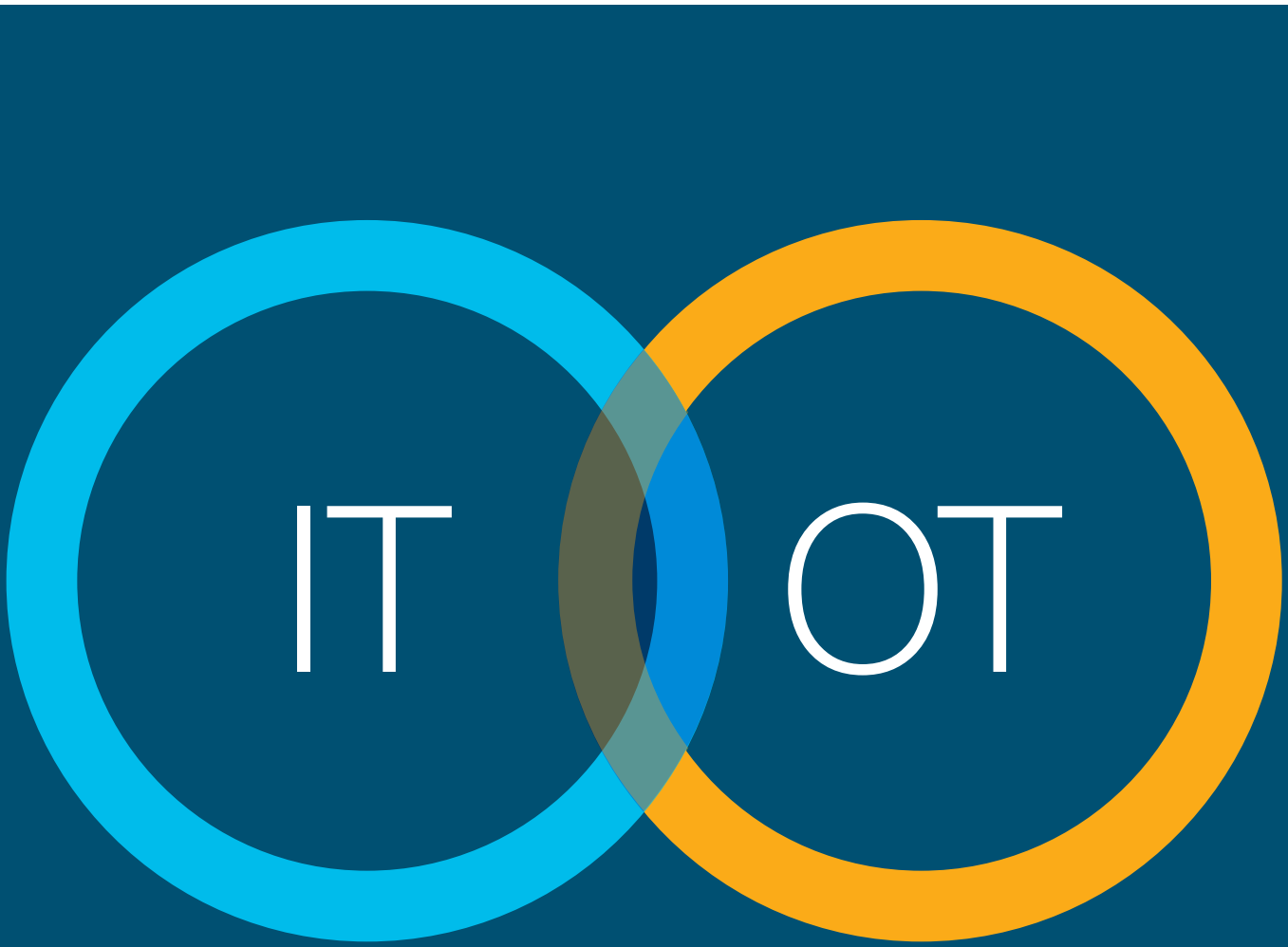
White paper

IT/OT Convergence

Moving Digital Manufacturing Forward



Historically, the information technology (IT) and operational technology (OT/operations) departments within an industrial manufacturing company could function fairly independently. Operations kept the plant running smoothly, and IT managed business applications from the front office.

The two teams occasionally collaborated on successful projects, such as implementing printers on the factory floor or servicing industrial PCs. Unfortunately, those opportunities were rare. Too often, it was a problem, not an opportunity, that brought IT and operations together. Whether it was a security incident, a system failure, or unplanned downtime, those encounters did little to breed trust and collaboration between the two teams.

But the world of manufacturing is changing. To keep up, IT/OT relationships must change with it.

