AUTOMATION.COM

Advancing Automation

February 2020

The Dangers of DIY Connectivity

How an integrated IIoT suite supports digital transformation

Sponsored by:

ptc

The Do-It-Yourself Dangers of Industrial IoT

By: Renee Bassett

CIOs understand that digital transformation is necessary. An Industry 4.0 cyber-physical connection can turn real-time data into real-time information that supports immediate problem solving and optimized decision making. But digital transformation isn't just about connecting Industrial Internet of Things (IIoT) devices, moving data to the cloud or leveraging machine learning. Industrial operations need network connections, contextualized data exchanges between systems, and a framework for adapting to inevitable change.

> The point of digital transformation isn't any one project or even any combination of projects, stresses Amit Zavery, VP of engineering for Google Cloud. The point is "to achieve an ongoing state of IT agility that lets an enterprise continually adapt to changes."

According to Deloitte's Tech Trend's 2019 report, advanced connectivity is "fast becoming the linchpin of digital business: proliferating mobile devices, sensors, serverless computing, exploding volumes of shared data and automation all require advanced connectivity and differentiated networking."

"Connectivity of tomorrow," continues Deloitte, will mean that one of the primary responsibilities of an industrial CIO will be getting data from where it is collected, to where it is analyzed, to where it is needed to drive automated operations—"at scale and at speed, in a data center, in the cloud, or increasingly on the edge, at the point where business occurs and missions are realized."

Contextualizing the data that Industrial IoT (IIoT) devices gather is another essential step on the path of digital transformation. LNS Research has highlighted the journey that Manufacturing Operations Management (MOM) systems are taking as they add context to become an integral part of IIoT-based systems and solutions. The integration of operational technology (OT) and the Information technology (IT) used by enterprise systems is moving

companies away from monolithic legacy MOM systems to “a new paradigm where most of the functionality will be delivered as IIOT apps,” says LNS.

“Those who work in a world of MOM are in a better position than many others making their way in the IIoT,” adds LNS analyst Andrew Hughes. “The ISA-95 standard has served us well, and the technical experts of the ISA are working to bring together existing control systems and the new IIoT devices and apps with new data and communications protocols.”

Standards can help, but industrial CIOs also need partners, like third-party connectivity specialists and integrated IIoT application experts. Partners mitigate the dangers of a do-it-yourself (DIY) approach to IIoT by sharing the load, reducing the risk and enabling agility, which is at the heart of digital transformation.

The point of digital transformation isn’t any one project or even any combination of projects, stresses Amit Zavery, VP of engineering for Google Cloud. The point is “to achieve an ongoing state of IT agility that lets an enterprise continually adapt to changes.”

Let’s look at some of the challenges of connectivity and data integration, and how those challenges can become DIY dangers. Then we’ll look at some of the partners who can reduce the risk.

Challenges of Connectivity

Building communications drivers and other connectivity components for industrial systems is fraught with challenges. The industrial control and automation industry started with proprietary control systems running on central computers that were hardwired to field devices. This evolved to distributed controllers connected over proprietary networks.

Adoption of new technology for industrial automation lagged behind the computer industry because industrial automation suppliers initially preferred their proprietary hardware and software, says Automation.com’s Bill Lydon. “Over time, smaller computers and PCs distributed functions over networks, and distributed computing has been refined in many ways with Service Oriented Architecture, HTTP, Remote Procedure Call (RPC), XML, and other functions,” says Lydon. But the integration of legacy equipment is slow and can be costly.

> The biggest challenges of connectivity is the high cost of tying together a disparate set of IIoT devices into a single solution.

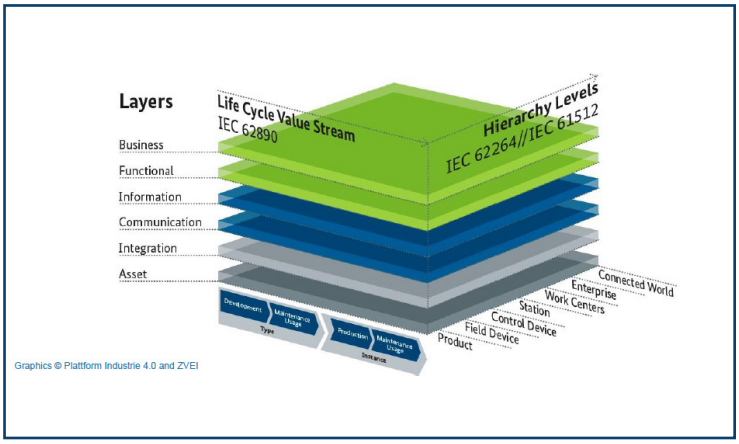
“IIoT was not even known when more than 90 percent of the current equipment assets were installed,” says Paul Nowicki, information design engineer at packaging equipment maker Heat and Control. “It takes a deep understanding of each individual equipment asset to determine what information to acquire and how to get through the low-level communications to make it available. This requires lots of detailed engineering, for which many manufacturers either do not have the manpower or expertise to build out. It makes the process of data integration slow and expensive.”

