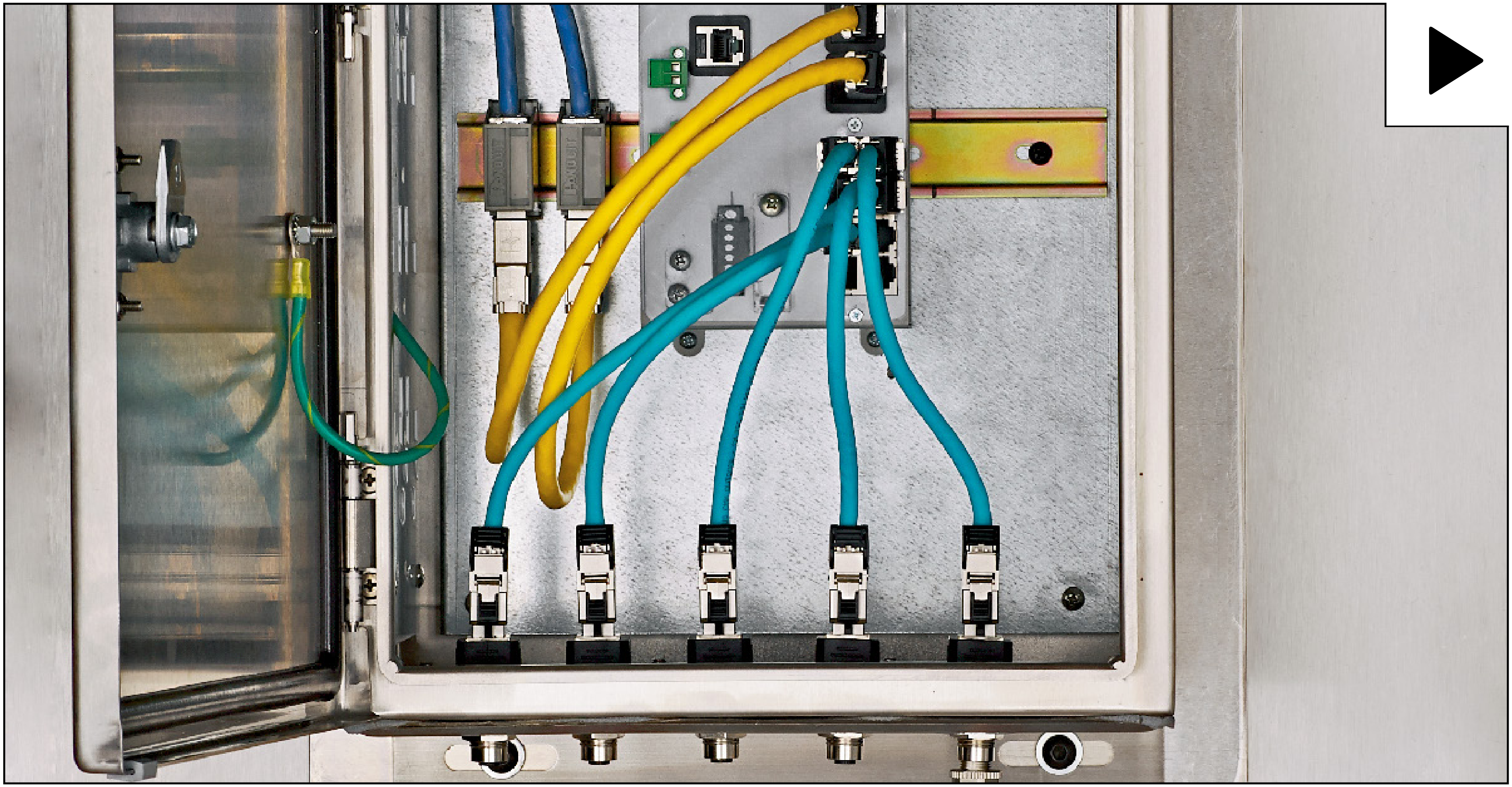


Automation World® TACTICAL BRIEF

Factory Floor Network Reliability

CONTENTS

SPONSORED BY PANDUIT®

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 (www.opto22.com).

