on equipment and infrastructure, and the need for complicated programming interfaces which require constant upgrades and maintenance.

To gain maximum plant efficiency that improves Overall Equipment Effectiveness (OEE), visibility to real-time operational performance of the factory network is required. Faster startup and changeover times are needed to manage installation projects around scheduled shutdowns. In addition, there is a need to reduce the time it takes to debug and troubleshoot performance issues. Simplification of the network is especially important when personnel resources are limited.

Another trend that requires attention is the growth in quantity of Ethernet nodes on the plant floor. Ethernet has entered the domain of real-time production control and is becoming common at the device level to include communications between drives, Input/Output (IO) devices, Human-Machine Interfaces (HMIs) and more. As Ethernet-enabled devices have been added on the plant floor, questions arise relating to the domain in which the associated network should be managed. Since Ethernet networks are traditionally the realm of the IT functional groups, the implementation of this network is frequently assigned to the IT organization. However, the devices and network are critical to the plant controls environment, therefore manufacturing and process engineering teams are critical stakeholders and often take full responsibility for the portions of the network that impact immediate operational performance. The result is a network that does not fully accommodate future needs of the plant such as scalability and operational visibility, and can sometimes present reliability risks.

In addition to the growth of Ethernet from the device level in the plant, the network has also been expanding organically from the control room out to the plant in order to enable Manufacturing Execution and Enterprise Resource Planning (ERP) Systems, operator access to tools such as work instructions, and plant security systems. The presence of both the ERP/Security network and the manufacturing controls network raises questions regarding appropriate network architectures and their physical manifestation, since improper application of the architecture can raise the risk of contamination of the controls network and potential reliability issues or security flaws that can be exploited.

Building Tomorrow's Network

View the Entire Plant Network

The first step to building an effective, scalable plant network is to view it in a holistic manner to understand the software and computing environments that interact with the plant floor, the critical devices at the edge of the network, and everything between these levels, which is shown in the ISA 95 model illustrated in Figure 1. In an enterprise network the edge devices are viewed as elements from which the network infrastructure must be protected. In the plant network the uptime performance of the edge devices are more critical than the network itself, because the activity of these devices drives plant uptime, and ultimately, operational revenue. These edge devices can also be used for critical data to enable objective measurement of OEE and identify opportunities to improve operational efficiency.

Viewing the network in this manner allows the designer to build an infrastructure that removes speculation on how much expansion a switch cabinet will require, which brings consistency and simplification to the design of the backbone cabling. Understanding the holistic architecture in the plant, including the type and positioning of switches and other networking gear that makes up the architecture is key. This awareness allows the systems to be arranged using the most logical approach, given the priority and type of traffic that moves over the network.

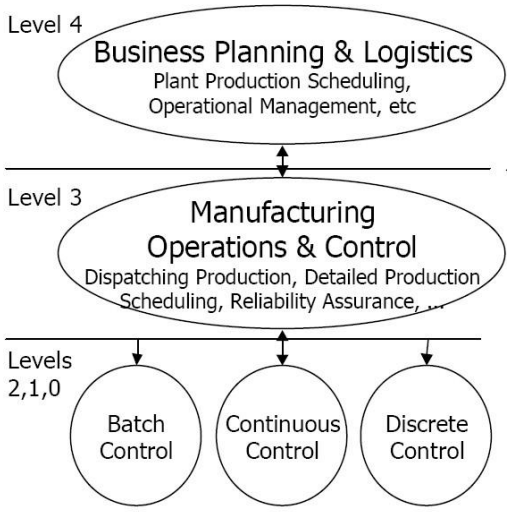

Figure 1. This framework describes the connectivity between the enterprise and industrial zones at a logical level, an important first step to network implementation.

Network Architectures

Considering the plant network architecture is important to understand and articulate how and what type of data flows between various nodes within the plant-wide network. This helps to optimize the efficiency of the network; it enables visibility to potential security flaws within the network; and it can help to provide guidance for how the network can be scaled as the plant expands and as systems are updated and more devices are added to the network. Ultimately, this architecture will affect the physical realization of the network infrastructure.

