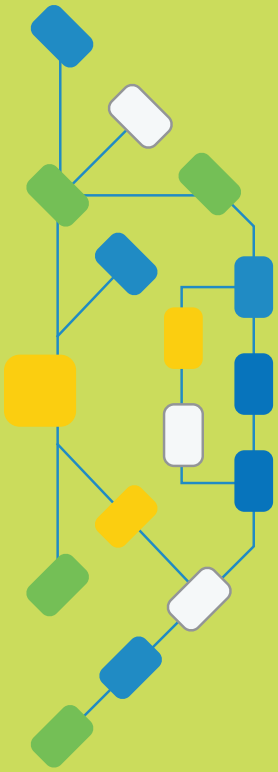
Orchestrating the Commercial Internet of Things

What happens when building equipment is connected?

By Martin Flusberg
CEO, Powerhouse Dynamics



Introduction: What is the Internet of Things - and Why Should We Care?

The term "Internet of Things", or IoT, has been around since 1999, when it was coined by Kevin Ashton, but it's only become well known recently. The availability of low cost sensors and communications has enabled IoT to gain momentum in the market. Of late, the term has been getting an incredible amount of attention and use. In fact, it's so ubiquitous now in so many industries that it can be hard to sort out a clear definition, and if anything the definition has been shifting over time. As it is commonly now understood, IoT enables physical objects to communicate with the cloud and, as a result, with various applications and potentially with each other.

IoT is being used, or has been proposed for, a wide range of applications, ranging from health care to city management, from energy production and generation to commercial building management, from industrial processes to supply chain management, and many more – not to mention numerous consumer applications.

Gartner reports that the industries that are leading the digitalization of everything include manufacturing (15 percent), health care (15 percent) and insurance (11 percent).

Each of these applications, taken on its own, has enormous potential. But, the implications in terms of the number of devices that will be connected is staggering. Gartner predicts 30 billion connected devices by 2020, up from 2.5 billion in 2009. Other sources project as many as 200 billion devices. Whichever number proves to be more accurate, this is an extraordinary number of "things" to be connected and monitored - which represents an extraordinary challenge.

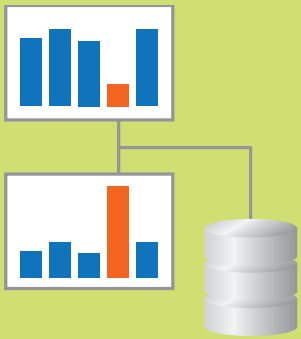
In addition to growing awareness of the Internet of Things over the past several years, the hype surrounding IoT has also begun to grow. More and more companies report that they offer an IoT solution or leverage one in the course of their operations – even if they are doing nothing new. The suggestion that the term is being hyped is supported by a recent Atlantic Magazine survey of 100 Silicon Valley executives, in which "Internet of Things" was ranked the #1 buzzword, beating out #2, "Unicorn".

While IoT clearly offers enormous potential, some of the hype may suggest the potential for chaos. For example, major appliance manufacturers have been touting connected home appliances for years. What are the implications of all appliances being connected to the Internet? How many "things" do you want reaching out to you? Do you want your Internet-connected refrigerator ordering milk when it senses you are low? Does that mean that the refrigerator will need to look at your personal calendar to know when you are going on vacation? What happens when your refrigerator, hot water heater, washer and dryer, dishwasher, and garage door opener are all bombarding you on a regular basis; how do you make sense of all of that information? And who else may be using the information, and for what purposes? Will multiple connected devices create multiple paths for hackers to get into your home network?

The implications of this type of connectivity are only intensified in a business environment.

Harnessing the Commercial Internet of Things

Not only are home appliance manufacturers connecting products to the Internet, but so are makers of commercial equipment. And this creates a potential challenge. A restaurant, for example, may have 20 or more major pieces of kitchen equipment from perhaps 10 or more manufacturers. It will also have several – perhaps as many as 10 – heating, ventilation, and cooling (HVAC) units, also generally from different manufacturers. From the manufacturer's perspective it is logical to want to provide additional value to both its customers and itself by connecting its equipment to the Internet, providing access to real-time data. But does it really make sense for the customer to have 10 different web accounts to get information on 10 different manufacturers' equipment? To juggle multiple interfaces



"While it's undeniably useful to connect inanimate objects and sensors to the Internet, that's only a first step in terms of doing something useful with all those connected devices. "The Analytics of Things" (AoT) are just as important, if not more so."

and different types of functionality? To wade through tons of data that may not be actionable – and that are not coordinated? Is there a risk that the customer may get conflicting alerts from different manufacturers, and that optimizing one piece of equipment may have unintended consequences on another?

