Level 6, 412 Collins Street
MELBOURNE VIC 3000
Ph (03) 9642 0655 Fax (03) 9642 5177
www.rayagroup.com.au
ABN: 89 122 203 196

ASX Release

23 December 2015

Independent Technical Expert Review on Xped

Raya Group Ltd (**ASX: RYG)** ("**Raya**" or "the **Company**") is pleased to announce that Dr Daniel Floreani of Flocom Consulting has provided an independent Technical Expert Review on the technology developed by Xped Holdings Limited (**Xped**).

The review was prepared on behalf of Raya Group with the report attached below.

About Xped

Xped has developed revolutionary and patent protected technology that allows any consumer, regardless of their technical capability, to connect, monitor and control devices and appliances found in our everyday environment. It's as simple as two people shaking hands. By enabling the Internet of Things, Xped's Auto Discovery Remote Control (ADRC) platform will bring benefit to Manufacturers, Retailers, Service Providers and Consumers.

Under a conditionally accepted Heads of Agreement signed on 25th October, 2015, Raya Group Ltd are in the process of acquiring Xped Holdings Ltd, including its subsidiaries and assets.

At Xped, we're ***Making Technology Human Again***.

ENDS

For further details please contact:

Raya Group Inquiries:
Company Secretary
T 03 9642 0655
E info@rayagroup.com.au

Company Advisor:
Faldi Ismail
Otsana Capital
M 0423 206 324
E Xped@otsana.com

Xped Holdings ltd

Technical Expert Review

Flocom Consulting

www.flocomconsulting.com

danielf@flocomconsulting.com

Executive Summary

The IoT market has been estimated to grow to 50 billion devices, and an addressable global market of $80 billion by 2020. If IoT is implemented correctly, integrating people, places, and things into our cities, industries and homes, it is expected a grand total of $14 trillion worth of value would be released to the global economy. Unsurprisingly there are many competitive companies chasing this market. IoT requires solutions that encompass cloud services, analytics, communications, things and thing services. This requires companies to become part of larger ecosystems for solutions and standards.

Xped have created one of the world's first human friendly solutions for the on-boarding, control and management of an IoT enabled "thing" by a smart device (PC, phone, cloud app). In a world where there are currently no overriding standards, and many large players are jostling for position, Xped has real technology that can be integrated into devices by manufacturers, reducing their time-to-market.

The key aspect of the solution is to utilise the NFC function that is increasingly found in our smart phones and smart watches to interface with a wide range of IoT devices, extracting information from the "thing" to carry out a large range of tasks. Xped's solution leverages existing standards wherever possible. Where they have defined new open standards, such as their markup language for data within a "thing", they seem to be closely aligned to other standard body's activities.

The Xped go to market model of open sourcing their protocols and languages, but retaining the right to sell their IoT stack via a number of form factors, aligns with the trend adopted by some participants in the IoT marketplace. Xped has protected its key intellectual property via patents. In addition, they have developed other related technical concepts that are also patented which may generate future revenue streams.

The IoT market is in a stage of flux, with strategic partnerships forming, security risks being ameliorated, and new products being brought to market. In this dynamic stage of development, Xped is offering the ADRC solution to speed up the go to market plans of other players who wish to develop IoT based products. Xped is also intending to introduce other IoT devices of its own for sale. Adopting a flexible business model allows Xped to pivot into different IoT markets (hardware, cloud services, and subsystems).

Whilst Xped is in a very competitive market, the approach adopted by ADRC is appealing due to its simplicity and ease of use. I am confident that other vendors would look at ADRC, either to integrate some functionality, or to licence the technology for their own hardware.

KEY POINTS

The IoT Market is expected to be $80 billion by 2020.

Xped have developed a novel solution that simplifies interactions with IoT devices, called the Auto Discovery Remote Control Protocol (ADRC).

Xped have protected their intellectual property via various patents.

The ADRC solution works in standalone mode, or in conjunction with cloud services to provide more value.

The Xped go to market plan is flexible, planning to sell to integrated circuit manufacturers, product manufacturers, and in some cases direct to the end customer.