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 (www.rockwellautomation.com).

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 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.

Continued
Ethernet: It's All About Availability

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."

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. (www.tricor.com) 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 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." (Scaling the Plant Network An Approach to Industrial Network Convergence" White Paper).

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 (www.rockwellautomation.com), 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. ("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/block-out 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 Technologies (www.mavtechglobal.com), 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."

Improve Industrial Ethernet Network Uptime

By Robert Reid, Panduit- April 2014, Industrial IP Advantage Article

What we are seeing today in manufacturing is an update of plant network architectures with solutions that securely merge information and control data to improve performance, security and safety within the plant. Network uptime is becoming increasingly important as Ethernet is starting to be deployed for critical and time-based processes, where keeping such discrete networks active through a fault without stopping critical processes is paramount.

Given that greater than 60% of Ethernet link failures are related to physical infrastructure (Grenier, 2011), it is important from the outset to design and build a resilient network that is architected to recover (converge) quickly from a failure condition.

Switching and signaling delays are affected by media type (Fiber/Copper), media length, number of switch hops and transceiver type, whereas processing and reservation time are independent.

Convergence occurs as a result of a change in network topology, i.e., a physical link failure. When this occurs, a routing algorithm is run to build a new routing table based on the failure condition/location. Once all the routing tables have been updated, convergence is complete.

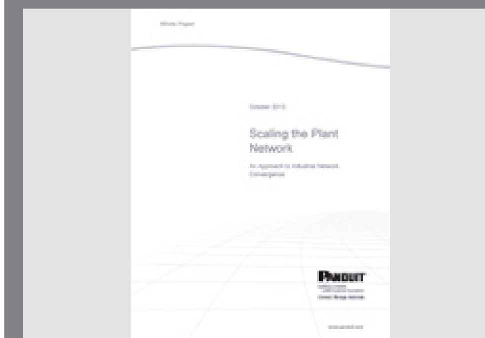
The convergence time to recover and restore from a failed path condition depends on several factors. In restoration, switching occurs after backup paths are computed following the receipt of failure notification. The convergence time to recover a single path is the sum of the following:

1. Signal delay: time to signal a network failure between nodes (largest component)
2. New path processing delay: time taken to compute an alternate path
3. New path reservation delay: time required to reserve on newly computed path
4. Switching delay: the time required to switch from affected path to new path

For a detailed experimental validation of convergence time over different media (copper fiber) and transceiver sets, refer to joint Rockwell Automation and Cisco work on network resiliency.

One of the main findings of this study is that fiber offers higher resilience through convergence

Scaling the Plant Network


Scaling the Plant Network

PANDUIT

This NEW White Paper describes how Panduit Industrial Network Deployment Solutions can improve reliability, security, and safety of Industrial Automation systems, offering up to 30% reduction in deployment costs and 75% savings in deployment time.

times for uplinks and rings as compared to copper. In the network architectures covered, network availability and performance benefits described can be achieved by deploying robust fiber optic cabling channels as shown in the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (ENET-TD001).

One way to achieve high resiliency on uplinks is to deploy a redundant star topology utilizing a redundant pair of fiber links on a single switch, one active and one acting as a standby (Cisco FlexLinks and LACP for example). Convergence times here can be less than 50 ms.

High resiliency/low convergence time on rings can also be achieved through protocol (REP - Resilient Ethernet Protocol) with fiber where we have critical processes that require a few ms of convergence.

Obviously, not all industrial ethernet applications have strict requirements on convergence time. Required convergence times depend on the tolerance of the system to withstand a loss of communications and the risk posed. Convergence time requirements vary from information processing, such as Human Machine Interface (HMI) applications, where less than 1 second is acceptable, to critical motion control applications where a handful of msec is required. Choice of physical infrastructure (architecture, media types, transceiver sets) vs convergence requirements should be studied in the light of total installed cost.

The most common pushback to deploying fiber in such networks, is that solutions tend to be expensive and "craft sensitive" with high learning curves. Fiber solutions today have evolved to be much easier to deploy in factories and plants and there are new ways to terminate that are more "electrician friendly". The "Deploying Panduit Polymer Coated Fiber (PCF) Cable" video shows deployment and termination of an Interconnect cable within a cabinet for an industrial application.

