Automation World® TACTICAL BRIEF

Factory Floor Network Deployment

CONTENTS

Deploying Fiber Optic Networks

As industrial networks get larger and the equipment on these networks perform more complex tasks at higher speeds, there's a growing need for more bandwidth.

By Terry Costlow, Contributing Editor, Automation World

Many network managers are turning to fiber optics to meet these demands while also gaining other benefits.

Many front office systems have already migrated to fiber, and it's seeing increasing use as a central connection for linking the plant floor to the business network. Many companies say that it's the best way to ensure that there will be enough bandwidth to handle growing needs.

Cisco and Rockwell recommend using fiber uplinks, saying it will always be faster than copper.

Fiber optic connections allow distances of up to several hundred kilometers, whereas copper connections only allow distances in the 100 m range. Another benefit is that it is not affected by electro-magnetic interferences. In environments where fire or explosions are likely, it's safer than copper. For many, these benefits make fiber an obvious choice for backbones. Fiber and copper both have their place in industrial applications. You just have to make sure to choose the best one for the application.

Where that divide occurs, however, is not simple to determine. In many applications, fiber is seeing little use beyond the backbone link between plants and offices. It can be beneficial in demanding applications like motion control and video inspection, but copper is also often a practical solution. Networks can be segmented so these demanding functions are isolated, obviating the need to shift to fiber.

One of the big drawbacks for fiber in the past has been its cost of installation. Panduit has developed techniques that eliminate many of the steps that drive up the cost of installing fiber.

"We've got a polymer-coated fiber, released last year, that you can just strip and clip on a connector without the gluing and polishing that's been required in the past," says Dan McGrath, industrial automation solutions manager at Panduit (www.panduit.com). "There's also less waste, and you eliminate the time of gluing and polishing."

Ethernet: It's All About Availability

The trend across the manufacturing and process industries is clear: Network users expect higher reliability, faster speeds and wireless connectivity.

By Terry Costlow, Contributing Writer

The shift to Ethernet has brought many benefits, but it's also created new challenges for those who manage industrial networks. Industrial users expect to not only have the bandwidth and ease of use they see in home and commercial applications, but to have it all live up to Google levels of reliability.

These high expectations are prompting many networking teams to reexamine their infrastructures. One of the foremost demands in industry is that networks never shut down.

"Companies like Google, Amazon and Facebook have set very high standards for availability," says Ben Orchard, application engineer at Opto 22.

Network managers are responding with a number of strategies. They're moving to faster versions of Ethernet, altering their networking architectures to provide fault tolerance, and expanding connectivity with wireless links. All this is happening in conjunction with steps to make industrial network environments more secure.

Speed Tops the List

Leveraging Ethernet improvements, driven by commercial applications, is one of the many rationales for employing the network in industrial applications. And what is perhaps the biggest advance in the commercial Ethernet world—ever increasing speeds—is what tends to attract a great deal of industry interest. Gbit Ethernet is beginning to already see increased use in automation environments, and 10 Gbit Ethernet is starting to see some acceptance.

However, there's still plenty of debate about where anything beyond 100 Mbit Ethernet is needed and where it's superfluous. Most observers feel that Gbit and higher architectures have a solid place as a backbone that connects the factory floor to the front office, largely because these backbones often also link many subnetworks together.

"We see a lot of Gbit Ethernet between switches and uplinks. It's mixed with 100 Mbit full duplex on the plant floor," says Gregory Wilcox, business development manager for networks at Rockwell Automation.

When and where those end devices need high-performance connections is open for discussion. Industrial devices often send small amounts of data, and many of them don't send these small data packets very often. Thus, there's little need for high-bandwidth links in these environments.

Others say that the economic downturn prompted many plant managers to closely examine their requirements when they buy new equipment. In good times, plant managers tend to adopt faster networks in many areas so they will be prepared for higher requirements that may arise in the future. But when money's tight, they design for real-world demands.

