PANDUIT®

Technical Article

Industrial Automation

Modernizing the Industrial Ethernet Network with Increased Visibility

Michael Vermeer, Product Line Manager
Panduit July 2016

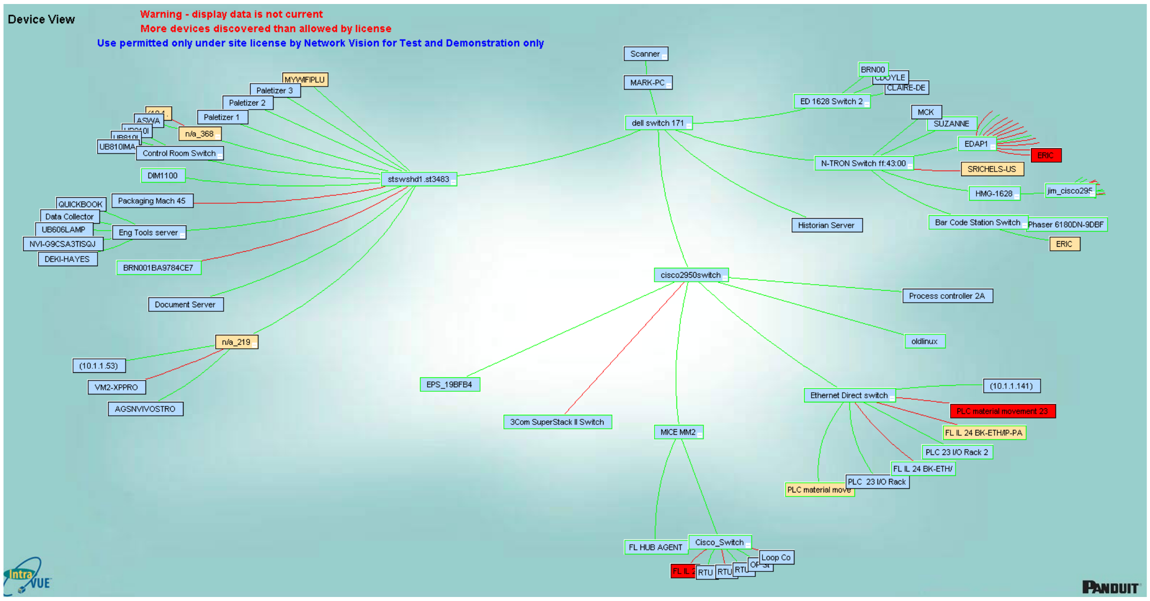
The Internet of Things (IoT) and smart manufacturing have become two of the hottest concepts in today's industrial automation world. Together, they are paving the way for the arrival of a new era in manufacturing – dubbed "Industrial IoT" or "Industry 4.0" – a world where sensors, devices, and machines will all be connected by the Internet, operate without human interaction, and offer massive amounts of data that can be used for powerful new insight and intelligence.

Core to the Industrial IoT is the phenomenon of a highly automated "smart factory," powered by connected devices, smart technologies, and seamless processes. This is the next big advancement in modern manufacturing that promises to make room for major operational efficiencies, unparalleled flexibility, productivity gains, and increased profit margins.

Despite these benefits, the factory of the future may seem like a daunting and expensive path to take for many of today's industrial facilities, which are constrained with hefty investments in legacy equipment, implemented the same way they were decades ago at a time when proprietary communications protocols did not need to talk to each other. Before now, there were only a few nodes to connect, control, and monitor, allowing automation engineers, controls engineers and technicians to effectively manage and troubleshoot their networks using programming software tied to the automation system. While this made deployment more complex at the time, it was inherently less risky since it created inherent network segmentation of different parts of the system.

With the connected world in manufacturing gathering pace, the reality of the smart factory is not a far-fetched vision of the future, but manufacturing companies must begin to adapt and innovate now, or risk being left in the dark.

Considering just 10 years ago, small- to mid-sized manufacturing facilities were effectively managing 10-12 Ethernet devices at each of their plants and are now running upwards of 300 devices, this is an extraordinary growth. Moreover, executives in the manufacturing industry anticipate that 95% of companies will take advantage of Industrial Internet of Things (IIoT) technology within three years, aiming to further automate their manufacturing processes by employing smart manufacturing and IIoT concepts and technology on their plant floors. This will radically increase the number of connected industrial devices on the plant floor in the future. As it stands now, numerous components on the plant floor are interconnected, including I/O devices, PLC controllers, human-machine interfaces (HMIs), drives, process instruments, and IP cameras.