Another big challenge is IT and OT personnel collaboration, says Nowicki. “IT and OT people have very different priorities which often conflict (i.e, security versus interoperability). They have established two camps that rarely work together but now must in order to make IIoT work.” Different concerns over security are a big source of conflict, he adds.

Development of information models such as the ANSI/ISA95 standard, OPC-UA companion specifications and others were an important connectivity advance, says Lydon. These provide the framework, modeling, and vendor-independent common information models that can be applied in any manufacturing or process industry production architecture.

But standards are continually evolving, and competing standards emerge. RAMI 4.0, Reference Architecture Model for Industrie 4.0 (Industry 4.0) is a newer industrial automation that started in Germany and now has many worldwide cooperative efforts including ones in China, Japan and India.

Hughes says manufacturers embarking on a digital transformation journey will get inundated with new technology and a potential clash of standards. “The Industrial IoT does not live alone,” he says. Consumers and business Internet of Things (IoT) users also have many layers of standards like IPv4, IPv6, JSON, and Web Things for semantic definitions of apps and their data, Hughes says.



RAMI 4.0, Reference Architecture Model for Industrie 4.0 (Industry 4.0) is a newer industrial automation that started in Germany. Source: Platform Industrie 4.0

“There are many standards to look to, but they are rapidly evolving, so today’s solution may not be the solution that is available in five years,” says Dennis Brandl. “It is important to recognize that, like industrial security, approaching IIoT is a journey.”

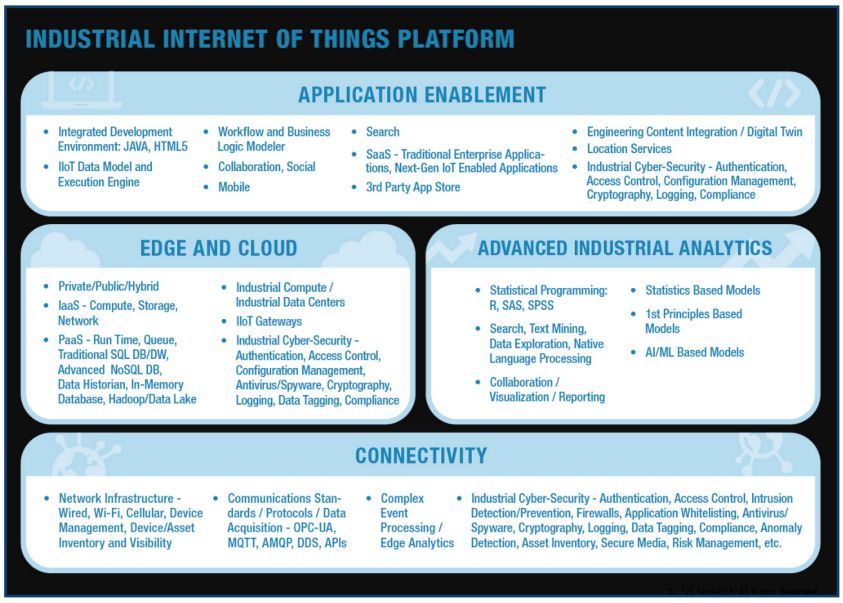
As a consultant specializing in Manufacturing IT and an active member of ISA’s SP95 Enterprise/Control System Integration committee, Brandl is keenly aware of the separate standards and many IIoT activities going on. Almost all are driven by vendors in very specific market niches, he says, but it’s end users who need to combine the different vendor niche products into a single system.

“This is hard and expensive work with the state of the art today. The biggest challenges of connectivity is the high cost of tying together a disparate set of IIoT devices into a single solution,” Brandl says.

Challenges of Data Integration

When it comes to integrating IIoT data to create actionable information, additional challenges arise. Functional fit varies from application to application. “How can you find the common abstract model from the forest of individual trees?” asks Nowicki. “It is sometimes overwhelming.” Information models really help by “showing how to model out the common abstract functional parts,” he says, but even with them and fully compliant MOM systems, results vary when users try to combine data from different sources. Says Brandl, “In this case, we don’t know what we don’t know.”

Many of the IIOT solutions focus on improved maintenance through early warnings, Brandl explains. “There are those looking to find patterns in their production that they have not been able to see, because they can collect more data. I think that the biggest challenge is



Components of an IIoT platform encompass basic connectivity, data analytics and application enablement. Source LNS Research

understanding what you will be able to do with more integration of data and finer control of processes."

"We are approaching the age where we will be able to solve problems that we have considered were unsolvable, and doing that requires good data and common references," Brandl adds. "All data, in the IIoT space must include the context of the data (units of measure, time and time zone, etc.) in order to have successful data integration."

