INTERNET OF THINGS
PLATFORM SELECTION GUIDELINE

This Internet of Things Platform Selection Guideline contributes to the furtherance of the adoption of IoT technologies via this simple and concise paper. V1.0 May 2018

This Guide was developed by the Platforms and Interoperability Workstream (E4) of the IoT Alliance Australia (IoTAA) – http://www.iot.org.au/

Disclaimers

1. Notwithstanding anything contained in this Guide:
    a. Internet of Things Alliance Australia (IoTAA) disclaims responsibility (including where IoTAA or any of its officers, agents or contractors has been negligent) for any direct or indirect loss, damage, claim or liability any person may incur as a result of any:
        i. Reliance on or compliance with this Guide;
        ii. Inaccuracy or inappropriateness of this Guide; or
        iii. Inconsistency of this Guide with any law; and
    b. IoTAA disclaims responsibility (including where IoTAA or any of its officers, agents or contractors has been negligent) for ensuring compliance by any person with this Guide.
2. The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Contents

1 General

1.1 Introduction

The Internet of Things (IoT) Alliance Australia (IoTAA) – http://www.iot.org.au/ – is an industry organisation of over 350 member companies/entities with a vision is to empower industry to grow Australia's competitive advantage through IoT. The organisation aims to accelerate IoT innovation and adoption by:

- activating and supporting collaboration across industry, government, research and communities;
- promoting enabling, evidence-based policy and regulation; and
- identifying strategic opportunities for economic growth and social benefit.

Work Stream 7 of the IoTAA was formed with the aim of:

1. helping buyers to understand and choose platforms, and
2. to address interoperability within and between platforms.

In regards to the former of these, there now exists an almost bewildering array of IoT platforms and systems on offer to buyers; at last count well over 400. It has been requested by various buyers, and recognised by the IoTAA, that one of the most useful contributions to the furtherance of the adoption of IoT technologies would be the provision of a simple and concise Platform Selection Guide.

1.2 Scope

This document – the Platform Selection Guide – has been formulated to provide concise and relevant guidance for private and government organisations to assist in the adoption of IoT technologies. It aims to create a guide that will provide a "running start" for buyers to select between platforms. The intention with such a guide is to enable buyers to rapidly realise the potential of IoT in their product and service offerings to their customers, and in their internal business operations.

2 Acronyms and Definitions

2.1 Acronyms

3G: Third-generation mobile network

ACS: Australian Computer Society

GPRS: General Packet Radio Service

IIC: Industrial Internet Consortium

IoT: Internet of Things

IoTAA: Internet of Things Alliance Australia

IP: Intellectual Property

LED: Light Emitting Diode

2.2 Definitions

For the purposes of the Platform Selection Guideline:

IoT Platform

The term "IoT Platform" is used by technology and service providers to describe products which sit at very different positions within the IoT "technology stack" and generally don't (and shouldn't) span all layers. For example, and without meaning to pick on any one technology, there are LoRaWAN radio access service providers who offer a "platform" which is largely a low-functionality connectivity service not dissimilar to traditional packet data network services (GPRS, 3G, etc). Similarly, there are middleware providers who offer a "platform" which is largely a device interworking and data normalisation entity with little consideration for connectivity, data analytics etc. For prospective buyers of IoT platform this wide continuum of offerings can be both bewildering and a serious trap for the unwary. Hence, for the purposes of this Platform Selection Guide the Work Stream 7 of the IoTAA has chosen to use a broad definition for the term "IoT Platform", encompassing all layers of the technology stack and encompassing the various (access and middleware) standards. We have done so, so that a buyer can both initially understand and then choose the most appropriate "platform" or platforms for their purpose.

3 Internet of Things

3.1 Background

The term "Internet of Things" neatly encapsulates a vision of a world where virtually any electronic device with a (micro) processing capability is visible to, and can interact with, any other device or system. This includes any device with the ability to sense and report its environment, be controlled, and anything that can be tracked via electronic means.

This vision of the "Internet of Things" – whereby billions of devices ranging from sensors/actuators to appliances, vehicles to farm animals, health equipment to home/building automation, and more are connected – is driving the development of a range of new enabling technologies and applications. Given the broadness of the vision though, there are a plethora of both competing and complementary standards, plus a bewildering number of small and large technology suppliers all aiming to establish their place within the market.

3.2 The Four Phases of IoT Deployment

As of now – early 2018 – many businesses are yet to embark on significant projects to utilise IoT. However, the potential for IoT is great, with considerable progress achieved over the last few years.

