AutomationWorld® TACTICAL BRIEF

Building an Infrastructure that Enables IoT

CONTENTS

Constructive Disruption: A Vision of Smart Manufacturing

Jim Wetzel, director of global reliability at General Mills and Chair of the Smart Manufacturing Leadership Coalition, asked attendees at The Automation Conference an important question: "Are You Ready?"

By Stephanie Neil , Senior Editor, Automation World

General Mills started its smart manufacturing journey in 1993. The first step was to network all of its plant floor equipment, PLCs, and devices. The company also had a Unix-based manufacturing intelligence system, because, at that time, they wanted to answer the question: "How are we doing?"

The problem was, they didn't know how much data they needed, so they sucked it all up in what Jim Wetzel, General Mills' director of global reliability calls "the vacuum cleaner approach." But even with all of that data, all they could do was look—as they didn't have access to production reports, system efficiency trends, or overall equipment effectiveness (OEE) information.

Twenty-two years and 700 billion data points later, the global food manufacturer has much more insight into what that massive amount of information means.

During his keynote this week at The Automation Conference in Chicago, Wetzel outlined the steps General Mills took over two decades to move the company closer to its smart manufacturing vision.

What is smart manufacturing?

"For us it is trending [data] in the cloud for traceability, transparency, and visualization," says Wetzel. "It is networking the supply chain, and shortening the time to get actionable information on the plant floor."

And, it is positioning the company to be ready for the Internet of Things (IoT), which Wetzel says will be a "constructive disruption" to the manufacturing industry. In other words, IoT is disruptive technology that will get us to places we haven't yet been.

To deliver on this vision for General Mills and other manufacturers, Wetzel took a proactive position as the Chair of the Smart Manufacturing Leadership Coalition (SMLC), a non-profit organization comprised of manufacturers, suppliers, universities, and federal agencies. The group is collaborating on a scalable platform that will drive industrial competitiveness. The goal is to enable companies of all sizes to gain easy, affordable access to modeling and analytical technologies that can be tailored to meet cross-industry business-case objectives without having to retrofit existing systems.

SMLC started in 2006 with a group of thought-leaders gathering at a workshop in Washington, D.C., and sharing war stories of how painful it was to create an interconnected ecosystem. SMLC was born from those discussions, and, perhaps more importantly, a challenge by the Department of Energy (DOE) for the group to deliver on their vision. So the coalition submitted a proposal to build out a smart manufacturing pilot—funded by the DOE—to drive down energy consumption in manufacturing.

Today, a few more pilots are in place, and the way these companies have been able to simplify the ecosystem is by using cloud technology for delivering apps, including data collected from the Internet of Things. The SMLC's framework is taking real-time data from sensors and figuring out how to add context so that apps can be created to do something-- to act on the information.

"At the end of the day, smart manufacturing is not about just getting connected, but getting connected so that you can do something to add value and optimize operations," says Wetzel.

The measure of success, Wetzel says, is having the ability to deliver value and evolve with changing business using a technology infrastructure that is supportable, quick, and delivers information that can be trusted.

General Mills is applying the developing smart manufacturing framework to its own operations, and, as a result, can easily answer the question "How are we doing?"

Now, Wetzel has a different question—one he asked the audience at the end of his presentation: "Are you ready for this journey?"

Improve Industrial Ethernet Network Uptime

Robert Reid, Sr Product Manager at Panduit

What we are seeing today in manufacturing is an update of plant network architectures with solutions that securely merge information and control data to improve performance, security and safety within the plant. Network uptime is becoming increasingly important as ethernet is starting to be deployed for critical and time-based processes, where keeping such discrete networks active through a fault without stopping critical processes is paramount.

Given that greater than 60% of ethernet link failures are related to physical infrastructure (Grenier, 2011), it is important from the outset to design and build a resilient network that is architected to recover (converge) quickly from a failure condition.

Switching and signaling delays are affected by media type (Fiber/Copper), media length, number of switch hops and transceiver type, whereas processing and reservation time are independent.

Convergence occurs as a result of a change in network topology, i.e., a physical link failure. When this occurs, a routing algorithm is run to build a new routing table based on the failure condition/location. Once all the routing tables have been updated, convergence is complete.

The convergence time to recover and restore from a failed path condition depends on several factors. In restoration, switching occurs after backup paths are computed following the receipt of failure notification. The convergence time to recover a single path is the sum of the following:

1. Signal delay: time to signal a network failure between nodes (largest component)
2. New path processing delay: time taken to compute an alternate path
3. New path reservation delay: time required to reserve on newly computed path
4. Switching delay: the time required to switch from affected path to new path

For a detailed experimental validation of convergence time over different media (copper fiber) and transceiver sets, refer to joint Rockwell Automation and Cisco work on network resiliency.