When considering logical architectures for plant floor Ethernet deployment, a number of options are available which range from complete separation between different networks to a fully converged plant-wide Ethernet network. The architecture where networks are completely separated is commonly deployed in a plant environment. In this architecture, networks operate on different hardware and different physical layers, so there is no communication between these networks on the plant floor or in the control room. This is often selected as the solution for maintaining the security and independence of the manufacturing controls network apart from networks intended to distribute order management, quality and security operations systems to areas within the plant. To maintain consistent separation between the plant floor network and enterprise networks using this architecture, a firewall or alternative gateway which restricts unauthorized access to the control system is typically implemented.

When coupled with a robust physical topology, this option can be a secure method to deploy an Ethernet network for a manufacturing plant. This architecture closely models the historical plant controls networks in which proprietary networks were completely separated from enterprise networks, except where custom-designed gateways enabled data sharing between the networks. This approach becomes challenging since it requires separate server and storage infrastructure which can require its own maintenance effort. While conceptually simple to plan, it is not scalable and becomes expensive and challenging to deploy, since each new network-enabled system, such as VDI, HMIs or security video, require new home run or backbone cabling to deploy. Besides the increased effort associated with network installation and maintenance, a key limitation of this architecture is that it restricts the ability to share data between the different areas of the plant network. Given the need to improve operational efficiency and visibility across the enterprise, an effective architecture to securely and efficiently enable integration of data is required. This architecture will simplify the integration effort required to develop reports on operational efficiency, quality and regulatory metrics.

Unified Network

Attempts to converge and simplify deployment of separate networks have taken several forms. One method involves the use of the same fiber backbone infrastructure that operates completely divergent networks. In this network topology, the same physical conduit (or distribution cable) and Intermediate Distribution Frame (IDF) infrastructure is used to deploy two completely separate networks. Therefore, the actual infrastructure and cabling on which the network operates are different, although they are housed in the same conduit and networking cabinets. Structuring the network in this way does not allow for efficient switch utilization because separate switches are required to segment functional areas. For this reason, virtual local area networks (VLANs) are commonly used to enable efficient traffic segmentation across a group of switches. However, both of these topologies introduce the risk of circumventing plant network security layers through simple cross-patching or other installation errors, which can create gaping security holes in a plant network.

Answering the Challenge

The potential for these security holes has led to the development of a new architecture which addresses security and simplifies convergence within the plant using a standards-based Ethernet network. The Converged Plant-wide Ethernet architecture, a logical networking architecture, was developed by Rockwell Automation and Cisco, and extended to the physical layer as described in the *Panduit Industrial Ethernet Physical Infrastructure Reference Architecture Design Guide*. These resources are proposed as a model for unifying the many disparate plant networks into a single network which helps to address the challenges around implementing, maintaining and scaling the factory network. This architecture uses VLANs to efficiently segment traffic across the Layer 2 and Layer 3 network infrastructure, however all plant control traffic stays below the Demilitarized Zone (DMZ) layer, while any information needed in the enterprise zone is accessed through a server in the DMZ rather than allowing direct traffic between the enterprise and manufacturing compute systems. The implementation of this architecture has a significant impact on how the physical layer is deployed, because a unified architecture can be deployed on a unified physical layer. A unified physical layer translates into lower total cost of ownership in the implementation of the backbone infrastructure, pathways, equipment frames, compute resources, and their associated labor costs.

Realization of a Unified Plant Network

The portion of the network which distributes Ethernet beyond the control room throughout the plant floor is often the weakest part of the network's physical realization. However, as Ethernet expands further into the manufacturing environment, and as a unified architecture is put in place to manage all plant networking and control traffic, those facilities that have a well-planned and structured physical network realization will be positioned to improve operational efficiency and to take advantage of growth opportunities.

