The convergence of IT and OT—and how federal CIOs can plan for it

Billions of new internet-connected devices promise big payoffs for federal enterprises, but also pose new challenges for CIOs.

The coming convergence of information technologies (IT) and operational technologies (OT) presents a new era of data-driven opportunities for organizations—and a new set of technical challenges for enterprise CIOs.

The exponential growth of internet-connected sensors, control systems and other devices—the Internet of Things—and the real-time data they provide are unleashing all kinds of innovation across a wide range of industries, from manufacturing to transportation to healthcare to energy.

But CIOs in both the commercial and public sectors are starting to wrestle with a host of new questions:

- How to integrate IT and OT systems that were designed for fundamentally different purposes;
- How to effectively handle all the data those devices will produce;
- How to work with disparate groups of industry players and equipment makers toward more unified, interoperable systems; and
- How to resolve ongoing concerns around security.

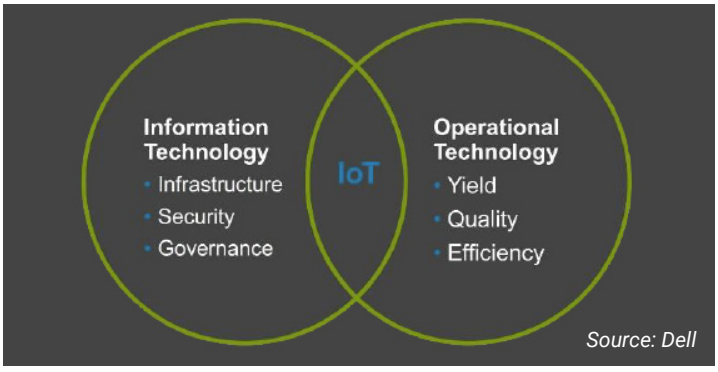
Inundation of devices

The Internet of Things (IoT) Age has arrived, and the inundation of devices is beginning to impact traditional IT ecosystems. A PricewaterhouseCoopers report last year estimated industrial firms globally plan to spend more than $900 billion annually until at least 2020 on industrial IoT-related hardware, software, services and connectivity. McKinsey Global Institute projects upwards of 50 billion devices will be connected to the Internet by 2025.

Military and government agencies—among the earliest adopters of IoT devices to support supply chain logistics—are ramping up IoT investments too.

The U.S. Army, Air Force and Navy, as well as the departments of Defense, Transportation, Health and Human Services, Veterans Affairs and Homeland Security, spent more than $2.5 billion in IoT sensors and related devices in fiscal 2016 to improve their operations, according to a report from immixGroup released in May. And that spending is expected to grow to $3 billion a year by fiscal 2018.

The U.S. General Services Administration, which manages more than 375 million square feet of rentable building space, is continuing to demonstrate how IoT devices are helping agencies better monitor and manage energy costs in federal buildings and utilize office space more effectively.



IT and OT devices tend to be managed by separate organizations, but those devices are starting to share the same network infrastructure.

Payoff potential

With 5G wireless communications and exponentially faster data transmission speeds on the near-term horizon, all those IoT devices promise big payoffs in the form of increased awareness, automated response and improved system performance.

Yogev Shimony, Marketing Director for Embedded Solutions at Dell EMC, including IoT strategies, sees four primary ways IoT can help enterprises:

1. **Drive operational efficiency—**IoT can reduce costs and improve operational effectiveness by reducing unplanned downtime and identifying underperforming assets.
2. **Improve customer experience—**By capitalizing on supply chain logistics and other data, organizations can make smarter decisions on how to optimize products and services.
3. **Reduce risks—**IoT devices and data analytics can help detect system failures before they happen and reduce or mitigate their potential impact.
4. **Uncover new business value—**By monitoring how assets move, how products are used or how operations consume energy, organizations can discern new ways to create value or develop new business models.

These types of benefits are already taking shape in the federal government, where IoT is improving operations supporting defense, energy and logistics, law enforcement and public safety, science and healthcare.

