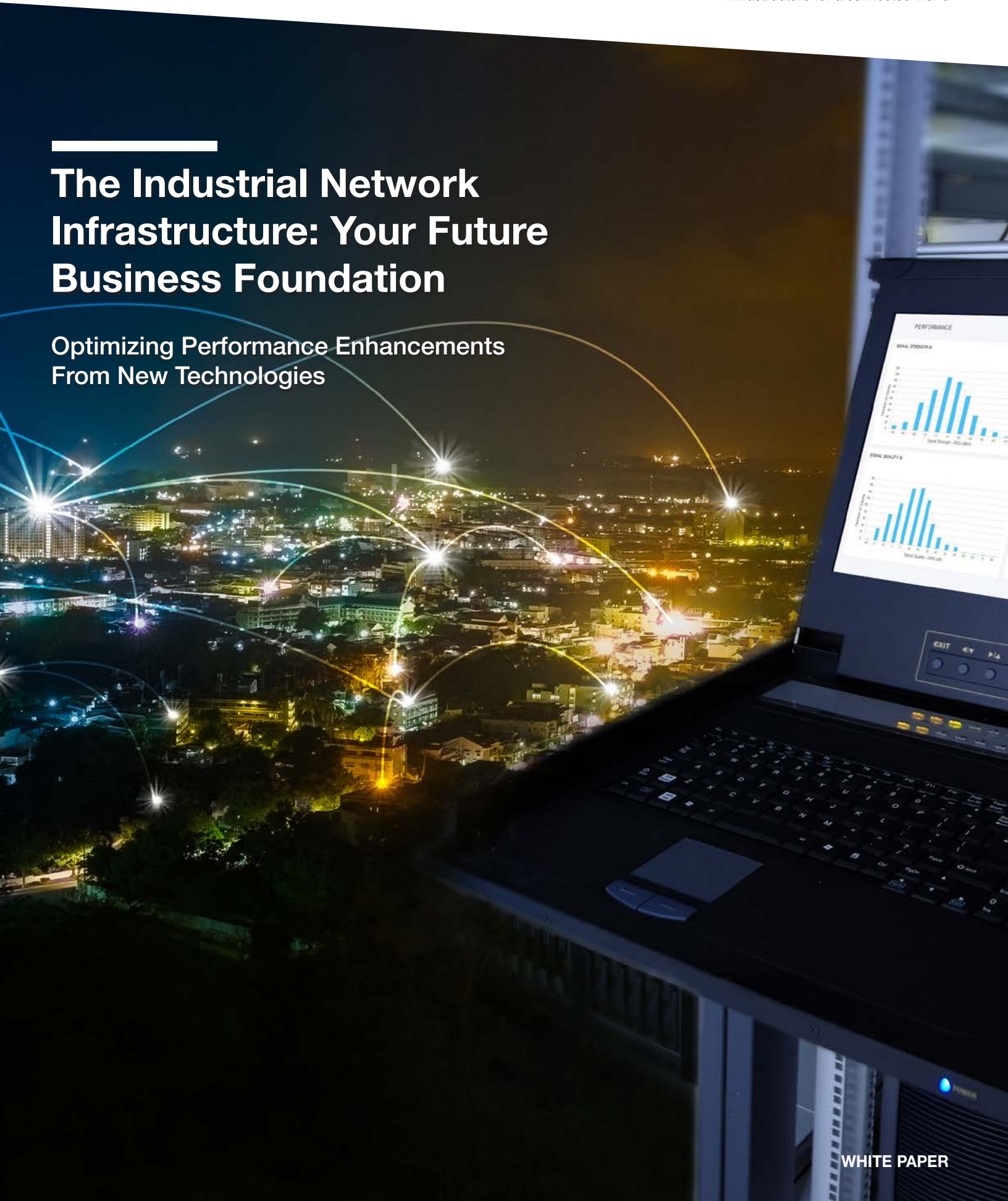
PANDUIT®
infrastructure for a connected world

The Industrial Network Infrastructure: Your Future Business Foundation

Optimizing Performance Enhancements From New Technologies



WHITE PAPER

Introduction

Network infrastructure is one of the most vital yet undervalued business assets. Lose the network and you lose phones, email, Internet, access to business systems or control/visibility of the manufacturing process. Many businesses strive to provide optimum versions of the devices connected to the network, such as computers, phones, machines, etc., yet attempt to economize on the network infrastructure that supports these devices.

This paper discusses essential knowledge and tactics in current, near future, and distant future time domains that guide your network plans. It also suggests resources and strategies to assist you in the design, implement, operation, and maintain phases.

PANDUIT®

Current Day Industrial Networks

Today industrial networks are a composite of Ethernet protocols and what industry experts term, “legacy protocols.” Legacy protocols are a telling term because like other legacies, we must live with them for a while. Legacy protocols age and become more difficult to support over time. This issue is further exacerbated by the aging workforce megatrend. A large portion of the support staff for legacy protocols has reached retirement age. Forward-thinking organizations instituted plans to retain this outbound knowledge. Other companies meet the need by engaging professional services organizations backed by major automation manufacturers.

Protocol Distribution in Industrial Networks

Legacy industrial protocols (Fieldbus) account for over one quarter (27%) of the industrial network nodes sold. Ethernet variants account for 66% of nodes while wireless nodes have 6% share. The telling aspect of this story is that Ethernet and wireless are growing double digits while Fieldbus is growing at a shrinking single digital rate (Figure 1).[1]

