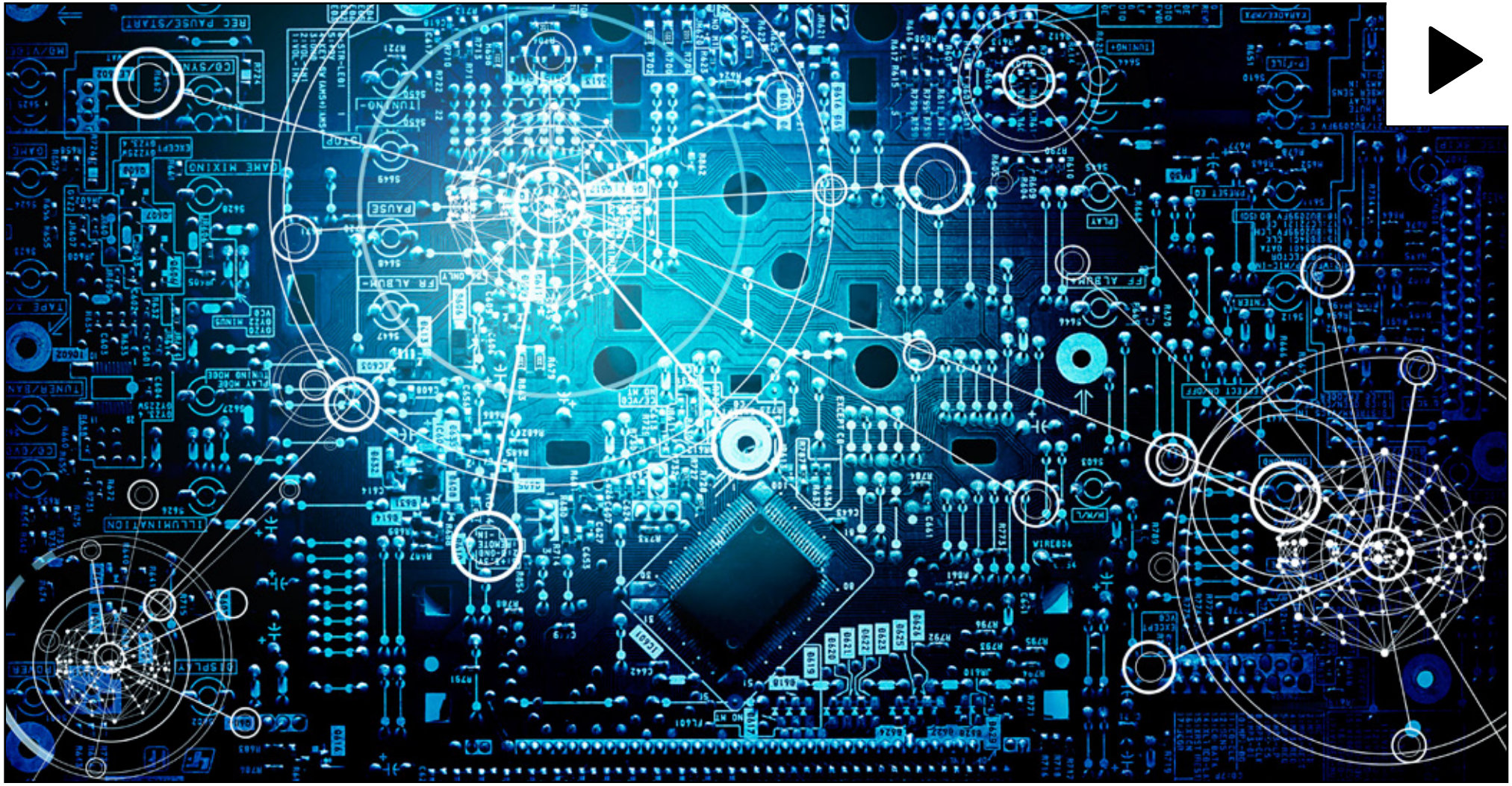

AutomationWorld® TACTICAL BRIEF

Reduce Network Complexity

CONTENTS

02. Standards and Best Practices in the Integrator/ Manufacturer Relationship

04. Partnership Solidifies Work Toward IT/OT Convergence

07. OT Has a Mission-Critical Role

09. Down to the Wire – Building a Resilient Network Infrastructure

15. Resolving Ethernet Connectivity Issues for a Panduit Industrial Automation Customer

SPONSORED BY PANDUIT®

Standards and Best Practices in the Integrator/ Manufacturer Relationship

With the correct blend of experience, standards and best practices, you can focus on the more complex aspects of the automation system, which have the potential to generate more value while reducing the overall development time.

