AutomationWorld® TACTICAL BRIEF

Plant Floor Traffic

CONTENTS

SPONSORED BY PANDUIT®

Creating a New Breed of Manufacturing IT

The convergence of information technology and operation technology on the plant floor is igniting the need for a new skillset that combines computer science and plant engineering.

By Stephanie Neil, Automation World Contributing Writer

Like many CIOs, Howell Hicks is on a mission to connect the enterprise and the shop floor. For the past few years, his technology team at McElroy Metal, which makes building components, has been trying to tie together enterprise resource planning (ERP) software with machine control systems to share files related to materials and scheduling. Connecting these two worlds together would eliminate the need to rekey order information on the production line and drastically reduce potential errors, as each milling job is highly customized.

Though the mission is straightforward, the execution is not—not because of system interoperability challenges, but human obstacles related to expertise. Specifically, there are very different skillsets required for enterprise information technology (IT) and industrial operation technology (OT).

People trained to work in IT are focused on computer systems, networks and enterprise applications. They are used to reacting to trouble tickets and troubleshooting problems to get systems back online to avoid inconveniencing end users. OT folks, on the other hand, work proactively and in real time; their machine downtime doesn't mean the company will miss a few emails, but rather a few hundred thousand dollars.

Not only do these two groups work in different ways, but they also speak different languages—from the technology lingo to the actual communication protocols. As a result, traditionally, there's been a clear line between these two domains, and never the twain shall meet—until now.

For example, Hicks hired a person who not only has experience programming PLCs, but also knows Microsoft .NET. "[This person] bridges that gap between someone who has purely shop floor control experience and someone who knows more conventional development languages," Hicks says.

The coming together of IT and OT has been happening slowly over the past several years as a result of the adoption of Ethernet on the factory floor and industrial gateways connecting legacy field devices to the TCP/IP network infrastructure. Now, as manufacturers move toward the use of Big Data analytics, adopt virtualization software for resource sharing, and add more intelligent devices to create their own Industrial Internet of Things (IIoT), that indelible line between the plant and the enterprise departments is fading really fast.

These technology trends are creating a need to cultivate a new skillset that blends IT and OT. That has many manufacturers turning to system integrators, vendors and technical colleges to find this new type of talent that has no official name. Some call it manufacturing IT, while others refer to this role as an information engineer. Ultimately, it is not the title that matters, but the ability to develop this combined skillset. And, to be successfully implemented, companies will also have to change their cultures and organizational structures as they nurture a new united workforce.

"This falls under the category of 'what keeps you up at night,'" says Chuck Edwards, president of Lenze, which manufactures automation technology and drives, "because the wall between the office and the plant floor is going away."

With the wall crumbling, there are requirements for hybrid competencies. People with native technology skills, coupled with the ability to learn and the ability to communicate, are what's needed, Edwards says.

Out of control

Though McElroy Metal hired someone with dual expertise, they are not focusing on one person who can do it all—instead they are focusing on a team of people who are exposed to the cross-functional requirements and who work collaboratively within the system integration group. Integration of the ERP and shop floor scheduling software has been completed at one of McElroy's 12 plants. The plan is to initiate a widespread roll-out to all of the plants throughout the country and to add new kinds of IT/OT capabilities, such as the ability to bring post-production statistics into the manufacturing control systems to compare what was supposed to run, based on the ERP order, to what actually happened on the line. They are also working on bringing data produced by the shop floor controllers back to the ERP system for reporting purposes.

Leading these integration efforts are two people who are supported by the entire IT department. "No one person knows everything—especially with the disparity that exists between shop floor control and back office processing and programming," Hicks says. "So we have to put the right people together."

Sometimes the right people come in the form of third-party control system integrators, since these folks are on the front lines of the IT infiltration of the factory floor. More and more, manufacturing customers ask system integrators to handle hardware, software and network requirements in addition to automation integration.

Larry Asher, director of operations at Bachelor Controls, a system integrator and member of the Control System Integrators Association (CSIA), recently created a new role within the organization called "operational technology analyst." This specialist is responsible for the application of IT to industrial control, including hardware, network topology and remote access technology.

In addition, to keep the OT analysts up-to-date, these individuals also support the IT infrastructure within Bachelor Controls. "We believe this will keep them current in their skillsets and help us bridge the gap when dealing with customers," Asher says. "That's because now we have a peer-to-peer relationship [with customers] when we talk about implementing technology on the plant floor that is tied to enterprise systems."

