THE JOURNAL

From Rockwell Automation and Our PartnerNetwork™

2016 Special Report:

Industrial Internet of Things

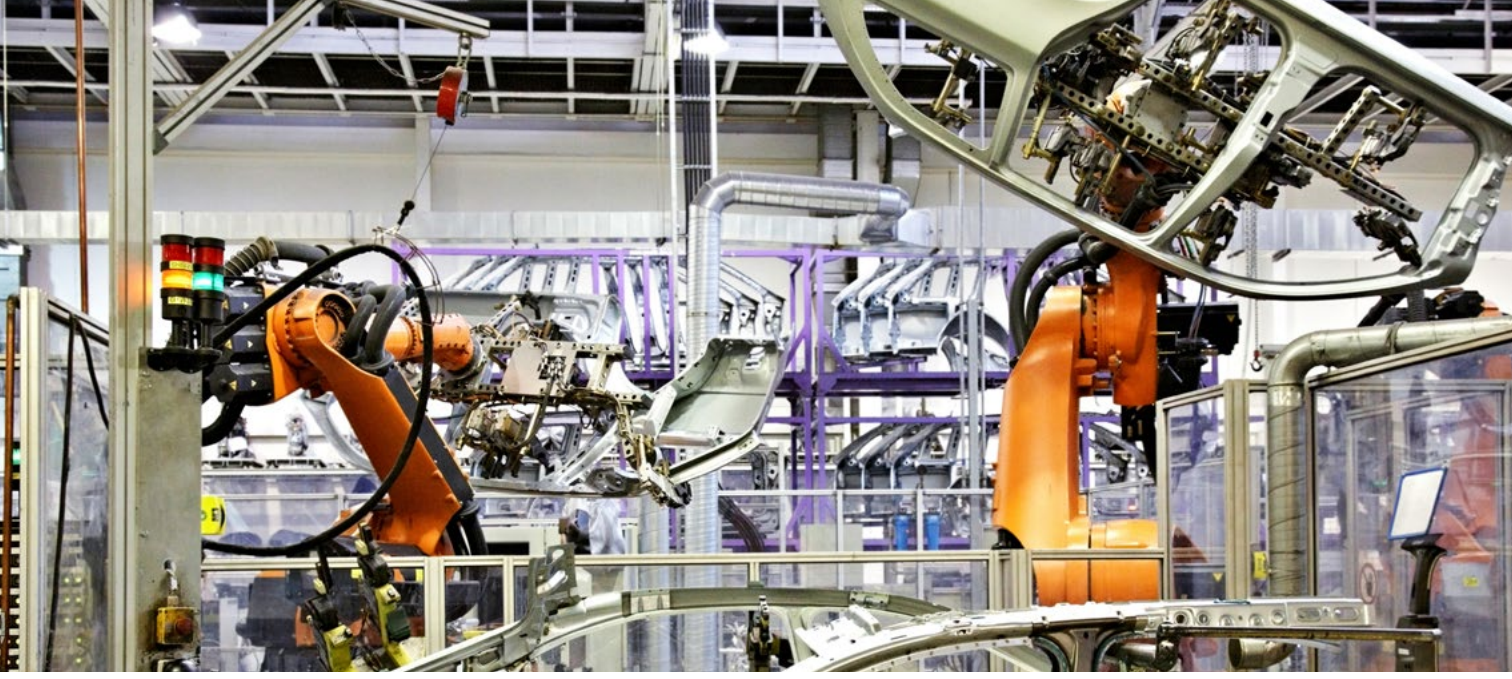
Get insight into how the digital transformation that is the Industrial Internet of Things (IIoT), also known as smart manufacturing or Industry 4.0, truly affects how you — and your competitors — are, or should be, operating. Learn why you should embrace the IIoT; what a Connected Enterprise is and how the IIoT supports it; how to plan for an information-enabled environment; advantages wireless technology, remote monitoring, the cloud and design automation provide; and much more.

Start ▶

TABLE OF CONTENTS

TABLE OF CONTENTS (CONT.)

AD INDEX



STABILIZE OPERATIONS WITH SMART MANUFACTURING

Learn how smart manufacturing helps improve employee safety, achieve environmental compliance and increase machine uptime.

By Beth Parkinson, market development director, Connected Enterprise, Rockwell Automation

>> The goal for a Connected Enterprise is a secure, productive and profitable organization guided by data-driven intelligence.

But what if a manufacturer has to make basic improvements before reaping digitally enabled benefits: predictable processes and equipment, a safer workplace, environmentally sound practices?

Here's the good news: The effort to stabilize operations also can be the first step toward a Connected Enterprise — and generate immediate return on investment.

Stability is elusive for many industrial firms: In 2014, there were more than 483,000 recordable injuries and illnesses among U.S. manufacturers, of which 126,000 required time away from work and 341 were fatal. That same year, the U.S. Environmental Protection Agency forced companies to invest more than $9.7 billion to control pollution.

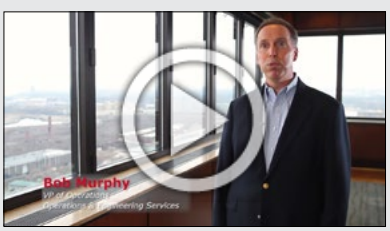
In addition, nearly one-quarter of U.S. manufacturing plants report machine availability at a pathetic 70% or worse, wasting nearly a third of their production capacity. Even worse, many plants suffer from all three of these issues.

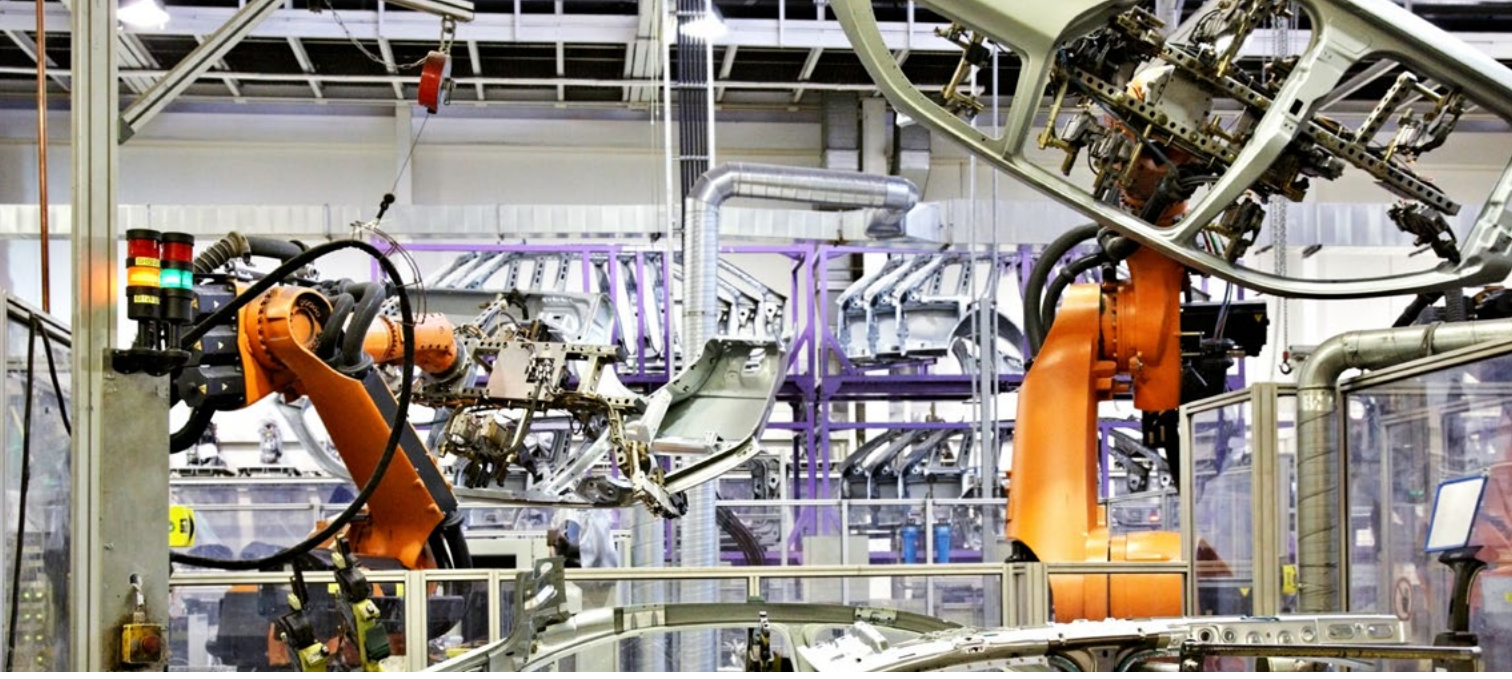
Smart manufacturing technologies won't magically fix safety, environmental and reliability problems; there's no digital elixir that can cure a toxic culture.

However, data drawn from automated equipment can connect to dashboards, illuminate key performance indicators, and lay the foundation for intelligent improvement. Integrated sensor technologies and the data they offer (vibration, temperature, energy draw, exhausts) are key to improving employee safety, achieving environmental compliance and increasing machine uptime.

>> VIDEO: The Journey Toward The Connected Enterprise

Rockwell Automation has implemented an enterprise-wide strategy allowing its integrated control and information portfolio to accelerate the business value of its Connected Enterprise. By integrating information across IT and operations technology (OT), and from the plant floor across the enterprise, the company has optimized its enterprise, plant and supply network performance and business agility. And now they're helping customers do the same. Watch the video.





Improving Employee Safety and Environmental Compliance

Manufacturers can systematically address safety problems by designing solutions that integrate safety and machine functionality.