By Larry Asher , Director of Operations, Bachelor Controls Inc.

Recalling the very first automation project I worked on, we were all very eager to deliver a solution that was exactly what the customer wanted. In this case the customer was very vocal in communicating his desires and, during factory acceptance testing, he demanded more changes. We gladly accommodated him. In the end, we delivered the system just as the customer described.

It did not take the customer long, however, to realize that some of his demands left no room for flexibility. Plus, as new controls engineers, the design we created did not easily accommodate the required changes. While the control system performed exactly as the customer wanted, it was not able to accommodate the dynamics and unforeseen events that happen daily in production.

When a system integrator partners with a manufacturer or OEM to deliver an automated controls solution, the integrator not only has to understand the needs of the customer but should consider: standards, industry best practices, and experience. The integrator can then help the customer make well-informed decisions, weigh alternatives, and work in the best interest of the customer with a goal of being recognized as a trusted advisor. The systems created in such a partnership typically have greater performance, lower cost of maintenance, increased flexibility, and a longer service life because they can more easily adapt to process changes and incorporate new technologies.

The Revelation of Standards

It's hard for me to believe now, but there was a time when I sat around a table with very well educated and experienced engineers discussing—for hours—the function of the "stop" button. Would it function as an immediate stop? Complete the batch then stop? Could we resume production? If so, how would we actually stop the process if we did not want to resume production?

This was my introduction to standards.

Later, as a new manager, I remember mentioning the word "standards" to a controls engineering group. They went silent. It felt like I was tossing a wet blanket on the fires of innovation. Many engineers believe standards will tie their hands. In reality, standards allow you to more easily address the routine parts of a process, rather than spending six hours debating the meaning of "stop." With the help of standards, you can focus on the more complex aspects of the system, which have the potential to generate more value for the customer—all while reducing the overall development time.

Continued
Standards and Best Practices in the Integrator/Manufacturer Relationship

Like standards, industry best practices have been developed over time with proven technologies and supported from major vendors. When engineers and developers ignore these best practices, they begin to limit the ability to support the solution and make it more difficult to incorporate advancements in new technology. This places a strain on integrators and engineering departments and increases the cost of system upgrades. It may even result in alienating vendors who are unwilling to support the implemented controls solution.

Of course, there are few instances where proprietary controls are the best fit for a project. However, the majority of manufacturing processes and machine control applications are well covered by best practices. Adopting industry best practices allows you to leverage support from your vendors, increases your hiring pool, and makes the customer less dependent on the solution provider giving them a greater sense of independence. There is a difference between having your customers "depend" on you versus having them be "dependent" on you.

Standards and best practices are the best place to start on any system integration project. The critical role of experience comes into play in the evaluation and application of those standards and best practices. To simply ignore experience is a mistake; to totally rely on experience is just as big of a mistake.

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%.

Partnership Solidifies Work Toward IT/OT Convergence

A decade-old relationship between Rockwell Automation and Cisco Systems has grown up around the insight that the plant floor would need to work more closely with enterprise IT.

By Aaron Hand , Executive Editor, Automation World

If you were one of the almost 19,000 people out at the Automation Fair in Chicago, I'm not sure it would've been possible for you to escape without hearing something mentioned about IT/OT convergence. Although the theme of this year's show from Rockwell Automation was the Connected Enterprise, much of the success of that concept is built around mounting cooperation between operations and the IT folks.

So it was also difficult at Automation Fair—whether you sat in conferences or walked the show floor—to avoid hearing of Rockwell demonstrating that cooperation at a macro level, through its cooperation with Cisco Systems.