Similarly, another system integrator and CSIA member, Process and Data Automation (PDA), has, as the company name implies, two internal groups—one dealing with automation for process industries like food and beverage and water/wastewater, and the other dealing with the exchange of data between ERP and factory floor equipment. PDA not only goes to the client site to automate and integrate systems, but the company brings its clients back to its new SCADA Lab—built in the past few months and complete with a mock factory—to teach them about anything they want to know, from Ethernet switches to cybersecurity.

Client needs vary, says PDA president Joe Snyder, but the motivation—to bridge the gap between IT and OT—is the same. "We've always had a laboratory in our building as an area where people can physically play with things to help make sense of the physical world," he says. "But we added our SCADA lab because we can't ignore the growing complexity of software systems and how they intermingle with higher systems."

With Ethernet as the backbone between the office and the factory floor, as well as giant servers with virtualization software and thin clients populating the plant, there is no clear line of demarcation between the IT data guys and the OT process people. "That's why we built this lab," Snyder adds.

Getting schooled

Automation vendors are reacting to this occupational shift by creating products that offer a richer user experience, appealing to emerging IT skillsets on the factory floor.

"Experience trumps features today," says Rich Carpenter, chief of strategy for GE Intelligent Platforms' software business. In the past, people would compare product features, but now it is about allowing users to get up and running quickly by providing an interface that is different than the typical industrial design, he says.

GE understands the manufacturing IT dilemma that companies face, since GE faces the same issues internally. "It's a hard problem to solve for companies," Carpenter says. "I talk with a lot of IT leaders, and they all wrestle with the best approach."

For its part, GE created a center of excellence in San Ramon, Calif. The location was deliberate because it is where a lot of consumer Internet technologies are built, and GE is hiring people from Amazon, Google and SAP, for example, to integrate their skillsets with GE's domain expertise, Carpenter says. The center of excellence started in 2011 as part of GE's Global Research Division, where the Predix industrial cloud platform is being developed. "We've hired a couple hundred data scientists, engineers, cloud computing experts and user experience people who are now working with GE businesses to infuse the day-to-day thinking."

Continued

Creating a New Breed of Manufacturing IT

The organizational shift that GE is making is something every manufacturer should consider to prepare for the future workforce.

"Over the next decade, a whole new generation of manufacturing IT personnel will occupy these positions," says Subhajit Bagchi, vice president of engineering, industrial networking and security at Belden. "This will be the iPhone/iPad generation who will expect manufacturing systems to be as easy, intuitive and results-oriented as their smartphone apps. As a consequence, usability will become a key design consideration in future OT products."

The arrival of Millennials into the workforce is actually a boon for companies trying to fuse IT and OT skillsets because they have grown up with technology. They may not know how to "tinker" with things the way Baby Boomers do; Millennials are more used to Googling to find out how to fix something. But they are highly creative problem-solvers, says Shan Smith, a faculty member at Tri-County Technical College in Pendleton, S.C.

Smith encourages his students to leverage their smartphones as educational tools. "We have students who have never worked with PLCs before, and I [encourage] them to take the initiative to solve problems by finding the information they need," he says.

Tri-County keeps its industrial automation/mechatronics and computer programming classes separate, but increasingly they are looking for ways to accommodate manufacturing partners by evolving classes to better prepare students for the workforce.

Similarly, Wichita Technical Institute in Kansas has developed an 18-month integrated electronics program that includes industrial controls and networking. The school is looking at increasing the length of the electronics program and integrating an IT class because of the mixed technology emerging in manufacturing, says campus director Rod Moore. "We are seeing electronics students come back after graduation and go through the IT program based on what they are doing in the field," he says.

Identifying a need for continuing education while on the job, IT and automation vendors are

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%.

beginning to collaborate on new training and certification programs, too. Last year, Cisco and Rockwell Automation jointly rolled out the Managing Industrial Networks with Cisco Networking Technologies training course and the Cisco Industrial Networking Specialist certification to provide foundational skills. In May, they announced the addition of a five-day, hands-on course called Managing Industrial Networks for Manufacturing with Cisco Technologies and Cisco Certified Network Associate (CCNA) Industrial certification exam. The course offers deeper analysis of EtherNet/IP with industrial protocols, wireless and security technologies, and advanced troubleshooting. The CCNA certification ensures that OT and IT professionals have the skills needed to design, manage and operate converged industrial networks.

Beyond the cross-functional technical training, "my team realized they are not even speaking the same language in the classroom," says Glenn Goldney, Rockwell Automation's global business manager of training services. "We are bringing this together as well, with two new courses on the essentials of IT for the OT pro," and vice versa. It is a communication and culture connection, he says.

In addition, Rockwell, Cisco and other vendors, along with academia, have taken it a step further with last year's introduction of the IoT Industry Talent Consortium. This group will address the projected skills gap of 2 million trained engineers who will need specialized IoT training in the next decade. In addition, the consortium will focus on the fact that college graduates lack the skills to fill new jobs because of curriculum gaps in areas like IoT, analytics and cybercrime.

