IDC TECHNOLOGY SPOTLIGHT

Sponsored by: PTC

This IDC Technology Spotlight 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).

How an Integrated IoT Suite Supports Digital Transformation for Industrial Companies

January 2020

Written by: Stacy Crook, Research Director, Internet of Things

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 3 factors propelling near-term IoT investment in the manufacturing sector are boosting product quality, reducing operational costs, and driving internal efficiency and productivity.

AT A GLANCE

WHAT'S IMPORTANT

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.

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.

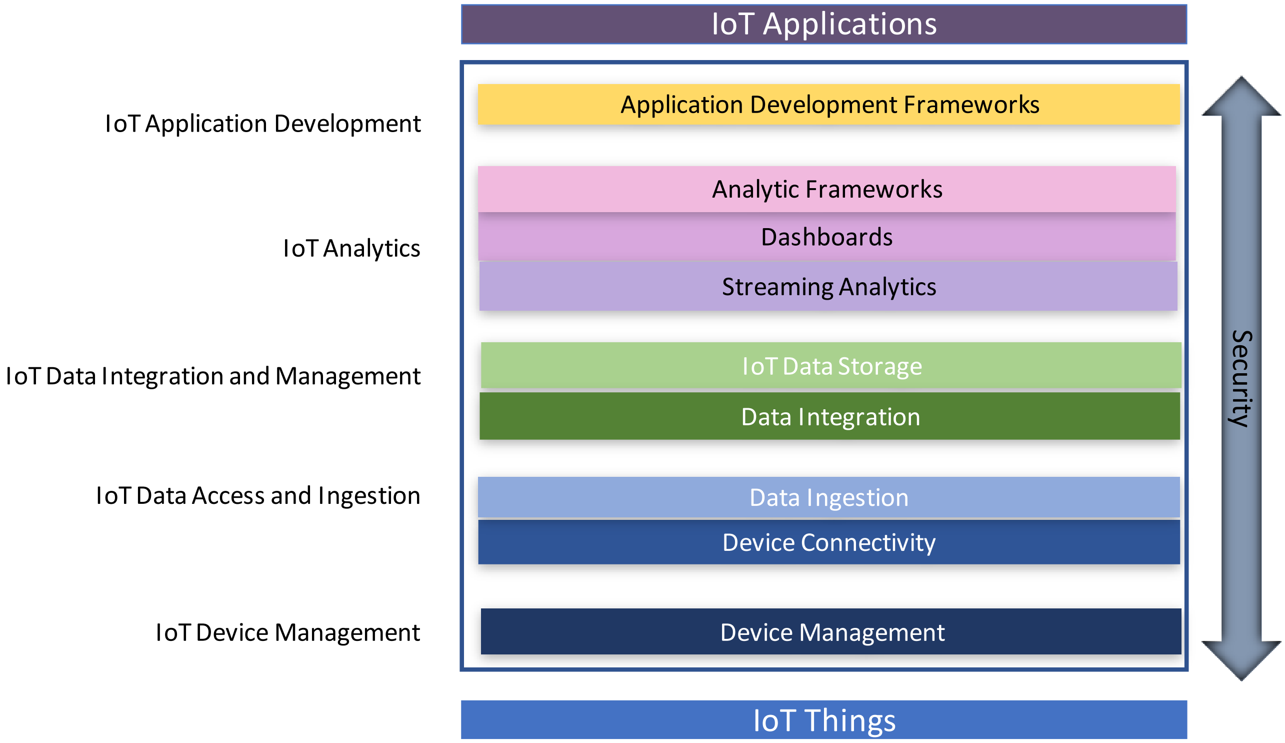
There are also significant people and process factors that go into creating successful IoT projects. In the industrial environment, new technology can create a major change in the way people do their jobs. Organizations must manage the fear of change by sharing how technology can improve job responsibilities. 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.

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.

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



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

Source: IDC, 2020

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

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.

- 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. 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.

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 Analyst

***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.

MESSAGE FROM THE SPONSOR

Together, Microsoft and PTC are bringing together the world's computer (Azure) with the world's leading Industrial IoT solutions (ThingWorx) to accelerate digital transformation across the enterprise. From manufacturing & supply chain and sales & marketing to customer service and engineering, our seamless, secure pre-built intelligent IoT solutions decrease time to value from months to minutes and unlock new growth opportunities for industrial organizations.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.