This process begins with heightened awareness of problems, identification of new requirements; system redesign (designing hazards out mechanically, removing hazards or building in automated alerts); and implementation of safer production systems.

All these require 24/7 monitoring and periodic reviews and upgrades as technologies and standards evolve.

Increasing Machine Uptime

Connecting smarter machine assets improves control of complex production processes and helps to reduce downtime by replacing obsolete or hard-to-connect automation systems.

Intelligent sensors and controls deliver data — such as equipment status for analytics, visualization, and exception-based reporting — that help reveal downtime issues.

Pushing this information to mobile devices on the plant floor offers access to real-time production information, including machine availability and overall equipment effectiveness (OEE), and delivers diagnostics data to maintenance personnel.

As a result, management will know the location of a downtime problem, the specifics of the machine failure, and what will be required to fix it. □

Learn more about The Connected Enterprise.

>> 4 Steps to IIoT Success

The path to higher profitability is via the Industrial Internet of Things (IIoT) — and it may be easier than you think. However, new profits won't materialize without a carefully crafted plan that prepares employees and their facilities to communicate, share and use information.

Four critical steps pave the way to IIoT success:

1. **Prioritize:** Develop a modernization schedule based on three factors:

- Performance improvement opportunities (quality, reliability, speed).
- Obsolescence issues that jeopardize production.
- Security concerns, given increased risk of intrusion via the Internet.

This schedule will determine which lines, machines, controls, etc. require replacement — and when.

2. **Balance:** Coordinate the modernization schedule with the capital-expenditure budgeting process over multiple years. Carefully document estimated return on investment from IIoT upgrades — including improved production performance, enhanced asset management, and increased plant capacity into those calculations.

3. **Replace:** After a modernization plan is established, manufacturers identify specific new equipment and devices to support the IIoT. These selections should provide smarter manufacturing out of the box, while also offering long-term flexibility to adapt to new technologies and standards.

4. **Repeat:** Savvy leaders know that modernization isn't a one-time exercise. These execs review automation opportunities on an annual basis, making sure that their companies keep pace with the IIoT — and with their competitors.

HOW TO PLAN FOR AN IIOT INFORMATION-ENABLED MANUFACTURING ENVIRONMENT

A unified network fabric based on standard IP with a strong physical infrastructure supports reliable, secure networks that take advantage of the Industrial Internet of Things.

From Panduit Corp.

The Industrial Internet of Things (IIoT) is expected to connect an astonishing 50 billion devices by 2020. This is providing deeper insights into operations and new opportunities to improve quality, productivity, efficiency and security.

New challenges come with new opportunities. The demand to collect and analyze production information in real time is driving the need for manufacturers to converge their historically disparate industrial and enterprise networks into a single network architecture. A well-designed and reliable physical layer, known as the "network fabric," serves as a critical foundation and strategic business advantage for forward-thinking manufacturers who want to differentiate themselves from the competition.

We'll discuss the importance of the network fabric in today's information-enabled manufacturing environments, the steps manufacturers can take to capture its value, and a methodology for improving an existing network to a higher maturity level.

Manufacturing in the Information Age

The IIoT is reshaping the plant floor. A rapid influx of smart equipment and connected devices that can communicate on an industrial Ethernet network is allowing manufacturers to understand machine and process performance like never before.

Equally important to **what** is being connected is **how** it's being connected. Innovative technologies are helping to manage the infrastructure, deploy devices and share information in new ways. Some examples include the following.

- Cloud computing can remotely monitor — in real-time and from a centralized location — equipment that is dispersed across multiple sites, and can provide expanded processing power and storage capacity as operational needs change.
- Virtualization decouples software from hardware, providing improved application uptime, increased deployment flexibility and faster upgrades.
- Wireless technology can reduce cabling costs and allow easier sharing of data, such as to mobile devices on the plant floor.

The result of this abundance of information and seamless connectivity is faster decision-making, improved collaboration and new opportunities to improve productivity.

It also represents a major turning point in how manufacturers design, install and maintain industrial networks. The traditional approach of using separate IT and operations technology (OT) networks impedes

seamless connectivity, and is too limiting and insecure to be a valid option. Instead, manufacturers require a single unified network architecture, built on a single physical network fabric leveraging the full power of internet protocol and security defense-in-depth (DiD).

The Unified Network Fabric

The unified network fabric includes all cabling, wireless, switching, computing and storage systems, and uses standard, unmodified IP connectivity to help provide secure and open communications.

Network fabric is an industry term that describes a network topology in which devices pass data to each other through interconnecting switches. Industrial plant automation systems are evolving from point-to-point, dedicated connections to a more switch-centric design where traffic can be passed seamlessly with much greater flexibility and enhanced throughput. Instead of inflexible direct connections between devices, switches and a converged plant architecture allow data to be switched and routed securely across the plant automation system and upstream.

In addition, the network fabric can be the deciding factor in an industrial firm's success. Similar to a "fabric unraveling," poor planning and reactive decision-making can make a network become a large tangle of connections and switches that can cause plant downtime, security breaches and safety issues.

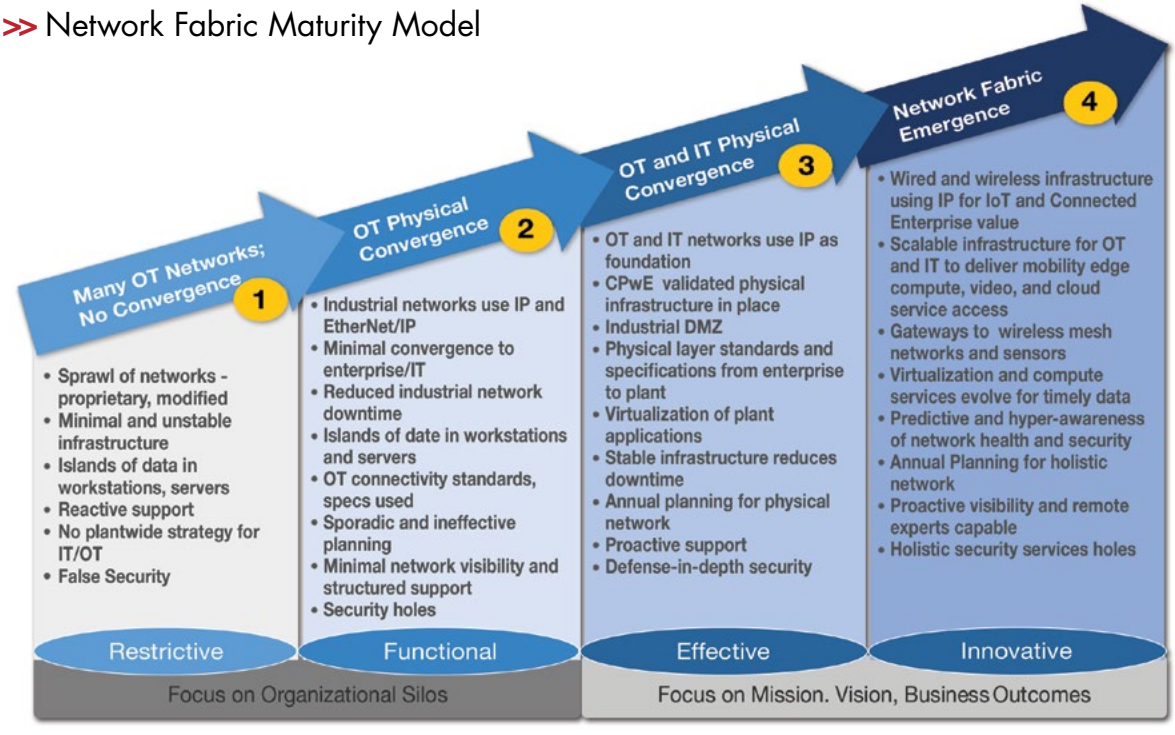
Consider these five key areas when designing and deploying a network fabric.

1. **Scalability:** Plant systems growth, new technology adoption or changing bandwidth requirements can be difficult to predict. Allowing for infrastructure growth and scalability can help avoid "rip-and-replace" upgrades, reduce reliability risks and shorten deployment times.
2. **Reliability:** Network downtime is becoming intertwined with machine downtime as more of the automated production process is brought onto the network. Base the network fabric on a robust architecture, follow industry standards and use IT/OT collaboration to help achieve high reliability across the industrial plant.
3. **Security:** A DiD security strategy is an industry-recommended best practice. It uses multiple layers of protection at the physical, network, computer, application and device levels to establish several security fronts.
4. **Ease of Deployment:** A well-planned, thoughtful approach to the network fabric helps ease design and deployment, and reduces the likelihood of start-up or operational issues. Use standards such as ISA-99 and TIA-1005 and validated architectures such as Converged Plantwide Ethernet (CPwE) to design the network fabric with greater confidence. Use structured cabling best practices and validated integrated solutions to reduce installation time and startup risks.
5. **Innovation:** The network fabric provides a platform for taking advantage of new innovations. For example, Power over Ethernet (PoE) uses a single cable to deliver power and data, which can reduce wiring complexity and lower installation and maintenance costs. A structured network of wired and wireless connectivity creates opportunities for deploying new services such as remote monitoring and edge intelligence for condition monitoring and predictive analytics.

A Maturity Model that Assesses Network Fabric

Panduit developed the Network Fabric Maturity Model

>> Network Fabric Maturity Model



The Network Fabric Maturity Model outlines the four levels of a network fabric, from multiple unmanaged plant-floor networks to a fully unified network fabric, to help industrial firms understand where they stand and provide guidance to help them progress through each level toward the goal.

(see **illustration** above) to help manufacturers map out their journey to a unified network fabric. This model outlines the four levels of a network fabric — from multiple unmanaged plant-floor networks to a fully unified network fabric.

