PANDUIT®

Technical Article

Industrial Automation

Down to the Wire – Building a Resilient Network Infrastructure

Andy Banathy, Solution Architect, Panduit

March 2015

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.org[1] 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 Gartner[2], 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,” said Andy Banathy, Solution Architect, Panduit. “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

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

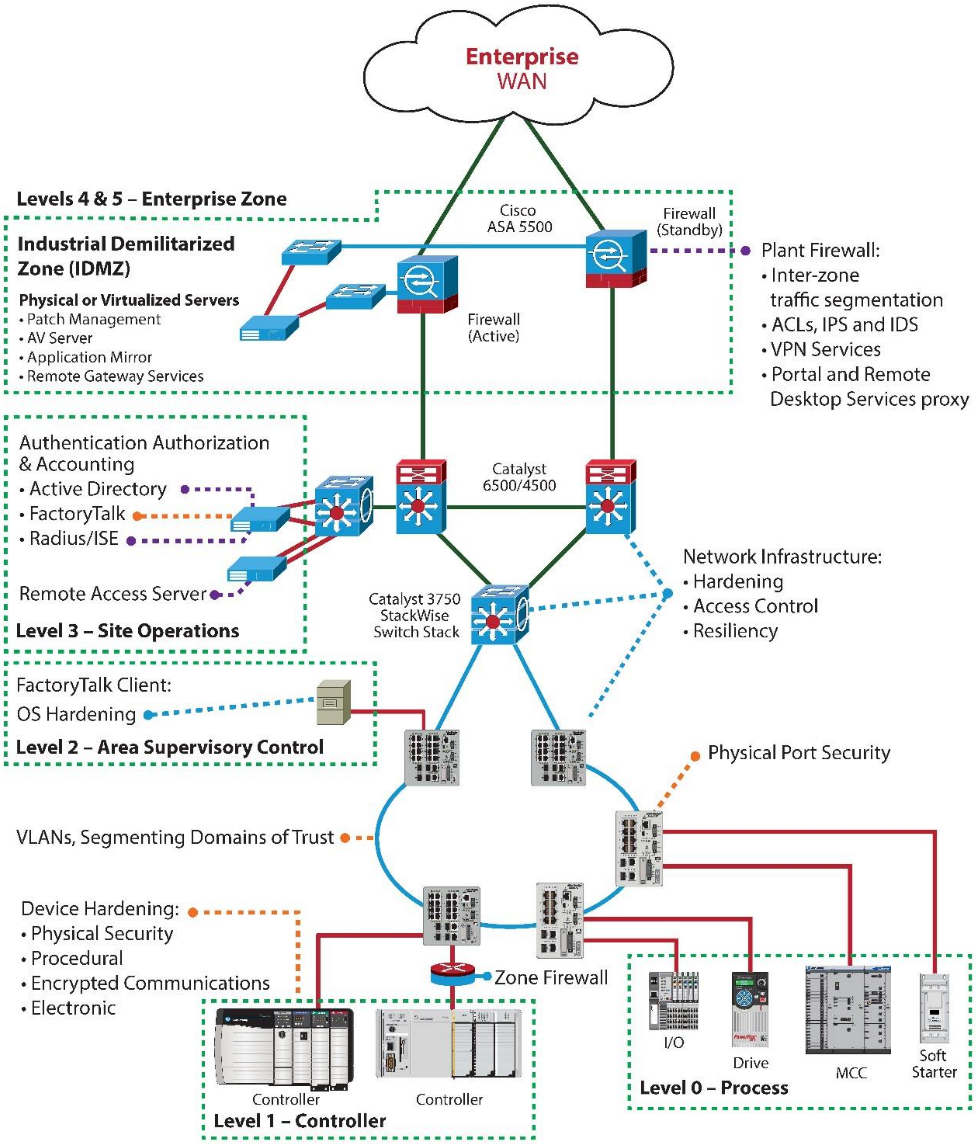
The industrial network is not an island. As part of the assessment, manufacturers should determine how to connect with the enterprise network, which has greater security needs due to the number of security attacks on the IT network.