Xped have also developed and patented other concepts related to IoT and ADRC that might generate revenue in the future.

Whilst the IoT market is real and huge, many issues threaten to slow IoT adoption such as security, cost benefits and standardisation.

Contents

Opening Statements

Statement of Work

This report has been prepared on behalf of the RAYA Group to provide an independent technical expert review on the technology developed by Xped Holdings ltd (Xped). The report is based on information gathered from Xped, material supplied by RAYA Group, and information collected from the Internet.

The following aspects have been addressed within the report:

- **IoT Opportunity** - the current state of the IoT market and how Xped fits within this market.
- **Business Assessment** – a description of, and comments on, the Xped business model.
- **Technical Assessment** - a description of the Xped solution, an analysis of the key technical functions, and lists of competitive technology and vendors.
- **Risk Assessment** - a list of technical risks in the IoT marketplace.

It must be noted that the IoT market is highly dynamic where many vendors are offering diverse solutions, void of an agreed standard architecture. In such an environment the analysis is a representation of opinions at a single point in time.

Statement of Expertise

Dr Daniel Floreani, Director Flocom Consulting.

Daniel has 25+ years of experience in the communications industry. He has worked for a major Internet solution provider in national and global roles and has been involved in defence, manufacturing and academia. In his career he has designed, sold and installed IP solutions, all the way up to business development for IoT consulting services. Daniel has a PhD in Communications, a Bachelor of Engineering and a Bachelor of Science, is TOGAF certified, and has a GAICD.

Disclaimer

The opinions expressed in this Report have been based on the information supplied to Flocom Consulting by Xped Holdings. The opinions in this report are provided in response to a specific request from RAYA Group to do so. Flocom Consulting has exercised all due care in reviewing the supplied information. Whilst Flocom Consulting has assessed the provided information based on experience and other resources, the accuracy of the opinions in the review are entirely reliant on the accuracy and completeness of the supplied information.

Flocom Consulting advises that:

a) Flocom Consulting has no interest in the outcome of the transaction between Raya and Xped.
b) Flocom Consulting has considered its independence with respect to ASIC Regulatory Guide 112: Independence of experts and is, in its opinion, independent of both Raya and Xped.
c) Flocom Consulting has the appropriate skill and experience to prepare the Technical Expert Review.

SIGNED  DATE 15 – 12 - 2015

Daniel Floreani, Director, Flocom Consulting

Introduction

The Internet of Things (IoT) requires the production of “things” that can communicate via the Internet with people, or to other “things”. The latter is often called machine to machine communications (M2M). These “things” can range from complicated machines such as automobiles, to household devices such as sprinklers. Some “things” are sensors, some “things” are actuators. Some “things” are neither, such as a bus stop, which is just a location where people need information. As a result the wider IoT ecosystem involves people, places, and “things”.

The driving force behind many IoT solutions is to gain deeper insight into systems via analytics to automate menial tasks, enhance productivity, create new business models, and generate new revenue streams. IoT is then seen as a generator of massive amounts of data by “things” that can be stored and analysed in the cloud or elsewhere. As such IoT is linked to the other big current technology drivers of “big data” and “analytics”.

Whilst IoT is deemed a new field, the principles behind IoT have been adopted by manufacturing, mining and defence industries for many decades. The recent IoT push is now taking the traditional process control ideology and applying it to everyday life. This implies applying it to our home, our cities, the environment, and our bodies to name just a few scenarios. In essence IoT aims to solve the mantra - ***you cannot control what you cannot see***. What is different is that past efforts have been in highly controlled environments with heavily engineered solutions. The current IoT environment is driven by consumer style devices, smartphones, and low power and sparsely connected environments. ***It is into this ecosystem that Xped intends to supply its solution in order to provide a robust scalable platform for IoT and M2M applications.***

The Xped solution evolved from a desire to revolutionise how “things” are controlled via remote control style interfaces. The intent was to replace the multiple remote control devices with a solution that enables any smart device to replace the functions of multiple controllers. This then led to the auto-discovery remote control (ADRC) technology suite that utilises near field communications (NFC) to provide an extensible and dynamic interface to “things” so that they can talk to people and other devices via a generic device browser, using a common language based on XML. Unlike most IoT solutions, Xped have not started with the premise that devices must contain an IP protocol stack in order to be part of a network. However the ADRC control mechanisms invented can also be used to run over a wide range of communication links, including IP networks.