The model can help industrial firms understand where they stand, and provides guidance to help them progress through each level toward the goal. It's about shifting industrial networks from focusing solely on the organizational silos of the plant automation system to a more holistic focus on mission, vision and overall business outcomes.

Improving From Restrictive to Functional — Level 1 to Level 2

Restrictive networks often result from disregarding OT/IT

best practices in favor of taking shortcuts. This can include using proprietary fieldbus and tiered networks to save on training and learning time, or using commercial-grade unmanaged switches to save on costs. Such shortcuts can lead to network sprawl, islands of data, and security holes.

Elevating the network infrastructure to the Functional level requires a more planned, standards-based approach, gradually migrating on a priority basis. These are three key objectives:

1. **Spend the time and resources needed to understand the plant-floor environment.** Identify physical and security risks, from the environmental conditions in which the equipment must operate to security holes such as open computer ports. Also, assess cell/area zone designs and apply best practices, such as using VLANs, managed switches and resilient topologies.
2. **Specify media, grounding and connectivity solutions that satisfy plant-floor requirements.** Follow OT standards such as TIA-1005-A for harsh environment connections. Use IT best practices, such as those outlined in ANSI/TIA 568-C and TIA-1005-A for structured cabling, which can offer higher cable density, greater network longevity, and better flexibility than point-to-point cabling.
3. **Close security holes in the physical layer.** Closing the security holes often found in Restrictive network architectures requires implementing a physical security foundation. This can include using physical and virtual segmentation to help limit user access to defined segments, and using lockable enclosures to secure plant connections.

Evolving from Effective to Innovative — Level 3 to Level 4

Converged IT/OT networks is the defining characteristic of an Innovative network architecture, as it provides new opportunities for collecting and using data across a manufacturing enterprise, and serves as the foundation for DiD security. Achieving a fully unified network fabric that can deliver on its full potential requires scaling the network foundation with adequate bandwidth and structure for the sudden increase of wired and wireless connections and compute resources at the edge.

These are three key objectives:

1. **Assess the network infrastructure's capability to support the extension of computing and mobile access capabilities with new IIoT architectures.** Designing an infrastructure to support remote-access technology, for example, can allow engineering specialists to monitor and access equipment from a centralized location, or allow IT personnel to service plant-floor computers from their desks. Mobile technology can deliver plant-floor visibility anywhere in a facility — rather than only in a fixed location — for faster responses and decision-making.
2. **Collaborate with IT/OT for network visibility documentation and diagnostic tools for sustainable value throughout the network life cycle.** Use of tools designed for network discovery and documentation of plant industrial Ethernet networks fills a gap for a comprehensive view of enterprise-to-plant convergence down to the device level. Likewise, providing plant-floor and operations real-time diagnostics of network alerts speed troubleshooting and improves plant uptime.
3. **Develop test beds and pilots for IIoT architectures that leverage cloud and fog computing for a broader network fabric that includes gateways and wireless mesh networks.** For instance,

the cloud might not be an option for manufacturers when real-time processing of manufacturing data is required. Instead, fog computing can use intelligent gateways and integrated services routers to provide local, real-time data processing closer to the machine. Additionally, wireless mesh solutions that connect to the network fabric can provide opportunities to deploy wireless sensors cost-effectively.

The journey to achieving a fully unified Level 4 network fabric begins with understanding your network's current maturity level. Check off the characteristics for each Network Fabric Maturity Model level in the illustration on page 8, or take our online survey at www.panduit.com/mapyourjourney to determine where your network resides on the model.

Fulfilling the Promise

IHS Technology predicts the industrial automation sector will account for nearly three-fourths of all connected devices by 2025. The potential for value generated by all these industrial connections will drive new business models, transforming productivity dramatically. The future competitiveness of almost all manufacturing companies hinges on how rapidly they can embrace convergence and IP technologies.

A unified network fabric based on standard IP with a strong physical infrastructure will serve as the foundation of tomorrow's information and connectivity needs, and will support converging the networks to gain robustness, visibility and reliability. Using maturity models can help guide both the OT staff and IT staff to accelerate progress to more effective and innovative networks that deliver on the promise of the IIoT. □

>> IIoT and Network Training Opportunities

Trained system integrator and installation partners as well as vendor-provided services from Rockwell Automaton® Network Security Services can help you bridge the IT and OT gap to support the IIoT.

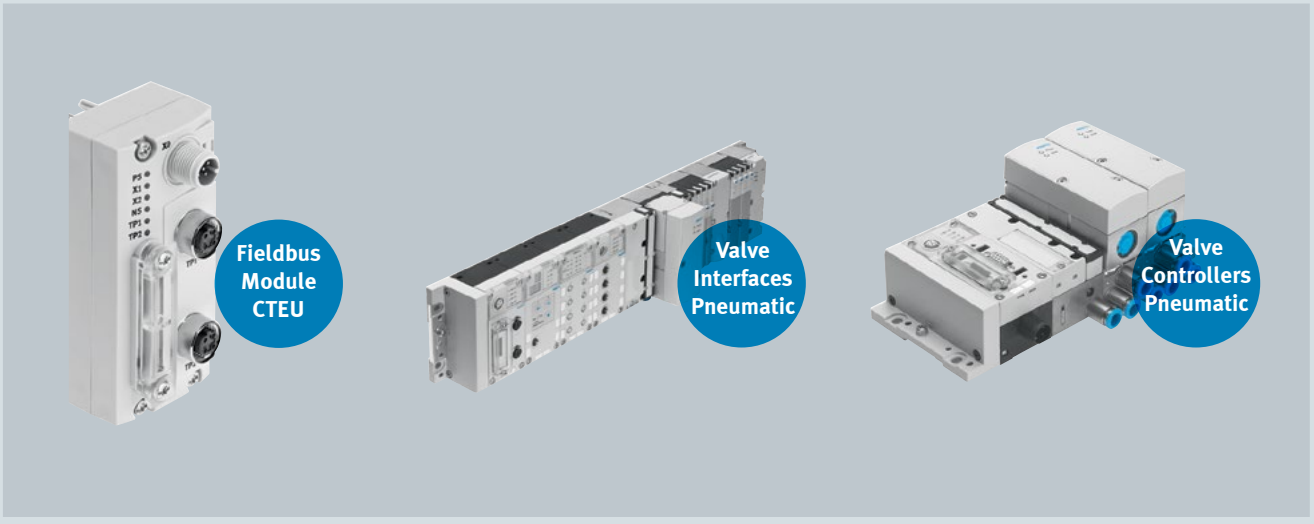
In addition, through the Industrial IP Advantage online, you can learn how to implement and manage networked industrial control systems.

Based in Tinley Park, Illinois, Panduit is a Rockwell Automation Strategic Alliance Partner. The company provides solutions that help users optimize the physical infrastructure through simplification, increased agility and operational efficiency. Panduit industrial building block solutions, tools and services are designed to simplify network deployment for better equipment optimization and broader risk management.

FESTO

We drive automation for your success.
We are your partner to inspire you.
We shape the future together.

→ WE ARE THE ENGINEERS
OF PRODUCTIVITY.



Rockwell Automation

Festo has been a recognized partner of Rockwell Automation for nearly 2 decades, starting with the Pyramid Solutions Program in the early 90's, to the Encompass Product Partner Program of today. We have a long history of integrating control technology into valve manifolds, with many "firsts" to our credit.

For more information:
Call: 1-800-Go-Festo
1-800-463-3786
www.festo.us/rockwell

Festo is a leading global manufacturer of pneumatic and electromechanical systems, components, and controls for process control and factory automation solutions.

5 CRITICAL LESSONS FOR CONNECTING THE ENTERPRISE

Benefit from lessons learned when Rockwell Automation implemented The Connected Enterprise into its own operations.

By Beth Parkinson, market development director, Connected Enterprise, Rockwell Automation

Rockwell Automation has *lived* The Connected Enterprise Execution Model. We developed and validated this approach for integrating IT and operations technology (OT). In doing so, we reached new levels of collaboration across the company and with suppliers and customers — linking processes and facilities in new ways, and reaping unexpected benefits. Most importantly, we learned critical lessons that we can share with you here.

1. Assessment

The assessment stage of The Connected Enterprise Execution Model is really about change management. Are people willing to innovate the processes that have led them to success? Can they envision what it will mean to have access to accurate, real-time information?

Even we were surprised by the challenges of connecting industrial automation and OT with legacy information technologies. The process helped open our eyes to just how many workarounds our legacy IT required (lots).

The assessment stage showed what we needed to change, where our network required upgrades, and how we would need to change practices and workflows, and identified potential risks. We then relied on established change-management procedures to implement a strategy that could securely integrate our people, processes and technologies. Still, every change encounters resistance — so be prepared.

2. Secure and Upgraded Network and Controls

Rockwell Automation is a global business with operations on every continent, so we expected to upgrade some controls, sensors and infrastructures, and you should too. You might be surprised at what your assessment uncovers, and that's a good thing — you need to find a problem before you can fix a problem.

We also quickly learned that we couldn't change everything at once; we had to prioritize upgrades by balancing short-term risks and long-term objectives. This approach allows you to fix pressing issues and still consider facility expansions and new technologies — strategically evolving a flexible IT/OT backbone that can deliver adaptable connectivity well into the future.

Another lesson we learned at this stage was how important it is to define the roles and authority of IT and OT engineers in a Connected Enterprise.

Even we were surprised by the challenges of connecting industrial automation and operations technology with legacy information technologies.

3. Defined and Organized Working Data Capital (WDC)

Get ready to be inundated with a wave of data. We like to refer to this stage as a "famine-to-feast information evolution." We went from having acceptable, usable OT data to an overabundance.