Top 4 Risks of a DIY Connectivity Implementation

Given the challenges of physical connectivity and data integration, considerably more risks emerge when you decide to tackle IIoT connectivity yourself rather than use a third-party connectivity expert or other resource.

Future-Proof or Failure-Prone?

	DIY	Third-Party
Implementation	Months to years	Hours to days
Maintenance	Months to maintain	Minutes to upgrade
Scalability	One-off connectivity	Scalable connectivity
Security & Reliability	Dependent on internal expertise	Independently tested; adheres to industry best practices

1. Lengthy time to implement
With potential industrial IoT projects on hold, players across the enterprise standing by, and your competitors getting ahead, a DIY implementation that takes months to years could delay your goals. Does it make sense to wait for your data, especially when implementing a third-party connectivity solution could take a matter of days—or less?

2. Continuous maintenance
Bugs, new features, and security updates are nothing new. But maintenance is no longer routine when it takes months to complete. For manufacturers who've implemented a third-party connectivity application, maintenance becomes a matter of minutes—and doesn't require the support of your in-house, in-demand IT team.

3. Lack of scalability
As your plant floor grows or changes, your connectivity implementation will need to grow, too. Unfortunately, the more assets, equipment, and software you add, the more development an in-house build requires to keep up. Using a third-party connectivity application with a wide breadth of connectivity to modern and legacy assets ensures that you're scaling from the start—and that changes to your environment don't stall operations.

4. Insecure and unreliable connectivity
With DIY connectivity that relies on in-house resources to maintain, security and reliability become critical concerns. On a good day, machine vulnerabilities and failures can lead to data loss and downtime. On a bad day, they can compromise worker safety. With that in mind, manufacturers are taking a more active role in security and reliability by choosing a secure third-party connectivity solution.

Source: Bates, Jeff, and Abby Eon. "The Edge: Providing the 'Things' for the IoT." Lecture, LiveWorx 2019, Boston, MA, June 13, 2019

Partners on the IIoT Journey

Digitally transforming industrial operations involves becoming agile—which is an entirely new approach for most business, especially industrial businesses. This agility starts with IT architecture, says Google's Zavery, but that doesn't mean cloud vs. on-premises deployments of huge, monolithic applications. Rather, he talks about small independently deployable "microservices" and parallel development teams that can quickly build and release new features and functions.

Parallel development teams can be formed with partners. They can take the form of a system integrator who specializes in data integration, for example, or a maker of a pre-integrated IIoT application suite specific to your vertical industry. "The best would be a system integrator that has experience in your business, and therefore also knows the type of IIoT devices that could be used," says Brandl.

Another type of partner is third-party connectivity specialists like PTC/Kepware. "If we see anything in the IIoT world, it is that the pace of change continues to accelerate. The only ones that can keep up with the technology advancements are those whose business it is to do so—the vendors providing connectivity," says Nowicki.

Users should leverage such suppliers and not build one-off, proprietary connectivity solutions, as those solutions will be outdated before they are fully implemented. "Suppliers like PTC/Kepware make it their business to always be looking to turn tomorrow's technology advancement into today's useful tool," Nowicki says.

One system integrator knows where his expertise lies, so his company partners with PTC/Kepware for connectivity. Tony Harris is president & CEO of e-Magic Inc., specialists in the global design, development and integration of large scale Industrial IoT systems that run on-premise or in the Microsoft Azure Cloud. E-Magic applications include centralized operations, smart buildings, facilities and cities, smart manufacturing, industrial production and artificial intelligence for prediction and optimization.

e-Magic was founded by Tony Harris and Eugene Woo who were 1980s pioneers of SCADA-linked artificial intelligence technologies—such as expert systems, neural networks, machine learning and genetic algorithms—that could control and optimize industrial plants and facilities. Today, e-Magic focuses on centralized control for facilities of all types, bringing a central system and dashboards, command and control and two-way communications to HVAC, lighting and power systems.

"We layer on intelligence and artificial intelligence (AI) for optimizing control of these systems," says Harris. "We're a Microsoft partner. We're building cloud-based systems on AZURE. And we use the Kepware IoT tool for bringing in the data and establishing the connectivity."

Connectivity is a big and important business, says Harris, and "it's expensive to build your own APIs [application programming interfaces]. The time investment is huge. The cost of taking resources off other jobs to do the connectivity is huge. Then there's a lack of resources. And then there's the maintenance aspect."

How do you talk to things? How do you talk to lots of different things? With lots of different protocols—each of which has to be monitored and maintained. "We have projects right now that require one-off APIs—for sound systems and speakers. Either [the sound system vendor] doesn't have an API, or they don't have a good one. People will build an interface for the scope at the moment, but it's not scalable. It's not maintained. And then I've got to worry about it," says Harris.