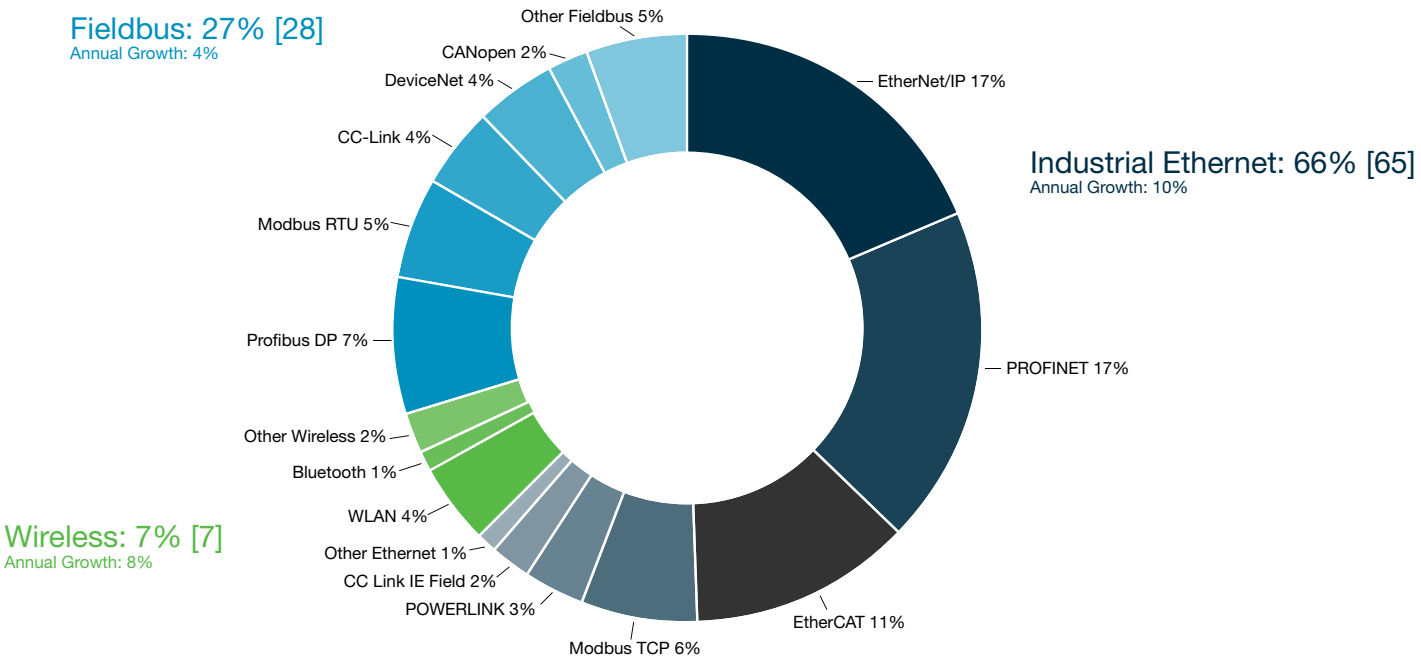


Figure 1. Protocol distribution in industrial networks.

Network Refresh Rates

Industrial networks have added expectation versus their enterprise counterparts. Not only does the business require them to operate at peak levels, industrial networks have the longest refresh rate of any business network. Where data centers are refreshed every three to five years, industrial networks are refreshed every 12 to15 years. Further, the supporting physical infrastructure is often in place for 20 plus years. A major capital expenditure is required to install and commission a new network. ROCE expectations are extremely high for all businesses (Figure 2).

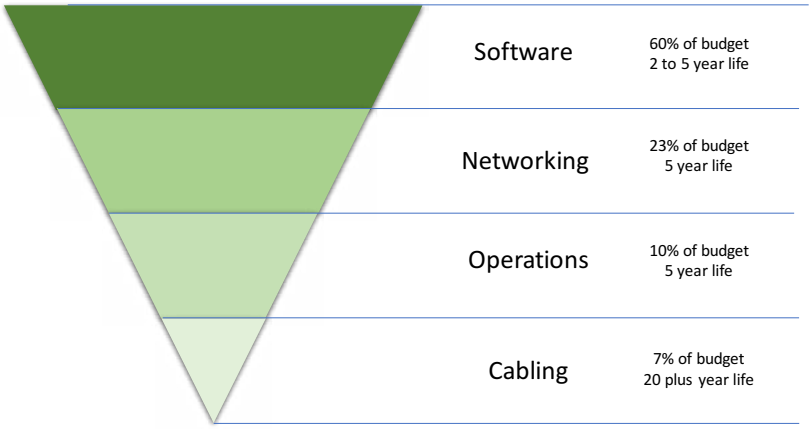


Figure 2. Infrastructure investment versus longevity.

Industrial network refresh rates are accelerating over time as companies work to balance investment performance and network performance. However, we must still anticipate longer than desirable refresh rates to make planning effective.

Network Planning and Management

Like other business assets, a rigorous process governing the network ensures efficacy and availability as time goes by. There is not a particular methodology that is superior to others. Realistically, the best run business networks result from a collection of elements intertwined with the governing process. Justification for creating the process is simple.

- Lowers the total cost of network ownership
- Improves business agility
- Helps the business respond quickly and effectively
- Increases availability

PPDIOO Process is a design and management methodology that spans the entire network lifecycle (Figure 3).

1. **Prepare:** Business agility is a result of good preparation. This phase is used to consider the broad vision, requirements and technologies you can employ to make your business more competitive.
2. **Plan:** Successful technology deployment must have an accurate assessment of the current state network, its security posture, and the business readiness to support the chosen solution.
3. **Design:** A detailed design reduces risk, avoid delays, and controls the total cost of network deployments.
4. **Implement:** Here the business works to integrate devices and new capabilities in accordance with the design phase without compromising network availability or performance.
5. **Operate:** The business proactively monitors the network to improve service quality, reduce disruptions, and mitigate outages while maintaining high availability, reliability, and security.
6. **Optimize:** Best-in-class businesses never stop looking for a competitive edge. So, continuous improvement is a mainstay of any network lifecycle.

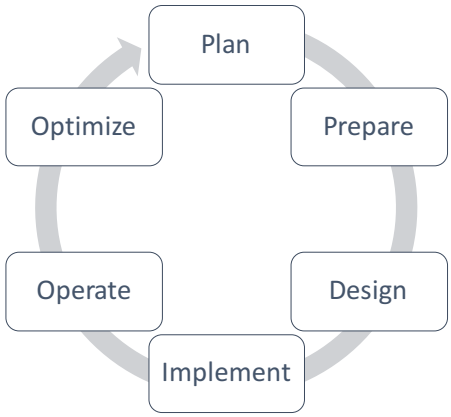


Figure 3. PPDIOO process.

Network Documentation: Does comprehensive, up-to-date documentation exist for your network? Most companies do not have the required documentation, but all of them should consider it an absolute necessity. Accurate documentation and identification substantially shortens the time to recover from a network issue. Many methods to generate this documentation exist, ranging from a summer intern project to engaging a professional services organization to assess and document the network.

Network Assessment: Professional services organizations, backed by a major automation manufacturer, perform cabling and network infrastructure assessments. Many use software that "crawls" unobtrusively through the network, discovering and visualizing the network footprint (Table 1).

Table 1. Network Design Assessment Criteria.