"The need to chase speed has plateaued in industrial environments," Orchard says. "People are finally getting their heads around the concept that 100 Mbits is adequate for 98 percent of what they do. When money was available, everyone wanted the fastest network. When the economy tanked, they looked more at their actual bandwidth requirements."

However, some suppliers remain bullish on faster versions, promoting both Gbit and 10 Gbit Ethernet. One of their rationales is that as applications are added down the road, 100 Mbit Ethernet may cause bottlenecks. They also note that, as more video is used, such as with video inspection and security cameras, bandwidth requirements will soar.

Rethinking Network Architectures

One of the key elements in a high-reliability communications system is the network architecture. Today's networks are laid out using techniques that prevent downtime caused by a single point of failure. In such layouts, problems like broken cables or switch failures won't cause communication outages.

There are many factors that help ensure that these ring architectures are cost-effective and provide both high performance and high reliability. One is that switches are no longer limited to standalone boxes. They're embedded into many different types of equipment.

"There's been a move to device-level topologies with switches built into devices," Wilcox says. "You can go from a switch-level star to switches on devices on a ring topology."

Many devices now provide more than one port, making it easy for installers to ensure that connections won't be interrupted even if a cable is disconnected or broken. These physical enhancements are being augmented by different protocols that help reduce downtime.

"More people are using the dual Ethernet connections we put on our controllers," Orchard adds. "Redundant networks are becoming much more common. Technologies like rapid spanning tree protocol are also seeing widespread use. Fault tolerance has become much more

Accelerate Deployments While Reducing Risks

The Panduit Integrated Network Zone System enables network communications between the control room and manufacturing floor within an industrial facility. Integrated with an Allen-Bradley Stratix switch, the pre-engineered, tested and validated system reduces deployment time up to 75%.

Continued
Ethernet: It's All About Availability

cost-effective for small and mid-sized businesses."

Adopting managed switches is another technique for reducing failures. They cost a bit more than unmanaged switches, but they bring several advantages.

Though many technical issues must be considered when high-reliability networks are being installed or upgraded, managers must also consider the human side when they're installing equipment. Installers must be trained to understand nuances that can cause problems.

The Rise of Wireless

Wireless links have become an integral part of the communications infrastructure for many industrial facilities, and there aren't any signs that its usage will subside. Cabled connections offer far higher speeds, but there are many areas where cables aren't beneficial or practical.

In recent years, tablets and smartphones have become another driving force behind wireless. Many of the early wireless networks were installed for sensors and laptops. As the computing power and availability of smartphones increased, more employees started using them in industrial areas. A growing number of companies are letting employees link their small handheld devices to the industrial network.

"Using your own device is really becoming a big deal. People aren't having to check their iPads or smartphones at the door anymore," Orchard says.

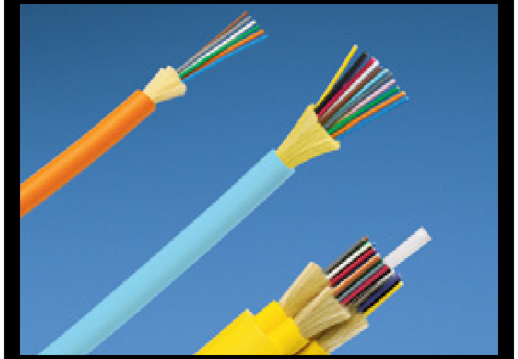
Proprietary networks designed specifically for industrial applications were once common for wireless industrial networks. But managers who already leverage the pricing volumes and technical support of Ethernet are adopting the commercial technology promoted by every coffee shop and hotel—Wi-Fi. Based on the IEEE 802.11 standard family, Wi-Fi is provided in every mobile device, and reliability has soared as usage has spread.

Wi-Fi is taking over in many areas, but it's not the only alternative for plant managers who want to install sensors, cameras and other equipment in their facilities. Other technologies let managers add nodes without the cost and trouble of running cables. Power over Ethernet (PoE) provides a simple way for users to add equipment in areas where adding a power cable might be difficult, but stringing an Ethernet cable is not a problem.