As we've been reporting more and more, effective communication throughout the enterprise is becoming increasingly essential. Although operations and IT have not traditionally made nice—often at odds about what the priorities should be—they really can't afford to work in their own silos anymore. Although it's yet to really take hold, there's even a movement toward a new breed of manufacturing employees that combine the best of OT and IT skillsets.

"Central to achieving the Connected Enterprise is the convergence of IT and OT," said Keith Nosbusch, Rockwell's chairman and CEO, in a presentation to industry press. "Historically, these have been two different worlds with different priorities, and base technologies. True convergence between these two worlds has been a challenge."

Rockwell has been co-innovating with Cisco, relying on a standard, secure Cisco network infrastructure to better connect the enterprise, Nosbusch said. "This flatter, more open approach to the industrial network provides performance, flexibility and security that wasn't achievable before."

Industry is probably five to 10 years into blending IT and OT skills, commented Joe Kann, Rockwell's vice president of global business development. Rockwell is working on that mix even within its own company—an effort that is helped by having "the muscle of Cisco behind it," he added.

Rockwell and Cisco have been partnering for about 10 years, said Rick Esker, senior director of Cisco's Industry Solutions Group-EcoSystems, together managing an ecosystem of strategic alliances to help address manufacturing challenges. "There are people in Rockwell dedicated to managing Cisco, and I have a lead who eats, sleeps and drinks Rockwell," he said. "The relationship goes all the way up to the top of the house."

The two companies collaborate on products, services and educational resources to help manufacturers converge their network infrastructure and bridge the technical and cultural gaps between plant-floor and higher-level systems. Last year, for example, Cisco and

Continued
Partnership Solidifies Work Toward IT/OT Convergence

Rockwell launched a training course to help IT and OT professionals overcome the challenges of converging their network technologies. At the Automation Fair later that year, they announced a joint design and implementation guide for deploying wireless equipment.

"This is a space where, to be successful, you need to bring several different organizations together—IT, OT, local and global," said Tony Shakib, Cisco's vice president of Internet of Everything vertical solutions. He explained that success requires not only deep domain expertise of the network, but also the PLCs and other devices. "We want to do this thing in a way that's simple and repeatable, creating a blueprint for any company that wants to go through the journey."

Rockwell and Cisco have a joint lab to test out various device and control configurations, Kann noted, making sure the base connectivity is right for any grand visions of the Internet of Things (IoT). "We had an inkling a decade ago that the IT role was going to grow. We took a leap," he said, explaining Rockwell's choice to partner with Cisco rather than try to develop its own switches or other network know-how. "We bring all of Cisco's R&D power to bear, and their relationship with the IT customer."

The two companies co-developed the Stratix 5700, Stratix 8000 Layer 2 and the Stratix 8300 Layer 3 managed industrial switch lines. They combine the Cisco Catalyst switch architecture with the Allen-Bradley brand to provide secure integration with the enterprise network along with easy setup and diagnostics from within the Rockwell Automation Integrated Architecture. "Today, we're moving into collaborative selling activities," Kann said.

Rockwell has also teamed with Cisco to develop a reference architecture for security, said Sujeet Chand, senior vice president and CTO for Rockwell, in a separate conversation. It's a blueprint providing end-to-end security—from

the device level all the way up to the IT level, he said.

Pretty much by default, IT is taking on the responsibility of securing the entire enterprise. "There's really not much of a choice. Convergence is happening," Chand said. "At Rockwell, if there's a breach and the plant shuts down, we're going to hold IT responsible. It's not a plant manager who's going to be held responsible. That responsibility is going to be with IT."

Partnering to survive

IT/OT convergence has become a matter of necessity. "This digital transformation is not a nice-to-have thing anymore. It's a matter of survival," Shakib said. As the competition intensifies, people are starting to adapt, he added. "This digital race is on, and it's now coming to the manufacturing world. We're two companies working together, and we want to help."