Design Consideration	Assessment Criteria	Design Impacts
Connectivity	Number of devices, machines, etc.	Pathway capacity, switch port counts, number of cable runs plus growth factor
Environment	MICE table (TIA-1005-A)	Protection, separation from environmental influences, transmission media choice
Bandwidth	Current network utilization and estimated future load	Transmission media, network switch specs, installation practices
Cable Reach	Required cable run lengths	Transmission media, network switch specs
Safety	Nearby hazards, e.g. high voltage, heat, chemicals, etc.	Device access, O&M worker protection
Security	Threat level, isolation needs, accidental versus intentional threats	Port protection, enclosure access control, hardening of media
Longevity	Desired years of service	Infrastructure hardening, business growth

Legacy Protocols: During the assessment process, pay attention to legacy protocols, i.e., Fieldbus. If legacy protocols are present, plans to migrate them to a modern technology must be at the forefront. Legacy protocols migrate out of the network as it ages because they become difficult and expensive to support, even if their performance is adequate. Their replacement is infrequently a "rip and replace" proposition.

Network Longevity: Consider the age of the existing network and physical infrastructure. Are any of the active components, network switches, servers, programmable controllers, drivers, or other end devices, approaching "end of sale" or "end of support" from the manufacturer? Aged active components have support costs that grow exponentially after a certain age, so they need to retire before your business is frantically searching for good used replacements to get manufacturing up and running.

Evaluate the age of transmission media and its condition. Consider wire speed as well. Category 5e is adequate for 10Mb/s and 100Mb/s traffic but is insufficient long term. Pay attention to connections and the cable. Jacket materials are commonly thermoplastic which ages over time, particularly in challenging environmental conditions like UV exposure, temperature extremes, and chemical exposure. The same exposures age the metallic portion of connectors. Along cable routes, look for sharp bends and areas where cables appear to have been struck or deformed. With multi-pair copper Ethernet media, these physical deformations displace pairs in the cable, damaging its performance. With fiber optic media, there can be microfractures from physical deformation that attenuate or, in severe cases, interrupt signal flow.

Cabled Infrastructure

As the network grows the cabled infrastructure must evolve. There are two cabling topologies used for industrial networks, point-to-point and structured cabling. Older industrial networks employ a point-to-point structured cabling topology where each connected asset has a home run cable to the control room or data center. Engineers chose this solution in the belief that connection points were vulnerable and would cause reliability issues. More connections meant more risk. In the very early days of Ethernet connectors there may have been some credence to that conclusion. Connector and media design as well as manufacturing processes are significantly more robust today. So, in modern networks, this argument is no longer valid. Also, the flexibility and network resiliency gained from a structured cabling topology far outweighs the point-to-point reliability argument.

Enterprise networks were once point-to-point cabling. They quickly evolved to structured cabling for several reasons, notably:

- Structured cabling provides the needed flexibility to accommodate Moves, Adds, and Changes (MACs)
- Structured cabling can adapt network topology and configuration to business needs without pulling new cabling and resultant disruption of business activities
- Structured cabling topologies enhance network reliability and recovery speed from outages

Industrial networks are on this evolutionary path because the value proposition for structured cabling networks is so strong. Elimination of downtime is the strongest argument for structured cabling topologies in industrial networks. Industrial network downtime is easily monetized in lost production dollars. As such, a business can readily justify adoption of this topology.

Structured cabling enables patching or otherwise re-directing network traffic to rapidly address infrastructure-related outages. It allows outages due to fault in the horizontal cabling to be immediately addressed by patching to a different horizontal link. After the outage is resolved, the patching infrastructure permits technicians to quickly attach diagnostic instruments to the failed link. The link can be returned to normal service with minimal disruption in network operation. Table 2 shows the functional comparison between enterprise and industrial networks.

Table 2. Functional Comparison, Enterprise, and Industrial Networks.

Parameter	Office/Enterprise	Plant/Industrial
Connected Devices	80% clients 20% servers	20% clients 80% servers
Traffic	Infrequent larger messages that travel to/from data center	Frequent, numerous but smaller messages that travel between networked devices
Service Access	Many devices operated during normal business hours in accessible areas	Systems operate 24x7, scattered throughout the plant, often in hazardous locations
Downtime	Mostly nuisance. Client problems take up to a day to resolve	Direct result is lost profit. Downtime must be eliminated.

Installing Structured Cabling

When installing structured cabling, it's good to have a few guidelines in mind to ensure maximum viability from the new installation.

- Require the cable installer to connect a network analyzer to each link installed, including spares
- Measured link performance becomes one of the job completion deliverables;
  Doing so establishes that the link delivers expected transmission performance, not just electrical continuity
- Further, if there are problems with a link in the future, baseline performance data exists in your files
- Premium cable manufacturers extend a generous warranty in exchange for fidelity to their offering using a certified installer; It is a worthwhile investigation when selecting materials and installers

Network Management Software

Another important topic for the current day network discussion is a 3-letter acronym, NMS. NMS stands for Network Management Software. It is an emergent category of software for industrial networks. Just as the name implies, it is purpose-built software used to manage networks. There are Enterprise NMS solutions and have been for a while. Due to the unique properties of industrial networks, these tools are not suited for the job. When selecting this category of software, make certain the NMS solution you consider is purpose built for industrial networks.

The clarion call for this type of software rises from the increasing sophistication and complexity of business networks. The ability to quickly ascertain what's connected, the health and workload on the network, misconfiguration of devices and of course, failing devices or connections, is key to effective operations with minimum downtime.

Industrial networks have two main NMS use cases.

- A consultant or system integrator working with the business uses NMS software located on their computer to discover and visualize the network; This application is to assess and document the current state network in anticipation of service activities that the consultant undertakes on behalf of the business
- An NMS solution is installed permanently in the network, typically on a server in the DMZ so the entire industrial network is visible and monitored; This application acknowledges the dynamic nature of the network and acts as a watchdog sniffing out problems; visualizes the network so a common understanding of status is provided for varying worker experience levels and dependent on the NMS solution; and provides a portal for secure remote access when needed

The first use case focuses on the needs of network maintenance. An expert uses the NMS tool to discover and visualize the network. This step generates a baseline documentation package for the network. Typically, businesses retain this expert to perform maintenance, usually to upgrade or expand to the network. Up-to-date documentation for the network is a welcome latent outcome of the exercise. While the expert's NMS package is connected to the network, performance and health metrics can be seen, helping the expert spot deficiencies that must be corrected. However, these values are a "snapshot" in that the NMS solution does not remain connected to the network long term.