New installer friendly industrial automation fiber optic cables are designed with technicians in mind and are ideal for harsh, device-level industrial installations. Cost effective, large diameter, high strength GiPC fiber (Graded Index Plastic Clad Fiber), like hook-up wire, is easy to prepare and terminate with LC Crimp and Cleave connectors using hand-held tools and minimal training. A good resource for applying fiber with industrial applications is the Fiber Optic Infrastructure Application Guide.

A Structured Approach to Cabling

As more manufacturers deploy Ethernet with an eye toward the leveraging the possibilities of the Internet of Things and Big Data, it's easy to overlook the structure that make it all possible—cabling. Here's how a structured approach to cabling can future proof your industrial network.

By David Greenfield, Director of Content/Editor-in-Chief

Amid all the interest in Cloud Computing, Big Data, the Internet of Things, and wireless connectivity in industrial applications, one thing is certain—cables are not disappearing any time soon. Though industry's cabling requirements have changed dramatically in the Ethernet age, they remain central to industrial network infrastructure.

To get a better idea of what manufacturers need to focus on to ensure the viability of their network cabling infrastructure, I spoke with Andy Banathy, industrial automation solution architect at Panduit, a provider of electrical and network infrastructure systems and support services.

Panduit supports both structured and traditional point-to-point cabling, but it is structured cabling that is best positioned to support the future direction of automation technology developments. In essence, structured cabling refers to a set of cabling and connectivity products that integrate data, voice, video, and control, as well as system management technologies.

"Structured cabling systems are capable of evolving with the future," says Banathy. "Industrial data rates eventually will meet and potentially surpass the 10-gigabit per-second level already common on the IT side. Meanwhile, industrial processes and machines are becoming more intelligent, employing advanced instrumentation, sensors and wireless technology. Gaining the full benefits of structured cabling requires an equally systematic approach to conceptualizing, specifying, installing, testing and maintaining plant wide networks."

Banathy explained that structured cabling systems comprise several subsystems:

- The demarcation point, where the telephone or Internet company ends and connects to the on-premises wiring.
- The equipment or telecommunications room, which houses equipment and consolidation points.
- Vertical or riser cabling, which connects equipment rooms, usually between different floors.
- Horizontal wiring that connects equipment rooms to individual outlets or work areas, usually on the same floor.
- The work area, where user equipment connects through outlets to the horizontal cabling system.
- Entrance Facility — the location where external communications enter the facility. This serves as the demarcation point between the standards and regulation requirements for outside plant vs. inside plant.
- Equipment Room (ER) or Data Center (DC) — the top level of enterprise/building network and may link to higher level corporate network and business system tiers.

- Enterprise Telecommunications Rooms (TR)—Houses the horizontal and backbone cable terminations and distribution switching. Cross-connections of horizontal and backbone terminations using patch cords to extend services to telecommunications outlets may be performed here.
- Enterprise and Factory Riser (Backbone) Cabling — Connects the enterprise ER/DC to enterprise TRs and to the Industrial TR (micro data center).
- Enterprise Horizontal Cabling — Connects the enterprise TRs to zone cabling systems, intermediate distribution frames or wall outlets.
- Micro Data Center (MDC) — A specialized TR that provides a logical separation of equipment and facilities between the enterprise and factory networks.
- Work Area or Cell Horizontal Cabling — Connects the MDC to the factory outlets, zone cabling systems, control panels, consolidation points and zone cabling (routed via trays, conduits and J-Hooks).
- Enterprise and Factory Outlets/Cabling — Work area components from the outlet of the horizontal cabling to the enterprise or factory work area equipment (connected with equipment or 'jumper' cords).

Building a Structured Cabling Network

The most effective way of deploying industrial Ethernet networks, according to Banathy, 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. These systems are converged within a common pathway and then terminated within zone enclosures distributed throughout the plant. This accommodates frequent downlink moves-adds-changes typical to the factory floor.