These new educational movements will likely translate into new kinds of jobs. "Potentially, new personas could come out," says Kevin Davenport, Cisco's global solutions manager. "Maybe an IoT engineer with domain expertise on the plant floor and in the enterprise. We are trying to figure out what to call it. It will definitely be a title that conveys the blended IT/OT titles."

For executives like McElroy Metal's Hicks, it doesn't matter what you call the people working on the merger of IT and OT—just that they are working toward a common convergence goal. "We have no name for this team; it's just my guys working on what we see as our vision," he says.

Network of the Future

Though there's no way to tell exactly what the network of the future will look like under the effects of the Internet of Things, there are three universal network aspects worth focusing on to prepare yourself—and your network—for the future.

By Michael Bowne, Director of technology marketing, PI North America

What will automation networks look like in the next five to 10 years? Wherever the Internet of Things (IoT) trend leads us, the underpinnings of future industrial networks that are universally beneficial to adopters will focus on simplification, uptime and innovation.

Simplification

Using open standards in an automation network allows for manufacturers of all sizes to realize the same benefits as proprietary network solutions. Taking this a step further, what if the network were truly plug-and-play? What features would be required to enable such a network? Here are two in particular: effortless configuration and commercial off-the-shelf (COTS) hardware.

When using industrial Ethernet, effortless configuration can better be described as "allowing IT support without needing it." For example, today a machinery maker delivers a machine with an automation solution and network configuration. The plant operator (end user) integrates the machine into his plant. This requires changes to the plant's network configuration so that it conforms to his local IT requirements.

In the network of the future, the machinery maker will use a temporary network configuration to qualify the machine before sending it to the end user. The end user will be able to simply connect it, and the communication relationships are dynamically established at runtime. So there's still work to be done separating the automation solution and network configuration. Within Profinet, however, we've already taken the step of using name-based addressing. This makes it easier for the end user to get up and running, and a big step in the right direction toward true plug-and-play.

Another way to accomplish truly plug-and-play connectivity is through COTS hardware. This is not to suggest hardware from your local electronics store should be used, only that it could be. Why? Because though an inexpensive switch made for your home or office would work just fine, it might last only 5 minutes in a production plant. Industrialized products, with the same COTS technology built in, can withstand the moisture, vibration, dust and overall harsh environment.

What exactly is that COTS technology in the network of the future? For example, already within Profinet we have technology in place to ensure the real-time transmission of production data, while coexisting on the same wire as IT data (e.g. TCP/IP, more on that later). That technology might become more mainstream with what's known as Time Sensitive Networking (TSN).

For production data, the Profinet protocol is still required at the application layer. Its transmission, however, along with any other traffic, could be handled by TSN. TSN, as of this writing, is still very new, but has the potential to ensure real-time transmission of data like Profinet does today. If it becomes COTS technology, then this greatly clarifies the path between IT and operation technology (OT) by extending their common physical layer (Ethernet) upon which protocols like Profinet and others reside.

Uptime

What good is a manufacturing environment if it isn't up and running? In the network of the future, 0 percent downtime will be taken for granted. How do we maximize productivity by ensuring network uptime? Again, two features stand out as solutions to these issues, and are fortunately already available today: scalable redundancy and scalable security.

The most basic way to ensure uptime is at the physical level: by using a ring-shaped network. This topology creates two connections for every device. However, don't try this at home! Doing so would cause Ethernet packets to go around in circles, eating up bandwidth and causing major headaches. Technologies like Media Redundancy Protocol (MRP) account for this by managing traffic, and in the event of a broken connection in the ring, convert the ring to a line topology.

Such recovery can take tens or a hundred milliseconds. Going further, in Profinet "bumpless redundancy," the failover time is 0 ms. In bumpless redundancy, a sender uses two frames, going in opposite directions around the ring. So, even with a failure, a frame will still arrive at the receiver. To ensure 100 percent uptime, redundant devices and even redundant controllers can be installed, thus expanding upon simple network redundancy.

The single biggest perceived challenge to a converged network is security. In business systems, security objectives are typically ranked in terms of priority as follows:

1. Confidentiality
2. Integrity
3. Availability

In many automation systems, the ranking of security objectives in terms of priority is completely opposite:

1. Availability
2. Integrity
3. Confidentiality

To achieve scalable security, IT and OT need to agree on a security architecture that should be:

- As simple as possible but not simpler (Albert Einstein).
- As uniform as possible—if a rule is applicable in one case, it must also be followed in comparable cases.
- Understood and supported by all parties involved.
- A daily activity and not a one-time-only task.