The second use case addresses a greater portion of the network lifecycle. In this use case, the NMS solution resides in the network, typically on a server in the DMZ or the Manufacturing Zone. Residence in the network allows the NMS software to act as a dashboard, allowing network users to see network health and performance. Further, more members of the workforce interact with the network nowadays, all with varying levels of network knowledge. These workers need information out of the network to ascertain if there is a network-related problem slowing down production. A production planner can use that information to make better decisions but may not have the needed skills to access the information.

Living in the network NMS software tracks traffic and bandwidth, suggesting future improvements to the network. And of course, it is generating and maintaining an up-to-date view of the devices and connections in the network, solving the accurate documentation dilemma discussed earlier in this paper. Finally, best-in-class NMS packages facilitate secure remote access to the network so you can enlist the help of experts without the time and cost involved with travel. In addition, the resident NMS software approach lessens the reliance on outside experts for diagnostics and network management assistance.

Reference Architectures

Reference architectures are a considerable asset to the present and future states of business networks. Reference architectures streamline the deployment of standardized networking technologies and convergence of manufacturing and business networks into a cohesive whole. In short, reference architectures provide confidence and the necessary background to design, deploy, and operate a robust, reliable network.

Reference architectures provide valuable common ground to enhance the collaboration of OT (control engineers, manufacturing IT, etc.) and corporate IT staff. This common ground removes obstacles and speeds the combined team toward achieving business goals. Historically there has been some discord between IT and OT realms due to the proprietary and obscure nature of industrial networks, especially legacy protocols.

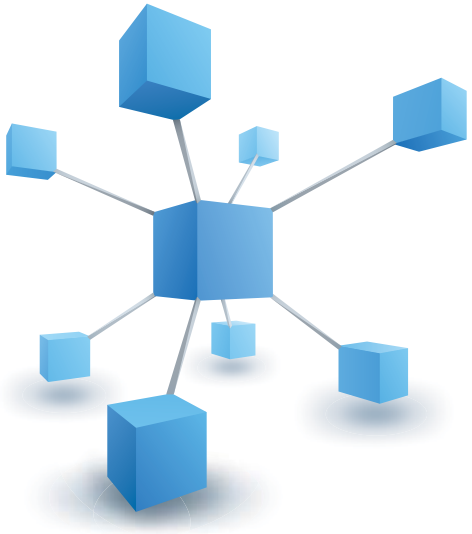
In the realm of reference architectures for industrial networks, the zenith is the Converged Plantwide Ethernet (CPwE), reference architecture. CPwE is a collection of industrial reference architectures that are use case driven and supported by rigorous testing and validation. The use cases selected represent important business needs and are garnered by exhaustive voice of the customer research.

The reference architectures are presented in a published document titled, "Converged Plant wide Ethernet Design and Implementation Guide."[2] The document content is dynamic; new architectures are proposed for inclusion based on VoC research. All networks are assembled, commissioned, and tested prior to publication. Validation and performance data is published for each architecture, along with a hardware bill of materials, firmware versions used, and any software included in the test setup. CPwE remains ever green; as new devices become available and older devices go end of sale/end of support, the core reference architectures, (e.g., resiliency) are refreshed with new testing/validation and published performance data.

Some businesses use CPwE architectures as a springboard to create architectures that suit very specific needs. However, because of their CPwE basis, the architectures are built on a solid foundation.

Network Building Blocks

Another practice that has risen to prominence are pre-populated and pre-configured network enclosures. The solution allows companies to rapidly deploy or expand without bearing the time penalty and expense of a bespoke enclosure. These solution elements follow the functions of the 3-tier architecture of Converged Plant wide Ethernet – Access Layer, Distribution Layer and Core Layer – with appropriate solutions for each network layer.



Enclosure designs are validated electrically and thermally to eliminate risk during installation and commissioning. Active component placement within the enclosure is optimized for function, thermal performance, and maintainability.

Since the network building blocks are built to a validated design, companies gain enhanced supportability through their use, avoiding the "snowflake" scenario where each bespoke enclosure is "just a bit different." This factor is important in a local deployment but becomes vital when multiple locations across a global footprint are considered.

Worker Education

Businesses need to invest in their personnel as certainly as they make other business investments. Creating productive collaboration between IT and OT staffs is of immense benefit to businesses. The progression towards more ubiquitous use of Ethernet sets the stage for this collaboration to occur. To hasten engagement, worker training investments are necessary.

Industry experts have long provided training and certification for IT staff in Ethernet-based enterprise applications. Training materials to support industrial staff in a similar realm have been sparse at best.

Two noteworthy training offerings for industrial staff are Cisco Certified Network Associate (CCNA) industrial certification offered by Cisco and Industrial IP Advantage (IIPA) Training offered by a three-way coalition of Cisco, Panduit, and Rockwell Automation.

The Cisco Certified Network Associate Industrial (CCNA Industrial) certification is for plant administrators, control system engineers, and traditional network engineers in the manufacturing, process control, and oil & gas industries, who will be involved with the convergence of IT and industrial networks. This certification provides candidates with the necessary skills to successfully implement and troubleshoot the most common industry standard protocols while leveraging best practices needed for today's connected networks. There are prerequisite certifications as a gateway to CCNA Industrial. These are Industrial Networking Specialist, CCNET, CCNA Routing and Switching or any valid CCIE certification.

Training offered by the Industrial IP Advantage is delivered online and therefore, is self-paced. The training targets control engineers, IT professionals, system integrators, and machine builders. This multi-part eLearning program combines practical guidance with reference architectures on IP addressing, network topologies, switches and routing infrastructure, physical cabling and wireless, virtualization and cloud technologies, security measures, and more.

Network Planning ≤ Two Years

Networks continue to evolve over time. Plotting the evolutionary path for the business network requires insight into future trends and possibilities. This section offers insight via identification and discussion of important technologies. The time domain for these technologies is within the next two years.

Power over Ethernet

Power over Ethernet (PoE) is an Ethernet-compatible technology created to enable Voice over IP (VoiP) telephony. DC power, at a nominal voltage of 48 VDC, is carried on one or more pairs in the Ethernet cable along with the transmitted signal. PoE-powered devices (PD) negotiate with the power source (e.g., PSE, typically a network switch) to ensure appropriate power is delivered. Businesses soon realized the potential of network supplied power. PoE now powers IP cameras, wireless access points, badge readers and access gateways, and office lighting (Figure 4).

