

White paper | September 2016



# GUIDE TO IOT SOLUTION DEVELOPMENT

**Target Audience:**  
**IoT Business & Technical Decision Makers**

Companies building IoT Solutions need a structured approach to enhance the development process. Find out key learnings from initial pilot projects along the 5 phases of IoT solution development - including a high-level comparison of major IoT solution vendors.



**IOT ANALYTICS**

*authored by Padraig Scully*

*Knud Lasse Lueth*

# WHY READ THIS WHITE PAPER?

Internet of Things (IoT) solutions are primed to revolutionize the way we do business – but how will you approach IoT solution development at your company?

This white paper guides you through the solution development process to accelerate your IoT endeavors, citing 16 examples from recent IoT projects. The findings presented in this paper are based on a number of executive discussions, customer interviews, an industry survey, internal sample data and desktop research of ongoing and completed IoT projects. The paper also includes several best practices from Microsoft, a leading provider of IoT technology and this paper's sponsor.

The focus of this white paper is on industrial and manufacturing scenarios but the lessons learned can be leveraged by any organization looking to implement IoT. The paper may be most beneficial to IoT Business and Technical Decision Makers (i.e., OEM, ODM, SI, ISV, Solution providers, End-customers).<sup>§</sup>

Insights include:

- **5 phases to structure** your IoT solution development effort.
- **Key learnings** from current IoT projects.
- **A high-level comparison** of 8 major IoT vendors.
- **Deep dives** on 3 important IoT aspects: security, interoperability, and manageability.
- **A detailed IoT solution blueprint example** highlighting the project approach and specific challenges.

**Note: This white paper is based on independent research carried out by IoT Analytics. All views expressed are that of IoT Analytics and not the paper sponsor, Microsoft.**

---

§ OEM: Original Equipment Manufacturer, ODM: Original Design Manufacturer, SI: System Integrator, ISV: Independent Software Vendor

# Table of Contents

WHY READ THIS WHITE PAPER?	2
1 Introduction	4
1.1 The Internet of Things is transforming businesses and industries	4
1.2 Demystifying the complexity in IoT Solution Development	4
1.3 IoT Solution development – Status Quo	6
1.4 Developing an IoT Solution in 5 Phases	7
2 PHASE 1: Developing a sound Business Case	8
2.1 Learning 1: IoT Projects take much longer than anticipated	8
2.2 Learning 2: Organizational & cultural change is often underestimated	9
2.3 Learning 3: The necessary skills are often not available in-house	10
3 PHASE 2: Build vs. Buy and Vendor Evaluations	11
3.1 Requirements Engineering – Understanding what is needed for your IoT Solution	11
3.2 The Build vs. Buy decision	11
3.3 The vendor selection	12
3.4 Comparing key IoT Solution vendors	13
4 PHASES 3-5: Proof of Concept, Piloting and Commercial Deployment	16
4.1 Security	16
4.2 Interoperability	19
4.3 Manageability	20
5 IOT SOLUTION BLUEPRINT: IoT Enabled ADR	23
6 Conclusion	25
Appendix	26
References	28
List of Exhibits	29
About	30

# 1 Introduction

## 1.1 The Internet of Things is transforming businesses and industries

The Internet of Things (IoT) at its most basic level is the idea of connecting any physical object, or “thing”, to the Internet. These connections produce information or data that can be used to create new experiences and improve the way we live and work. The vast implications of billions of interconnected devices are driving a major technology disruption today.

McKinsey estimates the potential impact of IoT to be an aggregated \$11 trillion business opportunity over the next ten years – equivalent to about 11% of the world economy.<sup>[1]</sup>

Organizations across all industries are realizing the huge IoT potential and making strategic investments. In a survey, 96% of senior business leaders revealed their companies would be using IoT in some way within the next 3 years, while 68% said their companies are already investing budgets in IoT solutions.<sup>[2]</sup>

---

### *IoT has matured tremendously over the last 3+ years*

---

- **2013 saw some early market entrants.**
- **2014 was the year of mass awareness of IoT,** mostly focused on enabling consumer scenarios.
- **2015** finally saw the emergence of a number of successful **enterprise IoT pilot projects.**

In 2016 we are currently witnessing widespread IoT solution development. Many organizations are making IoT a strategic priority. These companies are actively exploring new opportunities and identifying the best approach to reap the benefits of their connected product solutions. Whether companies are connecting elevators to the cloud for predictive maintenance or whether they are introducing remote monitoring of industrial machinery – firms are starting to develop compelling business cases for IoT.

---

### *IoT Solution Development brings a new level of complexity and confusion*

---

While there are tremendous potential benefits to IoT, one thing is often apparent during the process: IoT Solution Development brings with it a whole new level of complexity and confusion.

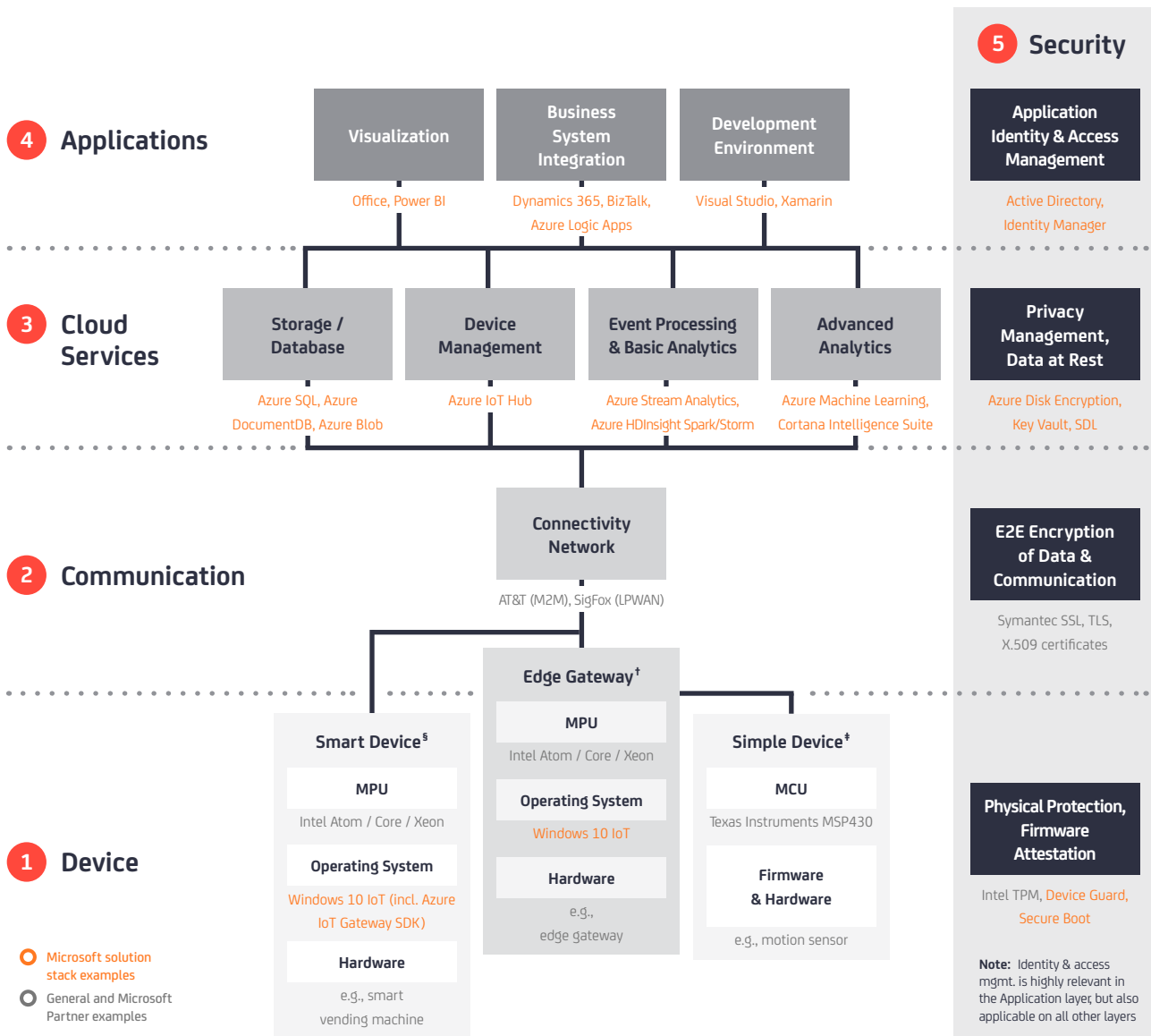
This paper explores some of the learnings of recent IoT projects in order to help any OEM and end-customer successfully guide their way through the challenging IoT development process.