Cabling in these subsystem areas follows a defined form referred to as "the channel," says Banathy. The channel is composed typically of an equipment cord (a patch cord at the equipment end), the permanent link (fixed, solid conductor cabling) and a work area cord (a patch cord connecting to a work station).

The permanent link is a pivotal feature of a structured cabling system because it allows the uplink to be tested from the machine to the higher-level network, helping ensure the connection and the machine both will perform as needed. "Likewise, in a ring network that connects multiple processes, a structured cabling configuration allows each link to be tested," Banathy adds. "In addition, having spare permanent links accommodates future growth on the factory floor."

Herein lies one of the biggest differences between structured cabling and traditional point-to-point cabling: Point-to-point cabling systems seldom, if ever, involve testing. "Instead, when plant personnel need to add another machine or extend the reach of a cable, they may simply use a patch cord and plug it into a switch panel," says Banathy. "Some experienced control engineers are accustomed to creating their own patch cords by stripping off the jacket on a wire and attaching a connector on each end. These patch cords terminate in a plug, rather than a jack. These practices don't always provide a future-proof cabling infrastructure."

One problem with such point-to-point practices is that they are often appropriate only for shorter patch-cord lengths. If a patch cord is extended to 80 or 90 meters, however, it can fail to deliver full performance due to less conductivity and higher insertion loss than the solid conductor cabling used in structured cabling systems.

Structured Cabling Checklist

To implement and maintain an optimal structured cabling infrastructure, Banathy suggests following these steps:

1. Get educated on common best practices for critical fiber and copper connections within network infrastructures. Banathy specifically stresses learning how to:

- Terminate horizontal runs to patch field connectors to form permanent link;
- Validate performance with standards-based tests and equipment;
- Easily replace patch cords if they are damaged or suspect. "You do not need to touch the horizontal cable," adds Banathy; and
- Improve troubleshooting with well-identi-

fied, structured connections that support staff can easily manage.

Banathy also suggests learning the standards and best practices established by organizations such as the Telecommunications Industry Association (TIA), the IEC, and industrial protocol groups such as ODVA and promoted by Industrial IP Advantage.

2. Establish goals and objectives. Assess your needs today, while keeping the future firmly in mind. Where will your operation be in 10 to 15 years? With structured networking, industrial plants become more scalable, especially if they invest in the recommended 30-to-40-percent high performance spare cabling at the time of initial installation.

3. Design the infrastructure and draft specifications. Develop a specification document that establishes your structured cabling standards, and the materials required for your particular operation. Specifications should cover how to implement the plant network for reliability, security and physical considerations. Those include the integrity of the cabling itself, since substandard cabling could come with serious consequences.

Banathy points out here that IT and automation personnel should collaborate on the specification document to drive best practices throughout their facility.

“Specifications often detail how to implement structured cabling to connect the enterprise level to distribution zones, and how to bring cabling into the process and individual machines,” he says. “This document also allows you to specify your standards on required bandwidth performance, so you have consistency for today and be ready for the future. You also can specify where it’s critical to locate testing patch points and what your requirements are for testing.”

4. Installation. Because of the many details included in installation, this is the step with the greatest potential for error. For example, plants that want to support gigabit per second communications may buy the correct Category 6 cabling, but it must be installed correctly to deliver that rate.

“Make sure your installer understands the intricacies of working with structured cabling,” notes Banathy. “They need to be aware of details like bend radius and the twist of the cable, the routing, and protecting the network from noise sources.”

5. Testing. Without testing, you risk startup delays, downtime, callbacks to the manufacturer and a host of other costly huge headaches. In addition, best practices call for documentation on testing results from your installer.

6. Operations and maintenance. The system ultimately becomes the responsibility of the industrial automation user. A common problem is the return of the old point-to-point practices, says Banathy. “Someone on the plant floor may decide to put in a new cord to solve a problem or serve a temporary need. But more problems can arise if they don’t bundle it correctly, or fail to identify the connection. Soon, you could have multiple dangling cords and no idea why.” He points out that such patchwork problems can be avoided by clearly establishing and strictly enforcing operational and maintenance policies regarding structured cabling networks.