An approach to selection of IoT Plafforms

Introduction

So, you've investigated and identified some ideas of where IoT could help your business. You've done a high-level business case which is positive and indicates this should be worth pursuing. All good steps but at some point, you need to get into the enabling technology.

Perhaps you want to run a proof of value exercise, look at a larger scale pilot or if you're feeling brave enough to initiate a large-scale investment. Herein lies one of the major challenges. Search for IoT and you will uncover a wealth of different vendors making all kinds of claims for their technology. Where do you start? Who should you talk to?

State of the market

There is a pattern that tends to repeat with any new or emerging technology:

1. One or two pioneers kick things off, the ideas suffer from technology hype and everyone gets (over-)excited about the possibilities
2. Lots of predictions are thrown around about how 'big' the market will be, the hype grows
3. All kinds of businesses jump in, from start-ups to large corporates. There is a lot of choice in the market, with overlapping functionality, that you're not sure whether you need and deciding who to work with is hard.
4. Reality sets in - immature technology that doesn't quite deliver, unproven or unfeasible commercial models - and the hype dies down.
5. The technology and its application both mature, usually by learning from mistakes. Use cases are developed, solutions have an element of repeatability and the business case for investment becomes clearer.
6. The market consolidates and typically a 'handful' of major players emerge, either SMEs that have done well or large corporates who have made acquisitions.

Currently, in relation to IoT, we are in stage 4. Therefore, we do not have the luxury of running an RFI/RFP process with the top five market leaders, all with many years of real implementation experience behind them, as they simply don't exist.

Lots of companies have run IoT Proof of Concept exercises, but few have implemented large scale deployments. As a result, many customers, having 'dabbled' but struggled with a credible business case, are sitting back waiting to see how the market develops.

Selecting your IoT technology

If want to move now and get ahead of the competition, what should you look for when selecting your IoT technology?

Firstly, you should be aware you are unlikely to 'get it all' from one vendor. Companies that manufacture sensors are unlikely to be the same ones that provide wireless networking services or that are highly experienced in enterprise-class cloud software applications.

One thing we have learned in the last 20 years is to avoid building large proprietary business solutions. These end up with a very high cost of ownership, leave the customer beholden to the vendor and do not provide agility expected by the business. The current trend is to look for open,

extensible, ***platforms***. These aim to provide core functionality but in theory are easily integrated with other technologies, to reduce implementation time, cost and risk. In IoT, this aspect is very important, given the range of technologies required to create a usable solution, it is not just a 'software' play.

The market has matured at least enough that there are several highly capable platforms on which you can develop your specific business solution(s). None of them are perfect but this approach will allow you manage and grow your solution as the vendor develops new capabilities and resolves deficiencies.

Our recommendations are based on a number of 'principles', those necessary for any modern business when selecting IT:

1. Secure. Protect reputation, IP and mitigate financial loss.
2. Flexible/agile. Ease of adapting to the business need.
3. Open. Ease of integration and lower TCO.

What to look for?

These are some of the important IoT platform features to look for:

1. **A flexible, distributed architecture**. One of the key benefits of IoT is the ability to provide compute capabilities at the most effective point in the process. This may be on the device itself, perhaps to reduce network traffic, provide real-time control or allow limited 'offline operation' when network availability isn't guaranteed; it may be on a local compute 'network' device filtering data from numerous devices; it may be on a cloud-based service providing advanced analytics and historical insight, or centralised device management; or different compute may occur at each of these stages. For example:

    1. A device performs basic 'delta' processing so that only 'changed' real-world data is sent e.g. how many pairs of socks are there in the sock area of a retail store. Has it changed since the scan was last run? If so, then send the new value, if not then don't send anything
    2. A network 'edge' device takes inputs from 100 devices across the retail floor and performs some 'event' analytics, so only meaningful data is sent to the cloud hub e.g. which items are getting close to running out of stock or which items have been left in the changing room
    3. The cloud hub analyses and actions the insight e.g. check the stock room, check the changing area, initiate an employee task to restock the shelf, if item sold then initiate a request to order more stock from central procurement.

    As compute capability, storage, power management and networking capabilities improve you need to ensure you can move compute loads within the architecture, without being locked to the original model. This will allow the solution to scale easily for other workloads, provide agility to the business for the inevitable change requests, and reduce the cost of ownership.