One of the main findings of this study is that fiber offers higher resilience through convergence times for uplinks and rings as compared to copper. In the network architectures covered, network availability and performance benefits described can be achieved by deploying robust fiber optic cabling channels as shown in the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (ENET-TD001).

One way to achieve high resiliency on uplinks is to deploy a redundant star topology utilizing a redundant pair of fiber links on a single switch, one active and one acting as a standby (Cisco FlexLinks and LACP for example). Convergence times here can be less than 50 ms.

High resiliency/low convergence time on rings can also be achieved through protocol (REP - Resilient Ethernet Protocol) with

fiber where we have critical processes that require a few ms of convergence.

Obviously, not all industrial ethernet applications have strict requirements on convergence time. Required convergence times depend on the tolerance of the system to withstand a loss of communications and the risk posed. Convergence time requirements vary from information processing, such as Human Machine Interface (HMI) applications, where less than 1 second is acceptable, to critical motion control applications where a handful of msec is required. Choice of physical infrastructure (architecture, media types, transceiver sets) vs convergence requirements should be studied in the light of total installed cost.

The most common pushback to deploying fiber in such networks, is that solutions tend to be expensive and "craft sensitive" with high learning curves. Fiber solutions today have evolved to be much easier to deploy in factories and plants and there are new ways to terminate that are more "electrician friendly". The "Deploying Panduit Polymer Coated Fiber (PCF) Cable" video shows deployment and termination of an Interconnect cable within a cabinet for an industrial application.

New installer friendly industrial automation fiber optic cables are designed with technicians in mind and are ideal for harsh, device-level industrial installations. Cost effective, large diameter, high strength GiPC fiber (Graded Index Plastic Clad Fiber), like hook-up wire, is easy to prepare and terminate with LC Crimp and Cleave connectors using hand-held tools and minimal training. A good resource for applying fiber with industrial applications is the Fiber Optic Infrastructure Application Guide.

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%.

How to be Sure Your Network is Futureproof

Manufacturers should carefully consider their infrastructure investments today to take advantage of the emerging wealth of industrial innovations enabled by the Internet Protocol (IP).

Paul Brooks, Business Development Manager, Rockwell Automation

Consider: The typical infrastructure lifecycle in the automation space is somewhere between eight and 10 years. Looking at the rapid advance of innovations using IP technology in the consumer and commercial sectors, it's clear that manufacturing must prepare for a similar evolution. Part of that evolution is predictable today and here we explore some of those predictable changes to our information landscape and its impact on infrastructure.

That's because IP isn't just some transitory consumer convenience or the latest iteration of a familiar business tool. IP is and will continue to be the defining technology of the Internet and the Internet of Things (IoT) – as well as the applications that convert the data generated by these things into an abundance of actionable information.

The IoT is re-defining the Internet as we know it, and its exponential growth is transforming myriad markets and socio-economics on a planetary scale. In 2014, for example, an estimated 100 objects per second were connecting to the Internet, ranging from digital tablets, to cardiac monitors, to sensor-enabled thermostats. By 2020, more than 250 things will connect each second.

On the factory floor, this phenomenal growth includes controllers, sensors, video cameras, and other devices and applications – some still awaiting invention.

Today, manufacturers can future-proof their operations by embracing business practices, customer approaches and technologies that leverage standard, unmodified use of the Internet Protocol.

Megatrends Favor IP

Many best-in-class manufacturers already are deploying a secure, IP-enabled communications fabric to improve connectivity between people, partners and processes in industrial applications. These "early adopter" companies stand ready to reap their share of the $3.88 trillion in global profits expected to be generated by manufacturers in the next decade because of the Internet of Things.

Still, many other manufacturers aren't ready or aren't convinced about the opportunities offered by a unified, IP-centric network.

So why should they believe? Because the megatrends that favor investing in a converged IP-enabled network are multiplying. And they'll significantly impact manufacturers within the lifecycle of automation equipment they buy today.

Worker mobility. The digital tablet is here to stay. Already, sales of handheld devices, including smart phones and tablets, exceed those of traditional PCs. While tablets are rare on factory floors today, it's safe to assume they'll become mission-critical devices within the lifecycle of current investment decisions.

That means manufacturers will need a network infrastructure that supports the type of authentication and encryption coded into tablets. And they'll also need to integrate wireless into their plant floor communications architecture, using standard IEEE 802.11 technologies.