Kepware [ThingWorx Kepware Server] APIs are multithreaded so each port is separate, Harris explains. Most people who build their own systems don't think of things like that, he contends. So, if e-Magic needs an interface and Kepware has one, "we will use it every time," says Harris. "Feature-set-wise, Kepware [ThingWorx Kepware Server] blows everyone else out of the water."

> Connectivity is a big and important business, and it's expensive to build your own APIs.
> —Tony Harris, president & CEO of e-Magic Inc.

Connectivity is hard

Digitally transforming industrial operations is essential, and the connectivity that underlies and empowers digital transformation is hard. The network connections and contextualized data exchanges between systems that industrial operations need require lots of different protocols—each of which has to be monitored and maintained. Doing it yourself can be a challenge and an expense. Third-party partners make it easier. Knowing they can trust their connectivity partner, system integrators and CIOs can focus on transforming their business.

Partners in Connectivity.

Heterogeneous industrial connectivity is one of the big challenges for creating a truly connected digital factory. PTC's portfolio of Industrial Internet of Things (IIoT) technology includes ThingWorx® Kepware®* Server, a component of the PTC ThingWorx® IoT technology platform. This integration enables users to combine external data inputs with industrial controls. Machine data can be aggregated into the PTC ThingWorx platform, integrated with a wide array of internal and external information, and then automatically analyzed using ThingWorx machine learning capabilities. Organizations can then gain enterprise-wide insight and to proactively optimize mission-critical processes to improve operational performance, quality, and time to market.

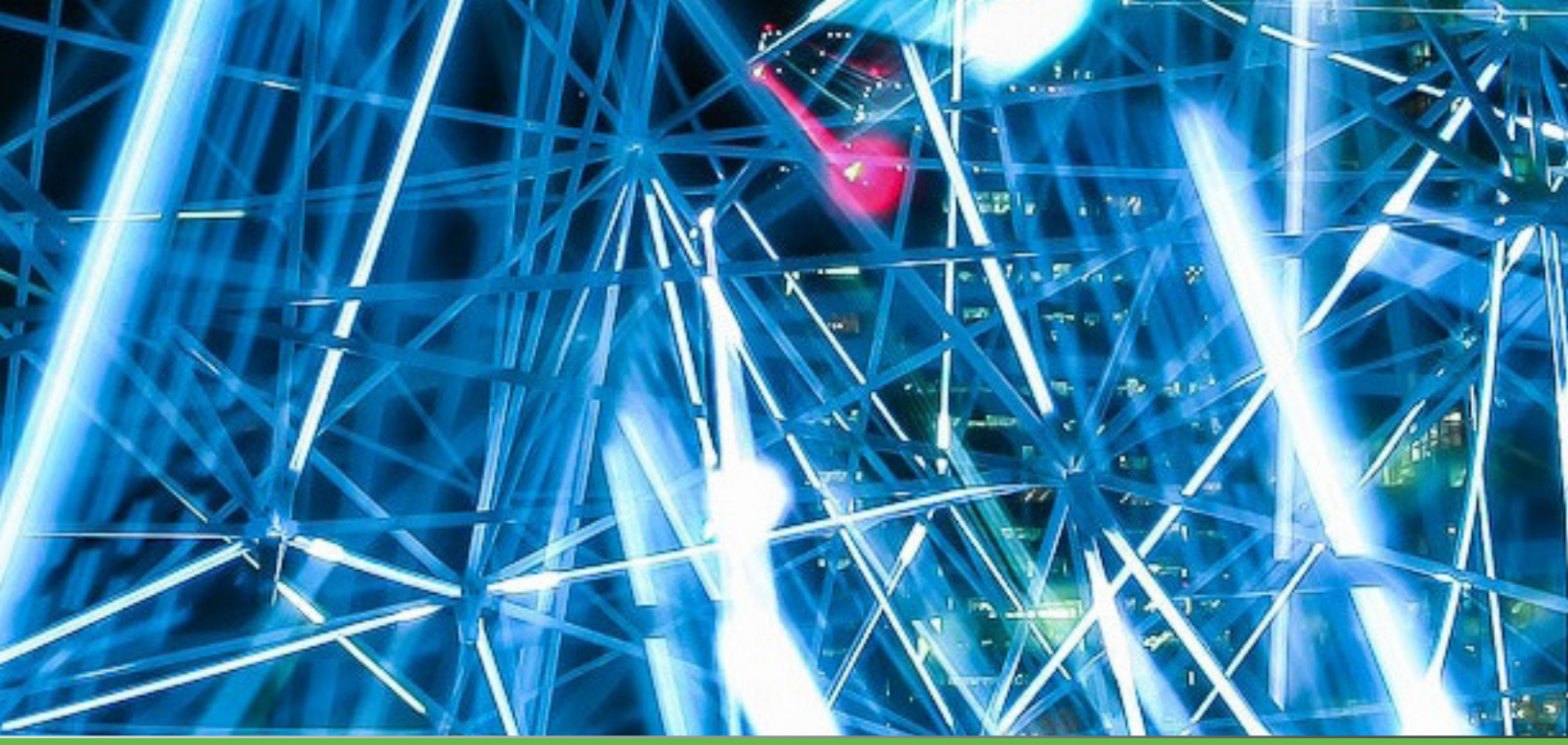
> Partners come in all sizes, ranging from Microsoft to PTC to specialized system integrators.