So it's perhaps no wonder that the Rockwell/Cisco partnership was referenced continually throughout Automation Fair this year. Luis Gamboa, global market development manager, oil and gas, for Rockwell, mentioned it during the Oil & Gas Forum on Wednesday, discussing the need to converge transactional information from IT with real-time data from OT into a common network infrastructure. "Working with Cisco, we have been able to achieve that," he said.

Ahmad Dean, senior instruments and automation engineer at mining and petroleum company BHP Billiton, mentioned the ease of managing its relationships with Cisco for its industrial data center. "We call Rockwell, Rockwell calls Cisco, and takes care of it," he said. "Rockwell handles all of that interaction."

There's nothing exclusive about the partnership between Rockwell and Cisco, Kann said. Cisco has 77,000 partners, Shakib added, but "Rockwell by far is the most successful."

Though Rockwell has its Encompass program in which it works with typically smaller, niche players, it has only four Strategic Alliance partners, including Cisco, Endress+Hauser, Microsoft and Panduit.

The relationship between Rockwell and Panduit is geared toward helping customers develop their physical network infrastructures for industrial environments. In a meeting to learn more about that partnership, Jim Neawedde, professional services industrial automation solutions architect for Panduit, marveled at Cisco's foresight when it identified the need or IT/OT convergence back in 2005. "They were spot on with the importance of it," he said. "We're now at an inflection point, and it has to become reality."

The physical network solutions from Panduit are developed to align with Rockwell technologies to help make deployment of the Connected Enterprise easier, faster and more secure. "We have a holistic solution that complements what Rockwell does," Neawedde said. "We're the physical backbone all that runs on." Panduit helped Rockwell build its Integrated Architecture lab with verifiable and customizable designs, he added.

OT Has a Mission-Critical Role

In an increasingly connected age, operational technology's importance continues to grow. Understanding and addressing that criticality will offer a competitive advantage and lead to greater profitability.

By Brett Brack and Larry Asher, Bachelor Controls

Last week while attending a presentation involving cybersecurity and cloud-first/mobile-first solutions, one of the attendees asked the question: "What is OT?" I found myself asking that same question at a conference a few years ago. Although OT has been defined for many years, many people are just now beginning to hear of it.

In simplest terms, operational technology (OT) is information technology (IT) applied to industrial control solutions—the plant floor. These days, the OT concept is growing exponentially, driven by a convergence of technologies that have found their way to the plant floor. This convergence is largely enabled by the maturity of existing technologies, including the standardization of Ethernet, robust and reliable Internet service, the cloud, low-cost data storage, and wireless connectivity.

This truly is a global phenomenon being described around the world in different terms: Internet of Things (IoT), Industrial Internet of Things (IIoT), Industry 4.0, Smart Manufacturing, The Connected Enterprise, Digital Manufacturing, Made in China 2025, Factory of the Future, and others. No industry will be left untouched. Manufacturing organizations are restructuring, creating new roles to better use data to work more efficiently and increase profits. OT is the backbone of the information system on the plant floor.

Industrial networks have existed for a long time. In the past, they were mostly isolated from the enterprise network, and the IT department, exchanging data on a limited basis. Today, plant floor networks are becoming more fully integrated into the enterprise network and beyond. Unlike traditional IT networks, though, OT is subject to harsh environments like electrical noise, dirt and other environmental factors. Successful OT requires the depth of knowledge of IT and an understanding of industrial control solutions.

Considering the characteristics of a mission-critical network, the first things that come to mind are uptime and service-level agreements (SLAs). SLAs are stated terms of availability that a company guarantees they will provide. It is likely that you have heard of the Five nines (99.999 percent), which has become the standard bearer for uptime. Companies have gone to great lengths to achieve that level of uptime through industry-leading equipment and redundancy where possible. Virtualization and clustering technologies allow companies to update and scale without disruption. Updates are tested thoroughly in simulation environments before being released to production, and a robust fallback system is in place with immediate recovery capabilities.