In selecting an IoT Platform, the IoTAA notes that it is useful to reflect on a few key lessons learned from early IoT projects. Experience has shown that projects can easily fail to recognise the long-term implications of adopting IoT, and in doing so therefore overlook key requirements when selecting an IoT Platform.

It is relatively common to see IoT projects unfold in four main phases. These phases are illustrated in Figure 1, on the following page.

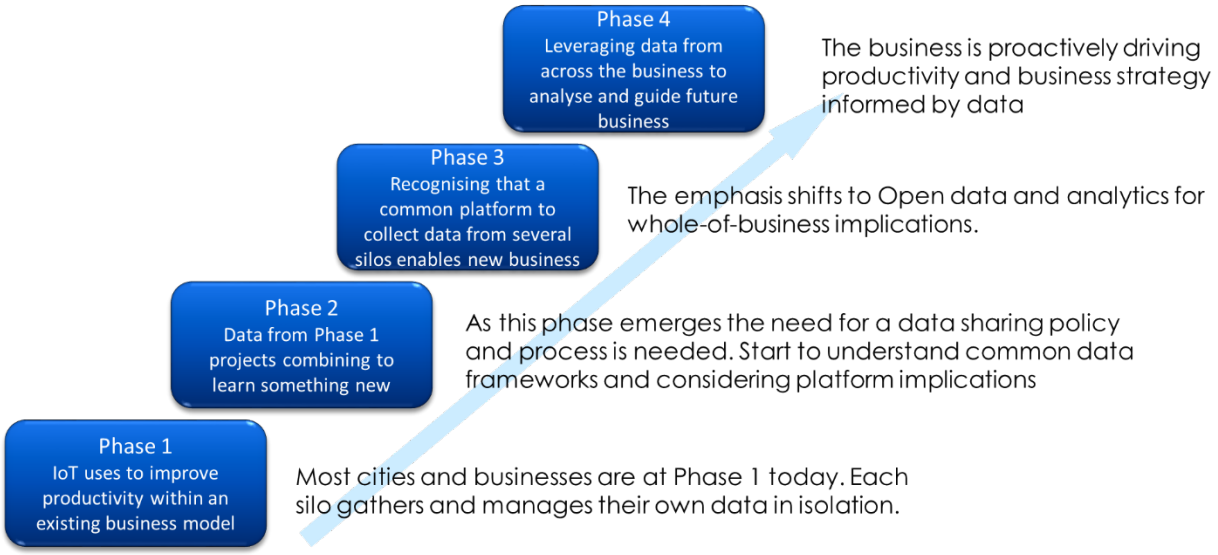

Figure 1: The Four Phases of IoT Projects

Starting with Phase 1, there are many initiatives today that fit this situation. Any project that sees sensors being added to existing business activities to improve efficiency fits here. A good example project is a "smart bins" project. Typically an existing waste management operation is looking to improve efficiency for possibly remote public bin emptying so sensors are deployed to advise the waste removal truck operator when to make the journey to empty the bin. The same can be said for a smart lighting project. Those responsible for lighting and energy efficiency may deploy LED lights with sensors/actuators for some form of remote control and monitoring. In each of these example, a single department makes a "siloed" decision for their own internal reasons. Today almost all projects are phase 1 style projects.

Phase 2 projects occur when a siloed project (Phase 1) recognises the potential of combining information from another department or silo to do something more innovative. So following our example, combining waste bin monitoring with smart lighting to offer a new service leveraging both data sets.

Phase 3 projects take this phase 2 thinking to the next level and then we see data being gathered from a range of sources and used for new business models that do not easily fit into any "traditional" silo.

Phase 4 is when the overall business is being strategically guided by data sources across the business. Today we have seen very few examples around the world of mature phase 3 or 4 initiatives however this is where the market sizzle is active. Phase 4 will see Artificial Intelligence come to the fore.

Consider the situation when two or more siloed departments embark on Phase 1 projects and in so doing choose an IoT platform to gather, store, secure and process the data. Then as Phase 2 emerges, each department wants to retain their platform for

more broad use across the business. Several platforms may have been purchased and the resulting internal competition to arrive at the "winning" platform cast valuable time and money. This is one of the reasons why it's so important to consider IoT Platforms and the implications of data sharing, and indeed interoperability, as early as possible in the IoT journey. Leveraging this guide and other sources, learn enough, early enough that your first steps along the IoT pathway are actually taking you forward and not in the wrong direction.