Expanding a Flat Network

In addition to security, consideration should be given to planned and unplanned future growth of the network. Each plant environment is different. There may be an opportunity for future green-field plan expansion at one facility, while another may experience frequent manufacturing line tear-down and re-build, or simply growth of Ethernet-enabled devices organically added to a machine. Regardless of the type of growth, the plant manager will usually prefer to avoid putting a large down payment on future growth by installing expensive infrastructure that is not yet needed, choosing instead to carefully consider the structure of the plant network.

The most important characteristic that will help the future scalability of the network distributed across the plant floor is its topology. A zone network topology describes how managed network switches are distributed across the plant, and is generally contrasted to a flat network in which most switches reside in centralized locations or in control rooms. The zone layout shown in Figure 2 distributes managed network switches closer to the endpoint device within an automation cell or process skid. This approach allows the network to follow modular layouts to the plant floor; therefore as the plant is expanded the network infrastructure can grow organically with the plant. Design and implementation of these plant expansions can be simplified by using a building block approach to the network which complements the modular plant layout.

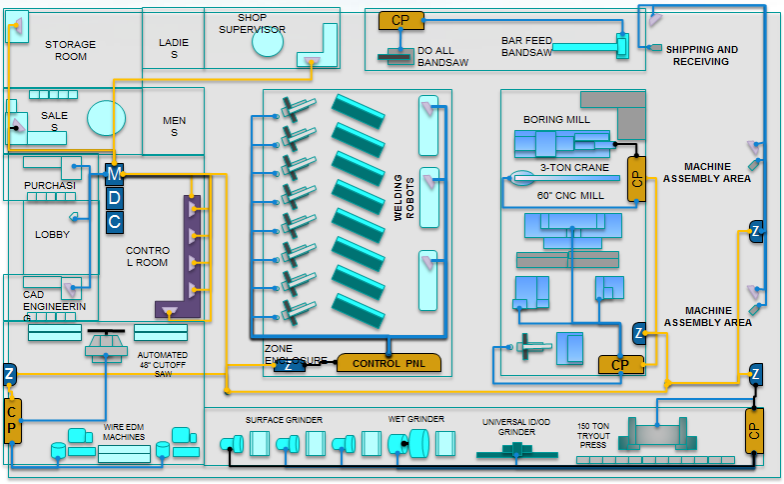

Figure 2. A plant network layout using zone architecture reduces cabling installation, localizes network traffic to improve network resiliency, improves capability for network redundancy and reduces cost of future expansion.

Discrete manufacturing plants tend to organically develop a network that roughly follows the zone approach. Their networks frequently have a clear demarcation between “IT-owned” networks which connect to an “Engineering-owned” network. The functional separation of these two networks provides a barrier to a holistic view of the network, and creates an environment where solving network problems becomes challenging. In this approach the IT portion of the network frequently utilizes commercial-grade 19” rack mount switches that are often deployed within cabinets that do not provide adequate protection from heat, mechanical shock and vibration, moisture, and dust. We frequently see this manifested as IDF enclosures driven down toward the floor level in an attempt to utilize commercial grade components in harsh environments. This is most often done as IT departments strive to control networks closer to manufacturing. However, at some point the actual “controls” portion of the network takes precedence as control engineers build firewalls to prevent undesired enterprise network traffic from interfering in manufacturing traffic.

One method for controlling networks closer to the manufacturing side is to use the Programmable Automation Controller (PAC) as a bridge, forcing control information to remain on one side of the bridge and enterprise traffic to remain on the other side. While this provides a distinctive demarcation line it prevents a clear view of operations and metric information that can be gathered directly from manufacturing hardware. Utilizing an Industrial “tuned” switch in place of the PAC-based bridge is a much better example of modern Industrial Network design.