Find out more at www.ptc.com

*KEPServerEX is now ThingWorx Kepware Server."

About the author:

Renee Bassett
is chief editor of Automation.com and InTech magazine, publications of the International Society of Automation. Reach her at rbassett@isa.org.



How an Integrated IoT Suite Supports Digital Transformation for Industrial Companies

By: Stacy Crook, Research Director, Internet of Things, IDC

Introduction: IoT Underpins Manufacturing DX

There will be 41.6 billion Internet of Things (IoT)–connected devices worldwide by 2025, according to IDC's Worldwide Global DataSphere IoT Device and Data Forecast, 2019–2023, and the largest share of these devices will come from the industrial space. IoT data is also expected to grow exponentially, from 13.6ZB in 2018 to 79.4ZB in 2025. This data is key to fueling digital transformation (DX) initiatives, especially within asset-intensive industries such as manufacturing. According to IDC, the top three factors propelling near-term IoT investment in the manufacturing sector are boosting product quality, reducing operational costs, and driving internal efficiency and productivity.

IDC Technology Spotlight

This IDC Technology Spotlight is sponsored by PTC and was originally published in January 2020. It discusses the opportunities presented by the industrial Internet of Things (IoT) and the challenges manufacturers have to overcome on their IoT-enabled journeys to digital transformation (DX). Author Stacy Crook is a research director with IDC's IoT Ecosystem and Trends Research Practice.

IoT data can enable companywide transformation by improving factory operations, providing a new level of supply chain visibility, and offering a digital feedback loop for engineering. Sales and marketing can drive targeted campaigns and upsell new products based on real-time customer data. The service arm of the organization can use IoT data to provide more proactive or better-targeted services to customers. Many manufacturers are assessing how they can offer their products in a services-based model moving forward; IoT also serves as a key enabler of this DX goal.

Challenges to Capitalizing on DX Goals

IoT has a significant role to play in the DX goals of industrial organizations. However, IDC has found businesses often face a series of technical and organizational challenges that hinder time to value.

Technology Challenges

The inherent complexity of the environments from which IoT data is collected causes many technical challenges. For example, consider a common manufacturing plant with multiple streams of data to analyze. These data streams can come from a variety of systems that each speak their own communications protocol. This creates issues around integrating and analyzing data at the edge, as well as in sending that data into cloud systems that need to accept it in IP-ready formats.

According to IDC's latest Global IoT Decision Maker Survey, security continues to top the list of IoT project inhibitors. In the industrial environment, many manufacturers have traditionally had separate technology systems for their operational technology(OT) environments and their information technology (IT) environments. The IoT has now created a communication link between the two. Organizations must be very careful to ensure that both environments and the network between them are highly secured so that the communication pathway does not become a point of vulnerability. While the IT environment typically has many security layers to protect endpoints, networks, and data, this rigor also needs to be applied in the OT environment. Some IT security solutions can have relevance in the OT world, especially as it becomes more IP enabled, but the proprietary nature of brownfield OT equipment means there will also be a need for OT-specific security solutions.

Data integration, management, and analytics represent additional challenges. IoT architectures usually require a combination of warm path storage and cold path storage to support analysis of both streaming data and historical data. While many companies have some kind of big data architecture in place, adding a streaming element to that is a new undertaking. IoT devices can generate a ton of data, so organizations need to decide how much data to store, how long to store the data, and the storage mechanism. A determination must also be made about where to perform the analysis: at the edge (meaning close to where the data was generated) or at a more centralized datacenter. Previously, we discussed the data integration challenges at the edge; this obstacle has to be overcome to then analyze the data.

Another consideration is how to integrate events generated by the IoT analysis system with other business systems to enable an action to be taken. Deployment complexity — or the fear of it — is another common roadblock cited by IDC survey respondents as IoT projects tend to have a large systems integration component.

One of the biggest IoT project hurdles is moving from pilot to production. While many organizations have started IoT projects, an average of only 25% of IDC survey respondents are currently in production with them. After security, scalability of the new technology was the second most frequently cited factor preventing organizations from moving into production mode.

Business Challenges

Organizations also struggle with business-related issues when they embark on IoT-oriented DX projects. One of the first issues is creating organizational alignment around a common vision and plan for IoT. If a company doesn't take this step, it runs the risk of having individual business units make their own technology decisions, which is not cost efficient, doesn't scale well, and leads to uncertain goals and success metrics.