3.3 The Digital Economy

The Australian Government has embarked on a consultation process to assist with the development of a Digital Economy Strategy. Building on the project phases and sentiments outlined above, prospective buyers for an IoT Platform are encouraged to consider how their enterprise initiatives – including enterprise IoT Platform selection – fit within the broader Digital Economy. For example in the context of future cities, as one prominent vendor has articulated, to realise the potential of the Digital Economy will require the establishment of a "City Digital Platform" that spans multiple departments, government bodies and enterprises. This is not necessarily one ubiquitous system. Rather, a federation of multiple systems, including individual enterprise's IoT Platform instances. It is for this reason that buyers are encouraged to view their selection of an enterprise IoT Platform within the wider context. This is particularly important in terms of Data Sharing: how an enterprise's data fits within the broader context. As the Digital Economy consultation paper notes (DIIS, 2017):

> *"Data is a key economic asset. It can stimulate economic growth and innovation and improve the delivery of services, but it is underused. Around 90 per cent of the world's information was generated in just the past two years—but less than five per cent of the potentially useful data is actually analysed and used. Three out of four Australian businesses have stated that data analytics is not important at all to their business. Australian businesses may find themselves at a disadvantage if they are not able to collect and use important data while effectively managing community concern about privacy, confidentiality and transparency".*

3.4 Data Sharing and Interoperability

As digital technologies are increasingly used across the economy more and more information is captured and stored in digital form. This is true with regard to data gathered about citizens, about all forms of infrastructure and the environment – urban, rural and remote alike. In most cases data is gathered for a specific use but today data is being shared across traditional boundaries. More data is being shared for more reasons across more boundaries and this represents both a huge opportunity to enable innovation while also introducing a real risk of potential abuse of private information.

Government and business needs a Data Sharing Policy and we at the IoTAA think this need is urgent. It's clearly not appropriate to share sensitive private citizen data and it clearly is appropriate to share environmental data containing no personal information but between these two extremes there is a need for careful risk assessment and a robust Policy framework within which guidance can be provided to data owners so that appropriate sharing is established with the right mix of "enabling innovation" and "protecting the citizens privacy". Platforms that gather IoT data will find themselves being one of the vehicles for sharing that data appropriately both internally to the business and externally with suppliers and clients.

The NSW Government has lead a collaboration with the IoTAA and the ACS and others to develop a Data Sharing Framework that offers an approach that can guide the creation of a Data Sharing Policy and can then inform the creation of a Risk Analysis assessment of opening and sharing data. There is growing support and alignment across most states and territories that this framework should be a consistent reference for Australia.

Some of the benefits of a structured and consistent approach to data sharing and a policy of opening data appropriately are:

a. Protection of citizen privacy
b. Transparency of Government
c. Enabling innovation and jobs creation in the rapidly growing data analytics sector
d. Fostering an ecosystem for problem solving through the use of data that can link between industry, government and academia.
e. Help protect critical infrastructure while improving efficiencies across the board
f. More effective management of the environment and resources
g. Improved performance of services such as waste management, transport, utilities, health, aged care and many others.
h. Better sharing of data with and across states and territories, and local councils. Without a common framework across all three layers of government, data sharing is costlier and much less efficient, suppressing innovation and reducing efficiency.
i. Where appropriate, supporting open data.

3.5 The IoT Platform Technology Stack

As noted in (IoTAA, 2017), there is no one accepted architectural model for IoT, and the rapid evolution of all areas of the end-to-end technology continues to drive new changes to architectural models.

Appendix A: IoT Taxonomy and Technology Stack – of this document provides a brief introduction to IoT Platform architectures and standards development.

Although globally there are multiple different architectural reference models and standards from applicable bodies, buyers of IoT Platforms can derive significant value from choosing and then consistently applying such a model. As the IIC notes:

> "*A reference architecture provides guidance for the development of system, solution and application architectures. It provides common and consistent definitions for the system of interest, its decompositions and design patterns, and a common vocabulary with which to discuss the specification of implementations and compare options.*"

It is this establishment of a "common vocabulary" or taxonomy for IoT Platforms that buyers generally find architectural reference models most useful, as it provides a tool that they can use to compare solution options and offerings from different vendors and service providers.

At this time the IoTAA has not adopted a preferred architectural reference model. This is an item for further study. Nonetheless, the existing reference models presented in the appendix and elsewhere may be used by buyers to assist in platform comparison and selection.

3.6 A Useful Analogy for Platform Selection

In closing this section of the document, let us invoke an analogy to assist with our further consideration of IoT Platforms. Like virtually all analogies, it is limited; the value comes from the insights provided by the familiar. "IoT Platforms" can be considered like "logistics vehicles". Logistics vehicles encompass everything from the local pizza delivery motor scooter to a B-double petrol tanker. All have common components (e.g. wheels, motor, a steering wheel) as they are all vehicles, and all are used for delivery purposes – they all tick the same boxes (e.g. have wheels). The point being that across the spectrum that such a broad definition as "logistics vehicle" encompasses, each category of vehicle is fit for purpose. You normally don't use a B-double to deliver hot pizzas. Rather, the shrewd/wise buyer selects the best offering within the fit-for-purpose category that suits their business. The same perspective is true for IoT Platforms.