Using this design practice does not come without challenges, mostly because not all Industrial switches are created equal. By making frequent use of unmanaged switches the control engineer can introduce communication problems for the parts of the network to which they are connected. Unmanaged switches are usually placed with little thought given to scalability of the overall network, with many small port-count switches distributed throughout the plant. This method increases the burden on the network and control room because unmanaged switches are not able to route traffic efficiently, but broadcast traffic to all nodes in the network. Layout problems occur within the infrastructure because a large number of smaller port-count switches increases the number of uplink cables that need to be brought to a zone or consolidation point. Requests for additional ports then create deployment implementation challenges.

Deploying a Zone Physical Architecture

The plant network architecture can be planned to enable effective and efficient management and scaling. A good place to start is by segmenting the automation cell or process control system requiring Ethernet connectivity into sub-systems where there is significant interaction between nodes, or where nodes are placed in close proximity. A brief review of each of these subsystems can identify if there is likelihood for future nodes being added at the automation level. It is important that this is performed at the automation level, because this is the most accurate method for sizing the system to meet the expected future needs of each cell. At this level of the plant, zone systems with industrial managed switches operating Common Industrial Protocol (CIP™) technology (see Figure 3) can then be incorporated into the cell or skid designs.

Figure 3. Integrated Network Zone systems from Panduit can offer 75% reduction in time to deploy.[1]

The practice of building the network with an industrial zone system that supports the automation cell has several critical benefits. Because requirements for scaling up the plant network are generally tied directly to expansion of automation or related plant systems, implementing the network infrastructure can improve overall project planning and deployment time, while reducing the effort required by the Manufacturing IT team to manage the physical layer. This also enables the Controls or Engineering team to incorporate visibility of the network system into the automation control system, to view operational status in real-time and monitor any potential control system problems related to the Ethernet control network. The use of industrial switches ensures that the most critical traffic is prioritized correctly to maximize performance. The most time-critical communications, such as motion traffic, are then prioritized higher than those that are not as critical to the automation system.

Proper design consideration should be given to the implementation of systems that combine commercial-grade Ethernet switch enclosures to support connectivity to Voice Over IP (VOIP) networks, ERP terminals and plant floor wireless networks. The cabinet selected should at least have National Electrical Manufacturers Association (NEMA) 4 for environmental protection, and a cooling system that addresses ambient temperature swings as well as switch heat output. Dust in the plant environment can cause problems with fans in commercial grade switches, for which air filtration and frequent maintenance can help prevent network downtime. Connectivity and power should be managed carefully in these systems, because unmanaged cabling causes challenges with configuration changes, restricts cooling airflow to devices, and makes trouble-shooting network issues nearly impossible. Additional concerns arise when network and power cables become pinched, damaged and/or

[1] Based upon internal timed study evaluating the effort required to design, procure, and assembly a completed industrial network system.

unplugged with the opening and closing of enclosure doors. Plant network risk management requires careful commercial switch deployment and potentially new solutions to help bring network connectivity to the plant floor.