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.



Converged Plant-wide Ethernet (CPwE) architecture

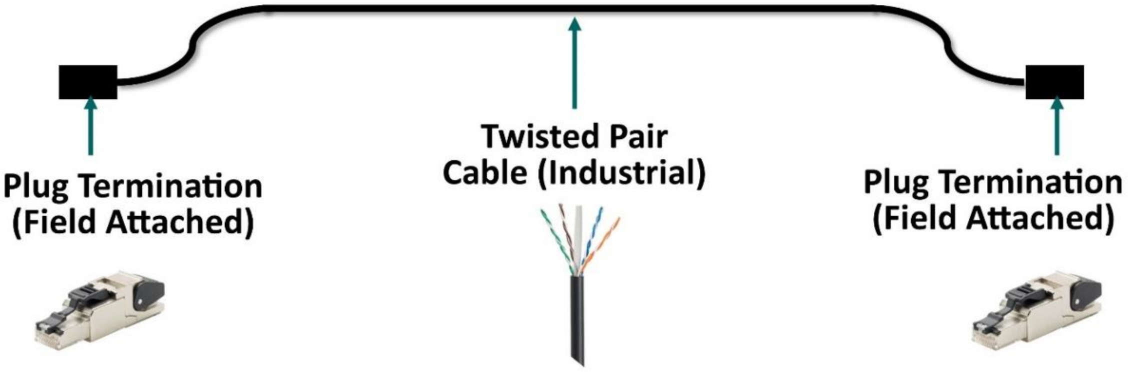
This architecture uses VLANs to efficiently segment traffic across the Layer 2 and Layer 3 network infrastructure; however, all plant control traffic stays below the Demilitarized Zone (DMZ) layer, while any information needed in the enterprise zone is accessed through a server in the DMZ rather than 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

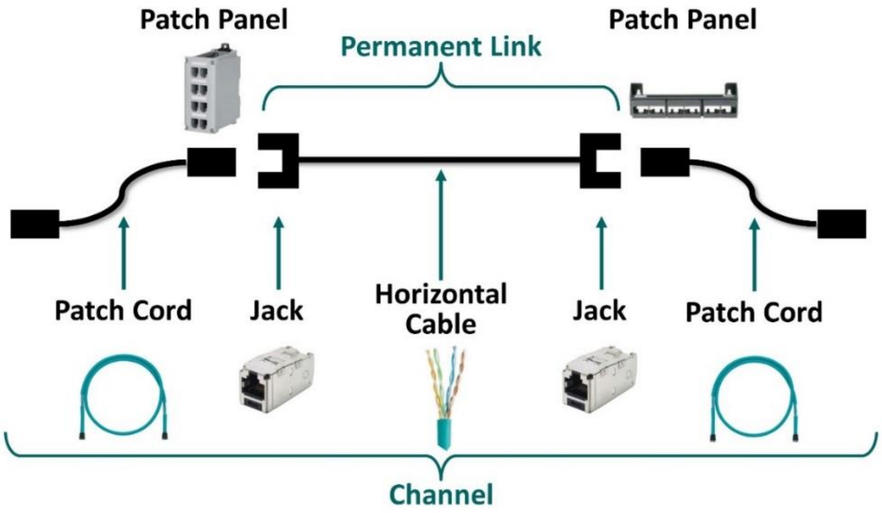
Traditionally, industrial networks have been set up in a point-to-point configuration, with a single cable terminated to plugs (i.e., a long patch cord). Structured cabling is emerging as a more robust and sustainable infrastructure because it better facilitates growth and troubleshooting, factors that 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.



Simplified example of point-to-point cabling

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.



Simplified example of copper structured cabling

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.