The end of standalone PCs. On the server side, something is occurring that's equally transformative to the rise of digital tablets. The cloud and virtualization are changing the way we scale, deploy and manage our compute resource, driving down both operational and capital costs. For example, some vendors are selling many medium voltage drives with cloud services and delivering real up-time benefits doing so.

Early adopters of virtualized servers are slashing the costs of server acquisition, deployment, maintenance and upgrades. The data center is coming to a plant near you – obviously industrialized, but also virtualized.

This has a real impact on manufacturing networks, significantly increasing data volume – and even more significantly, impacting the types of traffic flowing through the network. Today's networks must be designed to carry tomorrow's data flows and types. That means manufacturers will need to support all their virtual clients on different virtual LANs from their automation equipment. They'll also need routing capability for servers that are not physically adjacent to machinery.

These changes will demand a demilitarized zone, and servers running inside the demilitarized zone to provide access to the manufacturing zone.

The rise of remote expertise. The pool of engineers and technicians with expertise in automation systems is shrinking globally. In the not-too-distant future, manufacturers won't have a specialist in every technology in every plant. Instead, they'll increasingly outsource those skills.

The inevitable move of humans away from the plant floor – and often away from the plant itself – will increase the need for video and other electronic eyes to support both monitoring and human collaboration.

Remote access will become the norm, whether by machine builders with maintenance

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.

contracts, or virtual engineering teams, or simply by the expert on a specific machine working in a different plant.

This means the network architecture for manufacturing will have to support video and other collaboration tools. Remote experts also will require the ability to tunnel through the demilitarized zone from outside.

By committing to a common technology platform with the rest of the Internetworking world, manufacturers can increase their talent pool and reduce the barriers that keep much-needed expertise outside the door of the plant floor.

More productive machines. Tomorrow's manufacturing won't revolve around real-time control and making machines run faster. Companies running at an OEE in the 60-plus percentage-point range can't make their machines run 50 percent faster – the products can't handle it.

Besides, the traditional focus on building faster and faster machines already is eroding. Just look at the automotive industry, where cycle times are getting longer rather than shorter. That's because customers want more and more customized vehicles. And more customization requires a longer cycle time.

So the question isn't, "how many cars can we produce in an hour?" It's "how efficient is our manufacturing process – how lean is it?"

This requires manufacturers to look at long-term process optimization with a whole new set of sensors, historians, analytic software and decision-making loops – all co-existing on the same network. The sensors and historians commonly used today for real-time control aren't necessarily going to be the right ones for long-term process optimization.

Manufacturers also need to think about different measurements. The classic example of this is vibration monitoring. It's been deployed in industrial applications for years and years. But other technologies will come to the fore purely for long-term process optimization rather than for real-time control.

Automation drives investment. Fifty-five percent of all devices currently deployed on plant floors are connected to programmable controllers and use automation protocols, according to IHS Research. So for the foreseeable future, the automation system will continue to drive network infrastructure investments.

This means manufacturers must choose automation protocols that co-exist with the IoT universe – including innovations and inventions yet to be conceived.

We don't know all the transformative innovations that IoT will enable – if we did we would be working on them in our garages right now! But we do know that IP will be the enabling technology that fosters those innovations.

Commonality of technology enables and facilitates commonality of processes. Today, manufacturers can prepare for the advances of tomorrow by adopting Industrial IP.

The Plant of the Future: Seven Key Elements

By Todd Edmunds (Cisco), Bob Voss (Panduit) & Cliff Whitehead (RA)

For decades, manufacturing operations technology (OT) and enterprise information technology (IT) systems developed and evolved into separate physical architectures – remaining largely walled off from each other in the industrial and business spaces.

But in the Internet of Things era, in which an endless number of connected "things" communicate on the same network, the segregation of IT and OT networks can be a handicap.

As a result, manufacturers are converging their OT and IT systems into a unified network architecture, giving them nearly unlimited access to valuable production data that can help them make improvements and more swiftly react to market changes. On top of this, manufacturers also have access to new technologies, such as mobility, virtualization and cloud computing, that enable them to deploy their people, machines and infrastructure in ways that are more efficient and cost effective.

Given the vast opportunity that manufacturers are being presented with, nobody can say with certainty what the plant of the future will look like. Odds are there won't be a single archetype but rather many variations. Still, if we could peer into a crystal ball, we would probably see common characteristics across the plants of tomorrow.

1. Automation Network Infrastructure

Whether producing packaged meals, steel or automobiles, the plant of the future will be information driven, and that begins with a strong foundation in the form of a single common network infrastructure.