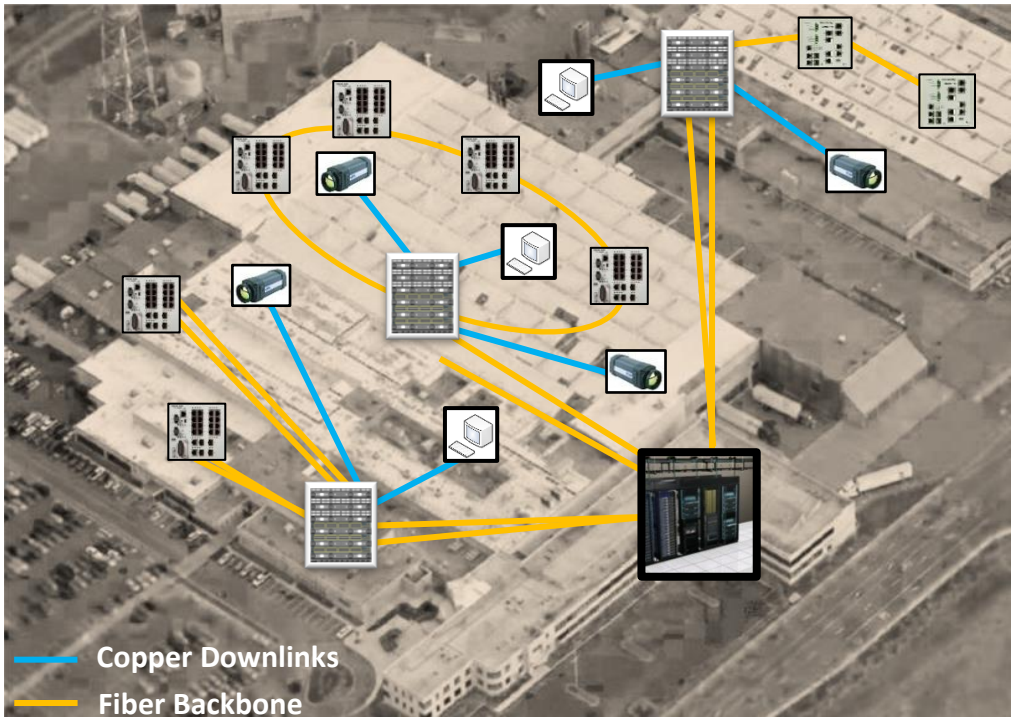

Figure 4. Physical topology of plant network.

Factory-integrated systems (see Figure 4) that are based on commonly accepted architectures and industry best practices can help simplify much of the design effort required to avoid the pitfalls of network deployment onto the plant floor. Using repeatable, validated and tested systems improves the network manageability for manufacturing IT, and provides visibility and reliability to increase the confidence of the plant operations team, and can also be deployed far more rapidly than field-built systems.

Total Cost of Ownership

With appropriate planning for the network architecture and installation considerations, steps can be taken to address risks associated with network expansion. On the plant floor, environmental conditions such as dust, ingress, moisture and temperature can negatively affect equipment lifecycles and uptime. The design of the Ethernet connectivity and media will impact the reliability of the control system network and lack of structured cabling risks incorrect terminations and terminations that do not pass transmission standards. Within the plant connectivity system, a simple cross-patch within a network cabinet or a duplex mismatch on a fiber-optic uplink cable can result in an inoperable network. Deploying multiple segregated networks across the plant floor without careful consideration of the media and structure of the network system adds unnecessary cost and increases risk of downtime.

Benefits of IP Convergence

Converting to standard unmodified Ethernet-based technology such as EtherNet/IP and implementing a converged plant architecture that encompasses all functional networks has a number of advantages to all areas of the organization. When the entire network uses industry standard Ethernet protocol, there is no need for costly translators and software to share data between functional networks or different parts of the plant. When comparing to standard unmodified IP-based robotic cell on a converged Ethernet infrastructure to a similar control system built on serial technology, *a minimum of 15% reduction in implementation costs is achieved* based upon the ability to use proven unmodified IP-based technology for the control system.[2]

When the network is considered to incorporate future needs such as improved security systems and mobility platforms, the manufacturing IT team is able to incorporate these technologies into the single converged plant network. This simplicity of having a network which can be readily scaled to enable future growth and new technology *improves the previous estimate to offer up to a 25% reduction in total cost of ownership*.[2]

Benefits of Zone Industrial Network Topology and Integrated Solutions

The Telecommunications Industry Association (TIA) Fiber Optics LAN Section (FOLS), zone-based network topology models show the relative value of implementing a zone network vs. a hierarchical star network in a manufacturing environment. As shown in Figure 5, the zone network utilizes cabinets at the cell level to manage Ethernet connectivity within the cell, and connects to the control room or IDF via fiber optic uplink. In this example, *deploying the network using zone topology resulted in a 30% reduction in overall implementation costs.*[3]