The issue is that connectivity itself is not a solution. What is done with the information collected through that connectivity is the real key. We are only beginning to see more attention being paid to this issue. For example, a recent article in IoT Evolution pointed to one IoT vendor who is making the shift from "connectivity" to "deeper insights", recognizing that just being able to capture data does not provide a real solution.

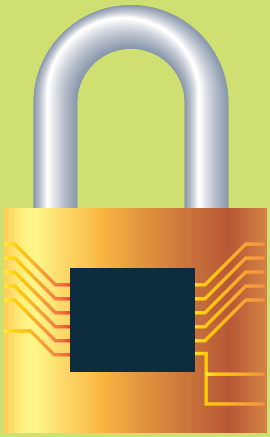
Making this point even more strongly is a 2014 article by Tom Davenport, a Babson College Professor, entitled "Analytics of Things". In that article and a subsequent report by Deloitte Analytics, Prof. Davenport points out: "While it's undeniably useful to connect inanimate objects and sensors to the Internet, that's only a first step in terms of doing something useful with all those connected devices. "The Analytics of Things" (AoT) are just as important, if not more so."

This focus on analytics begins to address the fundamental opportunity of IoT. Just as in other "Big Data" applications, the end goal is leveraging the vast amounts of potential information to achieve benefits.

Analytics, then, is a key to the effective use of IoT. But, the earlier restaurant example demonstrates another issue, which is the need for **aggregation and integration** of information from multiple sources. Does it ever make sense for every device to communicate independently? What is really needed for an effective IoT solution is a centralized system that captures data from disparate devices and analyzes the information as an integrated whole in order to take appropriate action – such as changing a setting - or provide actionable intelligence so that the user can make the right decisions.

Aggregation of IoT into a single a single communications infrastructure - rather than maintaining a unique path for each device - also begins to address another key issue – **security**. What are the security implications of many pieces of equipment communicating independently?

With the Target data breach in 2014, it was widely reported that the thieves came through the connected HVAC system. Even after it was



revealed that the breach occurred due to improper handling of a password to a different system by an HVAC contractor, there continued to be reports of an EMS breach. (I have personally heard that erroneous claim from an industry consultant at a conference).

But the fact that the Target breach was not caused by the connected energy management system does not mean there is no such threat. The threat is very real, and exacerbated by the explosion of connected devices.

A recent report by Deloitte entitled "Safeguarding the Internet of Things; being secure, vigilant and resilient in the connected age" does an excellent job of laying out the risks, and the steps that should be taken to minimize those risks. For example, it highlights the importance of developing an entirely new communications infrastructure rather than trying to retrofit an existing system not designed with secure machine-to-machine communications in mind. The report also highlights the dangers of relying on multiple systems from multiple vendors who may have differing levels of expertise when it comes to security. The report goes on to recommend some type of "hub" to integrate systems together and minimize the opportunities for breaches, and also recommends that organizations only work with firms heavily focused on security.

The report also highlights the dangers of relying on multiple systems from multiple vendors who may have differing levels of expertise when it comes to security.

So, for multiple reasons, in order for the potential of IoT to be achieved in each application there is need for a centralized system to aggregate the information from multiple devices and analyze and leverage the data as an integrated whole. This type of centralized system should operate like a conductor of an orchestra, making sure that the "musicians" – in this case the independent devices - work together in harmony.

With that analogy in mind, we at Powerhouse Dynamics describe this process as **"Orchestrating the Internet of Things"**.

What Can be Accomplished with an Orchestrated IoT Strategy?

In commercial building management, the Internet has already enabled us to move from "point" solutions to broader operational solutions that address multiple issues. For example, building management systems (BMS) have morphed from complex systems that require users to "dial-in" to each HVAC unit separately to enterprise systems where controls can be established and monitored centrally through the cloud. These new

energy management systems (EMS) have in turn morphed into systems that not only control HVAC and lighting but also monitor and analyze the performance of HVAC and other equipment. These systems deliver alerts in advance of equipment malfunctions, as well as other guidance on improving energy and operational efficiencies. This is a major step on the path towards an Orchestrated IoT.