The research suggests that executives are equally worried about established companies and startups, both within and outside their industry, deploying new technology and business models that will negatively affect their position in the market.

To outpace that potential disruption, manufacturing companies are working to adapt their processes, technologies, and business models. The most forward-thinking companies aren't just trying to survive the changes. They're working to be the ones that lead it – gaining a competitive advantage, improving operational efficiency, and maximizing profitability. They are leading digital business transformation in manufacturing.

Clearly, this shift is bringing new and challenging projects to the IT and operations professionals working within the industry. And the savviest IT and operations leaders also know that success in this new climate means working more closely together.

"According to the Global Center for Digital Business Transformation, manufacturing is one of the 10 industries that are most ripe for business disruption[1]."

Tweet this thought

1. http://www.imd.org/uupload/IMD.WebSite/DBT/Digital_Vortex_06182015.pdf

Visionary operations leaders recognize that the reams of operational data they use to support real-time decision making could create additional value for the company. But they need the support of their IT colleagues to make the data meaningful and accessible for use across the organization. Their IT colleagues can also help them better align with business systems, such as enterprise resource planning (ERP) tools and manufacturing execution systems (MES).

At the same time, IT teams want to achieve the vision and potential of a connected factory – from improving the supply chain to driving innovation and minimizing downtime. However, to get there they need the knowledge and support of the operations professionals who understand and control the equipment.

Both groups have seen glimpses of how their efforts might enhance the future of their companies and industries, but to take full advantage of this opportunity they must work together.

That's why the forced IT/OT interactions that often characterized security and Ethernet projects of the past are being replaced with more powerful, collaborative alliances. Together, IT and operations teams go beyond merely responding to problems. Instead, they're playing a key role in their companies' transformations, helping to seize new business opportunities that make them more competitive, more efficient, and more secure.

In this paper, we take a closer look at some of the key ways IT/OT convergence is enabling digital manufacturing transformation, including:

01. Enabling real-time decision making through fog computing

02. Eliminating unplanned downtime through predictive maintenance

03. Deploying wireless technology on the factory floor

04. Ensuring cybersecurity for a new world of connected machines

Customer Story

Mazak

Mazak required a common, standards-based method to securely connect and derive value from the rich, raw data in its machine tools. It also needed an advanced security system suitable for IT and operations technology (OT). The application needed to run on the network infrastructure on the factory floor, immediately transforming process, overall equipment effectiveness (OEE), and sensor data. They also needed an effective fog application and real-time analytics.

They implemented Internet of Things connectivity (Cisco® Industrial Ethernet 4000 Switch), a new application framework (Cisco IOx), a fog application (MTConnect), and real-time analytics (Cisco Connected Streaming Analytics).

Business outcomes included:

- Expanded market opportunity with Mazak SmartBox Connected Machine service
- Cost consolidation through running fog application and real-time analytics on IoT network infrastructure
- Rapid time to value with measurable customer impact: improved OEE, continuous customer service, and increased machine utilization

Read more

01. Enabling real-time decision making through fog computing

Thanks to the industrial Internet of Things, manufacturers are collecting more data than ever before. However, that data is only as valuable as the decisions it can support.

That's why traditional cloud computing alone isn't always the best solution for manufacturing. Extremely time-sensitive decisions should be made closer to the things producing and acting on the data, to minimize latency and address potential issues.

For years, manufacturers have relied on supervisory control and data acquisition (SCADA) systems to achieve real-time decision making. However, those systems don't typically allow for the same enterprisewide data sharing expected in the world of smart manufacturing.

That's why operations teams are turning to fog computing, which gives them real-time access to mission-critical data at the plant level, while also sharing that knowledge throughout the enterprise. This enables rapid decision making that improves safety and prevents costly downtime while also sharing information across different plants in different geographies, helping operations leaders see enterprisewide trends that can contribute to safety and operational effectiveness.

And here's the beautiful part: IT likes the fog as much as operations does. With fog computing, IT gains a veritable data triage:

- Time-sensitive data can be analyzed on the fog node closest to the device generating the data.
- Data that can wait seconds or minutes can be passed on to an intermediary node that keeps an eye on operational data.
- The least time-sensitive data is sent to the cloud for historical analysis and storage.

This approach conserves bandwidth, refining when and how data center resources are used. It creates a more scalable system, making room for a flood of new digitized devices and complexity on the factory floor. And because it also makes it possible to analyze sensitive data at its source, it improves overall system security.

Customer Story

FANUC

FANUC, a world-leading CNC systems and industrial robot company that supplies machines to manufacturers, uses big data analytics to identify maintenance procedures that can prevent breakdowns before they occur.

With the FANUC Zero Downtime solution, the robot is connected through a Cisco network into a Cisco edge computer data collector in the plant to access new robot operational data.