Note – for consistency this report uses the term “thing” to encompass products that are connected to the network and are controllable or provide input into some IoT process. It uses the term “smart devices” to refer to products such as smart phones or tablets.

The Internet of Things

Opportunity

Many of the largest players in the world IT economy such as Cisco, General Electric, IBM as well as the major consulting firms such as KPMG, Accenture and Forbes have predicted a massive growth in the IoT revolution. Numbers vary[1], but estimates of up to 50 billion devices connected to the Internet by 2020 and a total addressable market in the order of US$80 billion and an increase in global productivity of US$300 billion by 2020[2] . From a local perspective the Australian market for IoT is expected to be in the order of A$200 million by 2020[3].

The IoT market can be segmented into many smaller market verticals, as well as into horizontal vendors and service providers[4]. Some of the verticals include:

- Home (toys, security, automation, lifestyle/entertainment)
- Transport (public transport, personal vehicles, international transport)
- Connected cities (tags, public security, environmental monitoring, traffic monitoring, smart buildings)
- Person (fitness, healthcare, wearables)
- Industry (trackers, meters, sensors, actuators)

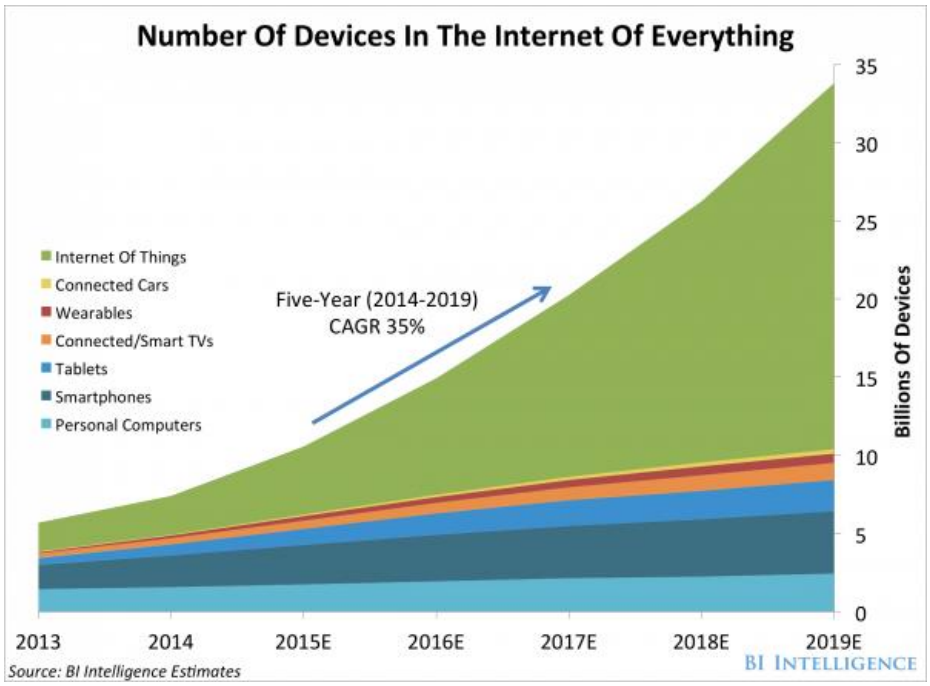

Figure 1 – IoT Device Number Predictions[2]

[1] http://www.ironpaper.com/webintel/articles/internet-things-market-statistics-2015/
[2] http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/
[3] http://www.iotaustralia.org.au/2015/11/06/iot-facts-and-forecasts/aussie-iot-in-the-home-spend-tipped-to-top-200m-in-2020/
[4] IEEE Standards Association (IEEE-SA) Internet of Things (IoT) Ecosystem Study

The providers of IoT hardware and services fall into a number of categories:

- Providers of sub systems of things (chips, firmware, modules).
- Providers of things.
- Providers of communications.
- Providers of applications.
- Providers of cloud services.

