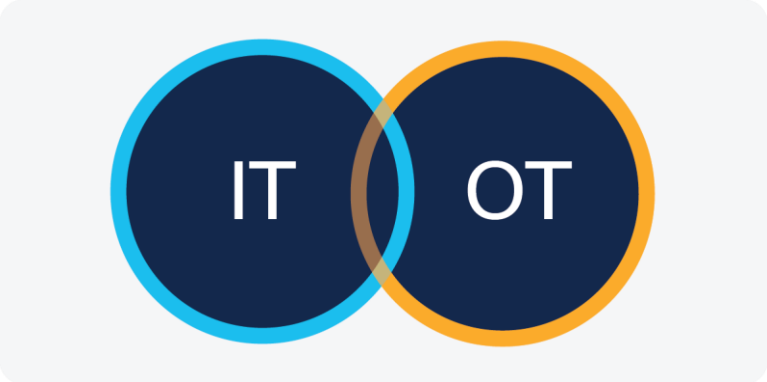
White paper
Cisco public

IT/OT Convergence

Moving Critical Infrastructure and Industrial Verticals into a Digital Era

Contents



Historically, the Information Technology (IT) and Operational Technology (OT/operations) departments within a critical infrastructure or industrial company could function 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 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, 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 critical infrastructure and industrial verticals.

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.

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 Supervisory Control And Data Acquisition (SCADA) systems.

At the same time, IT teams want to achieve the vision and potential of connected operations, 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 transformation, including:

1. Enabling real-time decision making through edge computing
2. Eliminating unplanned downtime through predictive maintenance
3. Deploying wireless technology in all environments
4. Providing cybersecurity for a new world of connected operations

Enabling real-time decision making through edge computing

Thanks to the industrial Internet of Things, industrial companies 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. 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, companies have relied on SCADA systems to achieve real-time decision making. However, those systems don't typically allow for the same enterprise-wide data sharing expected in the world of digitization.

That's why operations teams are turning to edge computing, which gives them real-time access to mission-critical data at the plant and field 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 enterprise-wide trends that can contribute to safety and operational effectiveness.

And here's the beautiful part: IT likes edge computing as much as operations does.

- Time-sensitive data can be analyzed on the node closest to the device generating the data.
- With edge computing, IT gains a veritable data triage capability.
- Data can be obtained in seconds or minutes and then 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. And because it also makes it possible to analyze sensitive data at its source, it improves overall system security.

For more detail about Cisco Edge Computing solutions click the link below.

Edge Computing

Customer story

Resolute Mining, LTD

Resolute Mining Ltd. is a successful gold miner with more than 30 years of experience as an explorer, developer, and operator of gold mines in Australia and Africa. Over the years it has produced more than 9 million ounces of gold. The company's IT team must support the technology needs of multiple business entities operating 24 hours a day, most of which rely heavily on core ERP applications and business management software. If the performance of those applications suffer, it can affect the company's inventory tracking, transaction processing, and truck dispatching capabilities.

What's good for business can be difficult for IT. Managing, supporting, and scaling distributed systems and workloads can be extremely challenging. Especially when they're in far-flung locations like different continents. Resolute chose the combination of Cisco HyperFlex Edge and Cisco Intersight, a solution that is tailored for edge environments.

The solution provides effective edge application with real-time analytics for remote mining operations. It improves infrastructure redundancy, increases network availability, so problems that used to require onsite intervention and days of downtime are now easily resolved in minutes from Perth.

"These are all critical capabilities delivered with Cisco HyperFlex Edge and Cisco Intersight that can truly help customers as they strive towards "anywhere operations" and help in the continued pursuit of operational efficiency." said Simon Duncalf, IT Manager at Resolute Mining.

Read more

Eliminating unplanned downtime through predictive maintenance

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

Planned preventive maintenance schedules rule the day in most industrial 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 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 industrial 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 users 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 industrial environment.

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 to intercede accordingly. It creates a more scalable system, making room for a flood of new digitized devices and complexity. And because it also makes it possible to analyze sensitive data at its source, it improves overall system security.

For more detail about Cisco Predictive Maintenance solutions click the link below.