A few years ago, the PoE standard was upgraded to provide 25 W using conventional Ethernet connections. Many companies have devised techniques that boost that to 30 W, with others pushing power capabilities up to 60 W. These upgrades have made it viable for many industrial products.

"We're seeing a lot more interest in PoE," Orchard says. "The cost of switches has come down, and people see how clean it is to have communication and power on one cable. We see even more usage as IPV6 (Internet Protocol Version 6) makes plenty of IP addresses available."

Provide a Strong Infrastructure



Opti-Core IndustrialNet Polymer Coated Fiber (PCF) Cables are ideal for installation in harsh, industrial environments and are suitable for applications that demand high mechanical integrity and reliability. They are available in both interconnect (FBSP52--WW-ENG) and breakout (FBSP51--WW-ENG) versions. Small form-factor simplex or duplex LC connectors (FBSP55--WW-ENG) are designed for use with graded index, OM1 and OM2, Polymer Coated Fiber (PCF) in industrial networks with minimal installer training.

Recipe for a Robust Ethernet Network

Ethernet has gained critical mass as the industrial network of choice. Automation and control engineers can dig into some of the details of cabling, managed switches and topologies here, and leave satisfied with ways to achieve optimum manufacturing network performance.

By Gary Mintchell, Co-Founder and Editor in Chief

There are two things we know about Ethernet used in manufacturing and production and one thing to be aware of for the future. First, Ethernet has become the de facto standard network in many industries. Its use even to the input/output (I/O) level has become common. Second, since Ethernet is used by both enterprise and industrial systems, it has become the focal point for the age-old battle between automation and control engineers and information technology (IT) engineers.

David McCarthy, president and CEO of TriCore, Inc. in Racine, Wis., says, “Industrial Networking is a whole new business area. The plant floor, front office and boardroom are all converging from an information-flow standpoint. Many of the plant floor networks in use today are not commonly understood well by corporate IT staff. Front office and enterprise networks are often not commonly understood well by engineering staff. Designing a robust network solution that satisfies the needs of the maintenance staff, engineering, production managers, plant managers and users of corporate IT systems—not to mention system integrators and other suppliers who may be remotely supporting a facility—requires a unique understanding of how all of this hangs together.”

Cooperation with IT

“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 start-up 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." (See White Paper, "Scaling the Plant Network An Approach to Industrial Network Convergence")

Security sticks out

Security is another sticking point with IT people, who never believe that automation people take it seriously. From engineering point of view you can implement VLANs (virtual local area networks), Layer 3 switching, firewalls with DMZs to combat the security issues. Think in zones and conduits. Know the traffic between zones and watch then alert if something not known is seen. And (remember that) there is never enough separation of networks on the control side.

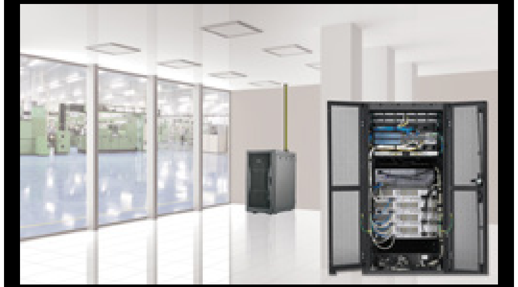
So, what do we need to know about the physical media of an Ethernet TCP/IP network?

As virtualization, consolidation, and convergence initiatives continue to be adopted, so do the demands placed on the physical infrastructure. Next-generation networking architectures deliver enhanced performance characteristics and capabilities to help reduce the risks associated with availability, reliability, and agility.

With today's Ethernet speeds, especially on the industrial floor, there is the necessity to have a good quality data cable that can withstand the harsh environment. Shielding in, or on, the cable is especially critical. It is essential to eliminate any interference coming from its surroundings. If there is the requirement to run a network cable alongside a power cable, two things should definitely be considered: A shielded cable is a must, but also consider a raceway or wire-way type of product.

Mike Hannah, manager of product development for networks at Rockwell Automation,

Increase Your Network Security



Prevent unauthorized access or accidental breaches by establishing a robust physical network infrastructure that offers barriers to network-wide security risks through the use of an integrated physical and logical architecture that includes Panduit Micro Data Centers.