If these can be reached, the network of the future can be a reality by allowing automation and business systems each to maintain their security objectives.

Innovation

In the network of the future, OT and IT need to share the same foundation (Ethernet) while exposing their data for vertical integration. The beauty of Ethernet is it allows enterprises to use the right protocols for the right task.

There will always be different protocols used for different tasks. As network architectures continue to evolve, these protocols will begin to share the same infrastructure. That common infrastructure is standard unmodified Ethernet. So long as an automation protocol uses standard unmodified Ethernet, the benefits "come for free" as Ethernet matures.

For example, the IEEE has continually updated the 802.3 Ethernet specifications to increase the bandwidth from 10 Mbps to 100 Mbps to 1 Gbps and beyond. Profinet is one such protocol that uses standard unmodified Ethernet. As higher-bandwidth Ethernet is installed to accommodate multiple protocols, this speed increase happens automatically.

It is not just the infrastructure that needs sharing to further innovation in the network of the future; it's also the platforms. If Ethernet is the "how," then protocols for the data are the "what." Profinet handles the controlling and gathering of data from devices within production systems. Via proxies, it also gathers data from non-Ethernet devices. Meanwhile, standards like OPC UA enable the communication between, within and from production systems. When used in tandem, they complete the clear path from shop floor to top floor and into the cloud where analytics can be applied.

IDF Front View as Shipped

IDF Rear View as Shipped

Is Your Network Ready for the Future?

As industry becomes ever more digitized and data-driven, automation technologies will change. This means the networks that connect them will have to change too.

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

Whether or not you're fully onboard with the big technology trends sweeping across industry—such as the Industrial Internet of Things, Big Data, and cloud computing—your automation technologies are likely in need of an upgrade. Doing so is not just a matter of keeping up with Joneses; it's about staying relevant in an increasingly digitized industry.

No matter which direction your upgrades may ultimately lead, the key place to start your journey is with your industrial communication network. After all, your network is the basis that will impact—in terms of scalability and flexibility—any future hardware or software upgrades.

A recent discussion with Andreas Rehm, product manager with Siemens, focused on the essential aspects of a modern industrial network. Before getting bogged down in the specifics of communication protocols, physical layer attributes, or data speeds, Rehm suggests taking a higher-level view of your network in light of overall business needs.

"It is essential to carefully design your network," Rehm says. "After all, if a flat network grows unimpeded, it soon reaches an extent where errors can be passed on to a large part of the plant. Modifications then become very time-consuming and costly."

To approach your network design in the best possible way, Rehm suggests careful consideration of four main issues that impact industrial network support of production operations and the business as a whole. Those issues are: the coupling of IT and automation; a holistic perspective to the selection of components and security; protection through redundancy; and network transparency and diagnostics.

Coupling of IT with automation

These two areas of every manufacturing business have different perspectives that are illustrated in the fundamentally different network components and topologies deployed in the two areas. Despite these differences, the push toward digitalization across industries means that the networks of both areas must be reviewed.

"Devices employed should support the necessary mechanisms and protocols needed for production," Rehm says. "However, they also have to be suitable for IT." As an example of this, he cites the need for support of command line interfaces or the support of 10 GB transmission rates for devices on the border of IT and production networks.

Holistic selection of components & security

Despite increasing cost pressures and long-held industry practices of purchasing on price, Rehm says that the digitalization of industry necessitates a more holistic approach. "Added value created by technology cannot be nominally compared through sale price alone," says Rehm. "The interaction of different components, consideration of environmental conditions, possibilities for energy savings, and the need for high availability are all attributes that can bring about enormous savings over the years, but are often not fully apparent at the point of sale or beginning of the project."

Applying a holistic approach to security is equally beneficial, contends Rehm. "Industrial control system and network security is multilayered and complex," he says. "Data security not only has to be planned well, but also consistently practiced by the user."

He suggests leveraging the expertise of external companies when it comes to security to ensure that any developed policies and procedures are not affected by a company's own "operational blindness."

Protection through redundancy

Because faults are possible even in the most perfectly planned networks, protection for the operator can be gained by installing corresponding redundancy mechanisms, which enable the industrial network to cope with the failure of a component or cable without affecting the communication.

"As components often already support a number of redundancy protocols, redundancy does not have to mean higher investment costs," Rehm adds. "However, since redundancy can be implemented in a variety of ways, care should be taken to design it according to your network requirements. The critical paths of network communication should be considered which, in case of a failure, could cripple the communication flow and thus shut down the production."

