To Build or to Buy? A Decision-Making Framework for Industrial IoT Solutions

Today's manufacturing plant floor is complex and multi-faceted. Of course, efficient production is the main goal, but there are numerous tools and processes supporting that objective—from legacy equipment to modern Raspberry Pi devices.

The complexity of this infrastructure only compounds as opportunities grow. And as manufacturers explore the industrial Internet of Things (IoT) and its promises of increased performance, uptime and data visibility, it's only logical that they wonder if a third-party is really needed for these benefits or if it would be easier to simply build an IoT-based solution in-house.

ROI is at the heart of this question. Can a third-party IoT platform meet your unique needs and efficiently scale with future growth? Or, is it more cost- and time-effective to dedicate internal resources to develop something fully tailored to your specific needs?

It's not a simple decision. The answer depends on the intricacies of your plant floor, your customers' expectations, upper management's and IT's understanding of your challenges and the offerings of vendor solutions.

But, however unique your plant floor challenges, there are common considerations all manufacturers must examine during their build-or-buy decision process. Thinking about the following industry-wide factors will help you better understand the intricacies of your options and move forward with the best possible solution.

Consideration 1: IoT is an Iceberg.

At first glance, the build-or-buy decision can seem simple. Key stakeholders weigh the options and decide that the answer is obvious—expand current workarounds to create a more connected plant floor, perhaps using some SCADA upgrades and smart sensor add-ons, and voila: in-house IoT.

The build process itself can also be disarmingly simple at first glance—after all, manufacturers have been creating workarounds to collect data for years. Internal IoT builds often focus on the basic framework of connecting all assets and collecting new data. But that new data needs somewhere to go and some way to be analyzed. Dashboards, historical data records, integration tools, and more—these are the user-friendly, data-digestion intricacies of IoT that most people don't think about initially. Yet they are a huge part of the IoT iceberg, waiting to be addressed and often turning into a massive issue after all the easier, high-level work has been completed.

Collecting data is one challenge, but displaying it, analyzing it and otherwise turning it into actionable information is a whole different issue. And IT teams that can solve all of these issues are hard to come by. Even when managing and sharing data can be addressed, the functionality and value of IoT isn't commonly understood by all key stakeholders.

Those with the authority to make the build decision likely won't be involved in the day-to-day operation of the IoT solution. And as a result, they often have a very different perspective than core users—even as they drive the major build decisions that will ultimately form the internal IoT framework.

Best Practice

Think Beyond Connectivity.

When researching and determining whether you will build or buy, involve all levels of users in the process. Examine the ways that your peers are incorporating IoT and what industry experts suggest—both for today's needs, and in the long-term. Think about how data will get to remote users and ways that different roles will need to get specific data—and project that usage into the future, as more data becomes available and more stakeholders need visibility.

Consideration 2: IoT is Often a Victim of its Own Success.

An early consideration in the build-or-buy decision is your in-house software development capabilities. Does your enterprise already employ a team of developers? If so, is the team large and skilled enough to build, support and continuously upgrade the new IoT system you envision? If the answer to these questions is *yes*, then building may be the best option for you. But if supporting the build will require you to add developers to your staff or hire a new development team, building is most likely not a good option.

Even if your IT team has capabilities and know-how to build an in-house platform, they may be the victim of their own success. For as soon as any IoT solution's value becomes apparent, other departments and personnel will want to try their own IoT projects. An in-house solution will always need to be enhanced and will require consistent support—it's not a project that your internal team can simply move on from, but one that will be ever-consuming, in both small ways (like adding new data management widgets) and large (like upgrading for security concerns). And even if you have the size and headcount to dedicate to a homegrown IoT solution, in-house experts are often good at maintaining one type of connectivity—but have trouble scaling beyond initial goals due to limited visibility and knowledge of the enterprise-wide IoT demands.

Best Practice

Build Your Business, Not Your IT Overhead.

When considering ROI, factor in the realistic resources required to not just build, but to perform long-term maintenance and support for an in-house IoT solution. This is likely to take the form of a development team that is solely focused on your IoT solution. This includes making sure security is proactively addressed by internal experts and that your solution keeps pace with the industry-specific features offered by best-in-class vendors' IoT platforms.

Consideration 3:
Speed of Initial Onboarding Can Be Crucial in the Long-Term.

IoT compounds on itself—the more you see what IoT can do for your enterprise, the more IoT uses you will want to explore. This can be a double-edged sword—it means you get more value out of your IoT, but as previously mentioned, it can turn your IoT solution into a victim of its own success. On top of that, this exponential value means that the longer it takes you to onboard, the further you fall behind others who have a faster on-boarding time. Internal on-boarding is typically a long process—the approval internally, then the project management, then timing around potential work interruptions—both at the software installation and connection stages, and during trouble-shooting of any issues. But before you even get to the implementation stage, there is the potential for scope- and time-creep as you figure out how to make the perfect internal solution to please everyone—and meanwhile, other priorities come up, budgets change and headcounts fluctuate. Every big project comes with some management red tape and unexpected roadblocks, but IoT implementations can be especially cumbersome since they usually entail stakeholders learning about the possibilities as they go—and then coming to expect more. In the end, your internal implementation timeline can turn into a roadblock in itself.