## 1.2 Demystifying the complexity in IoT Solution Development

Developing end-to-end IoT Solutions involves multiple layers that fuse together various components.

*“When we started our IoT implementation effort we had no clue what we needed and who to approach – to be honest, we didn’t even know what we were looking for.”*

**IoT Project Manager at a Machinery OEM.**



**EXHIBIT 1: Generalized 5 Layer Model of an End-to-End IoT Solution** - with a focus on software components (Source: IoT Analytics)

On a high level there are **5 major layers of an IoT solution including one cross-layer:** Device, Communication, Cloud Services, Applications, and Security.

- **1. Device layer:** Adding MCUs and firmware to basic hardware (e.g., sensors and actuators) creates “simple” connected devices. Adding MPUs and OSs makes these connected devices “smart”.

§ **Smart Device:** Enables edge analytics, time-sensitive decisions & local compute. Maximizes security, manageability, interoperability, solutions reliability and reduces bandwidth costs. In many cases, cloud enabled smart devices are equipped with a natural user interface. Note: MPU = Microprocessor

† **Edge Gateway:** May also be classed as a Smart Device.

‡ **Simple Device:** Generates data, performs instant actions & transmits data. Typically has constrained resources, low hardware costs, basic connectivity, basic security/identity, and no/light manageability. Note: MCU = Microcontroller

- **2. Communication layer:** Enabling communication to the outside world through various connectivity networks gives the devices a “*voice*”.
- **3. Cloud Services layer:** Ingesting, analyzing and interpreting the data at scale through cloud technologies generates “*insights*”.
- **4. Application layer:** Connecting and enhancing these insights to the greater ecosystem through a system of engagements enables “*action*” through a vast range of new applications and connected services.
- **5. Security cross-layer:** Securing an IoT solution is an element of such importance that it merits an established “*foundation*” in each of the other building blocks.

Each component demands a particular array of competences and proficiency to function within its own realm, not to mention the varied skillset required in bringing the end-to-end solution seamlessly together across all of these components.

Please see [Appendix A](#) for detailed component definitions.

## 1.3 IoT Solution development – Status Quo

IoT Analytics’ global database of IoT markets shows that approximately 7,700 Enterprise IoT projects have been initiated in the last 3 years – with a large number of projects still in pilot / development phase of the lifecycle.

---

### *More than 3,000 new IoT projects will be initiated in 2016*

---

It is expected that in 2016 alone, more than 3,000 new projects<sup>5</sup> will be initiated.<sup>[3]</sup> Some of these projects only involve a handful of people and are rolled-out to a small number of devices. Other projects involve massive organizational force, with sometimes more than 100 people involved in project roll-out.

It is becoming apparent that both the business case as well as the technical architecture of IoT solutions vary greatly by segment, and more specifically by use case.

For example, connecting remote industrial equipment (e.g., *Rio Tinto’s self-driving trucks* <sup>[4]</sup> in the mining industry) raises vastly different challenges to connecting smart irrigation systems in a Smart City (e.g., *Barcelona’s Smart City Initiative*)<sup>[5]</sup>. Challenges include varying requirements for security architectures, data models or protocol conversion.

Our [database](#) of 640+ Enterprise IoT projects shows there is clearly no one-size-fits-all approach to successful IoT solution development. However, a consistent methodology can guide your organization through the challenging process.

---

<sup>5</sup> Estimate includes IoT projects using modern state-of-the-art IoT platform architecture, based on a bottom up calculation established on known projects from the top 5 leading IoT platform providers and extrapolated to the overall market – centered on IoT Analytics market model for the last 3 years, not including consumer initiated IoT projects.



**EXHIBIT 2: 5 Phases of IoT Solution Development**– Business Case, Build vs. Buy, Proof of Concept, Pilot, Commercial Deployment (Source: Adapted from Microsoft<sup>6</sup>)

## 1.4 Developing an IoT Solution in 5 Phases

To get the best Return on Investment (ROI) from an IoT initiative, the following 5-step-process has proven as a suitable framework for IoT projects.

### 1. Business Case Development

Typically, the business case for IoT is handled by a cross-functional team and approved by business line executives or even the board of directors. It can be a fairly straightforward process, but companies often suffer from insufficient collaboration across the disciplines involved, and a lack of focus when it comes to potential benefits.

### 2. Build vs. Buy and Vendor Evaluations

After establishing what the solution will look like, most companies have a decision to make: Do we build it in-house, or find an external solution partner? The answer is often some combination of both, with internal expertise, technology stack and cost all playing a significant role.

### 3. Proof of Concept

The PoC phase is designed to validate a few key points, not every single detail. The best practice has been to just

start with 1-5 scenarios or feature designs that matter the most to the customer's business. It is important to "think big", however starting small during PoC enables companies to experiment quickly and keep iterating. Achieving a proof of concept in less than a year can be crucial to sustain top-level management support.

### 4. Initial Pilot Rollout

Once the concept is proven, it's time to evolve the scenarios and make sure the IoT solution can be integrated into the broader organization. A big challenge at this stage involves the training of employees to use the system and preparing for any organizational changes the new process will require.

### 5. Commercial Deployment

At this point, as the IoT solution is deployed to thousands of devices the manageability and scalability of the overall systems becomes a key aspect of the overall success. Seamless organizational change and implementation of new processes is also important to get users of the system to buy into the benefits of the solution.<sup>5</sup>

The remainder of the white paper will take a closer look at each phase of the IoT solution development process, with a focus on industrial and manufacturing scenarios for IoT business and technical decision makers.

<sup>5</sup> Read more on how Microsoft approaches<sup>6</sup> the 5 phases [here](#).

## 2 PHASE 1: Developing a sound Business Case

Developing a business case can be a lengthy endeavor dealing with different stakeholders, business lines and end customers. Further challenges arise in quantifying costs, business impact assumptions and ROI.

*“Many businesses approaching us require IoT and yet are not clear on how to take full advantage, on how to use the data or monetize the outcome. Due to external pressure they start their IoT projects even though the value is not clear yet. We work with these companies to nail the business case first.”, Aiden Mitchel, VP of IoT Global Sales at Arrow Electronics.*

### 3 major learnings to help develop your IoT project business case

Our discussions with select executives who recently implemented IoT projects revealed 3 major learnings related to the business case development. Incorporating these learnings will help avoid similar potential pitfalls in the development of a sound business case.

### 2.1 Learning 1: IoT Projects take much longer than anticipated

Companies that have successfully rolled-out their IoT projects often talk about how they underestimated the timeline of the project. Record IoT projects went from business case development to commercial roll-out in 9 months. But these are exceptions, the current average of time-to-market is rather around 18-24 months.

#### Example 1

A medical imaging solutions company that wanted to offer a remote service solution for their portable 3D CT-like scanning equipment for hospitals, took just 6 months to get from business case development to pilot. But it took 4 more years to actually go to market due to the highly regulated medical device industry that required additional certification and additional testing.

Reasons for prolonged project timeline are manifold including both business-related issues (e.g., not having the buy-in from the right stakeholders) as well as technical-related issues (e.g., not working with an infrastructure that supports scaling the solution in a commercial deployment scenario).

**TAKEAWAYS:** Rethink the revenue and cost savings assumptions for the IoT business case and plan for contingencies in case of project hold-up. Work with partners that bring in experience from similar projects.



## 2.2 Learning 2: Organizational & cultural change is often underestimated

- **EMBRACING NEW BUSINESS MODELS**

The disruptive nature of IoT is transforming the way businesses make money. Aligning the workforce with new business models requires attention from the start.



### Example 2

With the help of IoT the German cleaning equipment manufacturer Kärcher is now aiming to sell square inches of cleaned floor rather than a professional cleaning machine. *“It totally changes the way we need to approach our customers”,* says Friedrich Vöelker, who is in charge of Digital Products at Kärcher. *“Our salesforce is used to presenting physical products to the clients. All of a sudden they present virtual offerings such as an online machine dashboard. They have no experience in pitching this and they need to react to completely different customer needs. Rather than making a one-off sale they are in continued talks with the customer regarding the ongoing performance of the machine. This change in mindset as well as the actual education of the salesforce takes time and it is just one of many organizational challenges we are faced with.”*

- **PERFORMING CROSS-DEPARTMENTAL WORK**

IoT solutions are only successful when a number of different departments within a company work together, especially the hardware and the software teams. IoT solutions inevitably must break up silos within large enterprises to be successful. This often results in friction or even opposition.