Most IoT vendors work across some of the categories above in order to provide a working solution. This means those who traditionally specialise in the provision of “things”, now need to understand communications, applications and a level of cloud services. Alternatively providers of cloud services now need to understand how to interface to “things”. It is into this new dynamic market, complicated by a lack of standards, or conversely too many competing standards[5], that Xped is entering and attempting to solve.

Ecosystem

The recent interest in IoT is driven by the desire to access some of the US$ 14 trillion “value at stake” estimated by companies such as Cisco[6] between 2013 and 2022. This study factors in the ability of IoT to reduce costs and increase revenue. In order to make this a reality a new ecosystem is required that delivers the full suite of IoT related services to customers.

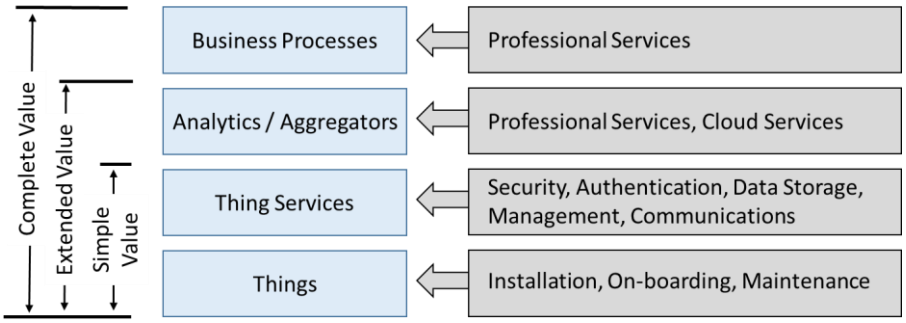

Figure 2 – IoT Ecosystems and Value at Stake

The installation of “things” and the basic services that sit above them, provide the first level of value and is based on simple self-contained IoT services. To gain extended value the IoT data is then aggregated to the cloud to gain further insight or automation via analytics. Interfaces with other IoT verticals is also achieved at this level (ie health systems interacting with transport systems). These solutions will need a level of professional services to conceive, design and implement. Finally in order to gain the full level of benefit from IoT, enterprises and organisations will need to invent new, or change existing business processes to unleash a new age of productivity and cost reduction.

Xped will need to select a range of partners that allows them to be part of a complete IoT ecosystem to ensure that their solutions release the promised “value at stake”.

[5] http://standards.ieee.org/innovate/iot/stds.html
[6] http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf

Business Assessment

Stated Business Model

The aim of Xped is to deliver a solution that "makes technology human again" by markedly simplifying the IoT on-boarding process and the provision of a single application or browser to control "things". Xped's ADRC IoT platform technology is now in the commercialisation phase. The company is currently engaged at various stages with a number of parties in Australia and Asia. To further drive acceptance and implementation of Xped's technology in a rapidly changing market, Xped has developed the following business models[7]:

- Xped's core business is to license ADRC to be integrated into 3rd party products. A diverse offering ensure IP can be integrated at any stage in a product's development cycle. The IP can be packaged and licensed in several forms including supplying a software stack, a pre-programmed chip or a chip on a module. Providing solutions that target semiconductor vendors, product designers and manufacturers provides greater flexibility and minimises barriers to entry.

- Xped have designed a range of consumer products that would be made for available through local and international distribution and retail channels. The preferred model is for these designs to be licensed as reference designs for 3rd party Original Equipment Manufacturers (OEMs) to manufacture and sell through their own channels. Xped would receive a royalty for each unit produced.