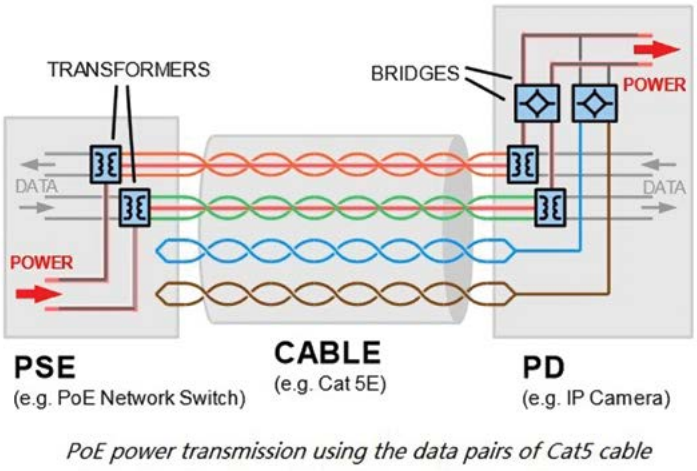


Figure 4. PoE general layout.

Today, PoE in industrial networks performs identical tasks to those it performs in enterprise networks today. These tasks include powering shop floor phones, wireless access points, and IP cameras. PoE holds a bright future as the standards community expands its capabilities.

Table 3. Power over Ethernet Power Levels.

Property	PoE IEEE 802.3af	PoE+ IEEE 802.3at	4PPoE IEEE 802.3bt	PoE++ IEEE 802.3bt
PSE Power	15.4 W	30.0 W	60 W	100 W
PD Power	12.95 W	25.5 W	51 W	71 W
Power Manage-ment	Power class levels, negotiated at initial connection or 0.1W steps negotiated continuously			

PoE is a key technology for the future of industrial networks because, with the advent of IEEE 802.3bt due to publish in early 2018, conspicuous amounts of power can be delivered along the Ethernet connection to a device. With 71 W available at the end of an Ethernet cable, device manufacturers can be very creative. This "one wire ideal" allows device power and communications in a single connection, simplifying all phases of the device life cycle. In doing so, PoE alters the DC power infrastructure of control systems.

Legacy protocol are serial communications to the device at a very modest data rate. No device power is delivered by the connection. Therefore, local DC power supplies are required near the device to meet its power requirements. Behind the DC power supply are many AC components (e.g., transformer, connection wires, circuit protection, etc.) to convert machine mains power to a usable input to the DC power supply. When this supporting infrastructure can be eliminated, control system DC power infrastructure is simplified and costs become lower.

PoE negotiates with the device at start-up to determine the appropriate power level to deliver. There is no need for pre-configuration of each circuit in a standards-compliant installation. Additionally, since device power is controlled by PoE-enabled ports in the switch above it, toggling device power can be done via network switch commands, simplifying service procedures.

PoE should figure prominently in new network installation to simplify powering needed by devices like cameras and wireless access ports. The transformative effect on the DC power infrastructure, while quite feasible, is going to take longer to become a reality.

Single Pair Ethernet

Work is underway in IEEE 802.3 to create standards for Single Pair Ethernet (SPE). Many variants are proposed from short reach (15 to 40m at 1 Gb/s transmission speed) to extreme lengths (up to a kilometer at 10 Mb/s transmission speed), all over a shielded twisted pair cable. For industrial network applications, the variant to watch is IEEE 802.3cg, the 1km at 10 Mb/s variant. All variants of SPE are considering a methodology for power delivery like PoE called Power over Data Line (PoDL), IEEE P802.3bu.

Single Pair Ethernet drives "Ethernet-to-the-edge" and is a vital portion of legacy protocol migration plans. For 802.3cg, its 10 Mb/s transmission speed provides more than enough bandwidth for end device and sensor data rates. For industrial networks:

- The reach objective of up to 1km is ideal for plants with large footprint, (e.g., oil and gas, petrochemical, etc.)
- Power delivery via the Ethernet connection achieves the aforementioned "one wire ideal" where device power and communications are enabled by a single connection
  - Given the power delivery aspect, it is conceivable that end device power infrastructure is greatly simplified by SPE
- SPE, being standard, unmodified Ethernet, supports purpose-built Ethernet forms like EtherNet/IP and ProfiNet without issue
- SPE can have a cost advantage versus 4-pair media in edge device applications. This is due in part to simpler cable construction; The silicon and magnetics used for SPE in switches and end devices are much simpler than 4-pair Ethernet
- Conductor wire gauge for SPE will need to be at least 18 AWG to achieve the 1km reach objective; A latent benefit of this cable construction is the ability to drive higher current levels than 4-pair cable, making LED lighting installations more effective
- SPE media should be easily field terminable; This aspect can reduce pre-terminated cordset inventories and address slack management issues

The "front runner" SPE standard is IEEE P802.3cg. This standard is in Task Force now with an estimated completion date of early 2019.

Single pair Ethernet will rise to prominence by taking Ethernet to the edge of industrial networks. Device manufacturers and network switch manufacturers are closely monitoring and contributing to the creation of IEEE standards that enable this future concept.

Power over Data Line

Power over Data Line (PoDL) is governed by IEEE standard 802.3bu. The PoDL acronym is frequently pronounced “poodle” in conversation. It represents a necessary adaptation of PoE. A reasonable question is “why can’t we just use PoE on SPE?” The reason is PoE requires at least two pairs to work. This is because there is an electrical connection between pair center taps (Figure 5).

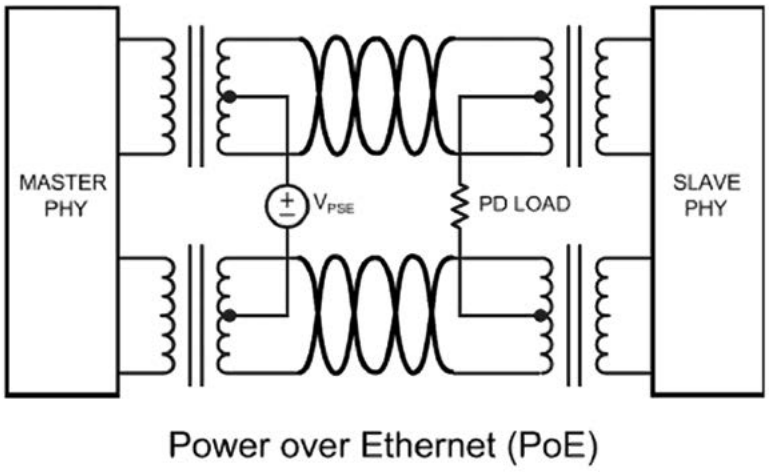


Figure 5. PoE example circuit.