### Example 3

During a Microsoft led IoT solution development project in a large manufacturing environment it became apparent that the information technology (IT) system and the operational technology (OT) system were operating on two separate WiFi networks within the same building. Justin Breese, Technology Strategist at Microsoft says *“They were not exchanging any information because collaboration between the two departments was viewed as threatening to their proprietary information base. However, for IoT solutions it is important to get all parties joining forces to align for the optimal solution.”*

- **INTRODUCING MODERN PROJECT MANAGEMENT PHILOSOPHIES**

Agile development, design thinking and lean startup techniques are making their way from the software world and are clashing with a more traditional hardware world where projects are handled traditionally in a less instantaneous and flexible way. However, due to the complexity and the innovative character of IoT solutions firms must adopt these techniques if they want to be successful. A leading executive with experience implementing Scrum processes in Hardware Development revealed *“Agile engineering enables rapid project development cycles. Adopting modular solution design and lean processes in IoT can shorten product testing and mass manufacturing lifecycles whilst enabling iterative improvements to products in the field.”* The problem is that most firms are not ready for it and are still using dated techniques such as Waterfall. The resulting mentality shift must embrace aspects such as learning by doing and iterative enhancement, however this is not achieved overnight.

**TAKEAWAYS:** Ensure early senior management buy-in to unify business lines, embrace new ways of cross-departmental working and introduce agile development processes.

the Internet of Things. Elements include session protocols such as MQTT or AMQP, communication standards such as LPWAN, and edge analytics that sit on the device but communicate with the cloud.

## 2.3 Learning 3: The necessary skills are often not available in-house

- **COMBINATION OF HARDWARE AND SOFTWARE EXPERTISE MISSING**

End-to-end IoT solution development requires a broad range of skills including embedded system design, cloud architecture, application enablement, data analytics, security design and back-end system integration (e.g., into ERP/CRM).

**TAKEAWAYS:** Map the IoT skill gaps, cross-train and up-skill the workforce with a focus on new technologies unique to IoT. Work with true IoT experts from different fields with deep domain knowledge. Later on choose a vendor that can bring in the missing skills either directly or through a strong partner ecosystem.



### Example 4

One OEM that developed a connected solution had highly competent hardware teams with specific domain and product expertise as well as good know-how with traditional enterprise software systems. However, they were lacking the experience with modern cloud architectures and software backends required for a full-scale IoT solution. They decided not to build in-house but to look for help outside the organization.

- **NO EXPERIENCE WITH IOT INTEGRATION**

Even when OEMs possess most of the necessary software and hardware skills in-house, they rarely have experience with real IoT projects. In most cases, they have limited experience working with the technology elements that are unique to

# 3 PHASE 2: Build vs. Buy and Vendor Evaluations

## 3.1 Requirements Engineering – Understanding what is needed for your IoT Solution

Once you have a clear vision and have double checked the assumptions for your business case you will need to formalize your engineering requirements. This is necessary (at least on a high level) so that you can craft the right IoT initiative for your organization, perform the Build vs. Buy decision and consult the right vendors or partners.

### 1. Asking the right questions

Firstly, you should come up with answers to operational questions such as:

- **What end points will provide the data?**
- **What data points should be collected?**
- **Which analyses will generate strategic insights?**
- **Which enterprise systems need to be connected?**
- **What services do I need to offer?**

Keep in mind that the true value of IoT solutions resides in the data generated by your connected products – from which you derive actionable intelligence and feed timely insights back into products, processes, and operations to transform the entire business.

### 2. Mapping the requirements by area

As a second step, you should make a rough draft of your end-to-end solution (according to the 5 layers laid out in Chapter 1). For each component ask questions such as: Do we have the technology expertise in-house? Can we keep pace with the technology evolution and future customer requirements?

For example, it is important to know how much data will be generated, in which form and how fast it will be retrieved. This will determine which kind of database and storage solution is required and whether you will be able to build this on top of your existing data infrastructure or not.

## 3.2 The Build vs. Buy decision

After assessing the engineering requirements, you need to decide which components of the solution you want to build from scratch. In many cases, it is beneficial to work with existing solutions by third-party vendors i.e., out-of-the-box solutions.

---

### *IoT projects increasingly rely on existing out-of-the-box solutions*

---

It can be observed that recently more and more IoT projects rely on existing out-of-the-box solutions.

## WHY COMPANIES GO WITH “OUT-OF-THE-BOX” SOLUTIONS

Benefits:	Reasoning:
a. Quicker Time To Market	Critical infrastructure in place by default
b. Access to crucial skills	Readily available partner network with expertise across domains
c. Secure by design	Secure development lifecycle builds in security from outset
d. Optimized to work with wider ecosystem	Aligned with industry standards across partner ecosystems e.g., IIC <sup>5</sup>
e. Scale with ease	Modularized and optimized for large scale deployments
f. Enable a more end-to-end offering	Multiple parts work together from one vendor e.g., OS <sup>5</sup> , Cloud, Analytics

<sup>5</sup> IIC: Industrial Internet Consortium, OS: Operating System

**EXHIBIT 3:** Why companies go with out-of-the-box solutions– benefits and reasoning (Source: IoT Analytics)



### Example 5

An industrial equipment manufacturer, started building their own IoT solution “*from scratch*” (together with a System Integrator) in late 2012. However, when asked how they would approach development today, the manufacturer stated there are significantly more “out-of-the-box” offerings available on the market and are now a serious option to consider.

Before deciding to go with an out-of-the-box solution, companies should however evaluate the related costs as well as the threat of becoming “*locked-in*”. Being “*locked-in*” with the wrong vendor may strip away certain degrees of freedom in the overall solution or lead to uncontrollable support, maintenance and customization costs in the long run.

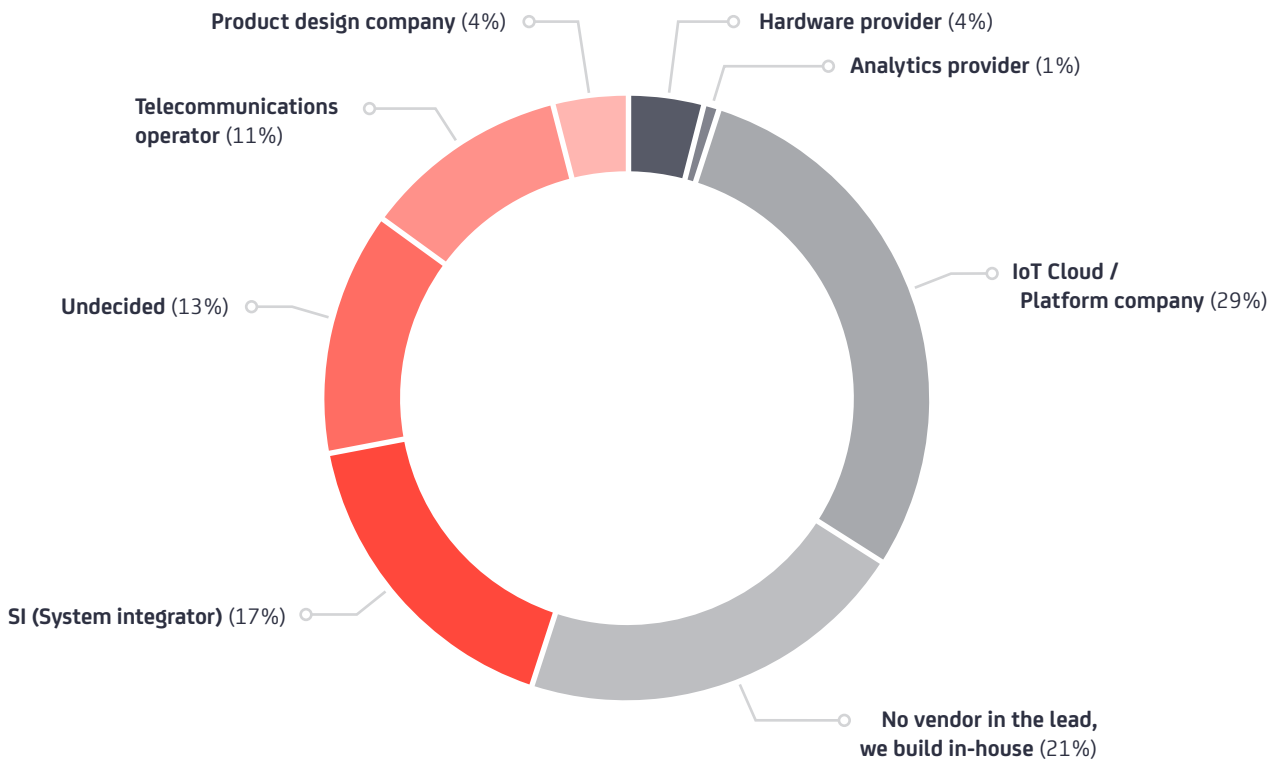
Most vendors offer the ability to perform an initial pilot trial. While companies may initially test some features for free, it should be noted that a certain budget needs to be planned in for the pilot phase as some integration effort and data modelling is always necessary to get the pilot project up and running.