- Xped's platform disrupts industry business models by transforming manufacturers from box movers to service providers fostering direct relationships between all stakeholders. The platform provides the ability to monetise services with revenue streams coming from cloud service charges through to e-commerce. Xped will continue to develop and explore opportunities to commercialise these services through partners

Comments on the Business Model

Novelty of Solution

Xped have the technology and the appropriate patent protection to execute against the business model listed above. The ADRC solution is a novel approach to interfacing between "things" and smart devices that is intuitive and quick to adopt. It requires the manufacturer to embed the information required to on-board a product within the device, reducing installation complexity. This is one of the driving forces of the IoT industry, taking complex IT technology and making it usable for the consumer. Xped have taken a significant step towards achieving this goal.

[7] http://www.xped.com/what/licensing/

Speed to Market

The Xped ADRC solution may appeal to vendors of “things” who are not tied to large vendors, or existing standards bodies, and who want to get to market quickly in an independent manner. The business model of supplying a simple IoT stack to insert into their devices and things is an attempt to lower the cost of entry into the IoT market.

The Xped customers would benefit as they can enter the market with the majority of the communications, applications, and cloud services already available. By adopting a proven solution they are also able to leverage off the software and security testing inherent in the Xped solution.

Application and cloud providers can develop and sell products and services based on ADRC as they have a known open interface when they interact with ADRC compatible devices. This would provide more incentives for hardware vendors to integrate ADRC firmware as their time to market will be quicker with already existing cloud providers familiar with ADRC.

Development Flexibility

The current Xped “go to market plan” is quite open, allowing them to partner with companies in all aspects of the IoT ecosystem (chips, products, cloud, etc). This is enhanced by the potential wide range of uses for the ADRC solution. At this early stage it is unclear which path will succeed, but the inherent flexibility brings with it the ability to develop the solution in many directions to meet future customer demand.

Competition

The IoT market is very crowded with many diverse solutions. This website[8] created in August 2014 lists 49 companies alone that are active in the IoT space. There are likely to be hundreds more in existence.

There are others who provide similar services to Xped such as Open Remote[9]. They provide design services, cloud and account services, as well as licencing technology for OEM or system providers who wish to enter the IoT marketplace. Whilst it is not clear how much of their technology is unique they do offer a complete service similar to what Xped plans to offer their customers.

Standardisation Issues

Xped claim to help fix the lack of an overarching IoT standard by releasing their own open standard for others to adopt. There are many paths to creating a standard, one is standardisation by size of market or customer influence which favours major vendors (Apple, Google, Cisco) and not Xped.

An alternate path to standardisation is to claim early adopter position which Xped can with its patents and ADRC technology demonstrators.

[8] https://blog.profitbricks.com/top-49-tools-internet-of-things/
[9] http://www.openremote.com/

However the easiest path to standardisation is for ADRC to be adopted by a number of major manufacturers or chip vendors which can carry out the standardisation effort on behalf of Xped in standards bodies.

For ADRC to be widely adopted it is crucial to be involved in standardisation in some way.

Single Browser Claims

Xped claim that their solution requires just one app to talk to IoT things. We suspect that any user would probably use with multiple apps, even in a pure ADRC world, for each IoT domain. There would be one for city based things, one for home things, and one for work things. This segmentation would be required for scalability, management, and security aspects. This is an opportunity as represents the ability to sell the solution multiple times to different customers for services delivered to the same end customer.

Possible New Services

If the ADRC solution is adopted by a number of significant hardware device manufacturers, then the owners of ADRC are then in a powerful position to develop extra functionality tied to ADRC that can create more value and revenue. Future services have been proposed within the ADRC and NFC payment framework such as sales vouchers, location based services and promotional material. Some aspects of these concepts have been patented by Xped.

A benefit of the ADRC solution is the ability to have unique information placed in the “things” IoT stack during manufacture. During the on-boarding process, the “thing” could automatically register with the manufacturer and carry out an automatic warranty initiation process. On top of saving warranty procedural costs, this could help the manufacturer understand where the product was actually installed for sales and marketing purposes. This includes investigating grey marketing practises.

The automatic warranty service could be used to develop a direct relationship with customers and allow direct marketing on product specials, security announcements, end of warranty announcements, device firmware upgrade notices and other e-commerce opportunities.