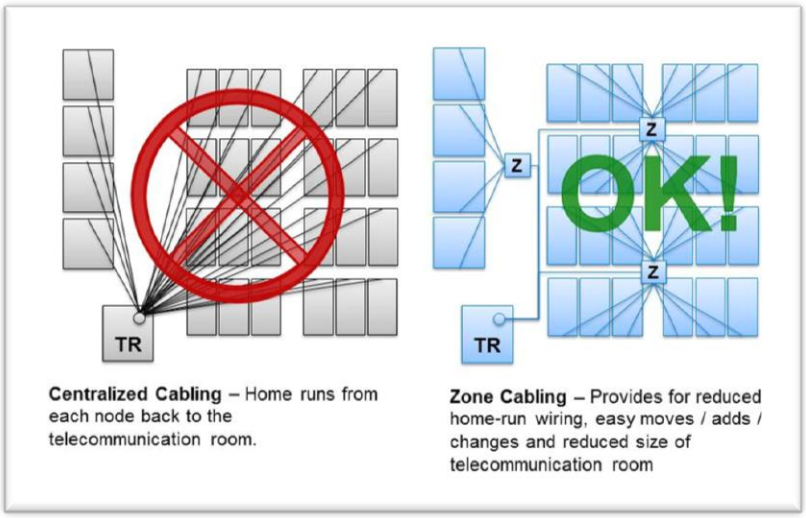

Figure 5. Flat vs.zone network.

The frequent manufacturing system upgrades and implementation of new manufacturing equipment in the plant can make it challenging to keep the industrial network infrastructure at the level of performance required to

[2] Savings estimated using a hypothetical robotic cell design using standard unmodified IP-based control compared to fieldbus or alternative protocols.
[3] Savings are provided based on the usage of zone architecture, estimated by a model developed by the TIA Fiber Optic LAN Section (FOLS).

support the critical plant automation systems. To help enable deployment of reliable, scalable plant networks, Panduit offers fully integrated industrial zone systems that are factory pre-built with industrial switch, power supply and backup. These systems are designed around structured cabling infrastructures recommended by TIA, and tested and validated to ensure performance for harsh plant environments. Structured cabling warranties and Panduit Design Services can help reduce the risk of plant downtime and enable fast, simplified deployment of a network infrastructure. A consistent design which follows best installation practices improves performance by enabling standardization throughout the network architecture on the plant floor. This standardization helps to improve speed to diagnose and repair network problems – Mean Time to Repair (MTTR).

Conclusion

As rapid advancements in networking, computing, data storage and software capabilities increase the value of automation systems, engineers are under pressure to refresh machine and plant-wide system designs with solutions that merge information and control data. To address this challenge, validated architectures and tested physical solutions that integrate information and control systems are growing in importance.

Network convergence is about understanding the trends, challenges and opportunities around the needs of an Ethernet network being distributed to the plant floor. Panduit is leading the effort to build this network from the control room to the industrial network endpoints with our innovative fiber optic connectivity solutions for fast, efficient and simple network backbone deployment. Panduit factory-integrated industrial zone systems significantly reduce the process of deploying a reliable and secure plant network. These systems reduce the time to deploy by up to 75%, while reducing the deployment effort and improving repeatability. At the same time, they enable architectures that can provide 30% reduction in the total cost of system ownership.

Developing visibility to the network beyond the control room and across the plant floor requires you to view the network differently. Panduit can help guide you through this transition with our Advisory Services team, which provides professional network assessment, design, and deployment services to help build an infrastructure that enables the integration of information and control.

About Panduit

Panduit is a world-class developer and provider of leading-edge solutions that help customers optimize the physical infrastructure through simplification, increased 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, unified business foundation. Panduit provides flexible, end-to-end solutions tailored by application and industry to drive performance, operational and financial advantages. Panduit's global manufacturing, logistics, and e-commerce capabilities along with a global network of distribution partners help customers reduce supply chain risk. Strong technology relationships with industry leading systems vendors and an engaged partner ecosystem of consultants, integrators and contractors together with its global staff and unmatched service and support make Panduit a valuable and trusted partner.

www.panduit.com · cs@panduit.com