We developed processes that efficiently filter insights from the "nice-to-know" data that likely would not impact day-to-day operations. We also learned that new information requires new workflows, schedules and responsibilities.

4. Analytics

During this stage, we found many ways to use our new IT/OT network capabilities. We also learned that we had to stop ourselves from running too many analyses. We ultimately selected persistent problems based on key performance indicators (KPIs) by location, and then connected the information to authorized recipients with authority to act.

We also set up standard action protocols for our workforce that this new information would set in motion, minimizing the need for executive oversight and maximizing response.

Despite our best efforts, though, we still encountered "data disbelief" — people who insisted the data couldn't possibly be correct. We learned to convince naysayers by linking information, process capabilities and KPIs to show, "This process is driving this outcome, and here's the data to prove it." Most importantly, the information highlighted lead metrics that could prevent negative lag measures from occurring.

5. Collaboration

The biggest lesson we learned in the final stage was that our work — and investments — in the first four stages were more than worth it. Each step more than paid for itself. During this fifth stage, we used our experiences to help and encourage customers and suppliers in moving forward with their own Connected Enterprises.

Collaboration allows our supply chain to collectively see and react to emerging market conditions, driving operational excellence and cost savings across the board. Our supply-chain partners are mostly supportive of our efforts. Here the lesson is patience — every collaborative endeavor takes time, especially one of this magnitude and one in which you're asking for and sharing proprietary information.

The other big lesson in this stage is that everyone in the IT/OT data stream — whether business units or supply-chain partners — must adhere to strict security standards. Incorporating a defense-in-depth (DiD) approach, which adds both physical and electronic layers of enhanced security to the IT/OT infrastructure, improves the likelihood that any threats or unauthorized accesses will be detected and prevented.

Establishing clear scope for these protections will give others the confidence to join you, use domain specialists across the supply chain, and share best practices. □

Learn more about The Connected Enterprise.

WebPort

COMPLETE REMOTE ACCESS

CELEBRATING OVER 15 YEARS OF REMOTE ACCESS INNOVATION

WebPort is a complete remote access solution focused on end-to-end connectivity, data access, and event notifications, all while being simple and easy-to-use.

- Simple Setup
- Easy-to-Use
- Global Turnkey VPN
- Remote Programming
- SMS Notifications
- Reporting & Alarming
- Data Aggregation
- And much more!

"Remote access has been available in one form or another since I've been working in this industry, but it has never been as easy to integrate as it is with WebPort"
Kontrol Automation Inc.

"I have been using the WebPort from Spectrum Controls for about a year now. Simple to set up and use. No complaints." - **PLCTalk.net**

"When price, performance, and functionality are our concerns the WebPort is our go to device for communications in industrial applications."
International Chemical Provider

SPECTRUM CONTROLS

+1 (425) 746-9481
www.spectrumcontrols.com
spectrum@spectrumcontrols.com

Rockwell Automation Encompass Product Partner Global

WHY YOU SHOULD EMBRACE THE IIOT

More manufacturers are benefiting from the Industrial Internet of Things, but once on board, challenges can arise. Here are some tips for converging IT/OT and benefiting from analytics.

From Stratus Technologies

The Industrial Internet of Things (IIoT) is attracting more manufacturers' attention, especially as the Internet of Things (IoT) takes hold in consumer and business markets. Many manufacturers are getting excited about the opportunities presented by applying advanced analytics to information generated by plant sensors and business systems.

However, if you're still on the fence, we'll examine why the IIoT can improve operations, and once you're on board, how to adopt the IIoT into your operations and bring IT and operations technology (OT) together to support your IIoT initiatives.

Research Underlines IIoT Progress

A recent LNS Research and MESA International report, "Manufacturing Metrics In An IoT World: Measuring the Progress of the Industrial Internet of Things," validates the growth of the IIoT in manufacturing. Some key findings from the report are as follows.

Understanding of the IoT has increased. In a 2015 report, LNS and MESA found that 44% of those surveyed didn't understand the IoT. In 2016, that category plummeted to 19%. Also, more than 50% of respondents reported their companies were planning IoT initiatives in the next 12 months.

Manufacturing data is moving beyond the plant. More manufacturers are looking at predictive modeling, plant analytics and manufacturing intelligence. This indicates they're taking a more integrated view of manufacturing operations rather than focusing on point solutions.

Also, while most manufacturing operations management (MOM) and manufacturing execution system (MES) software is still deployed on-premises, movement toward cloud-based solutions is starting to take hold.

Manufacturers still care most about financial metrics. Nearly half of respondents ranked financial metrics as their top concern. The survey also reported that key financial metrics — manufacturing cost per unit, revenue per employee and net profit margin — are improving.

What's interesting is these gains largely come from quality and operational efficiency initiatives. The question is, how much more could be achieved with big data analytics?

Adoption of analytics is still limited. Surprisingly, only 14% of survey respondents have a manufacturing analytics program. The vast majority of these companies use analytics internally for process improvements. Few manufacturers are using advanced analytics that incorporate unstructured data such as climate data and images.

Manufacturers need to dive deeper into big data analytics to adopt capabilities such as real-time machine learning and predictive maintenance. This direction will lead to more operating efficiency — and ultimately drive greater financial improvements.

For manufacturers ready to further explore IIoT, the report recommends the following:

1. If you don't understand the IIoT, investigate its potential impact on your operations. Form a cross-functional team and plan some IIoT trials.
2. Explore analytics that go beyond shop-floor data. Vendors can recommend solutions that provide uninterrupted access to analytics and help you understand what private and public cloud options exist.
3. Once you've taken these steps, conduct a full-blown pilot with more complex analytics involving plant and business data.

Supporting Mission-Critical Applications

There are many components to consider beyond machine-integrated sensors. Networking and communications, data collection and analytics, automated controls and decision support are the connective tissue of the IIoT.

An important part of this is the hardware and software that helps protect this connective tissue. The benefits provided by an always-on infrastructure in an IIoT environment go beyond preventing unplanned downtime.

For starters, the evolution toward the IIoT helps deploy industrial automation technologies into new industries and places. For instance, many process industries, endpoints and stations, such as an oil pipeline, typically need to be manned. New technologies allow more of these remote sites to be monitored remotely and completely human free.

However, this remote visibility comes with a price. If the system that provides remote monitoring goes down, nobody knows what is happening. In the natural gas industry, this is called a "blind moment," and it's a big deal. This situation isn't limited to oil and gas pipelines. As factories in other industries get larger and more automated, the goal is to improve productivity with fewer employees exposed to potentially hazardous environments. Always-on visibility can help meet that goal.

In addition, compliance comes into play. While data generated by the IIoT is critical for production

Only 14% of survey respondents have a manufacturing analytics program.

efficiency and productivity, in some industries, this data proliferation will require oversight and reporting. A good example is the food and beverage industry. If you're subject to regulations, you can't afford to lose data, because it could result in expensive recalls, audits or even fines.

Lastly, the transition to the IIoT will come with implementation costs. Many organizations are taking their first steps toward the IIoT by deploying virtualization to reduce costs. However, the combination of the always-on requirements with virtualization in a non-data center environment can add costs and complexity.

Fault tolerance, virtualization, monitoring and downtime prevention built into a single solution can give you a smaller technology footprint that doesn't require a platoon of people necessary for many of the clustered environments.

Bridging the IIoT Gap

As companies look for ways to become more efficient and agile, the IIoT offers attractive opportunities. Harnessing sensor data, machine-to-machine (M2M) communication and big data analytics enables manufacturers to take automation and efficiency to new heights, while creating the foundation for new business models.

However, to realize the potential of the IIoT, companies must first bridge a yawning gap: the technological and cultural divide that often separates IT and OT organizations.

Why the divide? In most industrial organizations, including oil and gas producers, IT and OT traditionally have different priorities. For OT, uptime of production automation systems is paramount. Reducing risk is the top priority, which is why automation systems often are in service for years, if not decades.

For IT, innovation is the top priority, often leading to continual change and upgrading. This difference in priorities helps explain why OT often insists on keeping automation systems isolated from IT.

The IIoT changes the status quo, creating a new imperative to share data from machine sensors and automation systems managed by OT — including SCADA systems — with enterprise resource planning (ERP) systems and analytics platforms managed by IT. How can industrial firms such as oil and gas companies bridge the gap between these two worlds, while verifying the competing priorities of OT and IT are met?

Three approaches can help:

1. One approach employed by some energy companies is to merge the two, integrating OT within the IT group. On the surface, this seems like the most straightforward approach, essentially forcing OT and IT to work in coordination. In practice, however, the cultural differences can remain.

For example, IT might try to impose its standards-based approach on an OT team used to systems specialized for particular production tasks. Unless IT has a clear understanding of the requirements of these automation systems, the result can be a lack of coordination that decreases system stability. For this approach to work, OT must have a voice in the combined organization.

2. Another approach is to create a technology team free from these traditional distinctions, responsible for all OT and IT functions. This approach is feasible in an entirely new organization or for a large company spinning off a new satellite organization.

However, for most larger companies, such as complex oil and gas producers with established technology groups and lots of legacy infrastructure, it may not be a workable alternative.

With a foot in both worlds, industrial technologists play a key role in helping meet priorities of both OT and IT.

3. The third approach uses a new breed of "industrial technologists" who have a combined IT/OT perspective. They understand the need for stable, highly available automation systems, but also understand the enterprise system integration and analytics required to make the IIoT a reality. With a foot in both worlds, these industrial technologists play a key role in helping meet the priorities of both OT and IT.

Showing OT the Value

Overcoming the cultural divide between OT and IT will likely be a gradual process for many organizations. A key step in facilitating that process is showing the OT team the value of the IIoT and "opening the door" to their automation systems and data.