4 Guidelines for Platform Selection

4.1 Approach: It's all about Fit for Purpose!

With the increasing number of IoT Platforms on offer there are a number of papers which – similar to this Platform Selection Guide – aim to assist buyers in choosing an IoT

Platform. For example, (Bowen, Goel, Schallehn, & Schertler, 2017), (Lamarre & May, 2017), (Caceres, 2016), (Perry, 2016) and (Mobodexter, 2017). Not unsurprisingly given the strategic nature of such buying decisions, there have been key contributions from business consulting companies. The IoTAA offers this document as a further input built from the experiences of its authors in developing and deploying IoT solutions for customers over the recent years.

Note, this Platform Selection Guide is not written nor intended to be an off-the-shelf Request For Proposal template. Rather, it aims to present a methodology to help buyers gauge what is important to them and what is not, and from this, select an IoT Platform offering. Given that once selected the IoT Platform will likely remain embedded within the business for a very long time – as changing over potentially millions of closely tied end devices can be both costly and time consuming – finding the right platform is obviously a key strategic decision.

Drawing on the "logistics vehicle" analogy presented earlier in this document, the vast majority of IoT Platforms can claim that they tick all the boxes in terms of some coverage of the main components of the IoT technology stack. All have "wheels", a "motor", a "steering wheel", etcetera in some form. Hence, a tick-or-cross comparison is not overly insightful. Far more insightful is to understand the legitimate design constraints and decisions that each solution incorporates at each layer. These differences should be viewed in a positive light: not limitations but as necessary optimisations. For example, it is pointless to use an over-powered diesel motor in a small pizza delivery motor scooter. Hence, **one of the key aspects in selecting between IoT Platforms is understanding the design constraints and core characteristics of the platform, and hence to which category of IoT it best applies**. Beware the platforms that claim to be applicable for all IoT applications. In terms of the IoT technology stack, the "layers" (i.e. aspects) within which the optimisations are most impactful and evident are:

- The connectivity technology, including one-way or two-way communications
- The range of devices (i.e. protocols) that are or can be easily integrated and normalised
- The event processing and data analytics capabilities, especially relating to the depth of domain-specific knowledge that is already embedded
- Interoperability with other systems.
- The application build and execution environment, including edge versus centralised execution

Of course security, visualisation, data storage, etcetera are all important aspects as well, but the above four dot points are arguably the aspects for which there is the most impact and differentiation.

On the flipside of the coin to the above is knowing what you really want your IoT Platform to do. Are you running a pizza delivery business or a petrol transport business, or maybe both? To quote one of the IoTAA's own leaders: IoT Platform selection is "not just about hardware and software". As noted in (Caceres, 2016), it's all about the data and "By answering a few simple questions, customers can begin to define their capabilities and needs—a significant step toward choosing the right solution ..."

In summary – and to an extent it is motherhood, but its importance can be underestimated in the IoT space – **the key to successfully selecting an IoT Platform is focussing on "Fit For Purpose"!** That is, the most important step is understanding in sufficient detail the Purpose to be achieved, and hence discerning what design constraints/optimisations/emphases should exist within a platform to meet this Purpose. This discernment component should not be glossed over, hurried or downplayed by a supplier's claim that "our platform does everything for everybody". The buyer really needs to understand what type of "logistics vehicle" they really need and then buy accordingly.

4.2 What are you trying to achieve?

As noted above and echoed by other authors, the most important aspect of selecting an IoT Platform is knowing in detail the Purpose that you want the system to fulfil. What data do you want to collect and how do you want to use this data?

To assist buyers in identifying the key aspects that they should focus on, we will pursue a similar question-based approach as used in part by (Lamarre & May, 2017) and (Bowen, Goel, Schallehn, & Schertler, 2017). The aim is to isolate the aspects which will then enable a Best Fit offering to be selected based on a set of criteria derived from the answers to these questions.

In terms of ascertaining the Purpose for the IoT Platform, key questions to be considered are presented in Table 1.