Another consideration, especially in the age of connectivity, is cybersecurity. Mission-critical systems commonly include defense-in-depth principles such as firewall access rules, DMZs, intrusion

Continued
OT Has a Mission-Critical Role

prevention, breach detection systems, proxy servers, content filtering, application whitelisting, antivirus/malware, and data and network encryption. Workstation peripheral ports are disabled to prevent infection via external hard drives or flash devices. One of the most widely adopted cybersecurity frameworks is the NIST Framework for Improving Critical Infrastructure Cybersecurity, which is based on five main principles: identify, protect, detect, respond, recover.

Unlike traditional IT networks, OT networks could include the responsibilities of a safety-critical system with the ability to put processes and machinery components in a safe state to avoid safety, health and environmental consequences. Another difference is the use of real-time components in OT. In addition to controls and automation existing on OT networks, data analysis is being done in real time on the same networks. Looking at reports of the past 30 days, week or even shift can offer great insights, but still leave customers unable to take timely profit-related corrective action. Real-time data analytics offer an immediate contribution to profitability.

As we continue to move into this age of connectivity, the mission-critical role of OT will only grow. Manufacturing operations, to include automation, are becoming more and more dependent on network reliability. If the network is down, operations is down, and customers are losing money every minute they are down. Addressing OT as mission-critical will offer a competitive advantage and lead to greater profitability.

Down to the Wire – Building a Resilient Network Infrastructure

By Andy Banathy, Solution Architect, Panduit

The Internet of Things (IoT) encompasses everyday devices (e.g., smartphones, tablets, video cameras) embedded with technology that enables these devices to interact in new ways. The IoT also broadens outside the production space to connect Operations Technology (OT) with Information Technology (IT), thereby opening the door to an array of new applications and enhancing existing ones. These new capabilities are further bolstered by a standard Ethernet network, which manufacturers are now adopting on the plant floor as they migrate from proprietary networks.

The IoT revolution is expected to create tremendous business opportunities by 2022, especially in the industrial automation market. This translates into a value of $3.88 trillion linked to manufacturing, according to Industrial-IP.org1 and invites speculation on whether the physical cabling network infrastructure will be able to withstand the IoT flood of data flow.

The right design and cable installation are critical to overall network reliability. According to Gartner2, the average cost of network downtime is estimated to be $5,600 per minute, which is well over $300,000 per hour.

Manufacturers are acutely aware of the repercussions of downtime. In addition to the direct costs associated with down machines tied to the network, challenges exist even when machines are running. Although a plant may be able to produce manufactured goods, the company may not be able to ship or sell because it lacks quality-controlled electronic documentation, product serialization to track and trace, inventory management, and regulatory compliance data.

Enterprise applications, plant floor software, asset management and quality control applications, predictive analytics, and virus protection systems need a reliable network to work effectively. More importantly, the necessary network is comprised of more than communication protocols. The actual physical infrastructure (i.e., the cables, connectors, wires, cabinets, and panels) is often overlooked. This existing hardware —most of which has been in place for decades— will soon be overtaxed by an influx of networked devices resulting from the IoT movement.

As manufacturers standardize on Ethernet across the organization, they create synchronicity and visibility between the plant floor and the enterprise to achieve gains in efficiency and output. Still, plant managers worry that their existing reliable, proprietary configurations could be degraded in an Ethernet network upgrade. Therefore, it is critical for every CIO, plant manager, and systems integrator to assess each element of the network, from communication protocols to cables, and proactively focus on future needs as they expand or upgrade their network infrastructure.

The New Manufacturing Model

Today, organizations are challenged to transform due to disruptive technologies. From the proliferation of IoT to the globalization of manufacturing, the pressure is on to achieve lower costs, and deliver to new markets.

Manufacturers in the best-in-class category put a greater emphasis on network management, network reliability, and resilience. They build redundancy into network paths as a backup and map out a wiring strategy to ensure that data speed is maximized across the plant floor network. In other words, the "best-in-class network blueprint" plots every aspect of the infrastructure—*down to the wire*.

"It pays to be forward-thinking with your physical infrastructure. "Deploying the right media will help avoid performance issues and keep costly upgrades to a minimum. Late in the game, when the network is already deployed, it is very expensive to fix issues," Banathy said. "In my experience, something that costs $10 in the planning stage may cost $10,000 to fix in the field."