Predictive Maintenance

Customer story

Nissan

Nissan Motor Corporation, the global car manufacturer, headquartered in Yokohama Japan, leads the industry in new technology developments for electrified, intelligent, and connected vehicles. The company rolled out a high-speed, secure Cisco IoT network that streamlines operations to support production lines at the Tochigi Plant. The solution uses big data analytics to identify maintenance procedures that can avoid breakdowns before they occur.

"We wanted to obtain quality data on a real-time basis and use the same data to analyze trends to help prevent defects before they occur. In addition, we want the person in charge to be notified immediately if any of the equipment malfunctions or if there is an outage so that we might reduce the time the production line is down to a minimum," explained Masayoshi Chiyoda, Engineer of the Powertrain Production Engineering Department, Nissan.

By standardizing network design they improved manufacturing efficiency with a fully automated production line. The combination of Cisco IE switches and Cisco Identity Services Engine (ISE) makes it possible for Nissan to securely manage and control network access, production lines and equipment, creating a secure and highly functional IoT network that can obtain information from the production line.

Capturing data this way allows both the IT and operation technology (OT) departments to work together by merging manufacturing-related data from the OT space and information related data from the IT space.

Read more

Deploying wireless technology

It's hard to imagine an industrial site 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 was not always a viable option.

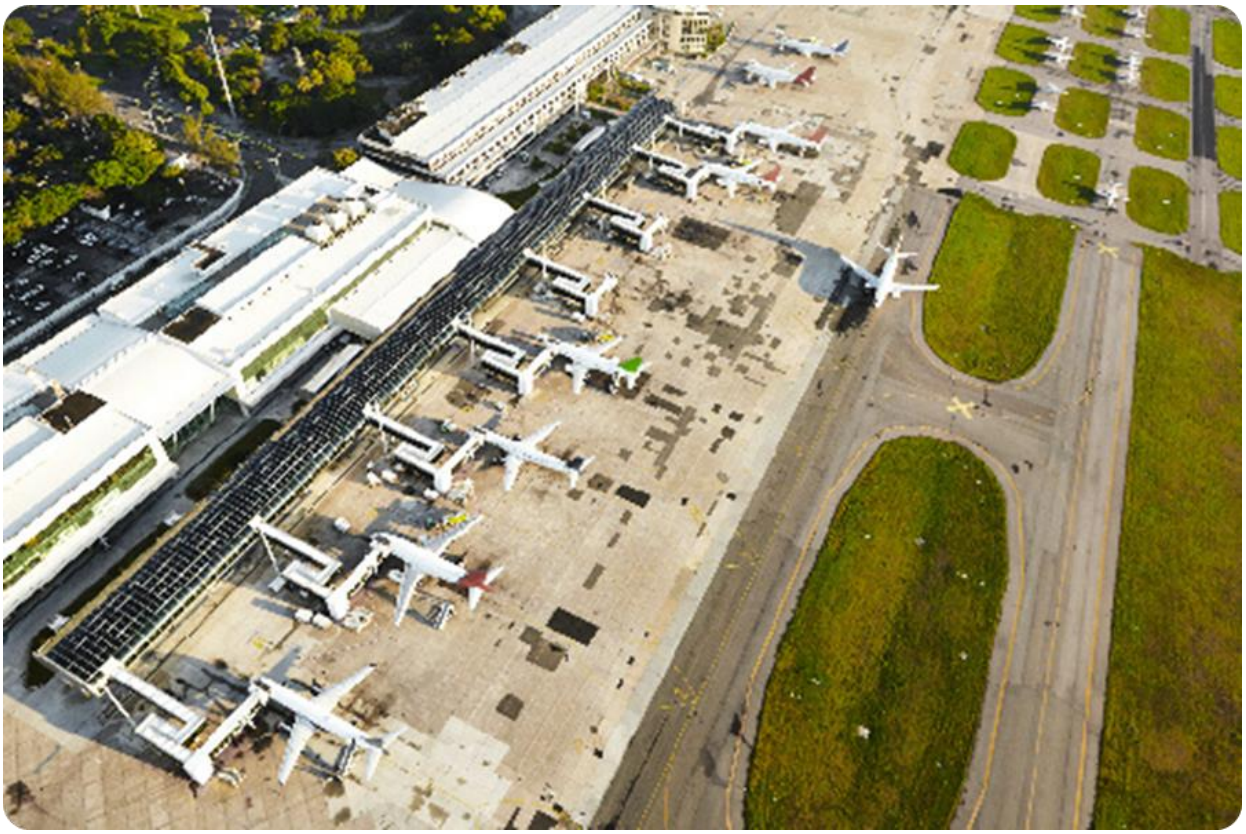
Industrial environments vary greatly, from challenging building layouts to harsh environmental conditions such as dust, excessive humidity, temperature, and vibration. Operations managers were also skeptical about whether wireless could support the number of devices, bandwidth, latency, and security required for mission-critical applications. So they 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. 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 Jay Werb of the ISA100 Wireless Compliance Institute, "A wireless deployment saves significant costs compared to an equivalent wired installation, resulting in savings of 20 to 30 percent in simple configurations. Cost reductions can be even more compelling in scaled installations or in remote locations. Where wiring is cost prohibitive or infeasible, wireless enables best-practice instrumentation wherever it is needed for efficient and safe industrial operation."[1]