Xped plan to develop a cloud version of their Hub which will allow simpler collection and dissemination of IoT data, as well as accessible cloud analysis applications in the future. Cloud based solutions are important for larger smart city based solutions. They are also important for sharing data between IoT domains (home, work, city). The development of an Xped cloud service could open up other revenue streams for Xped in the future.

When Xped starts to build cloud services they will need to build and test cloud security features, including securing the data at rest in the cloud.

Xped is currently in a flexible position as it has protocols and software, multiple form factors for its IoT stack, and the intent to sell IoT devices via an OEM model. This makes it well positioned to enter many of the IoT verticals, and maximise its potential addressable market size.

Technical Assessment

The IoT Models of Operation

IoT solution providers have adopted some common models to deliver IoT solutions. The first option is that creators of “things” start by building an Internet connected device, then build a cloud based service for it to talk to. This serves the dual purpose of providing a secure interface to a smart device and to provide a common and secure interface for “things”.

If a customer has multiple separate vendors of “things” at home then they will have just as many apps and cloud services on their smart device. If a customer wants to integrate separate solutions they need another cloud service to interface to their existing cloud services to share information. This is called the cloud centric model shown in figure 3(a) below.

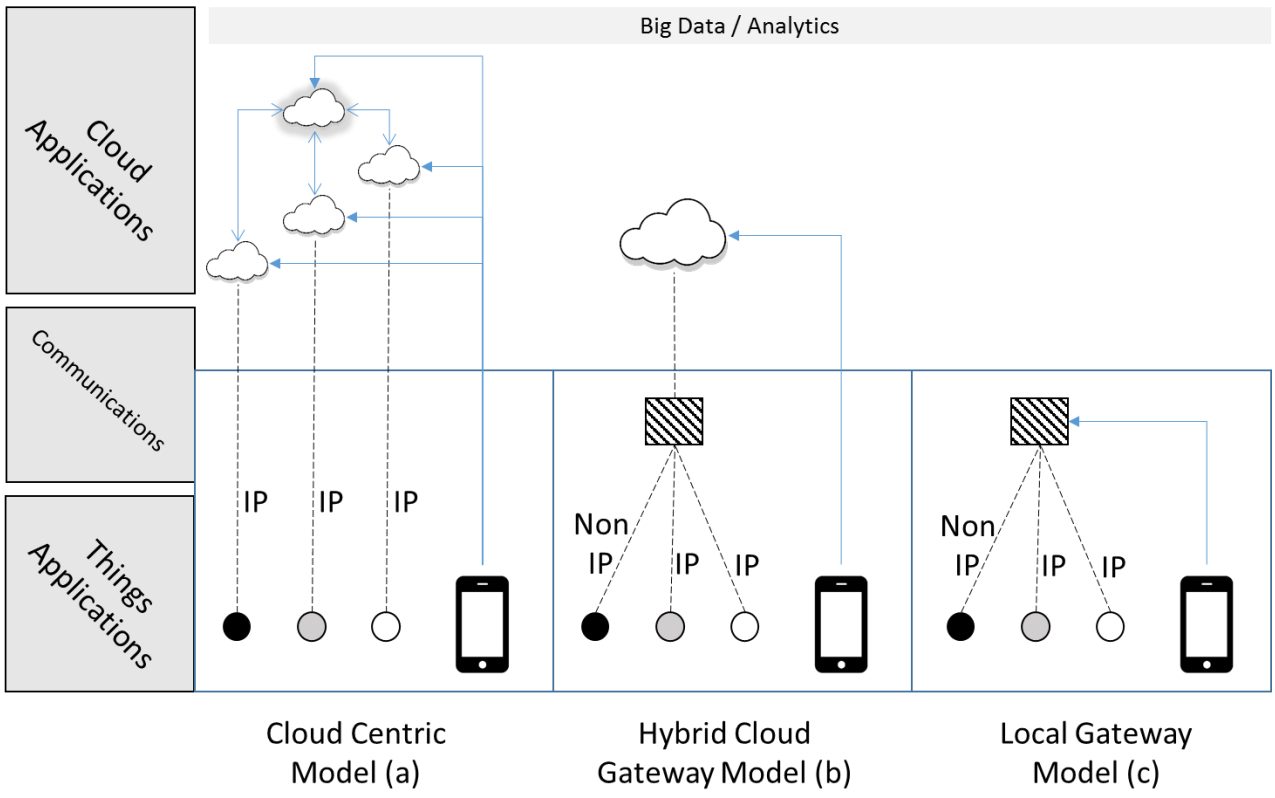

Figure 3 – Traditional IoT System Models

The simplest approach is to provide a gateway that does not need to connect to the Internet or any cloud service. This is the oldest approach and is inherently the most secure model as well. This is the Local Gateway Model shown in figure 3(c). Gateways allow “things” to have the option to utilise low power Non IP radio bearers for communications as well as power hungry and CPU intensive IP based protocols such as TCP/IP or 6loWPAN. This allows

simple “things” to be connected that have low power and communication overheads, but still have access to an IP connected smart device via the gateway.