Transparency and diagnostics

Industrial networks are constantly being expanded either by adding on devices or linking existing islands with each other, notes Rehm. "As a result, constant and thorough documentation of your network situation becomes an important task which cannot be adequately performed manually," he says. "Thankfully, this task is assumed by modern network management systems which monitor and document the industrial network structures including all necessary identification and maintenance data."

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.

Due to this type of automatic record keeping of network data, weak points in the network can be quickly located and networks can be more easily expanded and optimized.

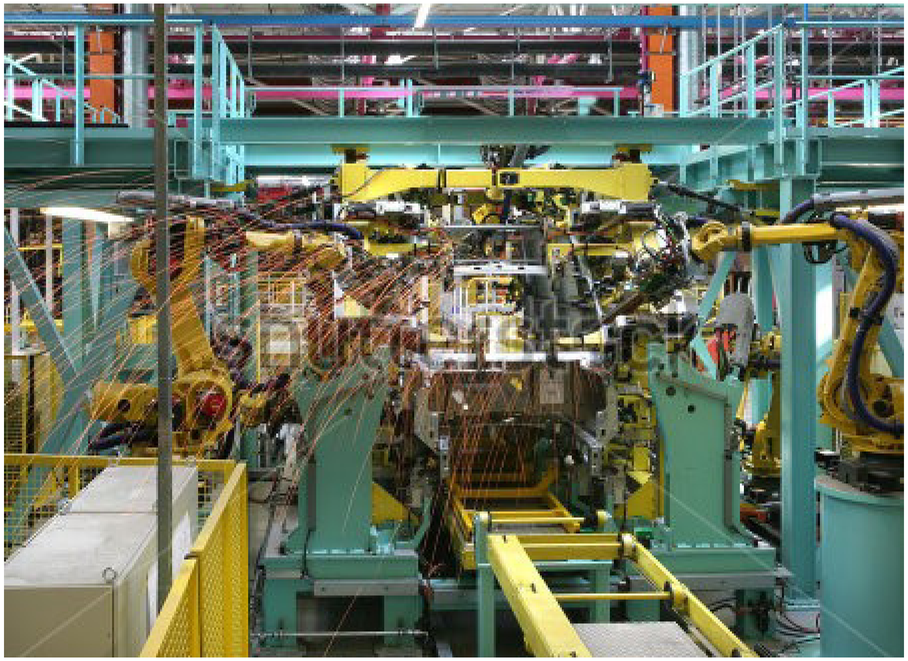
Rehm notes here that diagnostics is often perceived as a financial burden, since it doesn't initially represent an added value to the production process. However, the benefit of diagnostic tools can be financially measured when downtimes in the industrial network have been reduced or even prevented. As a result, diagnostic tools that continuously monitor the network are fast becoming considered to be almost indispensable. With this level of insight, "problems can thus be corrected before they lead to a failure," he says.

To ensure that your network transparency and diagnostic capabilities are fully facilitated, Rehm says it is important "to use tools that can be integrated into your existing HMI/SCADA landscape. Only then can it be ensured that messages or fault notifications are not lost or noticed too late."

Automotive Manufacturer Case Study

Customer Profile A manufacturer of premium passenger vehicles with internationally recognized brands, a global distribution network, and strong research and development capabilities.

By Panduit



Challenges

Engaging numerous automation providers to supply its industrial network infrastructure created challenges involving equipment compatibility for a major automotive manufacturer. The company realized that its carefully selected and validated architecture of switches, routers, and servers required a robust physical infrastructure that consistently delivered across all equipment and integrator suppliers.

To avoid start up delays and costly operational problems, the company made the leap to globally standardize industrial Ethernet for its new production lines.

With this transition, the company needed to ensure that its plants would meet its uptime and performance goals as it collaborated with a diverse ecosystem of line builders and system integrators. The company also wanted to scale its business operations, meet customer goals, and comply with regulatory environmental standards. A secure, reliable, highly available network infrastructure would allow the company to achieve these goals along with the following:

- Support technology while maintaining high availability
- Accelerate the design and implementation of new production lines
- Update existing production lines for model upgrades
- Achieve fast deployment across the company's global facilities
- Reduce both troubleshooting time and risk of errors

The company needed global solutions partners to help design and provide global standard network solutions within a realistic budget. The solutions partners involved needed to identify and provide best practices to accommodate the company's anticipated growth and maintain a competitive edge through proven expertise.

Continued
Automotive Manufacturer Case Study

Panduit Solutions

Panduit held standards-based technical design seminars to assist the global alliance partner with identifying the knowledge gaps with the automotive manufacturer and its system integrators. Best practices related to managed switch deployment resonated with the company and resulted with the Panduit Pre-configured Network Zone System being deployed as part of its zone architecture design. Panduit also assisted with developing a physical infrastructure specification and component guide to simplify network design for the system integrators and line builders.