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

[1] https://blog.isa.org/cost-benefits-industrial-wireless-isa100-networks



For more detail about Cisco Industrial Wireless solutions click the link below.

Industrial Wireless

Customer story

BIAL

Bangalore International Airport (BIAL) caters to approximately 235,000 air transport movements and over 33 million passengers annually. It is known globally for innovation and digital transformation.

Given their annual growth and commitment to digitization, BIAL decided to optimize operations to facilitate rapid turnaround for incoming aircrafts. To do that they needed automation that would convert manual timestamping into the automated capture of real-time information. Cisco, along with its ecosystem partners, identified challenges and developed a custom-built solution to enable automation, collaboration and data-driven decision making.

A number of different wireless solutions can be used at airports to enhance communications including WiFi networks for data and voice, 4G LTE and 5G, as well as professional mobile radios. Computer vision devices, and IoT sensors deployed in the field collect data in real time from fixed and mobile air site assets like step ladders, baggage loaders, catering vehicles, fuelers etc. and transfer it back to a central control center where it can be analyzed and processed with the help of OT experts utilizing turnaround time applications.

“With Cisco’s advanced technologies we were able to track and monitor airside operations across various domains.” Shwetha Karunakar, AGM Innovation and Digital Programmes, Innovation Lab BIAL.

Read more

Providing cybersecurity for a new world of connected machines

Cybersecurity is mission critical for critical infrastructure and industrial companies. 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, these companies could feel generally comfortable with the security of their machines. Their proprietary systems and lack of enterprise connectivity created a sense of safety. However, linking the machines from the operations environment to the network has countless benefits. For instance, the data collected can be analyzed to reduce downtime and 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 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, 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, while avoiding unintentional downtime and preserving the company's profit margin.

For more detail about Cisco Industrial Cybersecurity solutions click the link below.

Industrial Cybersecurity

Customer story

CKW AG

CKW AG is the largest energy service provider in central Switzerland, supplying power to more than 200,000 customers. The company operates a power distribution network that provides electricity and other services to residential, commercial, utility, and municipal customers. It needed a network transformation to keep its operation traffic flowing swiftly, reliably, and securely on a shared infrastructure. At the same time, it had to ensure the integrity of the electrical system and protect it from external threats, including cyberattacks that can shut down or take control of power plants and distribution networks.

"We place a lot of value on operational technology (OT), hardware and software that monitors and controls the physical assets of the power grid, including network infrastructure." says Stefan Mattmann, Senior SE for Grid Communication.

CKW AG used the automated security capabilities integrated across multiple Cisco security products, including Cisco Secure Firewall Management Center to unify and streamline firewall management, application control, intrusion detection, and port and protocol control as well as Cisco Secure Firewall ISA 3000, an internet appliance explicitly designed for OT and IoT security applications.