Alternatively, other IoT solution providers offer a gateway that can interface with multiple different types of “things” over many different communications bearers (WiFi, Bluetooth, Zigbee, LPD433, etc). This requires the gateway provider to invest heavily in order to integrate large numbers of heterogeneous devices using many different standards. A cloud service is also required in order for the smart device to have a secure connection and allow the devices to be seen and controlled from anywhere. This is the hybrid cloud gateway model shown in figure 3(b).

Based on a few dependencies, Xped’s ADRC technology can be deployed in all three models above for IP, non-IP and legacy devices.

Xped Solution and IoT

The Xped solution[10] comprises 5 different modes of operation between “things” and smart devices.

Firstly a smart device can talk directly to an ADRC enabled “thing” via a bump mechanism where the smart device is placed near the “thing”, (figure 4(a)). This initiates a communication path for the commencement of the on-boarding process. The smart device and the “thing” initiate a NFC forums standards based process to transfer information called NFC Data Exchange Format[11] (NDEF). It then transfers the following information in order to initiate the ADRC process:

- Meta data such as manufacturer, model, icons, etc.
- Security keys for communications.
- Available bearers and MAC addresses for the “thing”.

Armed with this information, the smart device then communicates with the ADRC hub. The hub then probes the thing via the chosen PAN technology (Zigbee) and transfers resource meta language files (RML) embedded in the thing to the Hub and to the smart device. This all occurs within seconds. The on-boarding of the “thing” to the smart device’s device browser (DeB) can now occur. In its simplest form the smart device now becomes a smart version of the remote control for the “thing”. The key point here is the information about the “thing’s” capabilities are now known and can be stored on the smart device or the gateway for later use.

The second mode is that once the “thing” has been on-boarded, the smart device can now interact with the gateway or ADRC hub from anywhere in range of the local WiFi (figure 4(b)). The hub will have been placed in a location so that a personal area network (PAN) connection to the “thing” is possible. The hub will also have a copy of the RML file as a result

[10] ADRC Marketing Material, www.xped.com, Xped Corporation
[11] http://members.nfc-forum.org/specs/spec_list/

of the on-boarding process. Control can then occur via the ADRC protocol from smart device to the “thing” using a local fixed or wireless IP network.