## 3.3 The vendor selection

There are numerous reasons to choose one IoT solution vendor over another. In an industry survey we asked 144 companies currently building IoT Solutions: Which vendor is primarily in the lead to co-ordinate your IoT solution development?

## Which vendor is primarily in the lead to coordinate your IoT Solution development?

Companies (N=144) currently building IoT Solutions answered:



**EXHIBIT 4:** IoT Cloud / Platform companies leading the way in coordinating IoT Solution Development projects (Source: IoT Analytics)

### Most companies looking to IoT Cloud Platforms for solution development

The analysis shows that most companies developing IoT solutions see IoT Cloud / Platform companies in the lead (29%). While 21% of respondents see no vendor in the lead, instead they are building in-house. (See Exhibit 4).

However, finding the most suitable IoT Cloud / Platform vendor is difficult. Our [database](#) shows 360+ competing providers in the market today.<sup>[7]</sup>

One should also note, at this point (Q3/2016) there is no single IoT vendor that can provide the complete end-to-end out-of-the-box solution. However, some companies offer more than others and together with their partner

ecosystem some can provide complete end-to-end IoT solution support.

## 3.4 Comparing key IoT Solution vendors

### 1. Vendor comparison

Correctly assessing the capabilities of each possible vendor against your requirements definition is crucial for your selection. While the use case at hand determines your solution requirements, the vendor selection process largely depends on the components the vendors offer and how they fit into your solution.

		Components	Definitions	Microsoft	IBM	Google	amazon	ptc	intel	GE	SAP	
End-2-end stack	Application	Visualization	presents device data in rich visuals and/or interactive dashboards	✓	✓	✓	✓	✓		✓	✓	
		Business System Integration	enables integration with existing business systems	✓	✓	✓	✓	✓		✓	✓	
		Development Environment	offers an integrated development environment with SDKs for creating apps/services	✓	✓	✓		✓	✓		✓	
	Cloud Services	Storage / Database	cloud based storage and database capabilities (not including on premise solutions)	✓	✓	✓	✓				✓	✓
		Device Management	enables remote maintenance, interaction and management capabilities of devices at the edge	✓	✓		✓	✓	✓	✓	✓	✓
		Event Processing & Basic Analytics	processes events and handles big data analytics	✓	✓	✓	✓	✓			✓	✓
		Advanced Analytics	performs advanced stream analytics and machine learning	✓	✓	✓	✓	✓			✓	✓
	Communication	Connectivity Network / Modules	offers connectivity network / hardware modules enabling air interface connectivity							✓		
		Edge Analytics	enables analytics, time-sensitive decisions and local compute on a smart / edge device	✓	✓				✓	✓	✓	✓
		Edge Gateway (hardware based)	enables manageability, security, identity, interoperability based on a Cloud enabled hardware device							✓	✓	
	Device	Operating System	offers low-level system software managing hardware, software and runs applications	✓		✓				✓		
		Modules and Drivers	offers adaptable modules, drivers, source libraries that reduce development and testing time	✓	✓		✓	✓	✓	✓	✓	✓
		MPU / MCU	offers multi-purpose programmable electronic devices at microprocessor or microcontroller level							✓		
	Other	Specific Proprietary Enterprise Applications <sup>§</sup>	offers existing in-house enterprise systems (potentially connected to IoT)	• ERP • CRM	• BPM				• CAD, PLM • ALM, SLM		• MES	• ERP • CRM • EAM
		Augmented / Virtual Reality	offers an integrated mobile vision platform / related hardware for an IoT solution	✓					✓			✓
		Ready-to-go Solutions (i.e., preconfigured templates)	offers preconfigured IoT solution templates enabling quick setup, testing and data visualization	✓	✓				✓		✓	✓
Dedicated IoT Implementation Teams		offers in-house team with dedicated purpose of integrating IoT solutions	✓	✓				✓		✓	✓	

✓ denotes an internal solution offering available i.e., not through the use of a partner. See footnotes below and Appendix for clarification.

**EXHIBIT 5: Key providers with in-house offerings across the IoT Solution Stack – Microsoft, IBM, Google, Amazon, PTC, Intel, GE, SAP (Source: IoT Analytics)**

Exhibit 5 presents a high-level comparison of selected vendors across the layers and components laid out in Chapter 1.

Providers listed cover a major part of the overall IoT solution. Other large IoT vendors include Cisco, Salesforce.com, Vodafone and Ericsson among others. See the IoT Analytics [company ranking](#) for more details.

<sup>§</sup> Examples of specific proprietary enterprise applications i.e., list is not exhaustive. ERP: Enterprise Resource Mgmt., CRM: Customer Relationship Mgmt., CAD: Computer Aided Design, PLM: Product Lifecycle Mgmt., ALM: Application Lifecycle Mgmt., BPM: Business Process Management, SLM: Service Lifecycle Mgmt., EAM: Enterprise Asset Mgmt., MES: Manufacturing Execution System. **Note:** This is not an exhaustive list of all providers in the IoT space. The table presents a cross-section of providers which offer many in-house capabilities across the stack. Provider capabilities denoted are as of July 2016. Please note with the accelerated activity in the IoT domain, new offerings are being developed on an ongoing basis. The table presents a high-level comparison of key providers. In some solution scenarios providers may partner with each other/others to provide an end-to-end solution. Capabilities based on desktop research, verified with individual vendors, except for Google. See Appendix for further term explanations and specific vendor offerings.

When evaluating vendors for a pilot and commercial deployment of a connected IoT solution, you should try to deeply understand how each vendor together with their partner network will support your project, specifically in relation to the learnings outlined in this paper.

## 2. Understanding the partner network

A vendor with a strong partner network may be able to minimize solution development problems by building on existing experience and leveraging trusted expertise.

### *A strong partner network can be a key differentiating factor for vendors*

You should assess the breadth of the vendors partner network across a number of segments as outlined in [Exhibit 6](#).

See our IoT platforms [market report](#) for more details.

One of the main reasons why a strong partner network can become a differentiating factor is cross-system optimization. Partnerships between cloud platforms, hardware vendors, communication providers and edge ISV's can enable smooth deployment of IoT solutions across ecosystems.

For instance, a cloud platform vendor and a gateway provider that have both built their IoT systems on the OCF standard are working with the same common framework and can therefore offer a faster time-to-market and a more secure overall architecture.

Another reason to rely on a partner network is that certain project teams may have worked together before, making onboarding and issue resolution much easier. Being able to rely on a trusted partner for part of the solution development is a real benefit for both vendors and companies implementing IoT solutions.

*“The partnership we have developed with Microsoft over the past 15 years is very important. In the IoT era, it enables us to offer superior packages by combining our technology services with Windows 10 IoT and Azure IoT Suite.”* **Aiden Mitchel, VP of IoT Global Sales at Arrow Electronics.**

## PARTNER NETWORK

Partner Type:	Partner strength:
Device hardware vendors	Enable quick start prototyping
Original design manufacturers	Offer reference PCBs for “white label” solutions
Silicon / chip vendors	Customize specific designs for embedded systems
Gateway partners	Deliver security-enhanced data flows
Communication partners	Support connectivity across multiple networks
Cloud platform providers	Offer a cloud computing backend and supporting infrastructure
Independent software vendors	Bring holistic solution development expertise
Analytics professional service providers	Offer unique expertise in big data analytics and data science services
System integrators	Play a central role in stitching solutions together

**EXHIBIT 6: IoT Partner Network** – a number of stakeholders are required to develop end-to-end IoT solutions (Source: IoT Analytics)

## 4 PHASES 3-5: Proof of Concept, Piloting and Commercial Deployment

The goal of the **proof of concept** phase is to quickly assess your solutions feasibility. The key here is to focus on a small number of scenarios that matter most to your business. Once these are validated, further features can be evolved during the **pilot phase**.

Many IoT vendors offer a dedicated implementation workforce that are specifically tasked with integrating customer specific features when rolling out a pilot project. Some IoT platforms even offer pre-configured solutions that can setup initial pilot tests in a matter of minutes and help streamline **commercial deployments**.

Interviews with people that recently brought IoT solutions to commercial deployment revealed three areas that require specific attention during those final project phases:

- 1. Ensuring adequate **IoT security** is built-in.
- 2. Minimizing **interoperability** issues.
- 3. Integrating **manageability** functionalities that enables scalability of the IoT solution.