Best Practice

IoT Success Starts with Implementation.

Keep timelines in mind at every stage of planning and on-boarding. This could mean starting small and testing IoT initiatives—perhaps with third-party sensors—before building a full solution. It could also mean looking to third-party IoT platforms that provide out-of-the-box connectivity and can be installed with no interruption to uptime—and scaled accordingly, as needed. Getting started with IoT is crucial to keeping up with industry competition, especially at the current adoption rate—18% of manufacturers were already using IoT in 2014[1] , and 70% of manufacturers say IoT is critical to competitive advantage[2]. With careful planning, you can lay the groundwork to future-proof your factory, avoiding complex installation scope creep and setting your plant floor up for long-term success.

> Straightforward applications that can be brought into production are usually built whereas more complex systems and those that may require specialised technologies can benefit from expertise and economies of scale embodied in packages."
>
> - Farhad Daneshgar, "An investigation of 'build vs. buy' decision for software acquisition by small to medium enterprises", *Information and Software Technology Journal*

[1] https://www.sas.com/en_us/whitepapers/iot-analytics-in-practice-107941.html; accessed Sept. 8, 2018.
[2] http://www.verizonenterprise.com/verizon-insights-lab/state-of-the-market-internet-of-things/2016/; accessed Sept. 8, 2018

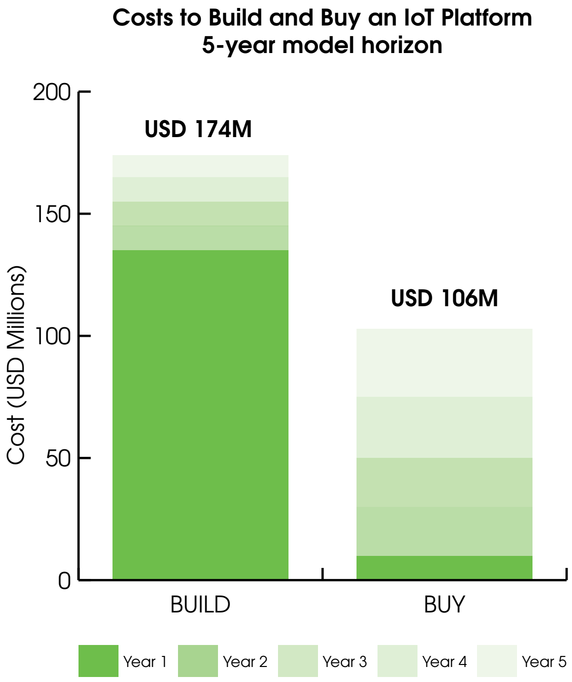
Consideration 4:
In-House Does Not Mean Customizable.

The sheer complexity of the manufacturing production ecosystem is often difficult for upper management and IT teams to understand—and equally difficult for expert plant floor stakeholders to convey. So, while it's logical to assume that an in-house solution would be customizable as needed, the devices, data, and protocols can be overwhelming—and that's before factoring in legacy machine integration and scaling toward future technology. The ongoing demands on your IT team and the difficulty of projecting long-term in a complex industry means that most IoT solutions built in-house will need to focus solely on their original purpose—and should not be expected to grow.

Best Practice

Focus on Your Long-Term Goals.

A long-term perspective will help you determine how complex your new IoT solution should be, how it will need to adapt to future challenges, and whether you will gain the most long-term ROI by building internally or buying an IoT platform.



Source: MachNation, 2016

> For years, my firm helped clients move into Smart Manufacturing through powerful but fairly pricey platforms, whose costs were a barrier to many. But today, there are a wealth of platforms at various cost levels; almost any manufacturer can find a solution to suit their needs."

– Andrew Waycott, Factora manufacturing consultancy COO and CTO; "Five Questions about Smart Manufacturing," *IndustryWeek*

Consideration 5: Security is More Than a One-Time Patch.

IT and data security infrastructures are constant considerations in today's world of ever-evolving technology threats. System security—and who is in charge of maintaining that security—is critical for your IoT data and the software that collects it. An in-house IoT solution must be secure from cyber threats, inaccessible to hackers and fully backed up in case of system failure.

Best Practice

Work with Security Experts at All Stages.

Whether you build or buy, security should be a top concern throughout the process. Ensuring that your internal team has a dedicated security expert—or that your third-party IoT platform has proven security protocols—will keep you ahead of any threats.

Final Considerations

Manufacturers exploring IoT solutions are naturally curious about building their own solution. The idea is logical—internal developers are experts on their specific manufacturing IT needs, and can, in theory, build the best IoT system for the least cost.

Sometimes it works out and a homegrown IoT system delivers as needed. But more often, roadblocks stack up and the internal solution becomes an internal behemoth—consuming more resources, building ever-higher expectations and creating new problems.

The considerations and best practices in this paper were built on industry-wide research and PTC's experience helping manufacturers of all sizes evaluate their IoT options. IT departments and other stakeholders exploring an IoT solution must examine their unique needs—both today and tomorrow—and perform a realistic analysis of scope, strategy and timeline before deciding whether to buy or to build.