But advancements in IoT create new opportunities for a much larger "orchestra". If manufacturers can connect their equipment to the Internet through an orchestrated system, there are significant potential benefits to the customers using the equipment, who now only need to deal with a single system. And, these benefits can extend back to the manufacturers as well, who can still gain access to the data to proactively identify equipment performance problems and help find ways to reduce equipment downtime.

Just a few examples of what can be accomplished with this approach follow:

- **Smart HVAC Management** – Many newer EMS systems analyze HVAC equipment performance by monitoring energy use and temperature, and perhaps pressure. But HVAC equipment from most manufacturers now generates significantly more information, and generally has built-in diagnostic capabilities. The problem has been that this information is typically available only to a local technician gaining direct physical access to the equipment. By capturing and uploading that information to the cloud, and integrating it with the information already available from a newer generation EMS, it is possible to develop an extremely powerful analytics and diagnostics capability that goes far beyond what has been available to-date. This can help to better maintain HVAC equipment, increase its useful life, and drive down energy costs at the same time. However, given that most facilities have HVAC equipment from multiple manufacturers, leveraging a stand-alone system from a single manufacturer will not deliver the same benefits as a system that leverages data from all manufacturers and integrates that data with other data to provide harmonized recommendations.

- **Food Safety/Smart Kitchen** – In a food service organization or food processing company, IoT can play a logical role in enhancing food quality and safety. For example, sensors are increasingly being used to track temperatures in refrigeration and food warming or cooking equipment. The data can then be uploaded and tracked and alerts sent if temperature readings are outside the required ranges. Some companies have started using systems like this to automate the time-consuming and very error prone process of HACCP (Hazard Analysis Critical Control Point) food safety reporting.

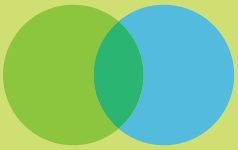
  Some manufacturers have developed ways to pull data directly out of kitchen equipment, including refrigerators, ovens, fryers, and dish machines, adding to the ability to better support food safety and food quality goals. With this type of monitoring, it is also possible, for example, to track the amount of chemicals available in a dish machine or how many times the fryer oil has been filtered in the past month. This clearly adds value; however, that value can only be maximized by orchestrating the flow of data from disparate sources into a single system that analyzes all of the data and provides alerts and exception reports. In addition, such a system may be able to adjust settings automatically and remotely if it identifies a problem.

  Moreover, additional data from other sources can be integrated into the same system to provide broader functionality. For example, energy monitoring of refrigeration equipment can be used to provide advance notice of potential problems, as well as additional diagnostic information as temperatures deviate from expected levels. Or, connected door sensors can be used provide notice of refrigerator doors being left open, even before the temperature begins to rise. The integration of data is only possible with an orchestrated approach to IoT.

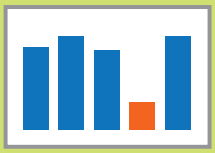
- **Smart Water Management** – Water costs are high and increasing in some parts of the country – and the impact of water leaks can be significant, particularly since the majority of water utilities bill quarterly or bi-monthly, meaning that by the time you realize there is a leak you will have already spent a considerable amount. This may be a particular issue for suburban banks, retailers and others with irrigation systems, where underground leaks may go unnoticed for extended periods. For this reason, water monitoring combined with analytics that identify leaks is an important instrument in the

orchestrated Internet of Things. Water can be monitored at the building level with meters that are able to be read remotely. It is also now possible to monitor water use at a more granular level using a variety of different types of sensors. Moreover, irrigation systems can be integrated directly into such a system enabling additional functionality, such as changes to schedules based on weather forecasts.

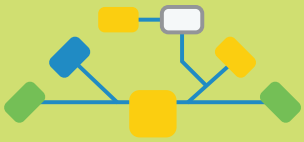
While these examples relate to different types of equipment, with an integrated IoT strategy all of these applications can be tied into a single system aimed at improving overall operational efficiencies.



Integration



Analytics



Orchestration

Security

End Note

The Internet of Things and the ability to connect more and more devices present many potential benefits across many industries, including the management of commercial buildings. There are numerous opportunities to capture and leverage data from equipment and devices in (and around) a commercial facility. To-date, there are few if any systems that address all of the opportunities outlined in this paper, much less the broader set of possibilities.

But the time is coming. If the Internet of Things is to deliver on all of the hype, we need systems that provide the right combination of:

- integration
- analytics
- orchestration, and
- security

This development will enable the true potential of IoT to be realized.