To turn the reliable, resilient network vision into a reality, companies are defining physical designs and establishing global standards. But before they can proceed, they must conduct an environment evaluation, otherwise known as an assessment.

Assessment Steps

Manufacturers should complete the steps outlined below to understand their bandwidth and cable requirements.

1. Number of Ethernet Devices

Start the assessment by tallying all the Ethernet devices that require connectivity not only for today, but for the next 10 to 20 years. This may include machines, sensors, cameras, controllers, drives, and switches.

2. Environmental Risks

Next, consider the environmental risks to the infrastructure. For example, caustic, wet conditions could affect cable jacket material, and areas with high electrical noise may compromise copper cable. The assessment is also the time to identify obstructions to cable routing and to optimize cable run lengths. Refer to TIA-1005-A for more information.

3. Bandwidth Consumers

Pre-Configured Industrial Distribution Frame (IDF)

The Pre-Configured IDF is specifically engineered to deploy and protect rack mount Ethernet switches in industrial applications. Extra-depth allows room for cable management, power management, and switch stack cables and accommodates up to 5 switches. The innovative design provides consistent equipment deployment with faster installation and can significantly lower the risk of downtime due to switch overheating.

After assessing environmental risks, consider the kind of traffic flow to determine bandwidth needs. Examine all the packet-producing devices and estimate data, control, video, and VoIP output needs.

4. Downtime

To properly architect the network, it is important to determine the cost of downtime to help establish network investment needs. High downtime costs require design considerations for greater resiliency, cable protection, and pathways.

5. Security

The industrial network is not an island. As part of the assessment, manufacturers should determine how to connect with the enterprise network, which has greater security needs due to the number of security attacks on the IT network.

The convergence of enterprise IT and the industrial network means a hacker could wreak havoc in a company's ability to manufacture. Therefore, it is important to adhere to best practices to build a bullet-proof security scheme when converging IT and plant floor networks. This in-depth defense scheme should cover everything from protocols to port physical security.

The Connected Plant

Historically, the plant floor and the enterprise have remained separate domains. However, with changing market dynamics that demand just-in-time manufacturing, scalability, and operational visibility, companies are now connecting these disparate networks.

Rockwell Automation and Cisco have developed an architectural model that safely merges the two standards-compliant Ethernet networks. The model, called the Converged Plant-wide Ethernet (CPwE) architecture, is a set of best practices referring to a logical network architecture that extends to the physical layer.

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. This setup allows the IT network and the operations network to share data, but they remain virtually isolated, so if the enterprise is breached or a virus is introduced, it cannot reach the production environment.

In addition to security, CPwE also considers planned and unplanned future growth of the network. As Ethernet expands into the manufacturing environment and as a unified architecture is put in place to manage all networking and to control traffic, facilities that have well-planned and structured physical networks will be best positioned to improve overall operational efficiency, productivity, and flexibility. Refer to the Panduit Industrial Ethernet Physical Infrastructure Reference Architecture Design Guide for more information.

The Industrial Network of the Future

Traditionally, industrial networks have been set up in a point-to-point configuration, with a single cable terminated to plugs (i.e., a long patch cord). Structured cabling is emerging as a more robust and sustainable infrastructure because it better facilitates growth and troubleshooting, factors that are important to manufacturing. However, there are pros and cons to each approach, depending on the implementation.

Point-to-point is ideal for short cable runs in an enclosure or small ring applications. However, plugs can be hard to terminate. Another consideration is stranded vs. solid cables. Stranded cables lead to reduced distance because of higher attenuation, while a solid conductor cable can break due to flexing. More importantly, fixed length, point-to-point cables cannot be readily extended or reconfigured as a structured approach with patch panels. In addition, some network test equipment excludes connections to the tester, therefore the entire channel is not tested.

