Mr. CTO, Tear Down This Wall! : Ushering In A New Era Of Industrial IT/OT Convergence

To achieve real digital transformation, industrial CTO's must unite IT and OT.

The divide between information technology (IT) and operational technology (OT) wasn't always a big deal. In simplistic terms, the IT department dealt with the flow of information, while the OT department managed the factory floor, and there wasn't all that much reason for the two to meet in the middle. That picture has now changed — dramatically. Connected industrial equipment is no longer a novelty, and with prices dropping, the IDC predicts that by 2021 some 90% of manufacturers will deploy IoT devices into their operations.

As a result, IT functions are rapidly becoming relevant to OT, and vice-versa. With the line between these two disciplines blurring, it's becoming harder to justify the organizational division — and all the more necessary to unite these teams beneath a single masthead. The answer lies in redefining these departments and equipping them to succeed with tools that truly take advantage of the IoT's potential.

The New OT

Within any given industrial company, the OT department is essentially the team on the factory floor. They manage the operational technology — the hardware (and increasingly the software) that directly monitors or controls physical devices and processes. Earlier iterations of Industrial Control Systems (ICS) have included supervisory control and data acquisition (SCADA) and distributed control systems (DCS), but these systems haven't traditionally been internet-connected, and have been geared toward performing functions rather than generating data.

But now a new technological wave, the Industrial Internet of Things (IIoT), has brought data into the historically analog realm of OT. The new OT includes networks of connected devices that can gather, analyze, and exchange data, monitor equipment, self-diagnose, and ultimately allow operators to control the factory floor. Tools can be tracked with RFID chips. Equipment sensors continually send data to analytics platforms. The software automates machinery for safety and efficiency.

Ideally, implementing IIoT devices has a number of advantages. OT can do their jobs more effectively, with greater insight into internal processes. The new OT can produce safer, more secure working environments — with sensors to detect and prevent equipment malfunctions, and alarms to prevent break-ins.

Why the Disconnect Exists

And yet, unlocking these new capabilities isn't an entirely straightforward affair. Data is traditionally IT's domain, and it isn't necessarily easy for IT and OT to share turf or even speak each others' languages. They come to the table with different priorities, expectations, and assumptions.

An oft-cited challenge is that of software/hardware patches and security updates. IT teams are used to this kind of periodic maintenance; if a system temporarily goes down for updates, it tends to be manageable. Not in the world of OT, where shutdowns (even planned ones) can mean substantial losses — even a single minute can equate to tens of thousands of dollars. Naturally, OT teams have historically put a great deal of effort into squeezing every last ounce of uptime out of their production lines. These sorts of differing perspectives can lead to conflicts that prevent productive working relationships.

The disconnect between these departments is something of a historical one — one that persists on the longevity of certain ingrained habits. As of 2016, a survey of manufacturers found that only around half of IT and OT teams had collaborated on technical operations issues and security, while fewer than half had worked together on legacy upgrades or linking data to business analytics. Some 8% had never collaborated at all. Those numbers will have to improve to unlock the real potential of the IIoT.

Mr. CTO, Tear Down This Wall!

In a sense, it won't take much for OT and IT to get closer — that's already happening, whether the departments are ready for it or not. What's essential, however, is that these teams are brought together in the right way. Rather than simply allowing teams to manage and resolve their own conflicts, CTOs can orchestrate a convergence that produces a better result, faster.

Many companies think of this convergence simply as a collaborative relationship. They may go so far as to have these two groups of specialists schedule regular planning sessions. Such measures won't go nearly far enough. In an era of (digitally) "transform or die," the challenges of today must be addressed today. What are the standards around security issues? Who's responsible for procurement? Who's in charge of managing vendors? How are IIoT investment budgets allocated across departments? On a workflow level, operational restructuring — where those departments are brought under one roof — would bring responsibilities in line with increasingly critical objectives.

In accordance, it's time for CTOs to ensure the cross-training of personnel. Operational specialists aren't going to start fixing the printers, but if they don't have a firm understanding of how IT supports their work, they won't be able to see the potential for these next-generation devices or manage their use. Meanwhile, IT may have to "get their hands dirty" in order to bring truly innovative IIoT solutions to the factory floor. In practice, that will likely take the form of a single, fully integrated team — headed by a truly dual-disciplinary CTO. Ultimately, we're talking about upskilling and re-skilling the teams of the technologists and engineers responsible for making factories run.

What's Possible with IT/OT Convergence

Even when IT and OT are "on the same page," there often remains a crucial missing element. IIoT devices may control individual functions; IT may leverage data resources for business analytics — what's missing is the ability to turn all those continuous streams of technical data into expedient action. This directive calls for implementing the right technologies — count situational awareness software among the most crucial.

A fully equipped industrial space could easily have hundreds or thousands of IIoT devices, including sensors — all from a variety of manufacturers, and designed for dozens of discrete capabilities. All that resulting data might be delivered to OT team members through a number of different applications, or perhaps stored in the cloud for later IT analysis. There are a number of possible configurations for these data flows, but they aren't all equally actionable.

With a situational awareness platform, however, everything from mobile industrial robots to humidity sensors can be united through powerful applications for simplified management and collaboration across all relevant IT and OT stakeholders.

Rather than relying on OT manually keep track of the growing number of data sources and alerts across the industrial environment, a situational awareness platform can make all that information accessible, digestible, and actionable. In addition, industrial IT teams can customize their applications to automatically push and prioritize urgent action items like gas leaks or duress alarms.

IT doesn't have to reinvent the wheel to make IIoT data as useful as it can be. Existing technologies can be easily integrated with brand new platforms. As the IIoT comes to big industry, many manufacturers will find they cannot simply avoid the competitive advantages that come with adopting these technologies.

To unlock these advantages, organizations must chart a new path toward an era of IT/OT convergence. Interdepartmental understanding will represent the bare minimum requirement for survival; the most successful organizations will achieve comprehensive situational awareness across IT and OT.