The relevant data is securely transmitted to the Cisco Cloud where the FANUC's analytics captures the "out of range" exceptions and predicts the maintenance needed.

An alert is then sent from the cloud application to FANUC service personnel and to the manufacturing customer about the need for service. Needed parts can be shipped to arrive at the factory in time for the next scheduled planned maintenance window.

According to Rick Schneider, CEO for FANUC America, "Preventing unplanned downtime is a huge savings for our customers and makes the FANUC robots with ZDT a tremendous value. With Cisco, we are helping our customers access this new value and also re-imagining our go-to-market strategy for after-sales service and support."

Read more

02. Eliminating unplanned downtime through predictive maintenance

IT/OT convergence is also creating a paradigm shift in factory maintenance.

Planned preventive maintenance schedules rule the day in most manufacturing settings. Operations teams perform preventive maintenance on a regular schedule to lessen the likelihood of equipment breakdowns. This approach requires a plant to maintain a database of its assets, track their condition, and rely on manufacturers' recommendations to determine when and how to maintain them.

While preventive maintenance is clearly better than just waiting until something breaks, it's not perfect. These methods are time-consuming and costly—and don't always account for special conditions. Since the maintenance schedules are based on best practices, not actual data from the machine being serviced, this approach almost inevitably leads to some amount of unplanned downtime and waste.

And unplanned downtime, in today's world, is simply unacceptable. In most manufacturing environments, profit margins are already slim. The costs associated with unplanned downtime — from production losses to wasted materials and replacement parts — all erode the thin cushion between a profit and a loss. This means that eliminating unplanned downtime is a critical business imperative.

Unlike preventive maintenance procedures, predictive maintenance technologies allow manufacturers to collect real-time data from the actual machines affected, monitor for any situation that might indicate a potential equipment failure, and then schedule repairs during planned downtime, while also extending the machine's useful life and dramatically reducing repair costs. Instead of using estimates or best guesses, these systems use real data intelligence from the factory floor.

Shifting to a predictive maintenance approach significantly improves uptime, and it's supported by IT/OT convergence. Operations does its part by collecting key data from PLCs, machines, and sensors, while IT provides the data analytics and other tools that give the data meaning. By digitizing the maintenance process, IT/OT teams make it possible to predict when any given device might fail, and intercede accordingly. resources are used. It creates a more scalable system, making room for a flood of new digitized devices and complexity on the factory floor. And because it also makes it possible to analyze sensitive data at its source, it improves overall system security.

Customer Story

Daimler

For Daimler Trucks North America (DTNA), success isn't just about controlling costs. It's about building an agile company that can deliver exactly what the market demands – today and tomorrow. Its Western Star brand of trucks are tailored to every customers' needs, but this level of customization presents a logistical challenge in a mass production environment.

DTNA decided that it needed to upgrade the network in its Western Star production facility in Portland, Oregon, to better coordinate customizations and support flexible and efficient operations, both now and in the future.

DTNA chose Cisco and Rockwell Automation as strategic partners, designing and deploying a new network based on the Converged Plantwide Ethernet (CPwE) validated design guides. Cisco Aironet® access points deliver secure and reliable Wi-Fi connectivity across the plant.

By combining IT and automation networks into one secure, manageable, and converged environment, DTNA managers gain real-time visibility across processes. Data is transmitted securely to managers, helping them make better, faster decisions that keep plants running efficiently. Software-defined networking (SDN) also supports remote troubleshooting to minimize downtime when equipment needs maintenance or repair.

The joint architecture scales to any size or configuration, allowing DTNA to use the Western Star factory as a template, which it is rolling out across other factories.

Read more

03. Deploying wireless technology on the factory floor

It's hard to imagine a smart factory without wireless. The numerous machines, sensors, and PLCs, plus the analytics platforms and ancillary technologies running alongside, all become more efficient and practical with wireless technology.

But until recently, deploying wireless across the plant floor was not always a viable option.

Industrial environments vary greatly, from challenging building layouts to harsh environmental conditions such as dust, excessive humidity, temperature, and vibration. Plant managers were also skeptical about whether wireless could support the number of devices, bandwidth, latency, and security required for mission-critical applications. So plants deployed miles of cable everywhere, which was expensive and time-consuming.

However, over the last several years there have been great strides in wireless technology. This increased resiliency makes wireless more affordable and practical for industrial environments than ever before, and it is also quicker to deploy.

And wireless can be a game changer for any factory. It enables more flexibility and adaptability for remote monitoring, assembly line changeovers, and quality or supply chain initiatives. At the same time, it can lead to significant cost savings. According to Control Engineering, "Wireless (in the factory) can be up to 10 times less expensive than cable, with more flexibility, mobile benefits, and reduced maintenance and troubleshooting[2]."