Structured cabling is the preferred implementation for longer and more critical runs, such as connecting enclosures, machines, test equipment, and cameras, as it provides a means for troubleshooting and testability, growth, and reliability. Utilizing patch cords, jacks, and horizontal cabling creates an optimized network channel. Also, the horizontal cable is easier and faster to reliably terminate to a jack versus a plug. By installing network cabling to create spare network channels for growth, technicians can connect to a different channel when adding equipment or in the event of a network cabling failure.

While there is a focus on channel resiliency, the value of structured cabling is its systematic approach to planning and deploying cabling and cable management based on the Telecommunications Infrastructure Standard for Industrial Premises (TIA-1005-A).

Media Selection

Cable media is influenced by cable reach, harsh environments, electrical noise, bandwidth, and switch convergence. For example, proper copper channel cable transmits 100m while single-mode fiber optic cable can reach distances of many kilometers, depending on the transceiver selection.

Corrosive, wet, and oily environments all impact network cable jackets, causing degradation. There are a variety of outer jacket coverings such as polyurethane, polyvinyl chloride (PVC), and thermoplastic elastomer (TPE), which have varying levels of cable protection. The toughest jacket covering, polyurethane, is abrasion- and tear-resistant, and resistant to oil, radiation, fungus, oxidation, and ozone. Beneath the outer jacket, metallic foil or braid may be used to suppress electrical noise. However, the ultimate in electrical noise immunity is the deployment of fiber.

Another media consideration is bandwidth, especially for large data consumers such as interswitch links and cameras. Bandwidth require-

ments may necessitate higher category copper such as Category 6 and perhaps multi-mode and single-mode fiber that can transmit up to 10Gb/s.

Recovery time from a network interruption impacts manufacturing downtime. This time can be minimized by deploying fiber cable for interswitch links in rings or redundant star configurations. With fiber the switches recognize loss of signal faster than copper interfaces, and can recover communications much faster than copper. In less complex, smaller networks, copper may be suitable, but the recovery time for network faults needs to be weighed against downtime costs.

Mapping Out Network Necessities

At this point, the network assessment is complete, the network topology is settled, the location of the point-to-point and structured cabling, and the cable construction/media have all been decided. Now it is time to design and deploy the infrastructure, starting with the plant drawing to overlay the logical network architecture on the physical layer.

By having a visual diagram of the network in place prior to the deployment, decisions can be made on routing and the environmental impact on cabling infrastructure. The ISO/IEC 24702 standard has a methodology to assess the environment with four factors - mechanical, ingress, climate, and electromagnetic (referred to as M.I.C.E).

M.I.C.E disruptions can be mitigated with the proper cable jacket covering and shielding to suppress electrical noise.

Keep the following in mind when assessing, designing, and deploying the physical infrastructure:

- Standards-compliant configurations (from TIA cabling standards to EtherNet/IP)
- Cabling methods, (i.e., structured vs. point-to-point)
- Network topology affecting media selection
- Fiber optic and copper cabling applications
- Appropriate jacket covering and shielding for harsh environments Infrastructure Matters

If approached in a systematic manner using standards-compliant methodology, cabling infrastructure can be a scalable solution that marries

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

the evolving aspects of the logical and physical networks and can adapt to an ever-changing dynamic industry. Data continuity involves media, wire covering, and topology. In addition, leveraging best practices and certified techniques outlined by technology vendors allows for an efficient and cost-effective installation.

The network must withstand the test of time. Wire it right from the beginning.

(1) Source: Industrial-IP.org

(2) Source: Gartner blog, "The Cost of Downtime" July 16, 2014

Referenced Resources

- ANSI/TIA-1005-A Telecommunications Infrastructure Standard for Industrial Premises
- ISO/IEC 24702 – Information Technology – Generic Cabling – Industrial Premises

Resolving Ethernet Connectivity Issues for a Panduit Industrial Automation Customer

IntraVUE™ software helps Panduit to increase awareness of the physical infrastructure by providing visibility into all levels of devices and connectivity

Business Challenges

One of Panduit's industrial automation customers faced critical challenges when tasked with deploying and maintaining Ethernet-based networks. Signi cant challenges included a limited capacity to promptly identify, troubleshoot, and resolve connectivity issues; the lack of skills to recognize and ef ciently address underlying reliability risks; and the inability to manage a rapidly increasing number of Ethernet-connected devices within the company's manufacturing networks. Given these challenges, time spent managing the infrastructure had been driving up the cost of detection, diagnosis, and resolution of connectivity issues.