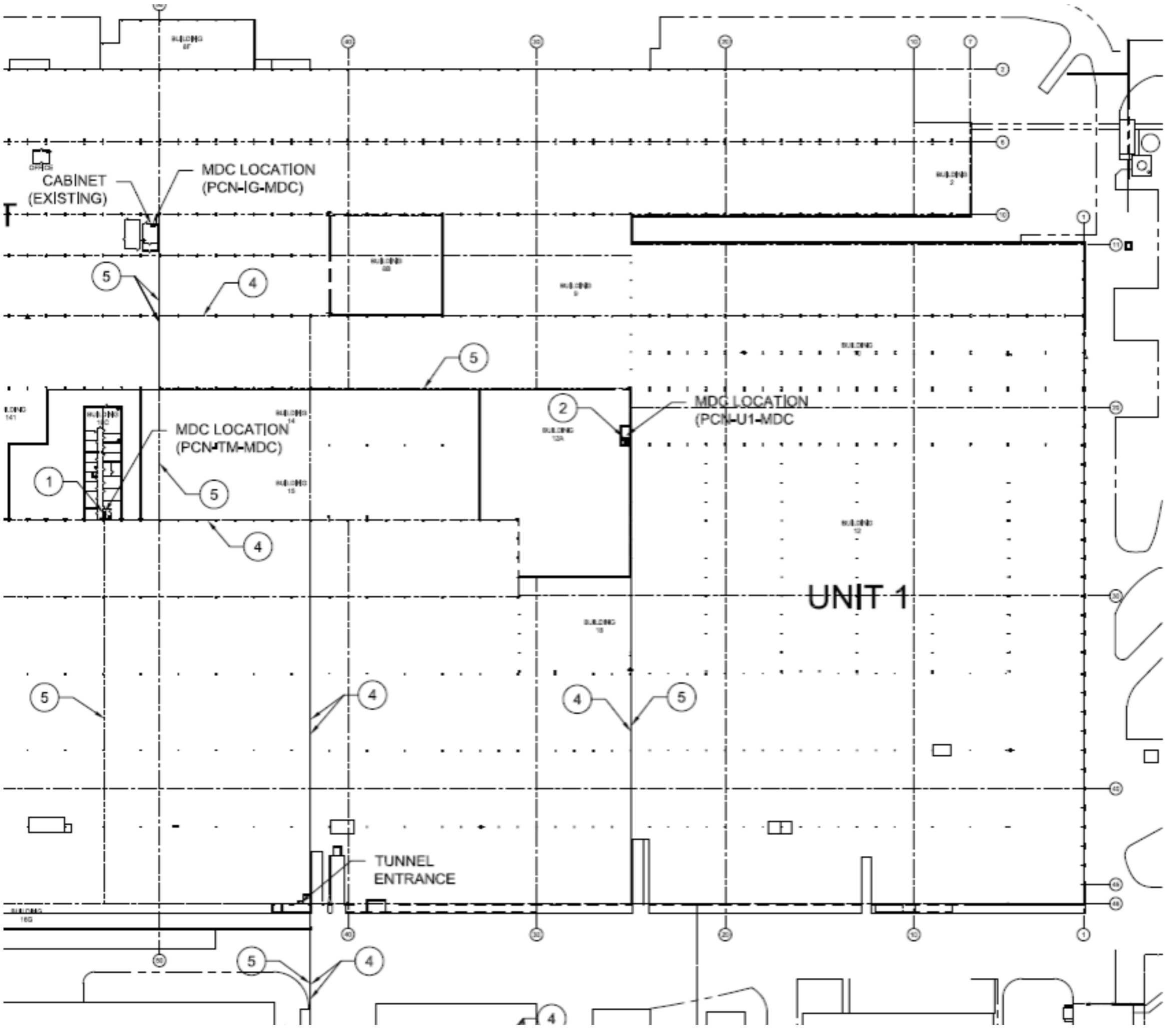
Corrosive, wet, and oily environments all impact network cable jackets, causing degradation. There are a variety of outer jacket coverings such as polyurethane, polyvinyl chloride (PVC), and thermoplastic elastomer (TPE), which have varying levels of cable protection. The toughest jacket covering, polyurethane, 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 requirements 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.



Example of a plant cable layout

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 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