Recipe for a Robust Ethernet Network

Milwaukee, adds, "You've got to assure good ground plane, cable management, grounding, bonding, shielding and good control panel design. Everyone knows Ethernet, but in an industrial setting, things happen like the tabs break off the RJ45 connector. When a machine has a fault and the operator calls maintenance, it may have just been the cable or a loose connector."

The optical performance expectations for optical channel links are specified in commercial cabling standards such as TIA-568-C.1 and IEC 11801. These standards specify the expected power loss in installed fiber cabling based on fiber type, number of mated pairs of connectors deployed, and number of fusion splices (if present). This assures that channel links comprising legacy fiber types, lower bandwidth fibers, or channels containing numerous connector interfaces or splices operate reliably. (See White Paper, "Fiber Optic Infrastructure Application Guide Deploying a Fiber Optic Physical Infrastructure to Support Converged Plantwide EtherNet/IP" authored by Panduit, Rockwell Automation and Cisco)

Topologies

Plantwide deployment of EtherNet/IP requires an industrial network design methodology. Following a methodology helps create a structure and hierarchy to help maintain real-time network performance. In addition, it helps enable the convergence of multiple control and information disciplines, including data collection, configuration, diagnostics, discrete, process, batch, safety, time synchronization, drive, motion, energy management, voice, and video.

The Fiber Optic Infrastructure Application Guide also points out that "A highly effective way to deploy EtherNet/IP solutions throughout the CPwE architecture is to physically distribute cabling runs using a zone cabling architecture for all plant networks. Zone cabling enables facility systems to be converged with Ethernet cabling pathways as they are being designed. This converged multi-technology backbone comprises Category 5e/6/6A copper, optical fiber, coaxial, RS-485, and other fieldbus cabling. These systems are converged within a common pathway and then terminated within zone enclosures distributed throughout the plant.

A zone cabling architecture with Stratix switches in network zone enclosures provides a platform for implementing small VLANs for cell/area zones as recommended under CPwE to improve manageability and limit Layer 2 broadcast domains. The VLAN approach allows one zone enclosure to feed network connections to high priority manufacturing control system nodes as well as lower priority connections for printers or data collection, while segmenting and isolating traffic. The network segmentation for these VLANs is made visible using features of the Panduit physical infrastructure, including color coding for the patch fields and physical security such as lock-in/blockout devices on connection points or physical keying solutions that prevent inadvertent patching mistakes.

Embedded switch technology embeds popular Layer 2 switch features directly into EtherNet/IP devices and controller hardware to support high performance applications, without the need for additional configuration. This technology enables device-level linear and ring topologies for EtherNet/IP applications. These types of devices are found in levels 0–1 of the CPwE logical model."

Gregory Wilcox, business development manager for networks at Rockwell Automation in Milwaukee, says, "They're building large flat Layer 2 networks, but networks still need a structure and hierarchy. You should build domains then into a Layer 3 switch where they can see things. You use structure and hierarchy to avoid network sprawl."

Since Layer 3 switches use IP addresses, setting those addresses for devices becomes crucial to finding them on the network. Wilcox, again, "There are a couple of ways to set IP addresses. One is on most devices we deploy

3-switch method. It could be rotary or push pin. You set last octet number. Since 192.168.1 is the first three octet default, so the 3rd shift guy only needs to look at the device, see what the setting is, set the new one, plug in and run."

Overall, "Ethernet is the enterprise technology enabler. It allows interaction of control and IT worlds," says Peter Esparrago, Maverick plant floor 24 of Maverick Technologies, a Columbia, Ill.-based system integrator. "Lots of plant and operations guys just don't trust IT. So they look at Maverick (and other system integrators) as a bridge. Regarding security, plant floor guys don't think they're vulnerable, but many are becoming aware. We apply same best practices, such as defense in depth."