Question	Rationale	Example Selection Implications
How extensive is the range of devices that you want to support? And does the range increase or change over time?	If a vast array of devices must be supported then integration must be easy. Alternatively, for your specific domain, support for a few complex devices may be what is required.	A telco service provider is likely to want an IoT platform that can support all the devices its broad range of customers will require. Alternatively, an IoT offering for microgrids is far more valuable if it offers deep integration for a very select few devices.
What data transmit and receive profiles do you require to support your devices? Are the devices fixed or mobile? Do you require connectivity to 100% of locations in your target area?	Connectivity technologies, especially radio technologies, have vastly different performance characteristics. This is further complicated with how service providers choose to deploy them (e.g. a "thin and crispy" network versus a "deep pan" network). Choosing the right one is akin to choosing the right size of motor for a vehicle.	Choosing a low data rate access technology usually precludes device software upgrades (e.g. to fix security issues) and greatly reduces responsiveness, but is all that is required for some scenarios (e.g. reading water meters). Power usage and (radio module) cost are important considerations in some contexts but may be immaterial for other scenarios (e.g. monitoring jet engines). Achieving reliable coverage in only 90% of locations (including hard to get places like on the ground behind the back shed) can make an IoT solution largely useless in some scenarios (e.g. meter reading).
Does your system need to react in a split second? Is the time between data collection and the system response critical? What is the balance you require between "hot" (real-time), "warm" (semi real-time) and "cold" (offline batch) event processing and/or analytics?	In most cases, a fast real-time response cannot be achieved with a centralised system, especially if the core of the system is located overseas.	If the IoT platform does not provide edge computing (aka fog computing) capabilities then it is going to be difficult to meet the requirements for real-time operation. "Warm" and "cold" event processing and/or analytics can generally be handled by traditional centralised cloud solutions.
Does your data require either complex processing or very domain-specific processing to provide the insights that you are seeking?	Most IoT platforms claim support for event processing and data analytics. However, for a large proportion of applications these implementations are largely useless as complex, domain-specific processing is what is really required to deliver the objectives.	Does the IoT platform already incorporate complex processing modules to support your particular domain and applications? Can external, domain-specific processing modules be easily integrated with the prospective IoT platform?
How often do you want to alter or build new IoT applications?	The ability to build, test, deploy and maintain applications within an IoT platform is a key requirement for virtually all IoT scenarios and platforms. However there are vast differences between IoT platforms in how successfully they support this paradigm.	For example, if you only ever want to infrequently build and deploy a small number of IoT applications then a basic set of Development Operations (DevOps) tools will suffice.

Table 1: Fit For Purpose – IoT Application considerations

4.3 What is the context of your business versus other businesses?

In the previous section, we sought to tease out the key aspects to what makes an IoT platform Fit For Purpose from a generic customer perspective. Buyers in the same market segment seeking to implement the same IoT application will largely provide the same answers for each of the above questions. Hence one may be tempted to assume that an IoT Platform which is Fit For Purpose for one type of IoT application would be applicable across all the buyers in that market segment. There is some truth in this. However, there are aspects of a business' operational context which can and should swing the IoT platform choice.

In terms of ascertaining how the business context can swing the choice of an IoT Platform, key questions to be considered are presented in Table 2.

Question	Rationale	Example Selection Implications
What assets do you already have and want to exploit in developing your IoT system? Does your board/CEO/executive have strong views on on-premise versus out-sourcing of systems?	Some businesses have significant assets (e.g. radio sites, data centres, in-house IT personnel, etc), and/or a history of doing-it-ourselves, such that an out-sourced model just won't fly. Similarly, a business may have a preference for capital expenditure rather than operational expenditure (typically required by "as a Service models).	Many IoT platforms and products are only offered by their suppliers as out-sourced, "cloud" solutions. Like other cloud services, such offerings generally have advantages in terms of time-to-deploy, cost, ongoing maintenance etc.
Is data sovereignty something that you are concerned about? Do you want/need to own your data? Do you want/need to keep your data within a given jurisdiction (i.e. it cannot be taken offshore)?	Data sovereignty and privacy is highly regulated. Further, organisations and governments often have strong internal policy positions as to where and how data is stored and what networks it transits.	Is there an option with the IoT Platform to have your data always remain on-shore and never transit (even briefly) offshore? How can you audit the data sovereignty at any time?
Can an IoT application generate revenue in a shared model with the IoT Platform provider? What is the business model which you are seeking to have with the provider/supplier? Risk versus reward. Partner?	Many IoT Platform suppliers have opted to only offer their products to buyers on a subscription basis. This does reduce set-up costs but is primarily used as a means of securing long-term, recurring revenue streams for the platform supplier.	In many cases governmental and related bodies are prevented from entering into subscription services, especially if the IoT Platform is to be classed as critical infrastructure. The government entity must have ownership over all assets so that they can continue to supply essential services in the event of supplier bankruptcy, war, etcetera. Equally though, IoT offers buyers an opportunity to change their