Different by design

However, while IoT and OT devices may be made from the same silicon and rely on the same underlying internet protocols as IT devices, they evolved as distinctly different products to meet many different needs than IT devices—and that poses a problem for CIOs, according to tech experts.

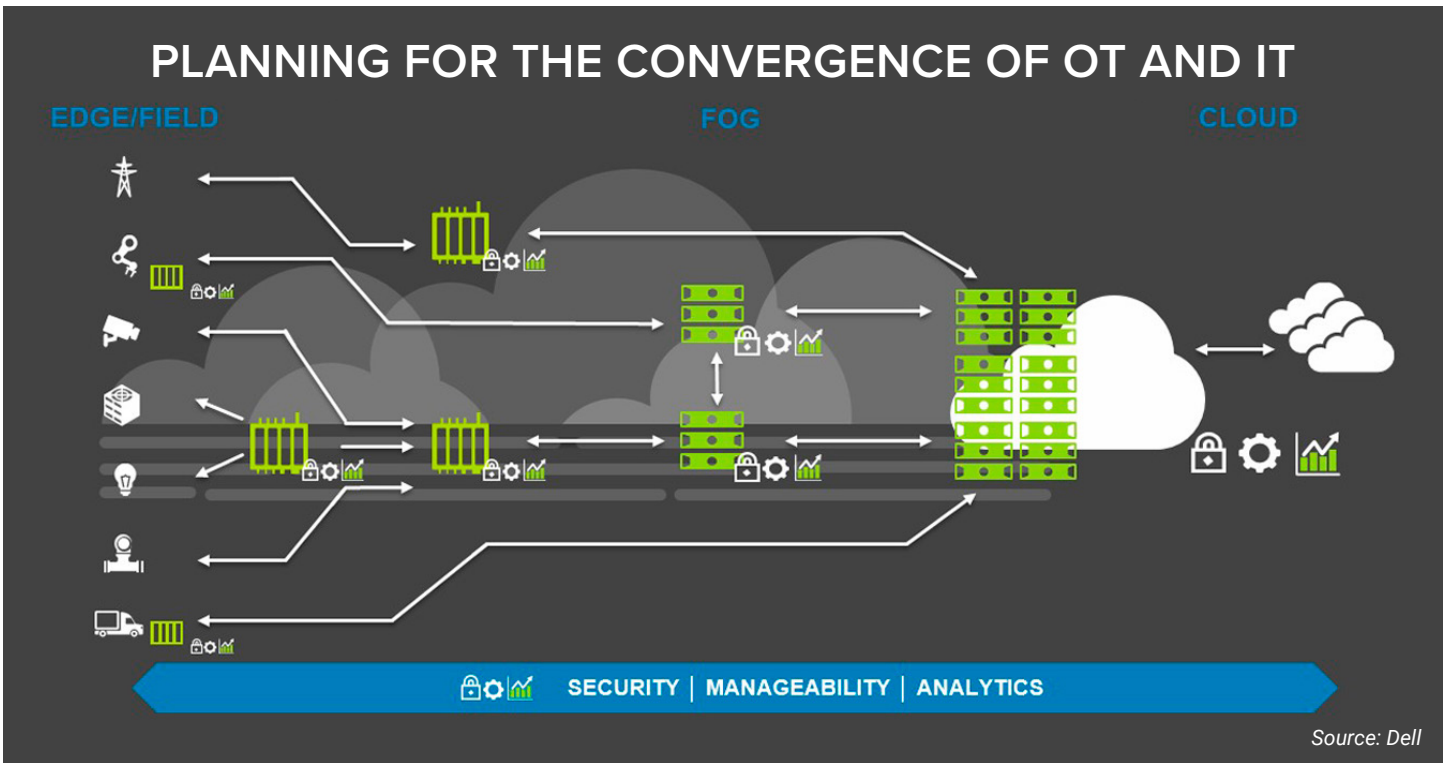
OT devices were designed to perform specific industrial functions in often-harsh environments. They needed to meet exacting size, communications and power requirements and last for years without human intervention.