IT and operations can work together to successfully deploy wireless on the factory floor, and doing this well benefits both groups. IT loves the cost savings, reduced troubleshooting, and increased bandwidth, while operations teams enjoy the benefits of additional agility, increased quality, and reduced downtime.

2. http://www.controleng.com/channels/manufacturing-it/case-studies/single-article/outstanding-industrial-wireless/4671e1ff860b0b2167e5b73b08a0c819.html

Customer Story

Ansell

Although Ansell is known for protective solutions, the company wanted to tighten its cybersecurity protections.

"We were basically starting from scratch, so we needed every security solution available to reduce our risk," says George Michalitsianos, IT Infrastructure Director.

"The Cisco Security Enterprise Licensing Agreement (ELA) gives us access to all of the security solutions we needed for one-third of the cost of purchasing everything separately, which allowed us to bring on security solutions we never had before."

Using the automated security capabilities integrated across multiple Cisco security products, such as Cisco Advanced Malware Protection (AMP), Cloud Web Security (CWS), and Cloud Email Security (CES), Ansell can now block thousands, of advanced and known threats daily, stopping phishing attacks, ransomware, and known malicious actors.

In the case of a breach, Cisco FireSIGHT™ Management Center provides centralized visibility and intelligence that enables IT staff to more quickly detect, contain, and remediate any incident from a single pane of glass.

Read more

04. Ensuring cybersecurity for a new world of connected machines

Cybersecurity is mission critical for manufacturing. Protecting intellectual property and customer information is paramount to a company's long-term viability and corporate reputation. At the same time, compromised production systems could affect quality, profitability, and even safety.

Not long ago, manufacturers could feel generally comfortable with the security of the machines on the factory floor. Their proprietary systems and likely lack of Enterprise connectivity created a sense of safety. However, linking the machines on the factory floor to the network has countless benefits. For instance, the data collected can be analyzed to reduce downtime, increase operational efficiency, and can lead to improved safety and product quality. However, this new change, combined with an increased prevalence of cybersecurity threats in general, requires a new approach to security. The old "security by obscurity" approach is no longer valid.

Today's solutions must connect networks and enable monitoring and secure data flow. It must be possible to deploy them in existing environments and on legacy equipment. And they must deliver defense-in-depth features to organize, harden, defend, and respond to threats.

Implementing this new approach to cybersecurity in manufacturing requires collaboration from both IT and operations. IT brings a deep understanding of cybersecurity protocols and policies, as well as experience in managing implementation and ensuring compliance.

But to make cybersecurity work for manufacturing, operations teams must also play a critical role in the process. For instance, a diligent approach to cybersecurity generally requires regular system updates, but deploying them without consulting operations is a potential downtime disaster waiting to happen. Operations must have a seat at the table to determine when to deploy those updates, ideally in line with planned maintenance schedules, and to evaluate any potential production system impact.

IT/OT must work together to make cybersecurity work for manufacturing, while avoiding unintentional downtime and preserving the company's profit margin.

Key Business Outcomes

48.9%

Decrease
in the defect rate

47.8%

Decrease
in unplanned downtime

17.5%

Decrease
in annual energy costs

34.8%

Increase
in inventory turns

23.1%

Decrease
in new product introduction cycle time

16.2%

Increase
in original equipment effectiveness

Conclusion:

A New World of IT/OT Convergence Fosters Unprecedented Business Outcomes

IT and OT convergence is transforming manufacturing in ways neither function could have imagined, while making both entities even more effective at their jobs.

According to the "Smart Manufacturing and the Internet of Things 2015" survey of 418 manufacturing line-of-business executives and plant managers by SCM World and Cisco, smart manufacturing can foster tremendous business outcomes[3]

At the same time, with OT's insight on the factory floor, IT is staying a step ahead of those who seek to compromise security and confidentiality.

As these two groups work more closely together, they're unlocking new opportunities for manufacturing. Although they may have different approaches, backgrounds, and key performance indicators (KPIs), both are heavily invested in achieving their companies' overarching goals.

3. http://www.cisco.com/c/dam/assets/docs/becoming-smarter-manufacturer.pdf

Connect With Us

At Cisco, we're helping unite IT and operations for digital manufacturing initiatives that save money, enhance profitability, amplify security, and improve operational efficiency. Ready to take the next step?

Learn more about Cisco's solutions in each of the areas covered in this white paper:

Fog Computing

Predictive Maintenance

Factory Wireless

Cybersecurity

Learn more about manufacturing at Cisco

Connect with us on social media or

Visit our website

CXX-XXXXXX-00 XX/XX