		operational cost structures and overall business model.
How is data shared? Is it clear what the data sharing policy framework is?	Sharing of data will be a key aspect to and success story for IoT. But if not implemented correct from the start, data sharing will fail.	Does the IoT Platform support data sharing and "cross tenancy"? How and to what level? Does the IoT Platform support open APIs and consistent data structures/models? Does the IoT Platform enable you able to quickly, easily and without expense gain access to your raw data?
How quickly do you want to be in market with your IoT-enabled product or service?	An out-sourced model with centralised systems in a limited number of data centres worldwide can greatly speed up and ease the development of new IoT applications.	How willing are you to place you IoT business in the hands of a "cloud" provider to gain a time-to-market advantage? Will this result in disintermediation or margin squeeze later on?
Do you or are you likely to have competing or siloed internal initiatives, projects and/or stakeholders? And if so, what constraints or prejudices does this bring	The interests of stakeholders can dramatically shift the selection of an IoT Platform. In most cases you are dealing with an established organisation which comes with its own history, preferences and aspirations.	In certain situations a single platform is appropriate, but in other situations separate platforms but with high interoperability (for data sharing purposes) may be appropriate.
Do you have external partners/stakeholders who will be sharing your data?	External stakeholders may have existing policies ad frameworks to deal with and negotiate.	For example, Academic partners may have different concerns about IP and commercialisation that need to be considered.
Are you interested in sharing revenue with application developers who leverage your shared data?	Mechanisms for sharing revenue can be complex and need to be considered early if it is desirable.	Does the IoT Platform accommodate this sort of business flexibility and provide tools to easily manage a range of sharing options?

Table 2: Fit For Purpose – Business context considerations

4.4 What makes a Minimal Viable Platform for you?

In the previous two sections we have explored the aspects of a Fit For Purpose IoT Platform Selection in terms of what the buyer is aiming to achieve and how a buyer's business context influences the selection. There are of course other dimensions which may, indeed will, be important to specific buyer. A number of these are what is commonly referred to as non-functional requirements. For the purposes of this paper let's categorise these as aspects as those that make a Minimal Viable Platform for a given buyer.

In terms of what makes a Minimal Viable Platform for you as a buyer, key questions to be considered are presented in Table 3.

It should be noted that two core requirements for an IoT environment are:

- privacy protection for personal identifiable data collected and stored within the environment, and
- system security ensuring that data is protected – both in transit and at rest – and that appropriate authentication is applied to any system providing data collection or device control.

Security and data privacy should be a paramount consideration if the system is collecting personal data or data relating to people. Further, it is always worth considering that malicious third parties will try to use any connected device/platform for nefarious purposes (for example, constructing bot-nets). The IoTAA provides specific guidance on security aspects in the IoTAA "Internet of Things Security Guidelines" (IoTAA, 2017).

Question	Rationale	Example Selection Implications
How much security and data privacy does your system require?	More security and privacy is preferable of course. High security can result in increases in cost and/or complexity. Too little security can lead to extensive downstream costs (actual or reputational). Lower levels of security may be acceptable where the platform is not collecting personal data. For example, data about dairy cattle movement may not need military-grade security and data privacy features.	Most IoT Platforms offer at least basic levels of security and data privacy. A thorough security and data privacy assessment should be a pre-requisite to the confirming of your chosen IoT platform. The "Internet of Things Security Guidelines" (IoTAA, 2017) is an excellent reference and guide to the security and data privacy aspects of IoT.
What end-to-end reliability and availability are you seeking?	Often buyer's expectations of IoT reliability are coloured by their experience with ultra-reliable communications systems like the Public Telephone Network (sitting at 99.999% or greater availability). Hence, significant attention must be paid to aligning a buyer's heartfelt expectations with IoT Platform offerings and actual needs while remaining cost effective and fit for purpose.	The IoT technology stack spans multiple different layers, each of which will contribute to an overall end-to-end reliability and availability figure. Evaluating all links in the chain for reliability is a very necessary part of any Platform Selection. This includes the time it takes to repair a fault and the details such as spare parts availability, as well as architectures that support appropriate duplication of critical elements of the system for example.
What level of integration with other systems is required?	Rarely can an IoT implementation reach its full potential if the data and insights remain siloed or an island inaccessible to other business systems.	Can the IoT Platform integrate seamlessly with your existing systems?