Today's proprietary and closed systems that dominate plants present a major challenge to sending data to the right place, at the right time and in the right context.

A common network infrastructure built on standard unmodified Ethernet and Internet Protocol (IP), such as EtherNet/IP, enables the seamless flow of data either within a plant or across an organization's global enterprise. It also offers new opportunities for increasing productivity, improving time to market and minimizing reconfiguration when conducting changeovers.

For assistance in designing and implementing a common network infrastructure, the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide from Cisco and Rockwell Automation provides validated networking architecture design principles, and the Panduit Industrial Ethernet Physical Infrastructure Reference Architecture Design Guide provides key considerations for the physical layer.

2. Security and Compliance

Before plants can unleash the true potential of IT/OT convergence in their operations, they must first protect and secure it. This includes protecting their intellectual property and physical infrastructure against unwanted access, as well as putting in strong oversight to manage network activity and potential application modifications.

A commitment to security and compliance will help minimize risk and unnecessary downtime, and allow organizations to confidently get more out of their operations.

How will plants accomplish this? Defense-in-depth security, which uses multiple layers of defense to protect information and assets, has emerged as the best-practice approach. A systems-oriented approach can leverage control systems, network hardware and software to, for example, limit communication between only defined entities or restrict users' ability to access specific pieces of control system content.

Other important measures will include implementing security enabled hardware and policies that span across applications, networks and systems, and deploying physical security safeguards such as access control and cabling lock-ins and block-outs.

3. Mobility

Mobile devices have the potential to permeate every aspect of the manufacturing world of tomorrow just as they are improving our personal lives today.

Early adopters of mobile technology in the industrial space are showing just how valuable it is by achieving up to 80 percent improvements in decision making times. More than that, mobile technology can be applied to equipment, such as for reconfiguring manufacturing processes to accommodate flexible operations and for wireless tooling.

Successful mobile deployment will be dependent on good wireless design practices and wireless products, as well as architecture implementations that help manage radio frequency interference.

4. Video

Get ready to think of video in an entirely new way in the plant of the future as more and more plants make the transition from analog video to IP-based video that resides on their converged networks.

For starters, IP video is improving how video can be used for security. More than funneling several streams of video for continuous human monitoring, IP video can be integrated with analytic software that can detect suspicious or unwanted activities and then notify security personnel. Higher-definition capabilities of IP video can also be used with facial-recognition software to manage personnel access.

But IP video offers more than security. It can help monitor the efficiency of a plant's people, equipment and production processes. Additionally, using mobile devices to video chat with remote service technicians from the plant floor can improve collaboration and more quickly resolve downtime events.

5. Industrial Compute and the Cloud

Among the many benefits a converged network infrastructure offers is the ability to deploy industrial compute resources at several levels – from edge computing on the plant floor, where the data is collected, all the way up to the cloud.

This allows you to deploy processing power in ways that can lower your deployment and maintenance costs, and improve your ability to collect and manage data from the production environment. It can also give you greater flexibility to add new intelligence and applications with minimal costs or disruptions.

For example, the advent of "fog computing" is allowing manufacturers to run software applications on networked devices, such as routers, switches and IP video cameras. Bringing applications closer to where data is generated provides another platform for computing that can make data easier to collect and process.

6. Remote Access

Whether it's a manufacturer with plants located around the world or an oil producer with rigs distributed across hundreds of miles, organizations have long struggled with having technical experts available on-site when needed and with empowering those experts to make the best decisions possible based on good data.

The truth is, many maintenance events don't require an expert on-site, and many maintenance activities are carried out using incomplete plant-floor data due to shortfalls in data availability.

Only a fraction of networks today currently have the capability to afford significant remote access traffic. The Internet of Things is changing that. Companies seeking this future state need to assess and plan to migrate their current network to this state so they can remotely monitor assets and proactively address issues before they become downtime events. Using wired and wireless technologies, remote experts working from a centralized location can securely monitor and analyze key metrics such as temperatures, flow rates and faults for plants around the world.

Should the remote experts notice an anomaly, they can immediately alert plant personnel of the

issue and work together to diagnose and correct it. This has the opportunity to minimize the frequency and duration of downtime events, and reduce unnecessary travel costs.

7. Energy Management

Energy is often merely treated as another cost of doing business, with most efforts to track it involving little more than month-to-month cost comparisons or replacing the least energy-efficient machinery.

But the plants of tomorrow will view energy as a manageable cost, with insights that drill down to more granular levels for better energy-related decision making.