### 4.1 Security

Security can't be done by the device or cloud alone. Rather, both must work together and with each component of the solution to reduce the overall attack surface area and keep the weakest link to a minimum. It is important to realize that one weak link can open up your whole system (e.g., hackers have gained access to entire company networks by simply entering the default device password for an IoT connected surveillance camera).

Combining hardware and software solutions (i.e., cyber physical) that go from device to cloud and cover everything in between will enable more seamless security in IoT. OEMs need to understand that threats can come from a number of different areas and may be unknown initially; the STRIDE<sup>5</sup> model outlines six possible threats to IoT.

#### STR.I.D.E. Threats Model:

- **SPOOFING IDENTITY** i.e., attacker uses another user/device's credentials to access the system.
- **TAMPERING** i.e., attacker replaces software running on the device with malware.
- **REPUDIATION** i.e., attacker changes authoring info of malicious actions to log wrong data to log files.
- **INFORMATION DISCLOSURE** i.e., attacker exposes sensitive information to unauthorized parties.
- **DENIAL OF SERVICE** i.e., attacker floods device with unsolicited traffic rendering it inoperable.
- **ELEVATION OF PRIVILEGE** i.e., attacker forces the device to do more actions than it is privileged to do.

<sup>5</sup> Find out more on the STRIDE<sup>[8]</sup> model [here](#).



## 1. Learnings

Our discussions with IoT experts revealed the following security-related lessons:

- **DO NOT MINIMIZE SECURITY FEATURES TO GET THE MVP OUT QUICKLY**

Companies developing IoT solutions often want to get to market quickly and overlook the importance of building crucial security features into their minimum viable product (MVP) or even beyond.



### Example 6

In 2015, an analysis of 6 smart devices purchased on the market found some disturbing flaws such as no encryption, lack of data protection, and inadequate security against man-in-the-middle attacks. Other hackers report examples in which device passwords were visible in the source code, encryption keys were easily accessible or default login credentials were not changed.<sup>[9]</sup>

In many cases, it is up to the vendor to make the customer aware of threats and push for security.



### Example 7

An OEM with no prior experience in IoT Solutions, commissioned an IoT platform vendor to lead their connected equipment solution development. The vendor found it necessary to educate the OEM of the downfalls of unsecure devices. One feature implemented was a device lock down that enables only authorized users and system components to access the equipment. If a competitor, for example, tried “*phishing*” to understand how the solution works, the device would restrict access and installation of any malicious software.

- **FORCE YOURSELF TO THINK SECURITY FROM END-TO-END**

IoT demands end-to-end security solutions that traverse the layers. Partha Srinivasan, Senior Product Manager at Microsoft says “*IoT Security must be consistent across the device OS, network, cloud and application.*” Unfortunately, not all IoT systems are thought out from end-to-end. For example, in many cases identity verification is only available on the device level. However, if a hacker jailbroke the device he/she could remove software restrictions imposed by the OS and permit root access to the file system allowing them to install untrusted applications on the device. In case of such a hardware compromise the other layers should also confirm authentication of device and user identity e.g., the cloud should know which device is compromised and restrict access to the network.



### Example 8

One of the most prominent IoT Security hacks to date is the attack on a vehicle in 2015. The hackers managed to take remote control of the car and disable the brakes. In this specific case, the solution in place was not secured from end-to-end allowing components that were lacking proper authentication to be accessed by an external “*man-in-the-middle*” (e.g., the brakes). This scenario had apparently not been tested for or protected against when the system was initially designed.

- **IMPLEMENT SECURITY-BY-DESIGN**

Security-by-design is a fresh approach that entails security experts, architects and engineers from each layer getting involved in full architecture design of an IoT solution right from the outset and to create a security development lifecycle (SDL).<sup>[10]</sup> Thinking about security across the product lifecycle

helps IoT developers build more secure software and address important security compliance requirements.



### Example 9

Microsoft has developed an innovative SDL concept that includes aspects such as secure coding, assessing risk, reducing attack surface, modelling threats, fuzz testing, and deprecating unsafe functions.

Another innovation related to security-by-design is the involvement of an “attacker” performing penetration testing to assess the system and look for vulnerabilities in the product development process.



### Example 10

A manufacturer of a Connected Medical Device employed a so-called “*ethical hacker*” whose sole role is to detect security vulnerabilities. This security-breaking expert applies typical hacking techniques to root a device, penetrate, lift and de-obfuscate code. The “*ethical hacker*” is well versed in reverse engineering, fault injection, unsecure code detection and side-channel analysis. Methods such as these facilitate a better understanding of the weaknesses in existing solutions and help to develop new features for products to increase their future security.

## 2. Security Takeaways/Best Practices

The most important takeaway from our interviews is that you should not rush to market with inadequate security. Map the attack surface to better understand threats and your weakest link. Defend in depth with secure solutions from end to end and build in security from the outset.

Some best-practices of engineers building secure IoT Solutions include:

- **Employing hardware-based security** such as TPM 2.0 to offer an additional root-of-trust.
- **Using unique identity keys** associated with the device (flashed into the hardware trust module or using manufacturer IDs e.g., Intel EPID).
- **Shielding devices** behind a gateway or firewall.
- **Enabling user-selected device IDs** verified across the stack e.g., on OS, Edge gateway, Cloud.
- **Employing secure boot processes** for malware resistance (e.g., only run secure signed images).
- **Using a cross-stack standards-based security approach**, thereby making it easy to adopt, easy to adapt (with the standard) and easy to justify to the stakeholders.
- **Auditing and monitoring events** and potential breaches in real-time, employing security analytics.

It is worth noting, if the hardware is designed with vulnerability the end-to-end solution may still be compromised. Thus, it is important to not only look at the software security aspects but also the hardware aspects e.g., root-of-trust chip security, board-level protection and anti-tamper measures.

## 4.2 Interoperability

The PoC phase should assess your IoT solution's interoperability capabilities. IoT interoperability largely depends on the communication protocols used and the level of standardization.

When assessing a vendor's level of interoperability, keep the traditional OSI or TCP/IP models in mind. Think about the following 3 layers (from bottom up) and focus on the protocols applicable for your IoT solution:

- **Physical layer** – how bits are transmitted/received over the medium. What radio technologies are supported? For example, Bluetooth, WiFi, 802.15.4, Cellular, variations of LPWAN or alternatively Ethernet.
- **Networking layer** – how the data packets are securely transported from device to cloud. What technologies are required to route data through your networks? For example, traditional IT systems based on IPv4 are now shifting towards IPv6. Most OT systems typically use proprietary protocols such as Modbus or Profibus (or alternatively open protocols such as OPC-UA) with TLS based authentication.
- **Application layer** – how the data is taken in and used in your applications. Which open lightweight protocols are supported? For example, MQTT, AMQP, CoAP, Restful HTML, DDS or web-sockets optimized for bursts of small amounts of data.

### 1. Learnings

Our discussions with IoT experts revealed the following interoperability-related lessons:

- **PROTOCOL TRANSLATION IS A MAJOR PART OF THE DEVELOPMENT EFFORT**  
Protocol translation still takes up a majority of today's IoT development efforts.



#### Example 11

An industrial OEM had the requirement of connecting its IoT solutions to the existing bus system in order to be able to open and close specific valves remotely. The IoT solution vendor brought in a specific partner company that specializes on lower-level protocol translations for industrial equipment. Even though a specialist performed the job, it took nearly 4 months to develop all necessary translations. Only then could all valves be controlled and data exchanged seamlessly between equipment components and the cloud.

- **CONNECTING WITH OTHER IOT SYSTEMS IS THE NEXT FRONTIER**

While establishing smooth connectivity within an IoT solution is essential to making it work, establishing a connection between different systems will be a major value driver in the future.



#### Example 12

A hospital in Boston, for example stores patient records on a Microsoft Azure backend. A doctor in France treating a Boston-resident who is on vacation would like to access the patient's x-ray history but his system is running on Amazon AWS. In addition to regulatory and privacy-related concerns – if this scenario should work out in the future, the backends need to be setup for communication. *“As IoT becomes more mature, we will likely see competitors moving to competition in order to unlock the full value of IoT”* according to Bob King, System Level Engineer at Microsoft.

## 2. Interoperability Takeaways

In order to reduce protocol translation and enable interoperability with other systems your IoT Solution should build on a standardized ecosystem, relevant for your use case and industry. Assess your vendors' device, OS, and protocol agnostic capabilities as well as their commitment to IoT standardization.

To understand the real value of standardization bodies, one needs to realize that it saves engineers endless hours of customization work in an IoT project. Building your IoT solution to industry-wide specifications ensures adhering devices can securely and seamlessly interact with one another, regardless of the underlying hardware, operating system, chipset, or transport protocol. This level of standardization not only greatly reduces the “*man-hours*” involved but also the complexity of overall solution development.