Since SPE has only one pair, the PoE circuit (above) does not work. However, a simpler circuit with a lowpass/highpass bandsplitting filter network works with SPE (Figure 6).

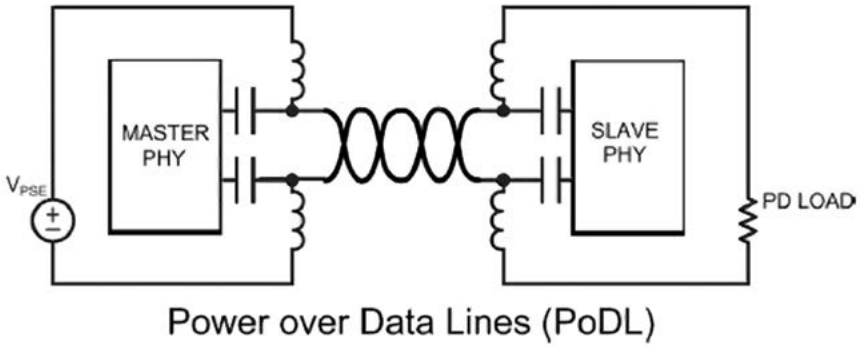


Figure 6. PoDL example circuit.

Using PoDL Class 8 and Class 9, PD power can be 30 W or 50 W respectively at 100m. New classes are required to accommodate the expected higher loop resistance of 1000m links seen in 802.3cg.

PoDL and SPE go hand in hand as technologies to watch and include in legacy protocol migration plans.

Wireless Sensor Networks

Wireless sensor networks are gaining popularity as businesses seek solutions that improve decision speed and quality. Wireless networks can be implemented quickly, speeding the availability of additional knowledge to achieve these goals.

Speed and reliability do not yet perform like wired connections. Critical control connections will remain wired for the foreseeable future. However, wireless connections provide a fast and cost effective means to collect additional data to propel analytics efforts, study new facets of an existing process, etc.

There are many wireless sensor networks worthy of consideration but two stand out for industrial applications. These are:

- Wireless Mesh
- LPWAN

Most wireless mesh networks (Figure 7) used for wireless sensor applications are based on IEEE 802.15.4. This is the technical standard which defines the operation of low-rate wireless personal area networks (LR-WPANs). Wireless mesh networks have a unique feature that make them a provocative choice for industrial data collection; they are self-healing. If a wireless sensing node is blocked from communicating directly with the sensor gateway, it will "hop" to an adjacent node to get back to the gateway. This feature is superb for industrial applications given the dynamic environment with material handling equipment and other large metallic structures often in motion. For example, the chances of a forklift mast blocking transmission at some point in the day is easily an "even odds" bet.

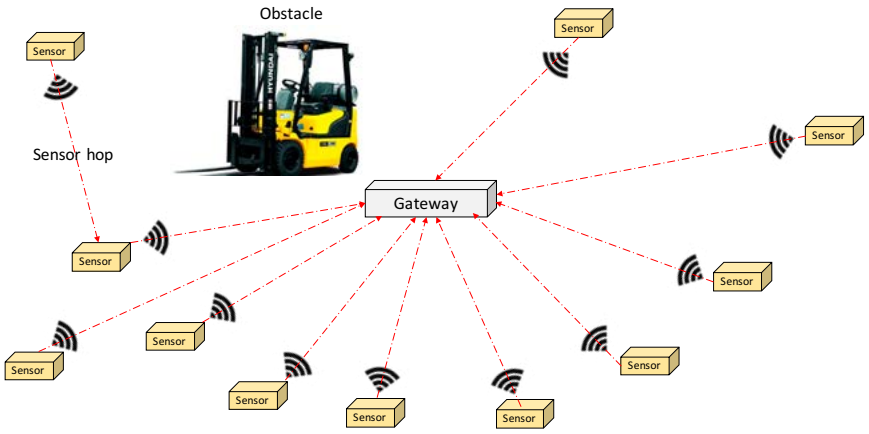


Figure 7. Wireless mesh network example.

Low Power Wide Area Network (LPWAN) is another technology worthy of note for industrial applications. LPWAN protocols are well-suited for use in industrial settings. These networks are nominally 900 MHz, a frequency range that performs well in highly metallic environments.

LoRaWAN is intended for wireless battery-operated nodes in a regional, national, or global network. It targets key requirements needed for the Internet of Things (IoT) like low data rate, low cost and long battery life while delivering vital features such as secure bidirectional communication, location, and mobility services. In Europe, LoRaWAN operates in the 868 MHz band. North American LoRaWAN installations use the 915 MHz band.

End devices using LoRaWAN can choose from three device classes, allowing different device behavior depending upon optimization needs:

- Class A – battery powered node
  - Class A operation optimizes communications to conserve battery power at the node
- Class B – low latency needed
  - Class B devices open extra receive windows at scheduled times to optimize communications but with shorter battery lifespan
- Class C – no latency
  - Class C devices have nearly continuously open receive windows reducing latency to its practical minimum

More information can be found at www.LoRa-Alliance.org.

LoRaWAN presents performance advantages for wireless sensing networks in industrial environments and is already gaining popularity for many IoT applications. This is a wireless network to watch and include in your future network planning.

Network Planning > Two Years

Industrial network evolution includes a strong influence of better IT/OT collaboration. As these two very capable groups act in concert to improve business outcomes, some advanced IT practices will find their way into industrial networks. These are Time Sensitive Networking (TSN) and Software Defined Networks (SDN).

Time Sensitive Networking

TSN gets a lot of attention from automation experts due in part to the increased interest in the Industrial Internet of Things (IIoT). Some of the data collected by IIoT sensor networks is not inherently time sensitive. However, some data is mission critical and time sensitive and must be shared with strict latency and reliability requirements. Further, all data is enriched by adding accurate time context as it allows correlation and analytics to excel. Therefore, TSN is an important technology both within the control loop and outside the loop in IIoT applications.