Table 3: Fit For Purpose – Minimal Viable Platform considerations

5 Concluding Remarks

There now exists an almost bewildering array of IoT platforms and systems on offer to buyers. As such, buyers can easily become overwhelmed when choosing between the platforms on offer, which in turn de-focusses and delays them in realising the benefits they envisage from their IoT projects. The IoTAA has authored this Platform Selection Guide to help buyers to understand and choose a platform. Given the vast breadth and depth of platforms on offer, the IoTAA advocates a meticulous and detailed Fit For Purpose approach, eschewing the temptation to believe that all categories of IoT platforms are created equal let alone implementations being equal. Further, that the context of a business is as important to choosing a platform as is the pure software and hardware on offer.

6 References

Bowen, P., Goel, A., Schallehn, M., & Schertler, M. (2017). *Choosing the Right Platform for the Industrial IoT.* Bain.

Caceres, A. (2016). Choosing and IoT System? Ask These 8 Questions to Platform Suppliers. *Electronic Design*.

DIIS. (2017). *The Digital Economy: Opening Up The Conversation.* Australian Government.

IIC. (2017). *The Industrial Internet of Things Volume G1: Reference Architecture v1.80.* Industrial Internet Consortium.

IoTAA. (2017). *Internet of Things Security Guidelines v1.2.* IoT Alliance Australia.

Lamarre, E., & May, B. (2017). *Making sense of Internet of Things platforms.* McKinsey & Company.

Mobodexter. (2017). *A Complete Guide to Choosing the Right IOT Platform.* Mobodexter.

Perry, M. J. (2016). *Evaluating and Choosing an IoT Platform.* O'Reilly Media.

Appendix A: IoT Taxonomy and Technology Stack

In 2014 Michael Porter and James Heppelmann authored an article in the Harvard Business Review that contextualised a structure for viewing the technology components which underpin the move to "smart, connected products" within the Internet of Things. This technology "stack" (depicted in Figure 2) defines the components which the authors assert are necessary to enable the move to smart, connected products, plus provides a new taxonomy to delineate the technology vendors and suppliers within the space. This taxonomy/delineation is also useful in highlighting the pivotal role that data plays in IoT and how component systems must seamlessly integrate to provide the full promise and value from IoT.

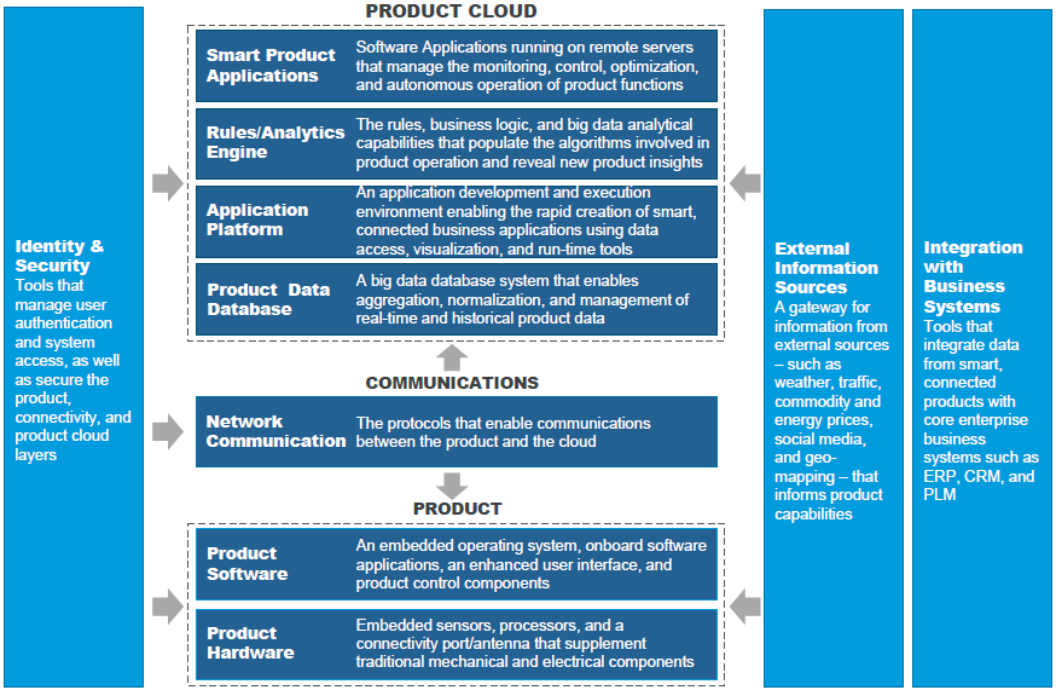

Figure 2: The IoT Technology Stack (Source: Harvard Business Review, Nov 2014)

Similar delineations have followed. The Industrial Internet Consortium (IIC) has developed the comprehensive Industrial Internet Reference Architecture as described in (IIC, 2017). Other contributions of note in the context of this Platform Selection Guide are the high-level IoT architecture described in (IoTAA, 2017) and depicted in Figure 3, and a recent IoT Framework contribution from Mr. Nam Nguyen depicted in Figure 4.