Some IoT vendors contribute several years of development work to help build connectors and bridges so their future IoT systems can seamlessly interact with the greater ecosystem. Thus, the standardization body that a vendor is part of can be a key differentiating factor.



### Example 13

The recent coming together of rival organizations (OIC, AllJoyn) to form the Open Connectivity Foundation (OCF)<sup>[11]</sup>, has the potential to become one of the defining global standardization bodies that delivers a comprehensive set of open IoT specifications and protocols. The OCF promise is backed by a broad ecosystem of key members including Cisco, GE, Intel, Microsoft, Qualcomm, Samsung and others. This level of consolidation could deliver on focusing industry attention to reduce the current patchwork of specifications and enable new levels of interaction in-line with the true concept of the IoT.

## 4.3 Manageability

When companies move from piloting to roll-out, one of the success factors becomes: How well does your solution deal with complexity? The more connected IoT devices get rolled-out, the more the overall system has to deal with different software, firmware, connectivity issues, data structures and security capabilities. During this phase it becomes apparent whether the system is designed for large-scale manageability or not.

### 1. Learnings

During our discussions with IoT experts we found that managing the roll-out is an issue. We highlight three distinct aspects that companies struggled with:

- **HARDWARE IS NOT POWERFUL ENOUGH**



### Example 14

A manufacturer of building automation systems realized that the processors that were powering their connected devices did not have enough horsepower when the company wanted to add new sensors to the devices. The initial system had not been designed for these sensors so that the product design had to go through a major design change half-way through the roll-out, integrating server-type processors to the devices.

- **DATA MODELS NOT SET UP TO PROCESS BIG DATA SETS**

It is important to understand the overall use cases in IoT to derive a data model, before you go into solution design. This applies for both the asset model and as well as the time series model.



### Example 15

A large manufacturer of construction equipment initially created neat dashboards to monitor their machines remotely. A year later, the project was amended to start performing predictive maintenance and fault analysis of the hydraulic systems. *“However, the team had not thought out the data model entirely. They soon realized that the way that data sets were stored horizontally in the database meant that in order to get a specific value, the whole database had to be loaded. This turned out to be a problem with backend processing capacity for their several hundred connected vehicles.”* says Audi Lucas, Director of Connected Products at Wipro.

- **IOT SYSTEMS NOT DESIGNED TO WORK WITH OLDER LEGACY SYSTEMS**

Equipment installed 2-3 years ago without any IoT integration is not likely to be replaced until its natural lifespan is reached. It will continue to operate in place for the foreseeable future. The IoT solution will have to make do with retrofitted legacy integrations until the equipment is naturally replaced. This situation is not optimal for IoT and brings along a number of challenges.



### Example 16

An OEM made the painful discovery that a lot of the custom-developed drivers, for their first-generation of connected equipment, had to be completely recoded after the second generation of connected equipment had switched to a newer operating system that was running on a 64-bit CPU rather than 32-bit.

It is not only the technical integration that is complex but in many cases companies are reluctant to let go of tried and trusted solutions that have functioned for years, fearing that a running system would collapse – perhaps rightfully so.

## 2. Manageability Takeaways

Building the system in a modular manner can make the overall solution more manageable. It is imperative not to limit the hardware capabilities early on to ensure a smooth roll-out from pilot to commercial deployment. Data models should be thought through leaving capability to develop for future applications. Developers must plan for integration with legacy systems in a structured manner.

Extending intelligence to the edge is a very important aspect to managing complexity as the IoT solution grows and scales with both existing and new equipment.

The introduction of IoT gateways is a modular approach to segment the overall solution; making it more manageable in terms of a). device management and b). dataflow management.

- **MANAGING DEVICES AT THE EDGE**

An IoT gateway can provide management services close to the device without the need to communicate with the cloud. Management services include querying devices for information, clustering IoT devices for easier control and orchestrating device jobs. Common jobs include device reboot, batch updates, scheduled patches, and modifying device configuration settings. Local processing and control functionality on an IoT gateway can make solutions easier to manage and scale e.g., adding a batch of new devices and performing initial setup provisioning tasks.

- **MANAGING DATAFLOW AT THE EDGE**

An IoT gateway sitting between the device and the cloud acts as a bi-directional communication enabler. More than just a mere traffic router, it plays an active role in managing access and information flow. It can filter or aggregate device telemetry and thus reduce the amount of data being transferred to the cloud backend. This enables developers to optimize and process data with lower latency and less bandwidth usage. Acting as a protocol translator, the gateway can communicate with legacy “*brown-field*” devices as well as non-IP capable devices. Common data models ensure data streams from various connected IoT devices can be aggregated and processed regardless from which device the data originates.

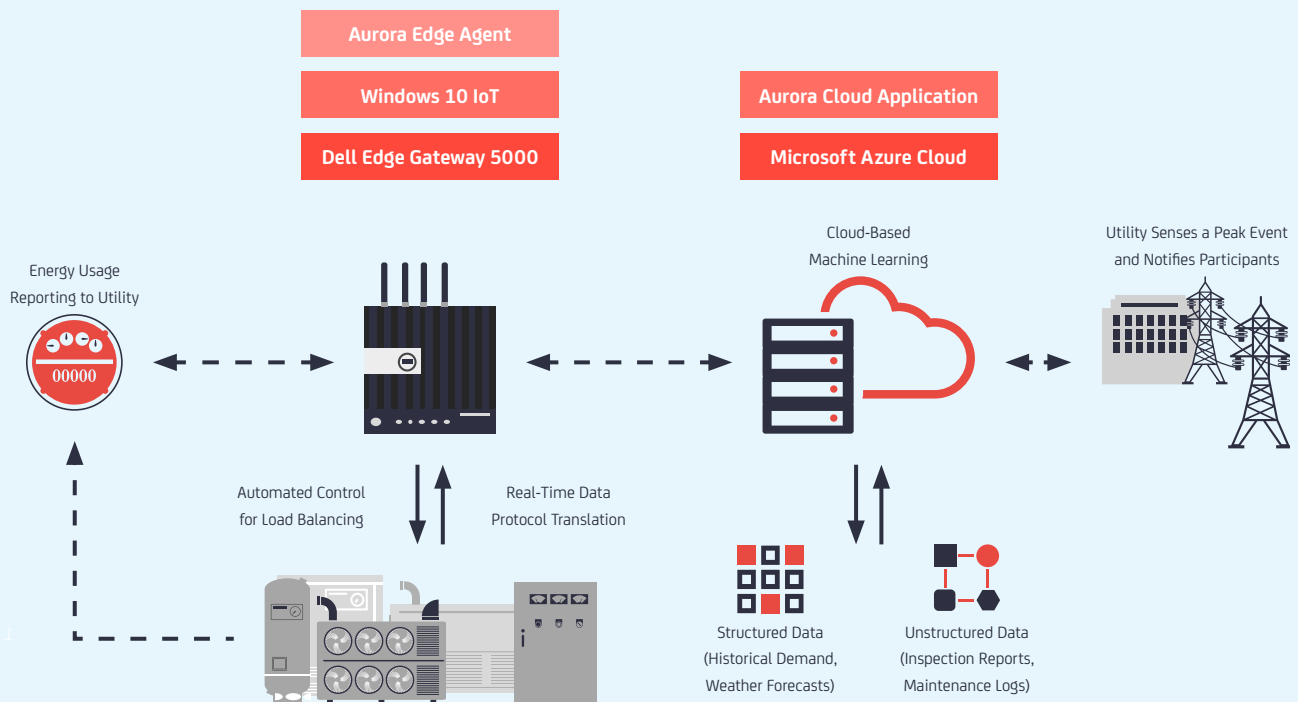
# 5 IOT SOLUTION BLUEPRINT: IoT Enabled ADR

## Business Case:

A shopping mall operator in California aims to reduce energy costs and avail of substantial tax credits through the use of an IoT enabled Automated Demand Response (ADR) solution. This ADR blueprint example represents a single solution provided by qualified partners (e.g., Dell, Blue Pillar and Microsoft)<sup>5</sup> as a flexible reference architecture.<sup>[12]</sup>

## Background:

Utility companies (and governments) offer standard Demand Response programs to get large consumers of power such as malls or universities to cut back on energy consumption during peak demand periods. This voluntary action addresses the variability of demand on the grid issue that causes stress on utility equipment. In return, participants receive substantial incentives such as subsidized electricity prices and tax credits. IoT enabled automation of Demand Response programs tackles inefficient operational challenges. For example, facility personnel might miss manual Demand Response setup notifications (e.g., via email, text or call) from the utility company to reduce power consumption. This can result in lost opportunities for cost saving and grid balancing.