For example, gas-gathering operations could lay fiber or use wireless in all of the remote facilities to relay sensor data to a centralized analytics system. This would allow them to access accurate imbalance sheet data for all production sources in near real time, without tying up valuable staff time on manual processes.

Predictive maintenance is another example. Sensor data for a range of operational parameters can be collected for individual equipment components and sent to analytics engines or machine learning systems to detect anomalies — such as vibration patterns on compression turbines or temperature excursions on a motor — before a failure occurs.

This can reduce unplanned downtime, the bane of OT, while also helping identify the optimum maintenance or replacement intervals, minimizing costly planned downtime and capital expense.

Reducing the Risk of Change

A critical success factor when merging OT and IT functions is effectively managing risk. OT must be assured that SCADA systems and data will maintain the highest levels of availability. That means building in fault tolerance for all mission-critical systems linked to production.

Availability is especially critical given the cost pressures the industry is under. With technology staffs cut to the minimum, it's essential that automation systems at remote locations — such as compression stations, well locations and storage facilities — stay up and running. If someone has to travel to the location to deal with an outage, production could be impacted for days. Moreover, building in availability helps avoid the inevitable finger-pointing between OT and IT if an outage were to occur in a converged IIoT infrastructure.

The benefits of the IIoT are too attractive not to take advantage of them. Bringing OT and IT together in a way that effectively manages risk is the key to unlocking the tremendous potential of the intelligent, automated enterprise. □

Stratus Technologies, based in Maynard, Massachusetts, is a participating Encompass™ Product Partner in the Rockwell Automation PartnerNetwork™. Stratus provides high availability and fault tolerant solutions to keep applications up and running.

IMPROVE PLANT-FLOOR OPERATIONS WITH IIOT

A roadmap that focuses on production goals such as increasing productivity, lowering costs, boosting security, and improving performance can help pave the way to smarter *and* better manufacturing.

By Beth Parkinson, market development director, Connected Enterprise, Rockwell Automation

Smart manufacturing doesn't mean much if it doesn't result in *better* manufacturing.

There's a fog of hype about potential gains available via the Industrial Internet of Things (IIoT), smart devices, and embedded intelligence. Yet, if upgraded production can't improve operations, what's the point?

A recent study on the IIoT finds that the top three objectives for incorporating smart devices and embedded intelligence into plants and processes are improved quality, costs and speed.

These are all possible, but require a plan — a roadmap — that identifies why, where, what and how a company should automate. Without a strategy, smarter equipment will simply capture and share more data — overwhelming managers and perhaps even damaging operational performance.

So how can you get started with modernization that embeds intelligence and delivers a return on investment? Focus on production goals:

Increase productivity: Identify production lines and cells where smarter equipment will support *jidoka* (automation with human intelligence), reducing the number of operators needed for tasks — such as loading and unloading — so that they can be redeployed elsewhere. Look, too, for lines and cells bedeviled by reliability issues, where self-monitoring equipment could help prevent downtime.

Lower costs: Most companies struggle to control manufacturing costs; in fact, just 35% have been able to

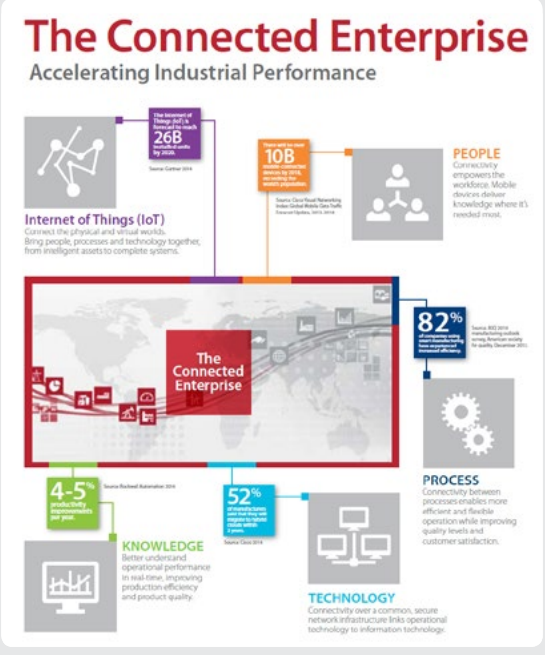
Bringing the IIoT into plants requires a roadmap that identifies why, where, what and how a company should automate.

>> The Connected Enterprise: Accelerating Industrial Performance

The most competitive manufacturing and industrial operation professionals are looking for seamless and secure working information capital — not simply more data — to drive better decision making, expose process inefficiencies, facilitate best-practice collaboration, and uncover new business opportunities.

The Connected Enterprise can deliver value in increased productivity and global competitiveness. Through the convergence of IT with operational technologies (OT), organizations can access and capitalize on operational, business and transactional data for improved enterprise, plant and supply chain performance. The Connected Enterprise helps manufacturers benefit from faster time to market, lower total cost of ownership, improved asset utilization and enterprise risk management.

CLICK TO ENLARGE



reduce per-unit manufacturing costs over the last three years. Explore how smart machines can lower energy costs, minimize scrap and rework (reduced labor and material costs), and help reduce cycle times (lower labor hours/overtime).

Secure assets and networks: Cyber threats don't need to enter your organization through corporate headquarters. Increasingly plant-floor machines are a target for cyber threats — and offer hackers back-door access to corporate IT networks. Conduct a security audit of current equipment to identify vulnerabilities that could threaten financial documents, proprietary data and customer records.

Improve manufacturing performance: Where on the plant floor can you identify repetitive quality problems? Smarter machines can help prevent quality problems or catch mistakes before they reach your customers. Even more important: Where on the plant floor do you have safety issues? Intelligent equipment doesn't just boost productivity — it saves lives. □

Learn more about The Connected Enterprise.

HOW REMOTE MONITORING CAN SLASH COSTS

Secure remote access combined with the Industrial Internet of Things helps reduce downtime, minimizes on-site visits, and provides data for more proactive and predictive maintenance.

By Micah Grotte, Spectrum Controls

Unscheduled system downtime results in loss of productivity and profits. Resolving it might require an on-site engineering visit. However, with travel and labor costs continuously rising, a better way is needed to reduce the immense costs of downtime while still providing quality customer service.

The Industrial Internet of Things (IIoT) has paved the way for a new era in accessibility solutions. Secure remote connectivity to your automation system minimizes the need for on-site evaluation and provides data for measuring diagnostics and key performance indicators (KPIs).

With this new wave of solutions, machine builders and system integrators are pushed to provide end users with a higher level of satisfaction. Increased pressures from globalized competition, heightened customer demands, limited qualified resources, and pricing constraints are driving the IIoT connectivity market toward maximizing profitability. Customers are continually evaluating machine uptime, reliability, efficiency, total cost of ownership and service offerings to find their perfect fit.

"Today, business demands (such as increased and faster online access to real-time data, using less resources) has led to the rapid deployment of modern networking technologies, which has accelerated the interconnectivity of these once isolated systems," says the U.S. Department of Homeland Security in their article Configuring and Managing Remote Access of Industrial Control Systems.

"This new connectivity has empowered asset owners to maximize business operations and reduce costs associated with equipment monitoring, upgrading and servicing, whilst creating a new security paradigm for protecting control systems from cyber incident."

In our experience, applications for secure remote access serve a number of industries. For example, remote access allows users in the power generation industry to analyze their data to establish regular maintenance schedules and help prevent excess wear and tear on their machines. In the chemical sector, end users can deploy solutions that monitor consumables to enhance their on-time replacement deliveries. It also helps packaging users compile their machine uptime and downtime for better warranty agreements.

Across all industries, manufacturers are responding to new business demands by deploying remote access solutions to maximize business operations and reduce costs tied to equipment monitoring.

Own Your Data

The key to developing a proactive service model is owning your data. IIoT users own their data by:

- Gaining access to their critical systems.
- Protecting their solution from external and internal threats.
- Analyzing their data for meaningful trends.
- Sharing their data to communicate performance and reliability.

Gaining Access

Before developing an appropriate service model, customers must establish their primary requirements for accessing their data. This process typically balances both technical and operational needs.

On the technical side, end users look for remote access that allows them to both monitor and maintain their machines. Business requirements demand remote diagnostics, performance measuring, custom reporting, uptime improvements, and a reduction in both travel and labor expenses to reduce the total cost of ownership. Harmonizing technical and operational needs is far from a short putt. However, convergence between these two organizations is necessary to realize the full benefits the IIoT can provide.

More and more, organizations are adopting remote access solutions that combine on-machine industrial hardware with a hosted VPN cloud service. This type of secure turnkey framework helps customers simplify their deployments while minimizing total cost of setup. Monitoring KPIs allows users to manage system performance and react to changes that may be indicative of degraded system operation.

Accessing system data over a secure VPN tunnel allows users to overcome IT security concerns while providing the necessary business insights to satisfy operations technology (OT) expectations. With the right solution, secure remote access can unify the ambitions of both IT and OT to discern crucial business insights.

Protecting Your Solution

While remote access is an excellent first step to converging IT with OT, it's useless without a robust security strategy to protect the data from external and internal threats. Fortunately, OEMs and system integrators are paying attention to end-user security demands.

IIoT providers have standardized on security strategy with multiple layers of protection. Aligning with Rockwell Automation and its Strategic Alliance Partner Cisco, we have adopted a defense-in-depth (DiD) security strategy, which allows engineers to build layers of security into their machinery and the end user's facility.

As explained in the United States Homeland Security article, Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, a DiD security strategy layers technical and nontechnical protection to detect and thwart both internal and external unauthorized activities. While the specific layers of protection might differ from solution to solution, the philosophy that users must protect the vulnerabilities of one security technology with the strengths of another remains the same.