There are four key benefits that TSN applied to industrial networking provides:

- Bandwidth: Machine vision, 3D scanning and power analysis applications running on an industrial network create large data sets which can strain available bandwidth; Propriety Ethernet derivatives industrial networks that are used in industrial control today are limited to 100 Mb of bandwidth and half-duplex communication; TSN supports standard Ethernet in full duplex with higher bandwidth options such as 1 Gb, 10 Gb and even the projected 400 Gb version in 802.3

- Security: TSN embraces top-tier Ethernet security provisions; Segmentation, performance protection, and temporal composability add multiple levels of defense to the security framework

- Interoperability: TSN integrates existing brownfield applications and standard IT traffic by using standard Ethernet components; TSN inherits many existing Ethernet features like HTTP interfaces and web services; These features enable remote diagnostics, remote visualization, and repair capabilities common to IIoT systems

- Latency and Synchronization: TSN prioritizes low-latency communications to provide fast response and closed loop control applications; It can achieve deterministic transfer times on the order of tens of microseconds and time synchronization between nodes down to tens of nanoseconds; TSN provides automated configurations for high reliability data paths where packets are duplicated and merged to provide lossless path redundancy; In doing so, TSN ensures reliable delivery of time sensitive traffic

TSN provides network designers with tools to ensure that critical traffic is received in a timely and reliable manner. It also frees up congestion to allow non-critical traffic to be converged onto the network and move as “best effort” traffic. This is an essential distinction in that almost all traffic is best effort. Wire speed and limiting traffic to only critical message streams is used to make the network function correctly.

There are two groups to monitor regarding TSN. These are:

– IEEE 802.1 Time Sensitive Networking Task Group, www.ieee802.org

– AVnu Alliance, www.avnu.org

IEEE 802 has united several domain experts under the auspices to 802.1 to create a suite of TSN specifications that are without equal. The group has led application needs from audio/visual, automotive, industrial automation, and consumer realms in creating these specifications.

AVnu Alliance focuses on the creation of an interoperable ecosystem through solution certification. Member companies include National Instruments, Broadcom, Cisco, and Intel to name but a few. The AVnu Alliance website presents superb resources to help companies understand and adopt these powerful concepts.

Software Defined Networks

Software Defined Networking (SDN) is an approach to computer networking that allows network administrators to manage network services through abstraction of lower level functionality.

The current state of industrial networks is illustrated in Figure 8. Along the bottom of the diagram are the solutions required by the manufacturing area – a robotics/welding cell solution, a conveyor solution and an error proofing solution. These solutions require automation to function and connections to the industrial network. Along the top of diagram are the domain expertise groups that design and specify the functional needs for each solution. The control engineers (OT staff) must translate the design and functional needs into an automation system and industrial network solution. These staffs are often quite modest so companies engage 3rd party experts to attempt to perform in a timely fashion.

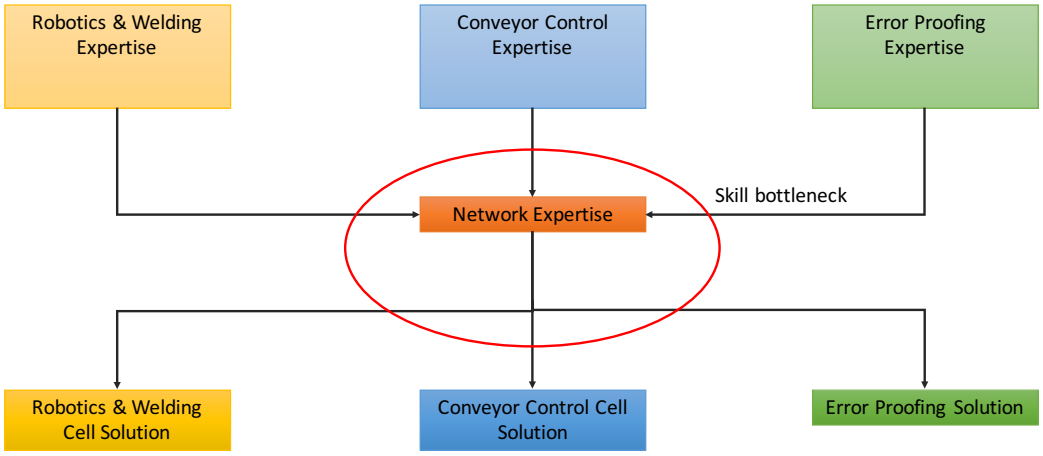


Figure 8. Traditional process/network design flow.

Once in place, the network and automation must be operated, managed, and maintained. A chilling statement from a Gartner blog post crystallizes the gravity of those functions. "… 80% of unplanned outages impacting mission-critical services will be caused by people and process issues and more than 50% of those outages will be caused by change/configuration/release integration and hand off issues."[3]

Traditional network design and maintenance practices tend to reinforce the problem. Significant time and planning are expended. Specialized domain expertise is required for each solution, both from a process and a networking standpoint. Unique manual configurations must be made for each network node. And due to pressing schedules and business priorities, change management and record keeping are often lacking.

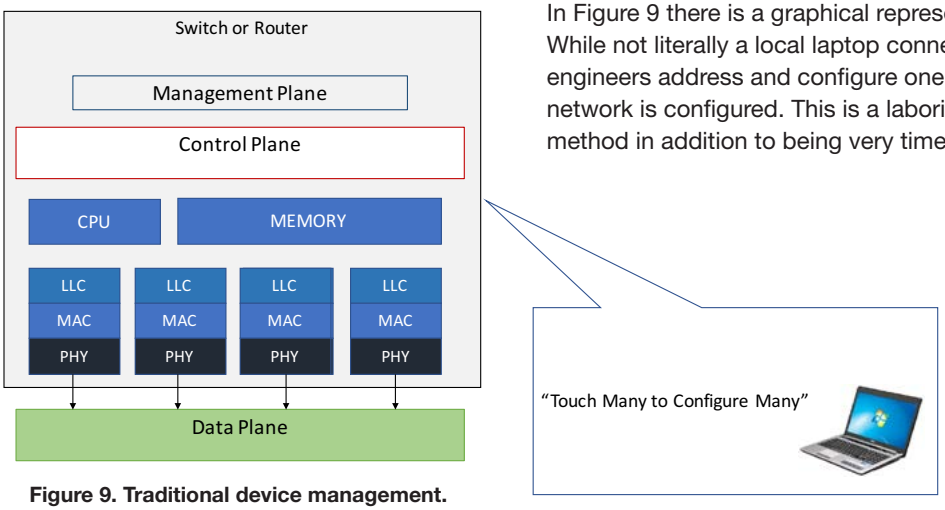


Figure 9. Traditional device management.

In Figure 9 there is a graphical representation of device management. While not literally a local laptop connection in all cases, traditionally engineers address and configure one device at a time until the whole network is configured. This is a laborious and potentially error prone method in addition to being very time intensive.