**EXHIBIT 7: IOT SOLUTION BLUEPRINT: IoT Enabled Automated Demand Response** – high level architecture diagram (Source: Adapted from Dell, Blue Pillar & Microsoft)

<sup>5</sup> Note: Specific ADR applications may involve a combination of these and other technology providers.

## Approach:

The utility company monitors consumption to sense a peak event that may overwhelm the grid. Once sensed the utility notifies the shopping mall (and other ADR participants) to reduce their power consumption. These events and notifications are received, managed, tracked, validated and responded to via the ADR server in the cloud.

In the shopping mall, an edge gateway that could run on Windows 10 IoT acts as a hub to automatically execute predefined directives for energy reduction. This reduces non-essential load on selected equipment (e.g., raising thermostats, turning off lights). Onsite energy generation can also be activated (e.g., renewable energy resources, generators or regenerative AC drives). Smart meters onsite indicate usage of energy for reporting back to the utility.

## Challenges & Learnings:

### 1. DEVELOPING THE IOT SOLUTION IN COLLABORATION

This ADR blueprint example demands a number of technologies to work together, for example:

- **Dell's Edge Gateway** collects analyses and relays real-time data from devices.
- **Windows 10 IoT OS** offers increased manageability and security.
- **Blue Pillar's Aurora platform application** allows protocol translation.
- **Microsoft Azure Cloud** enables machine learning to determine actions.

It is the power of a great working relationship between these parties that make an IoT ADR solution a success.

### 2. PERFORMING PROTOCOL TRANSLATION

The overall ADR solution requires gathering of diverse data sets (e.g., from PLCs, RTUs, meters, BAS, and SCADA systems). These types of equipment were never designed to be connected to the internet and are usually based on proprietary protocols. Therefore, protocol translation and subsequent streamlined data aggregation consumed a large part of the IoT solution development activities.

### 3. CODING THE APPLICATIONS FOR DEVICE AND CLOUD SIMULTANEOUSLY

Using MS Visual Studio, end-to-end applications can be easily created that seamlessly connect from device to cloud for the ADR solution. Predefined templates for Windows 10 IoT OS and Azure Cloud in Visual Studio simplify development, testing and deployment of applications both on device and cloud simultaneously. Comprehensive SDKs provide substantial source code and native libraries that take care of the “*heavy lifting*” required to get an application up and running (e.g., dynamic module loading, configuration and data pipelining). A natively optimized environment for both device and cloud can save many hours of development and ensure consistency in build automation and application interaction.

## Looking Ahead:

The shopping mall example presents a blueprint for IoT enabled ADR deployment based on a flexible reference architecture that can be rolled-out in similar settings. The main benefits of the solution for the shopping mall include improved profitability, mitigation of operations risk (e.g., by receiving advanced notices of outages), and easier adherence to compliance (e.g., via automatic reporting).

Read more on the IoT enabled ADR solution [here](#).



## 6 Conclusion

IoT is becoming a strategic priority for many organizations. This white paper helps in streamlining the IoT Solution development process by looking at the major process steps when developing an IoT Solution and highlights some key learnings from past projects.

### General Findings:

- **Approx. 7,700 IoT projects** have been undertaken in the last 3 years and **3,000 more are expected in 2016**
- When characterizing your IoT solution there are **15 components to consider** across the 5 layers of Device, Communication, Cloud Services, Applications and Security.
- IoT solution development requires a **structured framework of 5 phases**, from which early learnings include:

### Phase 1: Business Case Development

- **Projects take much longer than anticipated** – typically between 18-24 months, it is important to plan the business case thoroughly, plan for contingencies and work with experienced partners.
- **The necessary organizational & cultural change is often underestimated** - Ensure early senior management buy-in, embrace new business models and introduce agile development processes.
- **The necessary skills are often not available in-house** - Map the IoT skill gaps and cross-train the workforce. Work with true IoT experts and their partners.

### Phase 2: Build vs. Buy and Vendor Evaluations

- Understand what is needed for your IoT Solution by asking questions such as “What data points should be collected?” and **map the requirements by solution component**.
- **Go with an out-of-the-box solution** if you want to achieve quick time to market, access to crucial skills, built-in-security, and scalability.
- When choosing a vendor, **most OEMs look at IoT Cloud / Platform providers** for assistance (29%). Carefully evaluate a vendors’ in-house capabilities but also assess the value of their partner ecosystem to bring you an end-to-end solution offering.

### Phase 3-5: Proof of Concept, Piloting and Commercial Deployment

3 areas that demand special attention for the latter stages include Security, Interoperability and Manageability:

#### Security:

- Map the attack surface of your IoT Solution end-to-end using a systematic approach (e.g., the S.I.R.I.D.E model).
- Implement best-practices such as Security by Design, Secure booting, TPM or TLS.

#### Interoperability:

- Consider building on top of an existing IoT Standard to minimize interoperability issues and major protocol translation efforts (e.g., OCF).
- List adjacent IoT systems and design for potential future integration.

#### Manageability:

- Ensure your system is built in a modular manner on different levels (e.g., the data model).
- Use IoT gateways to optimize device management and data pre-processing at the edge.

# Appendix

## A. End-to-end IoT Solution Stack Term Explanations

The terms used in the IoT solution stack comparison table in Chapter 3 are explained with examples below:

### Application:

- **Visualization:** Presents device data in rich visuals and/or interactive dashboards e.g., MS Power BI.
- **Business System Integration:** Enables integration with existing business systems e.g., Azure Logic Apps.
- **Development Environment:** Offers an integrated development environment with comprehensive SDKs for creating applications and services e.g., MS Visual Studio.

### Cloud Services:

- **Storage / Database:** Cloud based storage and database capabilities (not including on premise solutions) e.g., Azure SQL.
- **Device Management:** Enables remote maintenance, interaction and management capabilities of devices at the edge e.g., Azure IoT Hub.
- **Event Processing & Basic Analytics:** Processes events and handles big data analytics e.g., Azure HDInsight.
- **Advanced Analytics:** Performs advanced stream analytics and machine learning e.g., Azure Machine Learning.

### Communication:

- **Connectivity Network / Modules:** Offers connectivity network / hardware modules enabling air interface connectivity e.g., AT&T M2M, Telit IoT Modules.
- **Edge Analytics:** Enables time-sensitive decisions, local compute, analytics on a smart / edge device e.g., Cisco Fog Data Services.
- **Edge Gateway (hardware based):** Enables manageability, security, identity, interoperability based on a Cloud enabled hardware device e.g., Dell Edge Gateway 5000.

### Device:

- **Operating System:** Offers low-level system software managing hardware and software resources and providing common services for running system applications e.g., Windows 10 IoT
- **Modules and Drivers:** Offers adaptable modules, drivers, source libraries that reduce development and testing time e.g., AWS IoT Device SDKs.
- **MPU / MCU:** Offers multi-purpose programmable electronic devices at microprocessor or microcontroller level e.g., Intel Atom processors.

### Other:

- **Specific proprietary IoT enterprise applications:** offers existing in-house enterprise systems e.g., IBM Enterprise Asset Management.
- **Augmented/virtual reality:** Offers an integrated mobile vision platform / related hardware for an IoT solution e.g., PTC's Vuforia.
- **Ready-to-go solutions:** Offers preconfigured solution templates enabling quick setup, testing and data visualization e.g., Microsoft's Predictive Maintenance template.
- **Dedicated IoT implementation teams:** Offers in-house team with dedicated purpose of integrating IoT solutions e.g., Telit Professional Services.