Once there is a centralized vision for IoT, the next step is deciding which project to start with. IDC recommends that businesses undertake a comprehensive process to determine all possible IoT use cases and then build a road map based on expected return on investment (ROI), feasibility, and how a case fits with the broader DX strategy. Going through this process will help ensure that technology choices align with near-term IoT projects as well as future projects.

A classic challenge many companies face with new technology projects is the “build or buy” decision. Sometimes, in a very new market such as the IoT, there may be limited products to procure off the shelf; however, as technology markets mature, the options to buy packaged solutions tend to increase.

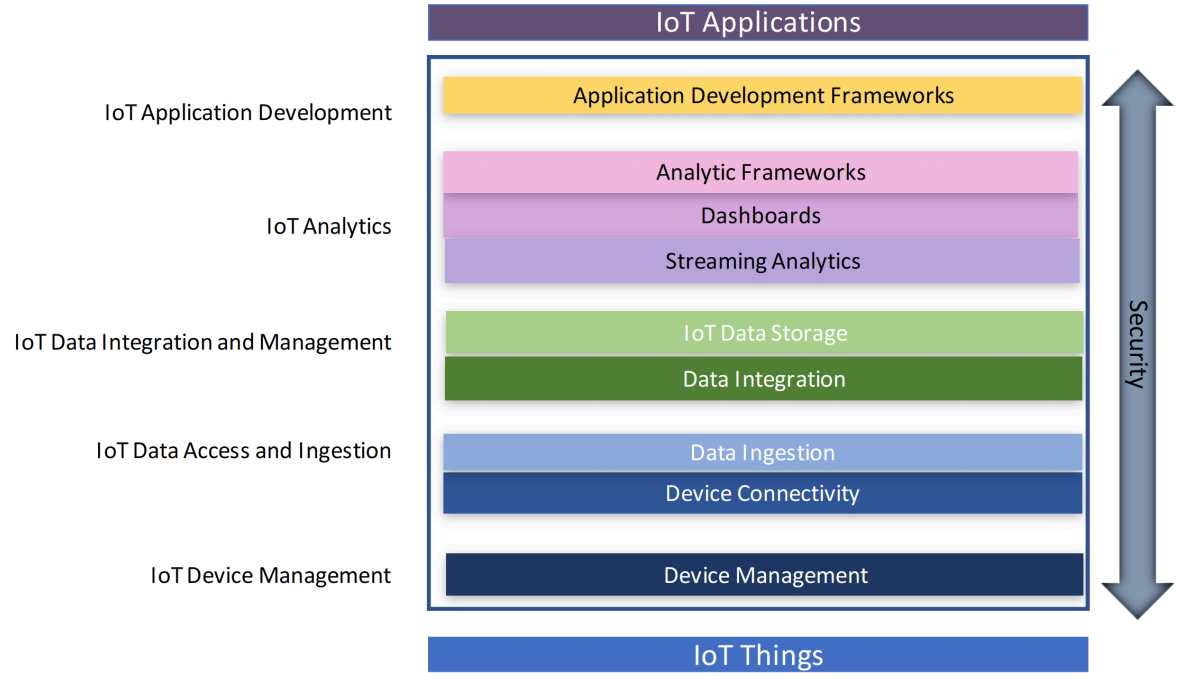
That being said, cost is the number 1 factor holding back progress on IoT projects, according to survey participants. These projects generally require hardware, software, connectivity, and integration services, so there are multiple angles to the expense factor. Costs can vary significantly based on the use case, existing infrastructure, and the architecture in which a solution is deployed.

There are also significant people and process factors that go into creating successful IoT projects. In the industrial environment, new technology can create a major change in the way people do their jobs. Organizations must manage the fear of change by sharing how technology can improve job responsibilities. New solutions often require some new skill sets to manage the infrastructure and the data and to make that data actionable. Businesses need to set up programs to reskill employees where appropriate and ensure that HR is attracting the right candidates for new roles that may emerge.

IoT Application Considerations

As businesses embark on their IoT journeys, the technical aspect of enabling IoT applications becomes an important consideration. Developers need tools and services to build, deploy, manage, and secure IoT applications and software. The technology stack contains data access and ingestion, data integration/management, device management, application development, and analytics capabilities as shown in Figure 1.

FIGURE 1: ***Technology Stack for IoT Applications***



Note: This diagram is meant to be edge/core agnostic.

Source: IDC, 2020

Organizations that build their own IoT application base will need to integrate these components together and then manage each one independently throughout the life cycle of the deployment. They will also have to manage the infrastructure on which the services are deployed, which becomes increasingly difficult as organizations move toward hybrid models. These two challenges can make it difficult to scale in this type of model.