Esparrago says integrators keep production up and running: "Corporate IT has been monitoring networks, but more at the WAN-Router-Business network and stop at DMZ (if there is one). They don't see much when going lower, so no one is monitoring at the control level. The need is to monitor from device layer to business layer. Engineers want us to monitor up to Level 2 because they don't trust IT."

Jason Montroy, client relationship manager at Maverick Technologies adds, "Ethernet networks allow for more remote monitoring. We can offer support 24/7/365. As Ethernet became established, plants that had issues could call in internal resources for trouble-shooting and repair. Now, we've developed a pool of resources so users can tap in and access resources without travel."

Sponsored Content

How to Design Networks for Plant-wide Communication

Learn how an integrated zone cabling plan can slash network deployment time up to 75%, cut down on material and labor costs, and allow for future expansion.

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.

To get connected globally into industrial operations, users need validated logical diagrams of the functions in the network and the interface with enterprise systems. This logical networking architecture, developed by Rockwell Automation and its Strategic Alliance Partner Cisco, is commonly known as the Converged Plant-wide Ethernet (CPwE) Design and Implementation Guide. This reference architecture describes the connectivity between the enterprise and industrial zones at a logical level.

Key within the logical architecture is the identification of communications pathways from the Level 3 Site Operations to Levels 0-2 associated within Cell/Area zones on the plant floor (see figure on page 13).

The physical layer architecture is the infrastructure required to achieve connectivity that addresses 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.

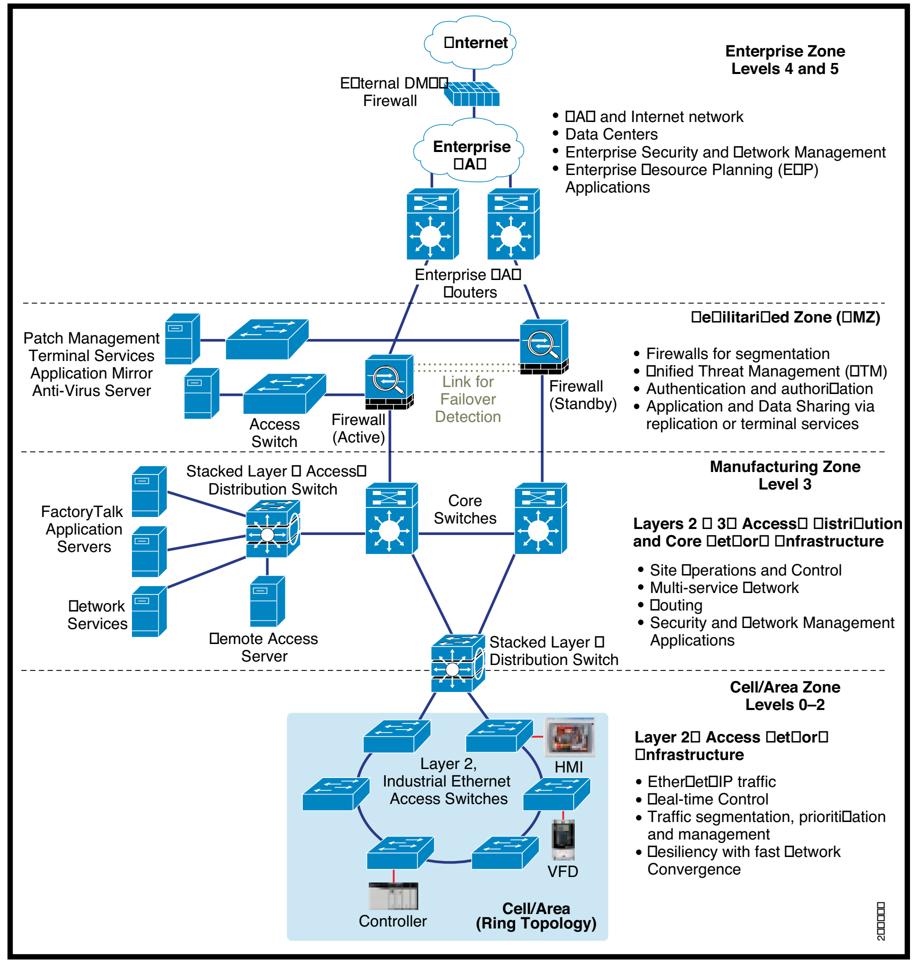
Making the Right Connections For physical architecture network support, Layer 3 switching is typically deployed in the Level 3 Site Operations (industrial data center). Layer 2, or direct physical connections, are made into zone enclosures or control panels, or are connected directly to equipment located within the Cell/Area Zone plant floor. The physical environment of plant floor equipment and the distance away from the control room, which acts as an interface to the Level 3 Site Operations, determines the characteristics of the cabling solution needed. Assess environmental risks by leveraging TIA 568-C.0 “Generic Telecommunications Cabling for Customer Premises, Annex F: Environmental Classifications.”