## B. IoT Solution Stack Offering Examples

This table outlines example product offerings (i.e., list not exhaustive) from vendors denoted in Chapter 3:









Components		 Microsoft	 IBM	 Google	 amazon	 ptc	 intel		
Application	Visualization	MS Office, Power BI, Xamarin	IBM Watson IoT Platform	Google Cloud Monitoring Dashboards	Amazon QuickSight BI, Amazon Elasticsearch	ThingWorx Product Relationship Manager		Predix UI, Dashboard Seed	SAP Business-Objects Lumira
	Business System Integration	MS Dynamics CRM/AX, BizTalk, Azure Logic Apps	IBM Cloud Integration	Google Business System Integration	AWS IoT SDKs	ThingWorx Integration Hub		Predix DevOps Services	HANA Cloud Integration
	Development Environment	MS Visual Studio	IBM Bluemix	Android IDE, Android Studio		ThingWorx Composer	Helix App Cloud, Intel System Studio, XDK IoT		SAP Web IDE
Cloud Services	Storage / Database	MS Azure SQL, Azure DocumentDB, Azure Blob	IBM Cloudant, IBM dashDB	Google Cloud SQL, Datastore, Bigtable	Amazon S3, RDS, DynamoDB, EFS, Aurora			Cloud Foundry, SQL Database, Blobstore	SAP HANA, SAP ASE / maxDB
	Device Management	MS Azure IoT Hub	IBM Watson IoT Platform		AWS IoT Device Gateway, Device Shadow, Device Registry	ThingWorx Utilities	Helix Device Cloud	Predix EdgeManager	SAP IoT Services
	Event Processing & Basic Analytics	MS Azure HDInsight, Azure Stream Analytics	IBM IoT Real-Time Insights	Google Cloud Dataflow	Amazon Elastic MapReduce, Redshift, Kinesis	ThingWorx Analytics Server		Predix Cloud Analytics UI, Time Series	SAP Smart Data Streaming
	Advanced Analytics	Azure Machine Learning, Cortana Intelligence Suite	IBM Watson Analytics / Machine Learning	BigQuery, Google Cloud Machine Learning	Amazon Machine Learning	ThingWorx Analytics Server		Predix Analytics Services	SAP HANA Spatial, Graph, Predictive Analytics
Communication	Connectivity Network / Modules						Intel Mobile / Connectivity Modems		
	Edge Analytics	MS Azure IoT Gateway SDK	IBM Watson IoT Edge Analytics			ThingWorx MicroServer, Edge SDKs	Intel Gateway Technology	Predix Edge Software	SAP Streaming Lite
	Edge Gateway (hardware based)						Intel NUC Gateway	GE Routers & Converters	
Device	Operating System	MS Windows 10 IoT		Android			Wind River VxWorks, Rocket		
	Modules and Drivers	MS Windows Driver Kit / Framework	IBM Watson IoT Agents		AWS IoT Device SDKs	KepServerEX Industrial Connectivity	Intel Edison, Galileo	Predix Machine SDK	SAP IoT Services
	MPU / MCU						Intel Atom, Core, Quark, Xeon		
Other	Specific Proprietary Enterprise Applications (potentially connected to IoT)	MS Dynamics CRM, AX ERP	IBM Maximo, IBM BPM			PTC Creo CAD, PTC Windchill PLM, PTC ALM, PTC SLM		GE Asset Performance Mgmt., GE Manufacturing Execution Systems	SAP CRM, SAP ERP, SAP EAM
	Augmented / Virtual Reality	MS HoloLens				Vuforia Studio Enterprise			SAP AR Warehouse Picker
	Ready-to-go Solutions (i.e., preconfigured templates)	Predictive Maintenance, Remote Monitoring	Buildings & Asset Mgmt., Automotive, Electronics			Codeless Mashup Builder Templates		GE Plant Applications, GE Efficiency Analyzer	Connected Logistics, Predictive Maintenance and Service
	Dedicated IoT Implementation Teams	MS Consulting Services	IBM Watson IoT Services			PTC Deployment Services		GE Industrial IoT Implementation Services	SAP IoT Consulting Services

EXHIBIT 8: Key providers with specific in-house offerings outlined across the IoT Solution Stack (Source: IoT Analytics)

# References

1. McKinsey (2015), report: “Unlocking the potential of the Internet of Things”, [http://www.mckinsey.com/insights/business\\_technology/the\\_internet\\_of\\_things\\_the\\_value\\_of\\_digitizing\\_the\\_physical\\_world](http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world)
2. PSFK (2014), report: “A Brief History Of The Internet Of Things”, <http://www.psfk.com/2014/03/internet-of-things-infographic.html>
3. IoT Analytics (2016), market report: “IoT Platforms Market Report 2015-2020”, <http://iot-analytics.com/product/iot-platforms-market-report-2015-2021-3/>
4. Business Insider (2015), article: “Australian mining giant Rio Tinto is using these huge self-driving trucks to transport iron ore”, <http://uk.businessinsider.com/rio-tinto-using-self-driving-trucks-to-transport-ore-2015-10?IR=T>
5. CreatingSmartCities (2014), blogpost, “Smart irrigation in Barcelona: introducing the new system”, <http://www.creatingsmartcities.es/blog/en/smart-irrigation-barcelona-smartcity/>
6. Microsoft (2015), blogpost by Jerry Lee: “How to make the most of IoT deployments: Minimize the timeframe and maximize the return”, <https://blogs.microsoft.com/iot/2015/11/24/how-to-make-the-most-of-iot-deployments-minimize-the-timeframe-and-maximize-the-return/>
7. IoT Analytics (2016), market datasheet: “List Of 360+ IoT Platform Companies”, <http://iot-analytics.com/product/list-of-360-iot-platform-companies/>
8. Microsoft (2016), blogpost by Yuri Diogenes, “Internet of Things security architecture”, <https://azure.microsoft.com/en-us/documentation/articles/iot-security-architecture/>
9. NSTAC (2014), report, “NSTAC Report to the President on the Internet of Things - Case Studies”, <https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf>
10. Microsoft (2016), website, “What is the Security Development Lifecycle?”, <https://www.microsoft.com/en-us/sdl/>
11. OCF (2016), website: “Open Connectivity Foundation”, <http://openconnectivity.org/>
12. Dell (2016) white paper, “Automated Demand Response Blueprint”, [http://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/Automated\\_Demand\\_Response\\_Blueprint\\_Final\\_April\\_8\\_2016.pdf](http://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/Automated_Demand_Response_Blueprint_Final_April_8_2016.pdf)

# List of Exhibits

**Exhibit 1:** Generalized 5 Layer Model of an End-to-End IoT Solution – with a focus on software components (Source: IoT Analytics)

**Exhibit 2:** 5 Phases of IoT Solution Development– Business Case, Build vs. Buy, Proof of Concept, Pilot, Commercial Deployment (Source: Adapted from Microsoft)

**Exhibit 3:** Why companies go with out-of-the-box solutions– benefits and reasoning (Source: IoT Analytics)

**Exhibit 4:** IoT Cloud / Platform companies leading the way in coordinating IoT Solution Development projects (Source: IoT Analytics)

**Exhibit 5:** Key providers with in-house offerings across the IoT Solution Stack – Microsoft, IBM, Google, Amazon, PTC, Intel, GE and SAP (Source: IoT Analytics)

**Exhibit 6:** IoT Partner Network– number of stakeholders are required to develop end-to-end IoT solutions (Source: IoT Analytics)

**Exhibit 7:** IOT SOLUTION BLUEPRINT: IoT Enabled Automated Demand Response – high level architecture diagram (Source: Adapted from Dell, Blue Pillar & Microsoft)

**Exhibit 8:** Key providers with specific in-house offerings outlined across the IoT Solution Stack (Source: IoT Analytics)

# About



IoT Analytics is the leading provider of market insights and industry intelligence for the Internet of Things (IoT).

More than 30,000 IoT decision makers rely on IoT Analytics' data-driven market research every month. IoT Analytics tracks important data around the IoT ecosystem such as M&A activity, startup funding, job developments, and company activity. The product portfolio includes: 1. Free insights on IoT markets and companies, 2. Focused market reports on specific IoT segments, 3. Go-to-market services for emerging IoT companies. IoT Analytics is headquartered in Hamburg, Germany.

Find out more at <http://iot-analytics.com>

You may get directly in touch with the authors:

Padraig Scully ([padraig.scully@iot-analytics.com](mailto:padraig.scully@iot-analytics.com))

Knud Lasse Lueth ([knud.lueth@iot-analytics.com](mailto:knud.lueth@iot-analytics.com))



Founded in 1975, Microsoft (Nasdaq "MSFT") is the worldwide leader in software, services, devices and solutions that help people and businesses realize their full potential. Windows 10 IoT provides one management and deployment platform to span the entire spectrum of devices, from simple sensors to complex systems. Azure IoT Suite brings the Internet of your things to life enabling you to connect devices, analyze previously-untapped data, and integrate business systems – and transform your company when you uncover new business models and revenue streams.

For more information on Microsoft IoT enabling products visit [Windows IoT](#) and [Azure IoT](#)

To find out more about Microsoft IoT contact [msiot@microsoft.com](mailto:msiot@microsoft.com)

**Note:** This white paper is based on the independent research carried out by IoT Analytics. All views expressed are that of IoT Analytics and not the paper sponsor, Microsoft.

# Copyright

© 2016 IoT Analytics GmbH. All rights reserved.

IoT Analytics is a leading provider of market insights and competitive intelligence for the Internet of Things (IoT).

This document is intended for general informational purposes only, does not take into account the reader's specific circumstances, and may not reflect the most current developments. IoT Analytics disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. IoT Analytics does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

For more information, visit <http://www.iot-analytics.com>