Benefits of Buying a Packaged IoT Application Suite

IDC's research finds that 90% of manufacturers use key performance indicators to measure the outcome of IoT projects. ROI is one of the top metrics used to measure a deployment's success. Although the expected benefits vary from project to project, the ability to get ROI on any technology implementation rests on the ability to get the solution up and running in a timely fashion without blowing the budget. Another related measurement is the total cost of ownership (TCO). Of course, TCO will be impacted if a company spends more than it allocated for a project, but it can also be influenced by other factors, such as an unexpected security incident. Given the inherent complexity and heterogeneity of the IoT environment, manufacturers are advised to simplify deployment wherever they can.

Many software elements are required to support an enterprise IoT application. In the early days of the IoT market, organizations tended to procure those pieces on a one-off basis and build their own application back end. However, this approach typically presented a major integration project in the near term and required a significant effort to maintain in the long term. Both of these factors are impediments to ROI and TCO. This method also introduces security risk, especially if the components come from different open source projects or vendors and do not sit upon a common security architecture.

The alternative is to buy a pre-integrated solution. IDC has observed the following benefits within enterprises that have taken this route:

Faster time to value

- Building a back end for an IoT application is a complicated, time-consuming task. Purchasing a pre-integrated solution allows developers to spend less time on the application plumbing and be more efficient in building the application functionality that will help the company reach its business goals.
- While many companies start with a single use case, the real value of an application suite comes into play when it can be leveraged across the business to support multiple global IoT applications. Therefore, it is important to vet these offerings for applicability across multiple use cases and geographies.
- Consider whether the solution can be leveraged by a variety of personas within the enterprise. While it is necessary for technical people to be involved in architecture decisions, faster time to value can be achieved if nontechnical people are also part of developing the application's business logic.
- Working with a vendor that has domain expertise can help companies avoid common pitfalls.

Reduced TCO

- A company that builds its own IoT application base must deal with not only the time and cost spent on the initial development but also the expense of maintaining each of the components over time. A business that buys a packaged solution is responsible only for maintaining a single code base.
- TCO can also be reduced by how organizations choose to deploy and maintain the code base. For instance, a managed cloud service based on a serverless event-driven architecture can save money on infrastructure because the server spins up compute resources only as needed. It can also save on operations because the cloud company—instead of an internal member of the IT operations staff—is responsible for spinning up those compute resources.
- Beyond the code base, companies that partner with a solutions provider can take advantage of the latest features and security patches to ensure they are staying current with the solution versus needing to maintain the solution on their own.

- It is expensive to hire and maintain staff for a series of one-off custom applications; deploying a common framework organizationwide can help alleviate this issue.

Reduced risk

- Complexity is the enemy of security, so the fewer separate software products a company introduces into its environments, the better.
- When choosing an IoT application suite, have the CIO/CISO organization vet the offering for high scalability, availability, and reliability; a common control plane to manage data across the cloud/core/edge; and a common security framework. Make sure secure application development practices are followed.
- Risk can also be reduced by selecting a platform that allows employees to maintain their focus on the highest-value tasks, such as building a strategic architecture to support the business or focusing on revenue-generating activities.

Considering PTC + Microsoft

Finding synergies within their respective IoT portfolios, PTC and Microsoft formally partnered in 2018. The companies offer a joint reference architecture for leveraging ThingWorx on the Azure cloud and have built integrations between the products to make deployment as simple as possible.

PTC is a global software company focused on helping industrial organizations take advantage of the innovation found at the intersection of the physical world and the digital world. In the IoT space, PTC offers its ThingWorx IoT solution platform and a suite of IoT applications, some of which tie into its other engineering and service life-cycle management products. Microsoft is one of the world's largest software companies with a portfolio that spans infrastructure, application development and deployment, and applications. It has a broad IoT product suite, much of which is based on the Azure cloud but that also ties in with other parts of the business such as the Dynamics portfolio.

Finding many synergies within their respective IoT portfolios, PTC and Microsoft decided to formally partner in 2018. The companies offer a joint reference architecture for leveraging ThingWorx on the Azure cloud and have built integrations between the products to make deployment as simple as possible for customers.

Microsoft Azure IoT

Within the partnership, Microsoft brings capabilities in the areas of scalable IoT cloud infrastructure and IoT and edge device support. Today, Microsoft Azure is located in 55 regions and offers availability for 140 countries. The company is strongly focused on providing the highest levels of security and compliance across the cloud and edge. Support for hybrid architectures is a key tenet of Microsoft Azure; the Azure hybrid portfolio currently consists of Azure Stack to support on-premises workloads, Azure IoT to support IoT implementations, and Azure Arc, an extension of the Azure control plane that enables delivery and management of Azure services across premises and platform. Microsoft is maintaining a rapid pace of innovation with over 1,000 capabilities launched in Azure over the past year.