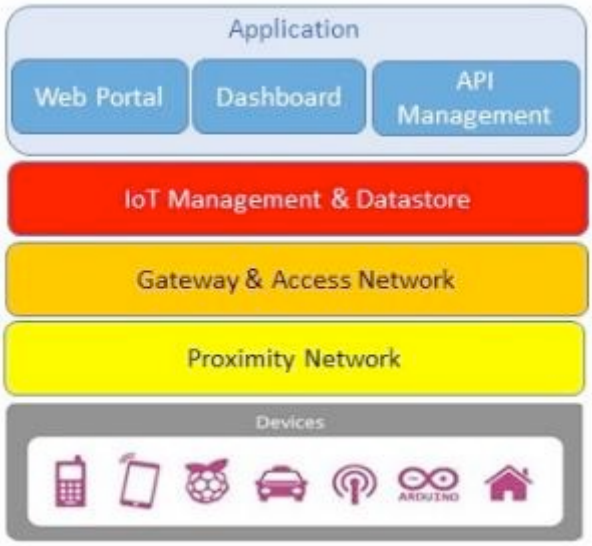

Figure 3 High-Level Reference Architecture for IoT

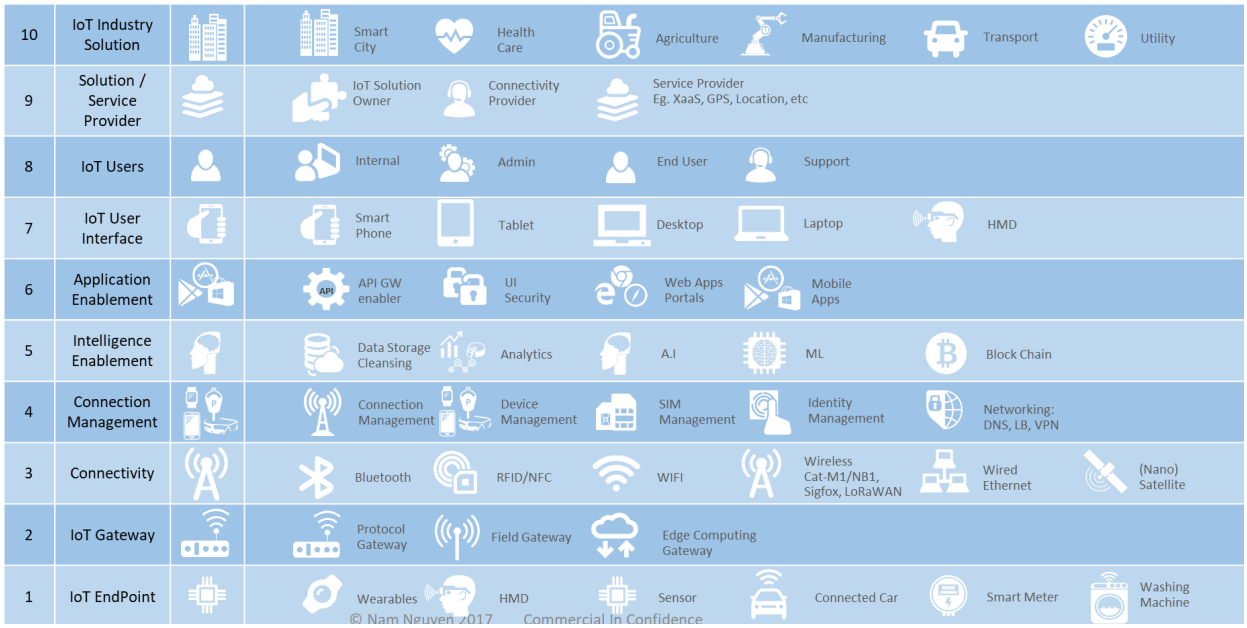

Figure 4 IoT Reference Framework (copyright Mr. Nam Nguyen)

Standardisation activities for the IoT technology stack have largely coalesced around two main areas:

1. The access connectivity technology, with low-power radio technologies being the key focus (including the associated network interface cards on the devices). Radio access has been a veritable battleground for competing technologies

include 3GPP NB-IOT, 3GPP LTE-M, LoRaWAN, SIGFOX, Ingenu, Wi-SUN, 802.11ah, etcetera.

2. The middleware software to control and manage devices, plus process data. Data analytics software and application development environments also sit at the upper end of this area. Key initiatives in this space include the now combined Open Connectivity Foundation IoTivity and AllJoyn activities, and OneM2M.