IT devices, in contrast, were driven by performance and security pressures to do computational work. They benefitted from common standards and a vast base of developers competing to improve them. But the race to build faster, more productive devices made even the best IT products obsolete within two to three years.

Shimony sees another distinction. “IT is primarily concerned with infrastructure, security and governance. When we see OT departments, they usually focus on yield, quality and efficiency,” he says. As a result, IT and OT devices tend to be managed by separate organizational silos and spring from different sources of supply.

The security divide

There’s a deeper problem facing enterprise CIOs and the technology community at large, however, argues Stephen DiFranco, principal at the IoT Advisory Group. IT and OT approach security differently.



Enterprise and agency CIOs will need to prepare for new data processing demands from IoT devices in the field, and new layers of gateway equipment on the network to support those devices closer to the field.

"We try to secure things at the network level, because that's how we [in IT] think," he says. "But the problem we have to solve starts with the little radio inside the device—and that's not going to come from any of the companies we currently have working on network security."

Recent cyberattacks, like the one that took down part of the power grid in Ukraine, point to the growing importance for IT and OT teams to work more closely together. Hackers are increasingly finding ways to use unsecured IoT devices to build botnets and disrupt targeted enterprises. As a result, there's growing consensus that organizations and their leaders must take steps to harmonize their IT and OT operations in order to identify and evaluate current and future risks.

Organizations recognize the need to integrate IoT and IT technologies, a recent Gartner report found, but most organizations don't yet have the skills, expertise or time to drive the IT/OT alignment requirements.

IoT systems, however, also pose other challenges for CIOs and senior leaders, including concerns about privacy protection and a host of safety risks associated with IoT-connected automobiles, medical and other devices, according to a new report from the Government Accountability Office. With more than 350 IEEE standards that can apply to IoT devices, interoperability issues will also continue to complicate CIOs' decisions for the foreseeable future.

DiFranco argues industry and standards organizations need to come together to develop systems that recognize when devices aren't behaving normally. Just as credit card companies can now recognize when activity doesn't match a predictable pattern—and disable the card—the IoT industry needs to devise the means to monitor and manage IoT devices, he says.

Planning for gateways and all that data

A potentially larger issue facing both OT and IT teams is the sheer volume of data and messaging demands that billions of new IoT devices are expected to place on local and wide area networks (WANs).

Enterprise CIOs must begin planning for a new layer of technology, and the need to add gateways to the architecture of networks, to process data streams closer to the nodes used to gather signals and data from the devices.

The volume and complexity of data generated by IoT sensors and devices can overload traditional network infrastructure and data management and analysis tools, experts say. They also warn that sending all that data to the cloud in many cases isn't cost effective—and it's potentially risky if automatic control decisions must be made locally and connectivity to the cloud is lost.

"As more things are located on the edge of the network, organizations will need hardware solutions that can also live on the edge," Shimony said. That will require IT products and solutions capable of withstanding a wide range of temperatures, harsh environments and work 24/7/365. "That requires a new kind of hardware that IT departments have not been necessarily looking at or deploying in the past," he says. It will also require new ways to power and protect those devices.

Additionally, while advances in software, storage technologies and the cloud are helping CIOs keep up with the relentless growth in data, IoT promises to add new strains on enterprise systems, says Ro Dhanda, Director for Federal business at Dell EMC Isilon. The potential of IoT to enhance operations is compelling, he says. But federal CIOs face "some major areas of concern when they think about the mechanics of IoT and how it will affect their organization."

He suggested CIOs consider three questions: "Is their infrastructure prepared? Do they have the right levels of security in place? And do they have the right personnel in place to be able to do analytics that will allow them to take advantage of the data they are collecting?"

Read more on how Dell EMC can help federal agencies better prepare for IoT's potential, and manage through the convergence of IT and OT.

This article was written and produced by fedscoop *for, and sponsored by,* DELL EMC.