They will use the power of their converged network to tap into energy-meter data or even turn assets into "smart" power meters themselves so they have a good profile of their energy consuming processes compared to their real time business needs. They will also use new technologies that can help them more intelligently manage energy through better control of their smart equipment, such as powering off unused equipment or switching equipment into lower power states when possible, to save energy and reduce costs.

The Future Is Now

It may be some time before most plants embrace these concepts, but the technologies needed to make them happen are all available today. Forward-thinking manufacturers and industrial operators are already embracing and adopting them. The question to ask yourself is: just how close is the future? And how ready are you?

The Evolving Automation Architecture

The Internet of Things is driving analytic advantage – is your plant ready?

By Jack Tyson former CTO at Panduit

A Cisco Consulting Services Study from 2014 found that 86% of manufacturers are investing in the Internet of Things (IoT) as they go after an estimated $4 trillion in benefits for manufacturing applications.

Why now? The cost of sensors, networking, storage and computing has dropped dramatically. New architecture models and technologies have emerged that ease deployment and accelerate time to value. Operations can increase overall equipment effectiveness and create new value through insights culled from existing control systems and by adding new sensors to track asset health and processing conditions.

Traditional automation architectures will continue to evolve to make machines and process skids grow smarter. However, there is a complication: These equipment assets need to be connected to the plantwide enterprise to unlock data and allow for wider scale and more innovative ana- lytic approaches. This plantwide network fabric is critical for advancing IoT.

Meanwhile, new approaches to acquiring sensor data through wireless mesh networks have been developed. These sensor networks do not connect directly to critical automation control systems but instead connect to com- puting resources close to the edge and to private/hybrid cloud resources. These new network architecture models advance what we can collaboratively achieve as end users and vendor communities.

What is the key to faster and larger return on invest- ment? It lies in leveraging reference models, architec- tures, and ecosystems to go from opportunity assessment to pilot project to full-scale value creation. The exciting part about these new IoT approaches is the potential to innovate on an ongoing, sustainable basis with access to deeper, richer data and more powerful, flexible data analytics for system-level insights. Let's look at three key areas to grow your IoT architecture.

Connecting Plant and Enterprise. A foundational IP network fabric that follows a validated architecture with security and scalability will enable the connection of people, processes and technology. This requires collabo- ration between IT and OT to execute. Maturity models exist to help frame the task at hand. A holistic architec- ture provides the power and flexibility to take advantage of innovations in sensing, computing, and mobile data access that are transforming value creation. Use the Converged PlantWide Ethernet (CPwE) architectures to provide the foundation for connecting the plant floor to the enterprise with defense-in-depth security, including an industrial demilitarized zone (iDMZ).

Scaling sensors with wireless mesh networks. Emerging wireless mesh solutions that connect to the IP network fabric provide the ability to cost-effectively deploy many wireless sensors across a plant floor. The inherent robust- ness, flexibility, and ease of deployment can be real game changers when calculating ROI or return

on assets. The ability to cost-effectively add more sensors on desirable variables can provide predictive diagnostics and system optimization inputs that could only be dreamed about in the past, without requiring rip-replace or risking complica- tions to existing automation systems and networks.

Computing at the edge. Analyzing data close to the machine or process is not a new concept, as evidenced by the continued success and evolution of industrial controllers. For IoT, the need to process data in indus- trial real time means that latency must be reduced in

the computing and storage strategy for data from new wireless sensors and other new connected assets such as video. The approach of sending all data to a public cloud for processing may not prove timely enough for most manufacturing environments, to say nothing of the bandwidth and storage issues as well as costs that this may generate. Thus, intelligent gateways and routers can provide computational services that enable local real- time decision-making capabilities.

Consider how you will assess and explore these new mod- els and technologies in order to innovate and compete. Mar- ket leaders have started down this path already, so you will not be alone. Great ways to start include obtaining educa- tion and training from organizations such as the Industrial IP Advantage (www.industrial-ip.org), becoming involved in organizations such as the IoT World Forum, and developing your own proof of concepts of these emerging models with ecosystem partners. Manufacturing is changing rapidly and will never be the same so the time to act is now.

Jack Tison is SVP of emerging business and former CTO at Panduit, a developer and provider of leading-edge solutions that connect, manage, and automate the physical infrastructure. Panduit is a founding member of Industrial IP Advantage (IIPA), which provides thought leadership on how manufacturing and industrial companies can build more successful businesses by deploying a secure, holis- tic digital communications fabric based on standard, unmodified use of the Internet Protocol. Discover more at www.industrial-ip.org.