When determining the cable solution, consider the mechanical, ingress, climatic and electromagnetic (MICE) conditions. This ensures the entire cable protection scheme — cabinets, pathways, grounding/bonding and cable selection — is appropriate for the environmental hazards present.

Traditional structured cabling deployed in CPwE automation networks involves multiple horizontal copper runs all the way from the Level 3 control room to each automation control panel within the Cell/Area Zone. This type of cabling is also called a “home run.” For very small deployments, this approach works ne. But in many environments, traditional structured cabling can mean hundreds of lengthy copper cables that are difficult to manage, present electro magnetic interference (EMI) susceptibility challenges, become virtually impossible to change, and are arduous to remove when complying with building codes that require removal of abandoned cable.

On the plant floor, traditional structured cabling is routed from the micro data center (MDC) to a control panel or zone box containing active equipment. Alternatively, a zone cabling approach involves a logically placed connection point in the horizontal cable, routing it from the MDC to active zone boxes. Shorter cable runs then extend from the zone box to each device in that zone (see figure on the right).

A number of factors must be addressed when connecting the Cell/Area Zone to the Level 3 Site Operations control room. Users must decide on architectures, physical media and connectivity to distribute networking that’s cost-effective while ensuring enough flexibility, environmental ruggedness and performance headroom to hold up to



Popular Configuration Drawings
To get started designing your industrial network system, to download your copy of our “Industrial Switch Deployment Popular Configuration Drawing”.
Visit www.panduit.com/IntegratedZone-CE

current and future manufacturing needs.

Integrated Network Zone Systems

In applications where switching equipment is used on the plant floor, it's necessary to place the switch in a protective zone enclosure. The zone enclosure also houses other ancillary equipment required for the switch, such as an uninterruptible power supply (UPS), copper and fiber connectivity.

Following a zone topology allows a highly scalable and flexible physical deployment of the CPwE architecture. Managed cabling reduces abandoned cable and the number of home runs throughout a facility, helping make the workplace run more efficiently and safely. An integrated network zone system is used to deploy plant-wide EtherNet/IP™ networks and helps ensure that management and network control won't hinder the most effective use of data available. An integrated system incorporates all active and passive equipment required for deployment.

Features and benefits of using an integrated solution system include:

- Reduced deployment time by up to 75% with a pre-engineered, tested and validated solution
- Touch-safe and UL508A-rated integrated industrial and IT networks
- Reduced downtime with a robust, future-ready, reliable network system that provides simple and easy moves, adds and changes (MACs)
- Reduced material costs up to 30%

Long-Term Benefits

Validated logical to physical network systems can help remote users manage productivity and profitability. With such a system, users can access real-time data on machine operations and take necessary action if pre-assigned metrics aren't met. Plant-wide communications become more efficient and future ready as users migrate proprietary plant floor networks to a single network technology using the EtherNet/IP open protocol.

Whether users are updating existing systems to meet growing information demand needs or planning plant expansions, the amount of development and implementation rework time can be costly. Implementing validated solutions in the physical design of a network system can reduce your deployment time by up to 75%, ensuring that optimum performance and reliability of your network's physical design are obtained. This helps maximize uptime and reduces costs associated with problem solving and network downtime.