By deploying a layered defense, the protection of all the layers guard against the unseen vulnerabilities of any single security approach. This strategy helps OEMs and end users reduce their susceptibility to any accidental or unauthorized activities that impact the safety, integrity or confidentiality of their systems.

An effective approach is a six-tier DiD security strategy in which:

- **Data encryption** is a must for modern solutions and guards the privacy of user data.
- **Network security** combines firewalls, intrusion detection/prevention systems, and port security to protect the network.
- **Application security** allows an administrator to authorize users by role, limiting access to exactly what the user requires and white/black lists, which protects data.
- **Device hardening** requires administrators and engineers to update firmware, patches, and antivirus software on any network appliance.
- **Physical security** places physical limits on access to devices, cabling, control panels, control rooms, and any other area of high-security importance.
- **Best practices** combine industry knowledge with modern solutions to help monitor, identify, isolate and counter any significant security threats.

Like oil and water, IT and automation traditionally have refused to mix. However, using this contemporary security strategy is helping many companies realize the benefits of adopting The Connected Enterprise based on secure IIoT technologies.

Analyze the Data

Once engineers have established a secure strategy to access their machine data, they can measure KPIs to monitor trends and overall health of the systems. Through data analysis, machine builders can improve customer support, avoid communication and language issues, set up remote diagnostics and proactively prepare for any maintenance intervention.

Perhaps most importantly, key insights can help reduce travel expenses by avoiding on-site troubleshooting during an emergency, routine or preventative maintenance cycle.

Share the Data

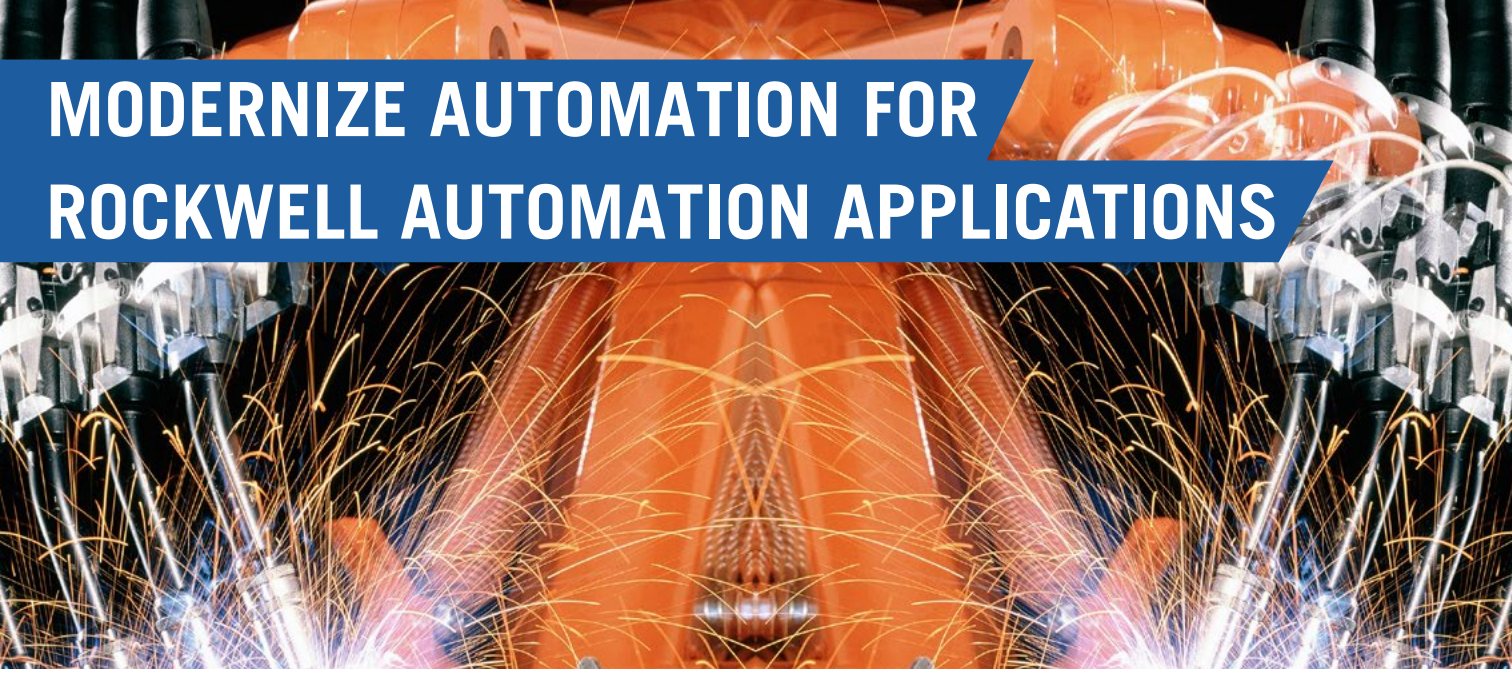
Analytics can transform from insights to revenue streams when engineers develop predictive monitoring and maintenance agreements to improve the cycle times of their systems.

Secure remote access also allows your company to create extended warranty agreements as additional revenue opportunities. The Connected Enterprise and related IIoT technologies make these types of response agreements that provide 24/7/365 service for issues related to reducing downtime and increasing productivity possible. As a secondary benefit, proactive service models help machine builders benchmark machine performance to realize possible improvements to optimize their machine engineering.

The combination of the IIoT, The Connected Enterprise, cloud computing and industrial Ethernet have allowed access to machines located throughout the world. These solutions help provide secure remote connections for diagnostics and troubleshooting. More importantly, they allow users to securely aggregate critical data, then analyze and share KPIs to generate indispensable business insights.

The IIoT and The Connected Enterprise technology helps systems integrators and machine builders to make informed decisions and drive proactive service models. □

Bellevue, Washington-based Spectrum Controls is a participating Encompass™ Product Partner in the Rockwell Automation PartnerNetwork™. The company provides hardware and related software products for the industrial controls marketplace, including I/O modules, LED displays and WebPort® remote access devices.



MODERNIZE AUTOMATION FOR ROCKWELL AUTOMATION APPLICATIONS

What Does Stratus Technologies do for Rockwell Automation Customers?

For over 30 years Stratus has been providing infrastructure based solutions that keep applications running continuously in manufacturing environments. As a Global Encompass partner, Stratus delivers continuous availability for Rockwell Automation customers running FactoryTalk® View SE, FactoryTalk® Historian, FactoryTalk® ProductionCentre® and other plant applications.

Stratus provides Rockwell Automation customers:

- **Fault-Tolerant Virtualization Platforms**
- **Redundant Always-On Solutions**
- **Plug-and-Play Simplicity**
- **Lowest Cost**

Rockwell Automation
Encompass™
Product Partner
Global

Stratus' always-on solutions solve our customers' biggest needs

Flexible

Our solutions support a range of environments – physical, virtual or cloud – on plant floors or in datacenters.

Easy

Our products are easy to deploy and manage, and require no modifications to MES, SCADA, Historian or other plant applications.

Trusted

SMBs and Global Manufacturing companies alike rely on Stratus to keep them up and running.

Stratus

www.stratus.com/

5 BEST WAYS TO SET UP WIRELESS IN YOUR PLANT

Implementing Wi-Fi by using standards-aligned security best practices and the right infrastructure helps you take advantage of plant-floor data and the Industrial Internet of Things.

By Divya Venkataraman, global product manager, Rockwell Automation

By using wireless technology, you literally can cut the cord and see your operations in new, transformative ways. In an age of the Industrial Internet of Things (IIoT), the need to collect real-time data from your operations is more important than ever.

You want to be sure you're making informed decisions so productivity can be maximized to meet the needs of automation environments. With all of the advances in equipment and manufacturing, there's no reason data should remain untapped. Here are the top five ways to bring wireless technology onto your plant floor and take advantage of data collection and analysis opportunities for the IIoT.

1. Go Wireless

Wireless technology can help minimize costs, and who doesn't like to save a little money? On the front end, you'll experience lower installation costs because of reduced hardware and cabling, meaning less maintenance and more options for further investing in a future-ready plant infrastructure.

When making these types of long-term decisions for your plantwide network, think about the overall cost savings you'll experience when you maximize your productivity with enhanced connectivity and equipment mobility.

2. Use Recommended Hardware

The right hardware for a wireless local area network (LAN) is necessary to attain your goals of achieving secure and reliable communications. Using wireless access point (WAP) and workgroup bridge (WGB) hardware that conforms to widely adopted IEEE 802.11 a/b/g/n standards with 2.4-GHz and 5-GHz spectrum availability will help you meet a range of operational needs.

WAPs serve as a router to bring wireless clients into a wired network securely, and a WGB can connect up to 19 wired IP address clients securely to a wireless network.

3. Achieve Real-Time Control

Achieve closed loop, real-time control in critical applications, where reliability is key. Do more than just remote monitoring, troubleshooting and collecting data from your operations with IEEE 802.11 technology, better known as Wi-Fi.

Wireless access points serve as a router to bring wireless clients into a wired network securely.

By using machine and equipment mobility, you can meet the unique demands of real-time control with minimal latency and jitter to achieve the desired, uninterrupted performance your application needs.

Enhanced machine mobility allows the possibility of increased productivity, maximized connectivity and innovative new designs.

4. Establish Single Network Infrastructure

Want to converge your existing Ethernet-based network architectures to create a single, plant-to-enterprise network infrastructure using an Ethernet-based industrial protocol, such as Ethernet/IP™?

With IEEE 802.11, you can use the same technology for both real-time control and on-demand information to gather metrics and view analytics on a mobile device for more informed decision making. At the same time, you can experience wireless plant-to-enterprise convergence contributing to higher productivity and less downtime.