The joint PTC/Microsoft offering is supported by managed services within the Azure cloud. These include services with the following functionality: enablement of bidirectional communication between IoT devices and Azure (capable of ingesting trillions of messages from billions of devices), scalable data storage for unstructured data, artificial intelligence services and cognitive APIs to help companies build intelligent applications, simple and secure location APIs to supply geospatial context to data, and the ability to process IoT events with serverless code.

In addition, Microsoft offers a number of products and services for IoT and edge device support that can be leveraged within the joint solution. These offerings consist of support for diverse operating systems including RTOS, Windows IoT, and Linux; device SDKs (available for C, .NET [C#], Java, Node.js, and Python); an edge appliance; an edge framework that extends cloud intelligence and analytics to edge devices with a container engine; a security service that securely

connects MCU-powered devices from the silicon to the cloud; a solution that unifies security management and end-to-end threat detection and analysis across hybrid cloud workloads and an Azure IoT solution; and a program that allows device OEMs to certify their edge and IoT devices for Azure.

PTC ThingWorx

PTC ThingWorx is a technology platform designed for the industrial IoT. It provides tools and technologies that empower businesses to rapidly develop and deploy IoT applications and augmented reality experiences.

The ThingWorx architecture consists of three layers: a solution platform, solution building blocks, and applications. These layers leverage Azure for the cloud infrastructure (IaaS) and the individual platform-as-a-service (PaaS) capabilities for scalable device management and storage, as well as specialized functionality, such as spatial and cognitive capabilities.

In the industrial IoT market, vendors must be able to create solutions with functionality that appeal to the line of business while aligning with the architectural principles governed by IT. It often takes a partnership approach to achieve this balance of OT and IT requirements.

ThingWorx Platform Architecture

- PTC breaks down the solution platform into five areas of capability:
  - **Source:** ThingWorx can source and integrate data from control systems, sensors, gateways, and business systems.
  - **Contextualize:** The platform helps organizations structure data in a way that makes sense in the industrial IoT and then enriches that data with contextual information.
  - **Synthesize:** Companies can use the platform to create and analyze simulations of data.
  - **Orchestrate:** Tools are provided for workflow composition.
  - **Engage:** ThingWorx enables the creation of engaging applications.

- Solution building blocks are reusable components that organizations can develop once and then leverage across multiple applications. They include things such as domain models, calculation engines, common domain logic, prebuilt workflows, and user interface (UI) modules.
- PTC offers applications and solutions in the areas of service optimization, product and service innovation, engineering excellence, sales and marketing, and manufacturing efficiency. It offers these applications on its own under the ThingWorx brand and in partnership with Rockwell Automation, based on the Rockwell Automation FactoryTalk Innovation Suite, powered by PTC.

Challenges for PTC and Microsoft

The IoT market is complex, and even companies that have been very successful in delivering other software solutions to market have found this space particularly challenging. In the industrial IoT market, vendors must be able to create solutions with functionality that appeal to the line of business while aligning with the architectural principles governed by IT. It often takes a partnership approach between two or more technology vendors to achieve this balance of OT and IT requirements.

With that said, technology partnerships can also be challenging for vendors to maintain. PTC and Microsoft need to keep their road maps aligned, coordinate their sales and marketing efforts, synchronize their channels and, most importantly, jointly manage the success of customers. Both parties must be equally willing to commit the time and resources required to make a partnership work.

Conclusion

Manufacturers can reap benefits from IoT throughout their organizations, but they need to take a methodical approach that includes considerations across people, process, and technology.

Organizations should consider how the technology choices they make will impact their time to value, TCO, and risk posture.

An organized approach to IoT is important given the range of use cases it can enable, the large number of stakeholders involved, and the various layers of enterprise and operational technology on which it depends. Organizations should consider how the technology choices they make will impact their time to value, TCO, and risk posture.

When organizations embark upon new technology projects, one of the first questions that come up is whether to build or buy the desired capabilities. For an industrial IoT project, enterprises should consider how they will gather data from the various IoT "things" in the environment, how they will integrate the data, and where they want to process and analyze data (for many companies, it will be both at an edge location and in the cloud). They also need to think about modeling the data so applications can use it, storing the data, managing all of the disparate IoT devices, and building engaging application logic and workflows. This kind of reusable application base with parity across the edge, core, cloud, and multicloud is challenging to create and maintain, even for a software company. In addition to technical complexity, the do-it-yourself route exposes the business to various risks that can seriously impact the overall TCO and ROI of the project. For many organizations, choosing to rely on trusted technology partners to handle this complexity will allow them to apply more focus to their own core competencies.

About the author:

Stacy Crook, Research Director, Internet of Things

Stacy Crook is a Research Director with IDC's IoT Ecosystem and Trends Research Practice. In this role, she provides coverage of key software trends across the IoT landscape, including the platforms organizations leverage to manage IoT endpoint devices and connectivity; collect, process, visualize, and analyze IoT data; and integrate IoT data into other applications, systems, and services.