Device View

Warning - display data is not current
More devices discovered than allowed by license
Use permitted only under site license by Network Vision for Test and Demonstration only

A schematic of a highly connected plant floor

With the IoT expected to add an astonishing 50-100 billion connected devices to the network in a short few years, manufacturing facilities are faced with the almost unfathomable task of overcoming a number of significant hurdles before realizing the advantages of the Industrial IoT. But, by adhering to the following three steps, manufacturing facilities can successfully unlock the many benefits the Industrial IoT promises to offer; some of which can be reaped in a mere six months:

1. Modernize the Industrial Ethernet Network
2. Adopt a proactive and preemptive approach to maintenance
3. Gain complete plant-level awareness and visibility

To better understand how manufacturing facilities can transition into the Industrial IoT and achieve complete plant-level awareness and visibility, let's first briefly look back at the backbone of manufacturing - the Ethernet Network; why it became the popular network choice in manufacturing, and how it compares to Industrial Ethernet.

Industrial Ethernet vs. Enterprise Ethernet

If you were a fish, knowing the difference between salt water and fresh water would be vitally important. Likewise, you would not wear a hard hat in an office setting, nor would it be a wise choice to wear flip-flop sandals on a factory floor with potentially hazardous equipment. Similarly, there are many subtle differences between Industrial Ethernet and enterprise Ethernet, each with their own benefits to be gained (or disadvantages) for the plant floor and office environments.

Office	Plant Floor
80% clients (Workstations) 20% Servers (Printers & Computers)	20% Clients (Operator Workstations) 80% Servers (PLCs, Drives, I/O, etc.)
Network traffic consists of relatively fewer, larger message sizes that travel to/from private or public cloud	Network traffic consists of a relatively more frequent, smaller messages that travel between networked devices
Many devices operate during normal business hours in accessible areas	Systems operate on a 24x7 basis and scattered throughout the plant
Network downtime is a nuisance. Individual client problems may take a day to solve.	Network downtime directly results in lost profit and must be eliminated
Local workers are not encouraged to directly address network-related issues	Local workers are encouraged to detect and solve any issues on the plant floor

This table describes the key differences between Enterprise Networks for an Enterprise (Office) Environment and Plant Environment

Decades ago, Ethernet became the popular network standard communication for enterprise office settings, given its cost-effectiveness, reliability, and overall high performance. For similar reasons, Ethernet made its way onto factory floor networks in the form of Industrial Ethernet, which uses the same standard-based networking protocols as enterprise Ethernet, but is uniquely designed to work in the harsh and rugged industrial environments of a plant floor. Such factors include extreme temperatures, humidity, vibrations, and other disturbances with manufacturing equipment that far exceed the ranges (and requirements) for IT equipment, which work just fine in their controlled office environments.

While enterprise networks tend to be bandwidth-limited, manufacturing facilities are more concerned with timing and collisions of traffic on the network than bandwidth. Using standard Ethernet protocols along with the high speed needed for manufacturing environments, Industrial Ethernet on the plant floor quickly became standardized; replacing its fieldbus networks predecessors in the factory. As a result, Industrial Ethernet networks have since become the universal preferred choice for manufacturing and automation systems and business systems. It simply provides a baseline for all manufacturers to work together, offering a consistent and robust system to easily connect computers, networks, data centers, machines, and a variety of automated devices.

Shifting toward a Proactive Approach with Increased Visibility

Now, with the vast number of connected devices entering the plant floor, Industrial Ethernet Networks are reaching the point of no return. Homegrown flat networks can no longer bear the requirements being placed on them by new applications. This, combined with the lack of visibility into these networked automated devices, which are fundamentally responsible for a facility's overall production output, is making detection, diagnosis and problem resolution a costly, time-consuming and a highly complex and painful undertaking. This too will all change as a byproduct of the Industrial IoT, including the way the plant floor works at many facilities, as automation and controls engineers need to integrate older propriety and serial industrial networks, with new networked systems based on an IT infrastructure. Essentially, for the first time ever, the technology gap between information technology (IT) and operational technology (OT) is closing.