5. Use Industrial Security Best Practices

Let's talk security. We understand the importance of minimizing the risks associated with wireless communications. We also know device authentication and data encryption methods that align with the IEEE 802.11 standard are essential.

Use the Wi-Fi Protected Access 2 (WPA2) security standard with Advanced Encryption Standard (AES)-level encryption in industrial WLAN applications and get the most advanced security available for industrial settings without affecting application performance.

Is an autonomous or a unified architecture better for you? If you're looking for a network that's independently configured and managed through stand-alone wireless access points to implement all WLAN functions, an autonomous architecture could be your answer. This type of architecture is ideal for small-scale deployments in which more granular control of Quality of Service (QoS) is needed to help control systems network traffic.

Does the autonomous network sound like it will apply to your needs? If not, a unified architecture might be a better fit because it's well-suited for large-scale, plantwide deployments that require a wide range of clients and applications.

In a unified network, functionality is split between Light-Weight Access Points (LWAP) and Wireless LAN Controllers (WLC) for centralized control and visibility and the ability to quickly recognize network threats.

On Your Way

By understanding the considerations for wireless technology, you're on your way to implementing Wi-Fi technology in your industrial automation environment and preparing your network infrastructure for the ever-evolving demands of industrial manufacturing processes.

These recommendations give you the ability to start building a Connected Enterprise when you follow standards-aligned security best practices. □

Learn about Rockwell Automation Stratix™ Wireless Routers.

THE IO-LINK STANDARD'S ROLE IN THE IIOT

The interoperability standard supports communication between sensors and actuators and automation and enterprise systems to empower the Industrial Internet of Things.

By Nuzha Yakoob, senior product manager, Electric Automation, Festo Corp.

One key to making the Industrial Internet of Things (IIoT) and smart factories a reality is two-way communication between low-level sensors and actuators and higher-level controllers, automation systems and manufacturing execution systems (MESs).

The IO-Link standard does just that.

What is IO-Link?

IO-Link is the first I/O technology to be adopted as an international standard (IEC 61131-9) and lets devices from various manufacturers communicate with each other. However, it's important to note that IO-Link is not a fieldbus. It allows point-to-point communication between field devices and the automation system.

Traditionally, integrating a fieldbus interface all the way down to the lowest field level device was expensive. IO-Link is a straightforward and economical system that transmits binary, analogue, parameterization and diagnostic data via simple, unshielded 3-wire cable.

IO-Link-enabled devices not only transmit machine data to factory management systems, they let a control system download parameter data to the device which, in turn, can send status information back to the controller. Thus, IO-Link devices facilitate machine commissioning and start-up, make adjustments while a machine is running, and provide monitoring and diagnostic capabilities. The end result is increased machine and process flexibility, better overall productivity and less downtime.

A basic IO-Link system consists of a master; devices like sensors, valves, motor starters and RFID readers; cables up to 20-m long (typically with factory-assembled M12 connectors); and configuration software tools.

The IO-Link master can have several channels, one for each connected device, and it can be integrated into a programmable logic controller (PLC) or controller and serve as a gateway to fieldbuses such as DeviceNet™, PROFINET® and EtherNet/IP™. As a result, it serves as the connection between individual devices and the plant automation system.

Advantages of IO-Link include:

- **Automatic detection and parameterization of the IO-Link device.** During initial setup, a device's operating parameters are stored in the master. Once connected, the master recognizes the device and enables automatic start-up. If a device such as a sensor fails, it can be swapped out and parameterization

IO-Link serves as the connection between individual devices and the plant automation system.

data stored in the master automatically downloads to the replacement device.

- **Device monitoring and diagnostics.** IO-Link permits equipment components and systems to be monitored and proactively managed. Diagnostic information supplied by IO-Link devices lets the control system track data and trends, facilitating preventive maintenance and improving machine uptime. In the event of a fault, it pinpoints the problem, helping to make troubleshooting easier. Maintenance technicians don't need special expertise.
- **Changes on the fly.** Parameters can be adjusted quickly for installed devices while the machine is running. For example, consider a pressure regulator controlling the force a pneumatic cylinder applies to a product. If the next product requires a different force, users can reconfigure the regulator's pressure set points on the fly and keep production running. That differs from the conventional, time-consuming process of having a machine operator manually reset pushbuttons or adjustment screws.

The controller's ability to change device settings quickly and remotely is a key attribute of the IIoT. It minimizes the transition time from one type of operation to another and gives machines greater flexibility to handle a wider range of products.

- **Reduced spare-part costs.** By exploiting the configuration capabilities of IO-Link, one device can be configured to have different output functions — such as a sensor that's normally open (N.O.) or normally closed (N.C.).

All these advantages, combined with vendor independence and interoperability, make IO-Link a significant tool for successfully implementing the IIoT and Industry 4.0. □

Festo Corp., Hauppauge, New York, is a participating Encompass™ Product Partner in the Rockwell Automation PartnerNetwork™. Festo manufactures pneumatic and electromechanical systems, components and controls for process and industrial automation. The company offers a range of IO-Link compatible products, including IO-Link masters, pressure and flow sensors, displacement encoders and position transmitters, valve terminals, proportional pressure regulators and stepper motor controllers. In addition, the company provides basic and advanced training.

>> How IO-Link Integrates Sensors into The Connected Enterprise

IO-Link Technology is a worldwide open-standard protocol that integrates sensors into The Connected Enterprise by connecting the IO-Link-enabled device into an IO-Link master module. Users can deliver data from the sensor directly into a control system in an efficient manner.

The flexibility of IO-Link-capable sensors allows machines to operate more effectively by providing the controller with diagnostics. In addition to product detection, sensors can provide detailed and accurate machine health status to improve uptime.

WHY DOES AUTOMATING DESIGN MATTER IN THE IIOT?

When a company combines design automation with the Industrial Internet of Things for smart manufacturing, it can increase efficiency, save money and accelerate time to market.

From EPLAN Software & Service

Most of what we hear about with the Industrial Internet of Things (IIoT) is mainly about the machine in a smart factory configuration. But how do machines get to this next step? How do they get to where production becomes fully integrated, where the power and speed of computer hardware, tied to advances in connectivity between networks and systems, allow all points of contact in the manufacturing process to work together?

Design automation is part of the answer. The enhanced connectivity between people, machines and processes offered by the IIoT is creating an evolutionary shift that allows for a more cohesive design experience. Here are just some of the ways design automation facilitates that.

In design automation, the IIoT environment is realized with software that increases engineering efficiency and design optimization. These premium computer-aided engineering (CAE) systems use a database-driven platform that ties in to your business intelligence and can fully integrate into your IT environment.

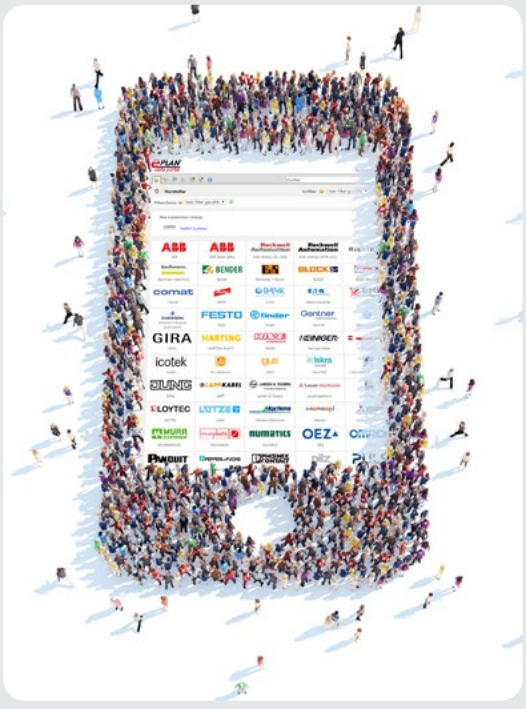
These CAE systems support a collaborative operation in which all stakeholders involved contribute their knowledge in a more horizontal, rather than vertical, structure. This means a more cohesive engineering and product planning process where all disciplines are working together, with the same data, in real time, rather than the more traditional patchwork approach, where the design moves from one engineering silo to the next. A collaborative approach allows team members to address collectively how best to meet the customer's needs and take advantage of the combined proficiency of the group.

With design automation, this enhanced collaboration also extends to relationships with vendors. Engineers can access the device data online for individual components,

>> Rockwell Automation, EPLAN Collaborate in Design Automation

Rockwell Automation and EPLAN Software & Service have collaborated to create software macros — descriptions of the products including dimensions and electrical connections — for all of the standard products Rockwell Automation offers. These macros are used to streamline projects and help machine builders reduce design time and time to market. Macros can be downloaded from the EPLAN Data Portal or from the Rockwell Automation EPLAN Macros page. www.rockwellautomation.com/rockwellautomation/support/eplan.page.

Also, the companies have focused on synchronizing controls configuration data between the EPLAN Electric P8 CAE and Rockwell Automation Studio 5000® programming software tools through RSLogix™ Architect. Users don't have to enter configuration information manually. It automatically updates, synchronizes and validates changes to model configuration information, including racks, I/O cards, I/O tags and descriptors. It also provides increased flexibility in engineering workflows to allow both disciplines to work concurrently rather than consecutively by beginning a project from any starting point.



and then insert those datasets into their design, reducing configuration work and increasing quality of the machine and system documentation.

These datasets can be acquired at an individual vendor's websites. However, it's faster and more efficient for engineers to use a single online database service that's resident in their CAE software and provides access to an extensive range of leading vendors' products. Users can access parts datasets from this source and drag-and-drop them directly into their project schematics. This same-sourced parts data comes in a common format and is vendor-certified, and will be populated automatically throughout the project documentation.