The complete solution Panduit recommended consisted of its Pre-configured Network Zone System, fiber optic cable and connectivity, In-Field™ fiber connector termination, IndustrialNet™ copper cable and connectivity, DIN rail mounted patching, and network identification.

The Panduit tailored physical infrastructure solution addressed the following areas:

Plant Floor – Pre-configured Network Zone System

Enclosures – IndustrialNet™ DIN-Rail Mount Patching Systems

Connectivity - Opti-Core® Om2 multimode LSZH (low smoke zero halogen) Fiber Optic Indoor Cable; IndustrialNet™ Category 5e SF/UTP and IndustrialNet™ Category 6 S/FTP Copper Cable

The Pre-configured Network Zone System rapidly deploys an EtherNet/IP network on the plant floor with a reliable, structured approach that reduces installation time and lifecycle costs. This solution is ideally suited for the automotive manufacturer's applications where the switch is part of a plant-wide Ethernet architecture, and allows the use of either fiber or copper downlinks.

With guidance from Panduit, the company installed Opti-Core® OM2 Multimode LSZH Cables to provide high-density connectivity and ease of installation for its cable runs of 80m or longer.

IndustrialNet™ Category 5e SF/UTP and Category 6 S/FTP Copper Cable provide reliability, high performance and availability, and quick installation as an integral component of the end-to-end solution for industrial Ethernet and EtherNet/IP-based communications networks.

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.

Continued

Automotive Manufacturer Case Study

Benefits

The structured, engineered approach to physical infrastructure design addressed the automotive manufacturer's need for a secure standardized network system that would improve reliability and security while reducing deployment and operating costs. In addition, the customer is now able to achieve:

Speed of Deployment

- Delivers up to 75% reduction in deployment time compared to systems that are not pre-engineered, validated, and tested.
- Reduces costs by removing complexity and delivering a validated solution optimized for partner technology applications

Mitigated Risk of Downtime

- Increases reliability with pre-tested dual fiber uplink and mitigated risk of the delayed plant uptime after scheduled downtime
- Allows rapid expansion of switch and ports as the network grows

Reliability

- Localizes network traffic to improve resiliency
- Provides enhanced manufacturing operations
- Significantly reduces costs and complications associated with integrating the manufacturing floor and enterprise networks

Standardization

- Leads to better operational efficiency, reliability, and lower operational costs

For More Information, Click Here

Physical Infrastructure for a Resilient Converged Plantwide Ethernet Architecture

By Panduit

Industrial Ethernet networking is advancing technology applications throughout the plant. These applications are rapidly being deployed from the plant floor to the enterprise. The integration of IT and Industrial Automation and Control System (IACS) Operational Technology (OT) introduces the need for increased security, ease of use, rapid deployment, and network management support. Panduit is collaborating with industry leaders, including Rockwell Automation and Cisco, to provide industry-leading solutions, architectures, and services that help companies reduce risk, enhance operational performance, improve reliability, and successfully implement EtherNet/IPTM solutions and architectures through:

- Optimized physical network infrastructure solutions from Panduit® that have been developed to align with the Cisco and Rockwell Automation Converged Plantwide Ethernet (CPwE) Resiliency Cisco Validated Design (CVD).
- Design guidance for aligning logical and physical industrial network architectures that utilize industry best practices. Strategic design guidance facilitates effective collaboration between OT and IT.
- Integrated solutions, tools, and services to simplify design and implementation for better equipment optimization and broader risk management

Deploying the Physical Infrastructure to Build a Resilient Network

CPwE is the underlying architecture that provides standard network services for control and information disciplines, devices, and equipment found in modern IACS applications. The CPwE architecture (Figure 1) provides design and implementation guidance to achieve the real-time communication, reliability, scalability, security, and resiliency requirements of the IACS.

Successful deployment of CPwE logical architecture depends on a robust physical infrastructure network design that addresses environmental, performance, and security challenges with best practices from Operational Technology (OT) and Information Technology (IT). Collaborating with industry leaders such as Rockwell Automation and Cisco, Panduit helps customers address deployment complexities associated with Industrial Ethernet from the plant to the enterprise. As a result, users achieve resilient, scalable networks that support proven and flexible logical CPwE architectures designed to optimize industrial network performance.

Physical Infrastructure Design for Resilient Networks

Increasing the resilience of an industrial Ethernet network requires identifying the challenges and risks for underperforming networks and network disruptions, and defining appropriate countermeasures to achieve high resiliency.