The result is a solution that provides deep visibility into the substation network, enhanced OT and IT infrastructure control, and a scalable environment with enhanced cybersecurity standards. CKW AG can now block thousands, of advanced and known threats daily, with centralized visibility and intelligence that enables staff to more quickly to detect, contain, and remediate any incident from a single pane of glass.

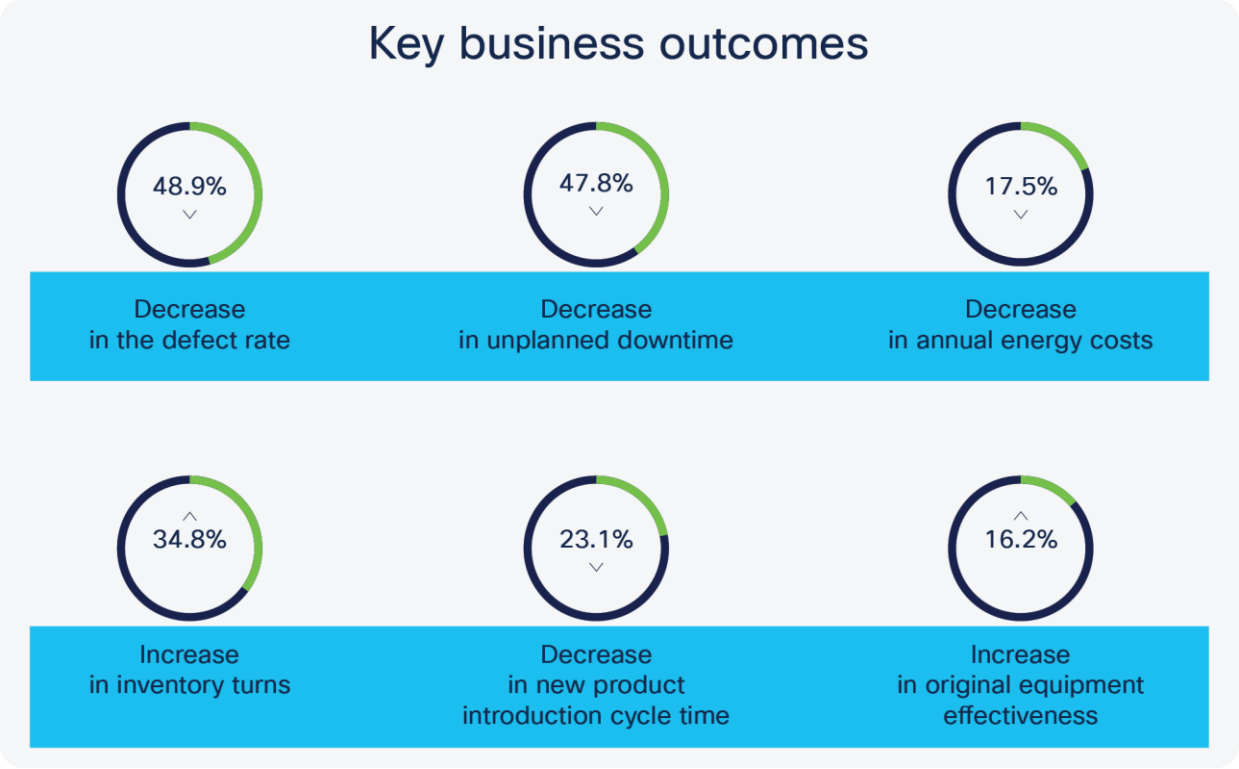
Read more

Conclusion

A new world of IT/OT convergence fosters unprecedented business outcomes

IT and OT convergence is transforming companies in ways neither function could have imagined, while making both entities even more effective at their jobs by improving internal processes, business decision making, productivity and competitiveness.

With OT's insight on the factory floor, IT is staying a step ahead of those who seek to compromise security and confidentiality while enhancing the value that both systems can contribute.



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

Connect with us

At Cisco, we're helping unite IT and operations for digital initiatives that save money, enhance profitability, amplify security, and improve operational efficiency.

Find out more about the industries referenced and other industry solutions by clicking the links below.

Utilities

Oil and Gas

Transportation

Manufacturing

Mining

To learn more about How OT and IT differ

Visit our website

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-3106568-00 09/22