The Panduit Industrial Automation Professional Services team recognized that its customers would be well served by Panduit's ability to offer a software diagnostic tool. The tool's primary functions would include evaluating a network's capability to effectively perform real-time control, data collection, and device con guration.

"Because the manufacturing environment is extremely unique, most IT networking tools do not adequately evaluate a network's capacity to meet the environment's demands," said Jim Neawedde, Solution Architect, Panduit Industrial Automation Professional Services. "For example, network sniffers and packet analyzer tools are too aggressive, requiring a large amount of bandwidth. This scenario carries with it the potential to ood an industrial automation network, causing downtime if it occurs during production. We needed a tool that was less invasive, and that could safely monitor the networks, especially during production."

While Panduit has an established Physical Infrastructure Assessment based on industry standards, the team saw an opportunity to deliver premium value to customers by providing quantitative data regarding the network's health and performance. After evaluating several solutions, Panduit selected IntraVUE™ software.

"Because the manufacturing environment is extremely unique, most IT networking tools do not adequately evaluate a network's capacity to meet the environment's demands."

-Jim Neawedde, Solution Architect, Panduit Industrial Automation Professional Services

Panduit Solution

"Panduit chose IntraVUE™ software because it was tailored for uncovering risks within automation networks," said Michael Vermeer, Sr. Business Development Manager within Panduit's Industrial Automation team. "There are other packages in the market that look at

network data, but they are typically designed for use at the top level of the network, and are not as helpful for uncovering risks with the devices at the edge of the network."

Vermeer added, "In the industrial space, there's a convergence taking place between the information technology (IT) and the operational technology (OT). The IT tools we considered were simply not suited for helping us diagnose the OT situation regarding plant oor manufacturing."

Panduit first used IntraVUE™ software to conduct an on-site assessment for a large food product manufacturer. The resulting report included a map of all devices in the network, how the devices were connected, how much bandwidth they were using, and device-speci c problem areas across the network. The quantitative data that IntraVUE™ software produced augmented Panduit's full Physical Infrastructure Assessment.

"We were able to detect real-time changes in the network utilization. For example, during our assessment we spotted one of the nodes consuming excessive amounts of bandwidth," Neawedde said. "It turned out they were just performing a Flash upgrade, a short ten minute activity. That event was one of many that served as a good demonstration that this is a powerful, highly valuable tool."

Neawedde also mentioned, "During this test, IntraVUE™ software identi ed rmware incompatibility issues and inconsistent network settings that the company has since resolved. The manufacturer was so pleased with the results of the assessment that it intends to standardize across all its facilities."

What is IntraVUE™ Software?

IntraVUE™ software is an application software tool that provides visibility into all levels of devices and connectivity. It is designed to increase awareness of the physical infrastructure; produce actionable data that speeds documentation and deployment; and more quickly pinpoint and resolve connectivity failures.

Business Benefits

"IntraVUE™ software was the perfect choice

IntraVUE

Automation networks are susceptible to interruptions which often result in downtime, and lost production. While conventional tools are frequently unable to detect many types of network interruptions, IntraVUE provides the capability to identify and report information critical to improving uptime of the Industrial Ethernet infrastructure.

to help our industrial automation customers gain more insight into and awareness of their infrastructure," Neawedde said. "Once we provide the data on where connectivity issues exist, customers can address them more quickly and establish a long-term foundation for increased uptime. That makes IntraVUE™ software invaluable to their operations."

"Because IntraVUE™ software is more OT focused, it doesn't use as much IT jargon. It really provides a user-friendly experience for controls engineers, including a user-interface tailored to accommodate how they see the world, as opposed to requiring an IT super user," Neawedde said.

Moving forward, Panduit will also use the software for inspections at deployment to verify that devices were properly connected and the physical con gurations were completed as designed.