Logical to Physical Mapping

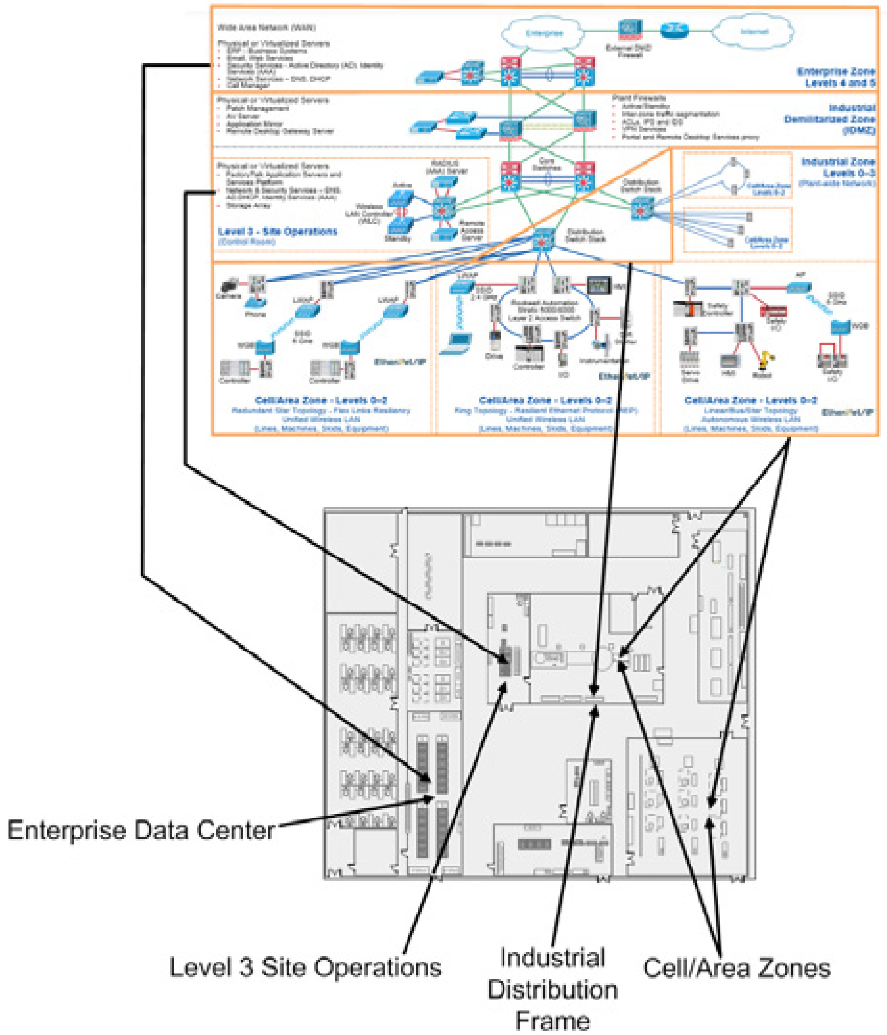
The challenge for network designers is to implement a reliable, secure, and future-ready network infrastructure across the varied, harsh environments of industrial plants. The networking assets must be placed across the plant floor with consideration of challenging environmental factors such as long distances, temperature extremes, humidity, shock/vibration, chemical/climatic conditions, water/dust ingress, and electromagnetic threats. These challenges present threats that can potentially degrade network performance, impact network reliability, and/or shorten asset longevity. Figure 1 shows the CPwE logical framework mapped to a hypothetical plant footprint.

Resilient Design Considerations

- Resilient network topologies
- Network channel layout and distribution
- Structured cabling
- Physical network zone architecture
- Network channel endurance as assessed using M.I.C.E. criteria

In harsh environments, industrial Ethernet networked communications systems must be extremely durable to avoid physical deterioration in cabling infrastructure. Physical deterioration results in defective network performance and safety issues, and leads to loss of

Figure 1. Mapping CPwE Logical to Physical.


Wide Area Network (WAN)
Enterprise Zone Levels 4 and 5
Industrial Demilitarized Zone (IDMZ)
Industrial Zone Levels 0–3 (Plant-wide Network)
Level 3 - Site Operations (Control Room)
Cell/Area Zone - Levels 0–2
Cell/Area Zone - Levels 0–2
Cell/Area Zone - Levels 0–2
EtherNet/IP
Enterprise Data Center
Level 3 Site Operations
Industrial Distribution Frame
Cell/Area Zones

data transfer, costly downtime, or catastrophic failure. Therefore, strategic selection of cable jackets for industrial environments is essential.

Physical Infrastructure Network Building Block Systems

Industrial physical infrastructure network building block systems comprised of integrated active gear can be deployed at most levels of the CPwE logical architecture. An industrial network building block system simplifies deployment of the network infrastructure required at each level of the CPwE.