    The interface for managing the architecture must be visual for ease of operator understanding and control but should have suitable governance controls so that changes are properly considered before deployment and can be propagated in a controlled manner e.g. per room, floor, factory, office, region, country etc.

2. **Open standards**. Avoid becoming constrained by proprietary standards. This will at some point limit the real-world data you can capture, increase cost of ownership and limit the business agility of the solution. Consider customers who were 'locked' into large scale ERP implementations in the 90's and 00's, who are still paying a fortune in support and maintenance and yet cannot easily move to lower cost, more agile alternatives. 'Open' doesn't necessarily mean 'open source' but you should ensure that any platform exposes its functionality via easy to use APIs and ideally is hosted with a PaaS (Platform as a Service) model, so you can just use the bits you need.

3. **Device management**. There is a large difference between doing a lab Proof of Concept with ten devices and implementing a global solution which could have hundreds of thousands of devices or more.
    a. How easy it is it to provision a new device? Ideally it should auto provision (but see below on 'Security'). You don't just want 'any old' device auto provisioning onto your network.
    b. How can you tell if a device is still working?
    c. How can you upgrade the device firmware to fix bugs, improve security or provide new functionality?
    d. How can you get a 'single pane' view of your device estate to ease monitoring?
    e. Do you have any 'self-healing' and resilience capabilities within your solution to fix or bypass faulty devices whilst maintaining the required service?

4. **Security model.** Much has been written about the need for effective security within an IoT solution and the threat is well founded. It is one thing to have customer credit card data stolen and people defrauded. It is a whole different world to have a power stations hacked, and shut down or overloaded. With this in mind, the importance of security will only grow as IoT solutions start to take on critical workloads. It is something that must be ***baked into*** the solution design from the start and not added as an 'after thought' once the rest has been built. An overarching model must be developed covering every component in the chain.

5. **Advanced analytics**. Collecting real-world data and managing those devices is a good start but unless you can build real-world data models and derive ***actionable insight*** you will show little value to your business stakeholders. Advanced analytics includes:

    a. **Stream analytics.** Analysing data in real time so the insight can be actioned in real time. Typically, operational technologies (OT) have this capability, but it is usually hard coded into the machine and not easily adapted to changing business need.
    b. **Historical 'Big Data' analytics**. Taking data from multiple sources, including your IoT data, to model the real-world better and understand cause and effect. Why does something happen? When might something happen again?
    c. **Cognitive Intelligence** such as Machine Learning, which can find insights that even the best data scientist would struggle with, given data volume and relational complexity.

    These approaches can allow your business to respond quickly and in many cases automatically to real-world events and allow you to predict when an important or critical event is likely to occur (e.g. machine failure), so that its effect can be mitigated (e.g. perform preventative maintenance outside core operating hours). It is perfectly feasible to source your analytical toolset from a different vendor than that providing your device management

and data collection capability, but there are some advantages to maintaining analytics within the same vendor product set.

6. **An existing partner eco system**. Most IoT solutions will involve multiple vendors. Having a pre-built ecosystem will make it easier, quicker and cheaper to deploy your solution as integration will have been pre-tested and ideally certified on your chosen platform, helping to reduce 'buck passing' when issues occur. Look for user groups where you can meet other customers who have already made deployments and where you can learn 'best practice'. Finally, think about what kind of field service is available for the installation or repair of devices that are not working. Again, when deploying devices at large scale this will be important to ensure continuity and quality of service.

Getting It Done

A final point to consider is whether you build a team in-house to design, implement and deploy, or whether you get some external help. At one extreme you can engage a 'Big X' consultancy or global System Integrator. Many will struggle to provide you with value for money or quick results, given the internal bureaucracy and process and one could argue are more interested in billing 'bodies' for as long as possible rather than achieving your outcomes. Building your own team keeps control in-house but skilled and experienced people are expensive, not that easy to find and time moves relentlessly.

A viable alternative is to blend these options, augmenting in house staff with a boutique consultancy with members that have 'been there and done that' to advise throughout the process, including platform selection. Typically, these have very experienced practitioners, are substantially cheaper than high end consultancies and can get things done with your agenda and outcomes top of mind.

Richard Braithwaite, IoT Advisory (http://www.iot-advisory.co.uk)
September 2018