By orchestrating all components in the design and manufacturing process, best-of-breed CAE software mitigates work inefficiencies that come from doing a design manually. For example, when users make changes to the design and documentation, those changes are applied

The enhanced connectivity between people, machines and processes offered by the IIoT is creating an evolutionary shift.

everywhere, automatically, throughout the project documentation. That avoids errors that come from manually inputting the changes into lists on Excel spreadsheets and the manufacturing equipment.

Much More Potential

Many companies that already have these CAE software products are only using about 20% of their functionality. By embracing the other 80%, they can make better use of their experience with the software and touch into fields such as IT Infrastructure, Workflows, Platform Setup, Codes and Standards, Process Integration, Project Management and more — all areas of opportunity for improving a company's performance in an IIoT environment.

Engineering schematics can be communicated to all touch points in the manufacturing chain. The software even can reach out to the machine and automate the production process.

Integration also helps advance the need for more standardization throughout design and manufacturing. The ability to standardize components by pooling pertinent data about product inventory, usage indicators and other variants allows for a modular approach to product design. Up to 80% of a machine's tasks are comparable to tasks performed by other like machines. By building a library of commonly used components and subsystems, a business helps speed up product design and verification of documentation and coding.

One of the headline benefits of the IIoT is how industrial firms can develop new and better products faster. In this smart environment, new product development is more easily accomplished with the availability of big data analytics and enhanced collaboration. They provide greater insight into customer demand trends and how machines are being used.

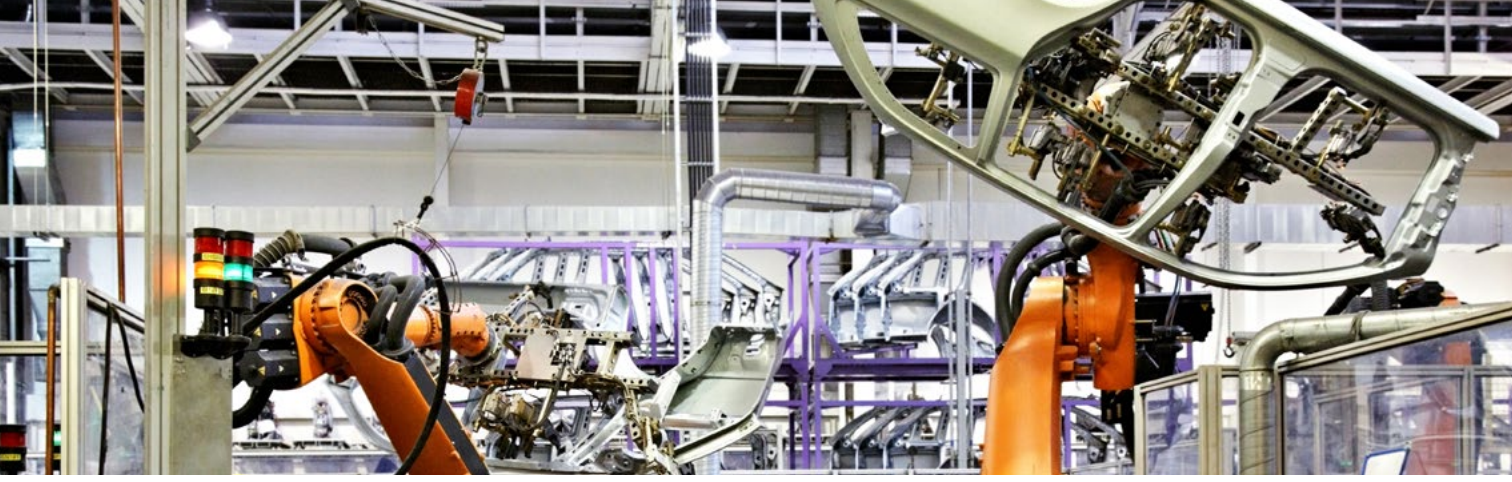
In addition, greater team member coordination in the engineering and development phase can lead to greater innovation. Compiling a library of standardized component and subsystem macros, which many companies are doing, can lead to new modular combinations in machine and process design.

Power of Data

Unlocking the potential in the IIoT can be the vehicle for continuing improvements in data utilization, allowing companies to reach new levels of cohesive functionality in all aspects of production. By connecting machines, data and systems, businesses can create intelligent networks along the entire manufacturing process and have it controlled autonomously.

When a company uses both design automation and the IIoT in creating its smart manufacturing infrastructure, it can expect a significant increase in efficiency leading to lower production costs and accelerated time to market. Businesses that embrace this movement can benefit from process improvement, increased productivity and cost savings. □

EPLAN Software & Service, Schaumburg, Illinois, is a participating Encompass™ Product Partner in the Rockwell Automation PartnerNetwork™. EPLAN is a global provider of fully integrated CAD/CAE solutions for design of electrical, fluid power, instrumentation and process control systems, and 2D/3D enclosures.



ADDITIONAL RESOURCES

Click on the resource below to access the desired content.

WHITE PAPER: SMART MANUFACTURING - LEVERAGING EMBEDDED INTELLIGENCE AND NEW SOURCES OF INFORMATION TO CONNECT AND OPTIMIZE THE ENTERPRISE.

WEBINAR: SMART MANUFACTURING AND THE CONNECTED ENTERPRISE

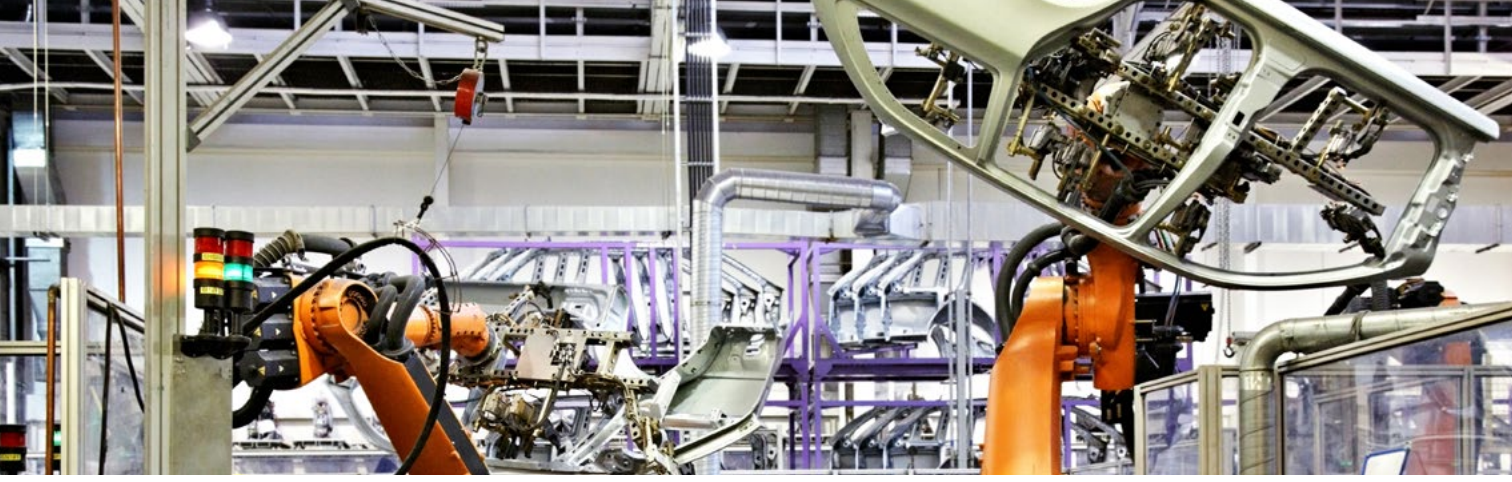
VIDEO: THE CONNECTED ENTERPRISE: THE FOUNDATION FOR SMART MANUFACTURING

WEBINAR: IMPROVE MANUFACTURING PRODUCTIVITY AND MINIMIZE RISK - INCREASE BUSINESS AGILITY BY CONVERGING MANUFACTURING AND BUSINESS SYSTEMS

VIDEO: STRATUS TECHNOLOGIES EXPLAINS HOW THE CONNECTED ENTERPRISE NEEDS THE SERVER INFRASTRUCTURE TO MAINTAIN RELIABILITY IN BOTH THE PLANT AND REMOTE LOCATIONS

WEBINAR: MOBILITY TRENDS IN MANUFACTURING - IMPLEMENT INDUSTRIAL MOBILITY TO IMPROVE PLANT PRODUCTIVITY & MAINTAIN SECURITY

WEBINAR: HOW REFERENCE ARCHITECTURES SUPPORT DEPLOYMENT OF THE CONNECTED ENTERPRISE



ADDITIONAL RESOURCES (CONT.)

VIDEO: PANDUIT SHOWS INDUSTRIAL AUTOMATION NETWORK SOLUTIONS WITH CONVERGED PLANTWIDE ETHERNET (CPWE) ARCHITECTURE

EBOOK: YOU CAN'T ACHIEVE SMART MANUFACTURING WITHOUT EMBRACING MODERN TECHNOLOGY

WEBINAR: THE CONNECTED ENTERPRISE OPERATIONS INTELLIGENCE – READY TO CONNECT PEOPLE, PROCESSES, AND TECHNOLOGY TO DRIVE HIGHER PROFITS?

WEBINAR: BENEFITS OF IO-LINK TECHNOLOGY – SMART SENSORS AND THE CONNECTED ENTERPRISE

VIDEO: SPECTRUM CONTROLS HIGHLIGHTS ITS WEBPORT INDUSTRIAL REMOTE ACCESS GATEWAY