Meanwhile, several manufacturing companies are falling into bad habits of looking the other way (whether deliberate or not) to apparent issues throughout their automation system, knowingly awaiting the impending problems that will follow and only continue to rise. When we monetize the cost of ignoring disruptions in the manufacturing world, over time an entire company could either go under, or pay a hefty price. For many companies, an outage could mean losing revenue at a rate of $2.50 to as much as $350/second.

For example, a major grocery retailer recognized widely disruptive Ethernet connectivity issues across almost their entire plant network. Specifically, devices on the plant automation network would inexplicably cease communications. One of their dairy farms, which produces 120,000 gallons of milk each day, experienced a network disruption so dire, they suffered from nearly a full day of downtime.

They were encountering data interruptions arising from certain programmable logic controllers (PLCs). Using IntraVUE™ application software, which provides visibility, diagnostics and analytics, the plant's team uncovered several PLCs with duplicate IP addresses, which were causing the network to act erratically. The IT team used IntraVUE software to isolate various devices on the network, locating an undocumented, non-industrial device that was mounted above a false ceiling, and removed it, which resolved the issue.

This grocery retailer has since standardized with IntraVUE software across all 33 plants primarily using it as an analysis tool for when problems occur as well as using its' alerting features to inform of any sudden changes in network behavior.

Unlike the above example, nearly 80% of companies have insufficient or ineffective preventive maintenance programs. There is a need not being met—and the demand for a reliable plant network infrastructure has never been higher. To evolve, manufacturing companies must shift away from the current reactive response approach (i.e., responding only when a disruption occurs) to a mindset of pro-activeness. This is the only way manufacturing facilities will greatly improve both the uptime and performance of these critical, real-time networks while also better ensuring valuable time and cost savings; an especially critical component to realizing the true benefits of the Industrial IoT.

Achieving Full Plant-Level Awareness of the Industrial Network

The bread and butter to the IoT are actionable intelligence and insight, which allows industrial controls professionals to make better-informed decisions. For the Industrial IoT, having the ability to know which devices and systems are connected where—and pinpointing what is creating specific disruptions that force downtime – will be critical. With real-time visibility, monitoring and insightful analytics into and from the entire network, those responsible for plant output can assure network uptime and quickly address risks as they appear, before they become an actual problem.

With a tool like IntraVUE software, automation and controls engineers have at their fingertips access to real-time information on how their automation system infrastructure is performing. They can use key performance indicators (KPIs) and analytics capabilities to monitor performance and quickly resolve issues as they occur, such as duplicate IP addresses (e.g., as in the example above), device failures, intermittent connection problems, switch resetting, and large file transfers between devices.

Achieving full plant-level awareness ultimately empowers industrial controls professionals with visibility into the growing complexity of their plant's entire automation system. And, with the Industrial Ethernet connectivity landscape that narrows the scope of where connectivity issues are occurring, plant technicians can get to the root of the problem faster. IntraVUE software allows a complete view into the industrial network, provides actionable insight, improves overall uptime, and reduces network support costs and response times by more than 50%.

The Industrial Internet of Things (Industry 4.0)

The plant of the future requires more automated communication throughout the supply chain that only a modernized, well-architected and managed Industrial Ethernet Network can provide. While each manufacturing company has its own unique challenges, the influx of connected devices expected from the Industrial IoT will inevitably increase the possibility of disruptions, making the need to rapidly detect those disruptions even more important.

Implementing a comprehensive tool that can reduce the potential for intermittent communication disruptions, enable continuous real-time monitoring, and provide remote support, can offer valuable time and cost savings to manufacturing facilities of all sizes today, and in the years to come. With full awareness and real-time visibility into the entire Industrial Ethernet device architecture of levels of devices and connectivity, operational field technicians can efficiently communicate with IT resources, who are also confidently armed with vital information to allow a shift from a reactive response approach to one that is proactive and comprehensive. This, with access to real-time insight and actionable intelligence to enable better-informed decisions are the keys to successfully unlocking all the benefits of the Industrial IoT.