The building block system provides redundancy by containing the specified switching, routing, computing, and/or storage elements required for a given zone in an enclosure, cabinet, or rack that is complete with cabling, cable management, identification, grounding, and power. These building block systems can be implemented in three ways:

- Integrated – Fully integrated, assembled and thermally tested building block solution including CPwE equipment and components delivered onsite for rapid deployment
- Pre-configured – Pre-assembled building block solution incorporating CPwE equipment and components to be assembled onsite
- Switch Ready – Pre-assembled building block solution including power supplies, fusing equipment, cabling etc., delivered onsite and ready for CPwE equipment and component implementation

The network building blocks are comprised of the following:

- Physical Network Zone System - A Physical Network Zone System within the CPwE Cell/Area Zone provides environmental protection for the industrial Ethernet switch (IES) and serves as a consolidation point for multiple network connections
- Industrial Data Center (IDC) - The CPwE Level 3 Site Operations, or Industrial Data Center (IDC), is one of four distinct cabinets that house equipment for several areas of the CPwE logical architecture
- Industrial Distribution Frame (IDF) - For

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](#)

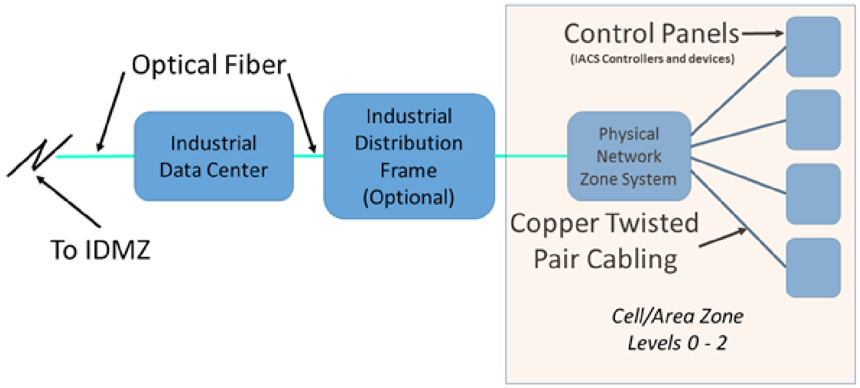
consolidation points of IES, an IDF solution may be used to house rack mounted IES to route traffic between the Cell/Area Zone IES and the Level 3 Site Operations IDC

CPwE Physical Infrastructure

Industrial Zone

The CPwE plant network backbone consists of the distribution layer that converges one or more Cell/Area Zones to the overall plant network, IACS controllers, and connections to the edge IACS devices. Figure 2 illustrates the logical building blocks diagram and Figure 3 illustrates the CPwE architecture below the Core Switches down to Level 0.

Figure 2. Logical Building Blocks Diagram.


Control Panels
(IACS Controllers and devices)
Optical Fiber
Industrial Data Center
Industrial Distribution Frame (Optional)
Physical Network Zone System
To IDMZ
Copper Twisted Pair Cabling
Cell/Area Zone Levels 0 - 2

Cell/Area Zone

The Cell/Area Zone represents the outer reaches of the network and provides the network connections to the machines, skids and equipment to be monitored, managed, and controlled. Figure 4 details the physical connectivity of an example switch-level ring topology.

Level 3 Site Operations

The Level 3 Site Operations includes virtual servers, security and network services, and a robust physical layer that addresses the environmental, performance, and security challenges present when deploying IT assets (e.g., servers, storage arrays, and switching) in industrial settings (Figure 6).

Industrial Demilitarized Zone (IDMZ)

The IDMZ is critical to securing the network both logically (e.g., malware, viruses, etc.) and physically to prevent unauthorized connections and network disruptions, leading to high resiliency. This is achieved by using active/standby firewalls and port protection (e.g., block-outs, lock-ins). Figure 7 illustrates a physical layout for the IDMZ.

Summary

Resilient plant-wide network architectures serve a crucial role in achieving overall plant uptime and productivity. The CPwE architecture provides standard network services to the applications, devices, and equipment in modern IACS applications, and integrates them into the wider enterprise network. It also provides design and implementation guidance to achieve the real-time communication and deterministic requirements of the IACS as well as the reliability and resiliency required by those systems. The CPwE Resiliency CVD solution can help provide manufacturers the guidance needed to meet the challenges of a fully integrated IACS and realize the business benefits offered by standard networking.

This paper specifically focuses on the physical infrastructure deployment for CPwE using best practices and a building block approach from Panduit. The methodology is reflected in the physical infrastructure details that complement A Resilient Converged Plantwide Ethernet Architecture, a white paper by Rockwell Automation and Cisco.

For More Information, Click Here