In Figure 10, a simplified view of device management using SDN is illustrated. Network switches and other compatible network devices abstract their control plane. The control plane functionality is transferred to a device called an SDN controller which provides control plane instruction sets to the subordinate devices. The SDN controller also contains management plane functionality. Therefore, a centralized controller handles monitoring, remediation, device behavior, and characteristics all from a central location. This architecture allows companies to create reusable configurations that can be replicated throughout multiple nodes using tested applications. Further extending the concept, it provides access to programmatically modify network nodes from the SDN controller. This functional change creates enormous benefits across the network.

SDN simplifies the configuration and implementation of network architectures by creating reusable configurations and designs that improve system performance. The simplified SDN also improves corporate margins because plants do not need to rely on network specialists on the factory floor, thus lowering personnel costs, improving implementation time, and reducing troubleshooting and repair costs.

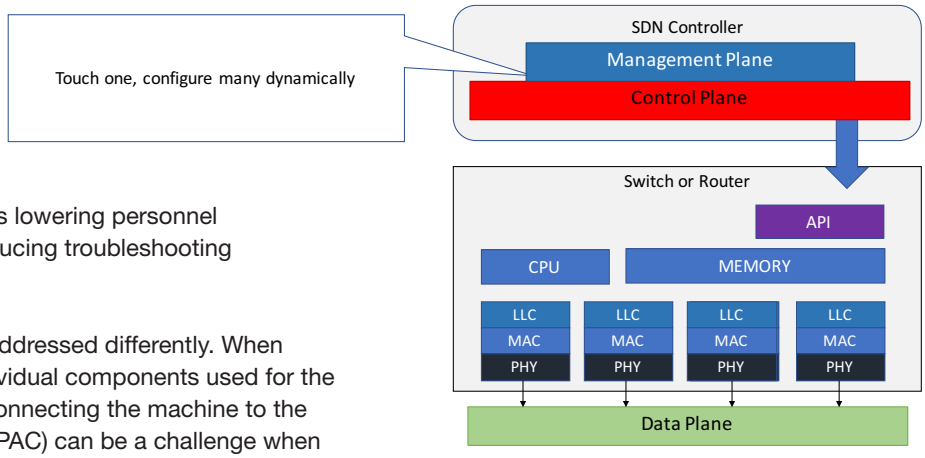


Figure 10. Device management using SDN.

Machine design is another area that must be addressed differently. When machine builders construct a solution, the individual components used for the machine are not often questioned. However, connecting the machine to the existing programmable automation controller (PAC) can be a challenge when Ethernet is not used and standards are not followed. Some machine builders leverage technology that is so disruptive that redesigns are required to some of those systems. To address this situation, it is critical for manufacturers to specify that wireless and Ethernet components communicate seamlessly with other systems.

An SDN for industrial network applications needs time to gestate and develop, hence its placement in the "> 2 years" time horizon.

One of the critical items for this concept is the retention of network switch features that are optimized for industrial applications. To explain, one artifact of SDN in the data center application space is that companies sought to deploy "white label" switches in the architecture. The "white label" network switches are minimally viable products with very modest feature sets. These are completely appropriate choices for the data center implementation of SDN. However, it could be a stumbling block for industrial networks.

Conclusion

The industrial network infrastructure is a valuable business asset. Investments in legacy industrial networks require a clear migration path to optimize return on assets while not missing out on performance enhancements from new technologies. A robust, well-executed physical layer is foundational to this asset continuing to deliver value. Rapidly emerging technology advances such as the Internet of Things, Wireless Sensor Networks, Power over Ethernet, and Time Sensitive Networking can further leverage your network with a little education and planning.

References

[1] 2022 Industrial Network Market Shares According to HMS Networks." 2022 Industrial Network Market Shares according to HMS Networks, June 30, 2022. https://iebmedia.com/news/tech-updates/2022-industrial-network-market-shares-according-to-hms-networks/.

[2] Cisco Systems and Rockwell Automation, "Converged Plantwide Ethernet Design and Implementation Guide," (2011 – 2017).

[3] Colville, Ronni J., & Spafford, George. October 27, 2010. "Top Seven Considerations for Configuration Management for Virtual and Cloud Infrastructures," *Gartner RAS Core Research Note G00208328,* https://img2.insight.com/graphics/no/info2/insight_art6.pdf

Since 1955, Panduit's culture of curiosity and passion for problem solving have enabled more meaningful connections between companies' business goals and their marketplace success. Panduit creates leading-edge physical, electrical, and network infrastructure solutions for enterprise-wide environments, from the data center to the telecom room, from the desktop to the plant floor. Headquartered in Tinley Park, IL, USA and operating in 112 global locations, Panduit's proven reputation for quality and technology leadership, coupled with a robust partner ecosystem, help support, sustain, and empower business growth in a connected world.

For more information

Visit us at www.panduit.com

Contact Panduit North America Customer Service by email: cs@panduit.com
or by phone: 800.777.3300

THE INFORMATION CONTAINED IN THIS WHITE PAPER IS INTENDED AS A GUIDE FOR USE BY PERSONS HAVING TECHNICAL SKILL AT THEIR OWN DISCRETION AND RISK. BEFORE USING ANY PANDUIT PRODUCT, THE BUYER MUST DETERMINE THE SUITABILITY OF THE PRODUCT FOR HIS/HER INTENDED USE AND BUYER ASSUMES ALL RISK AND LIABILITY WHATSOEVER IN CONNECTION THEREWITH. PANDUIT DISCLAIMS ANY LIABILITY ARISING FROM ANY INFORMATION CONTAINED HEREIN OR FOR ABSENCE OF THE SAME.

All Panduit products are subject to the terms, conditions, and limitations of its then current Limited Product Warranty, which can be found at www.panduit.com/warranty.

*All trademarks, service marks, trade names, product names, and logos appearing in this document are the property of their respective owners.

PANDUIT US/CANADA
Phone: 800.777.3300

PANDUIT EUROPE LTD.
London, UK
Phone: 44.20.8601.7200

PANDUIT SINGAPORE PTE. LTD.
Republic of Singapore
Phone: 65.6305.7575

PANDUIT JAPAN
Tokyo, Japan
Phone: 81.3.6863.6000

PANDUIT LATIN AMERICA
Guadalajara, Mexico
Phone: 52.33.3777.6000

PANDUIT AUSTRALIA PTY. LTD.
Victoria, Australia
Phone: 61.3.9794.9020

©2023 Panduit Corp.
ALL RIGHTS RESERVED.
CPAT55-WW-ENG
3/2023