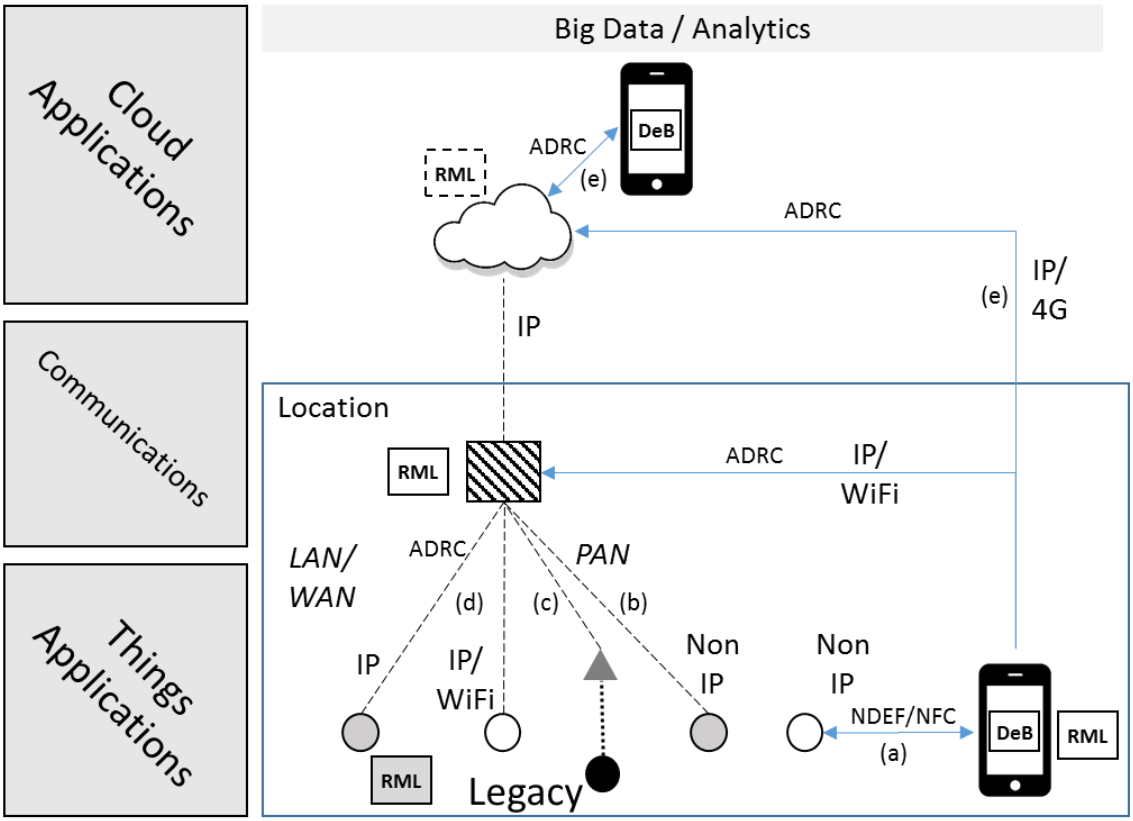

Figure 4 – Xped IoT System Models

The third mode is for legacy “things” that don’t support NFC or the ADRC protocol (figure 4(c)). Xped have developed intermediary devices that convert ADRC to native RF or IR control signals like traditional remote controls.

The fourth mode is for “things” that already contain IP stacks and can communicate via cables or over WiFi to an IP network (figure 4(d)). Smart devices could talk directly to the thing via IP via their proprietary interfaces, but Xped are proposing that they utilize the ADRC solution to unify their approach and have a common browser and resource description file for all “things” (IP and Non-IP enabled). A common laborious task of on-boarding IP devices is the initial setup and IP configuration. The ADRC on-boarding process is by comparison much simpler and would alone be a benefit to any traditional IoT solution.

The modes described so far are available in the offline mode where the gateway or ADRC hub is offline from the Internet. The fifth mode is when this gateway is connected to the wider Internet and it is then possible for the smart device to access its “things” from anywhere. This mode also includes the possibility of other applications in the cloud being able to automatically and remotely access, monitor and control “things” (figure 4(e)).

As described above, Xped modes (b), (c), (d), and (e) map to the traditional IoT models shown in figure 3. However even mode (a), which is purely local and non-IP, can still introduce a novel mechanism for placing uniform resource locators (URL) within the RML files (figure 5). This enables the smart device to browse the URL via a traditional browser and access relevant information. This could be seen as the equivalent to a quick response code (QR code). The differentiator is that if the "thing" has some mechanism for altering its URL then the information provided is dynamic and the "thing" is really part of the Internet of Things.

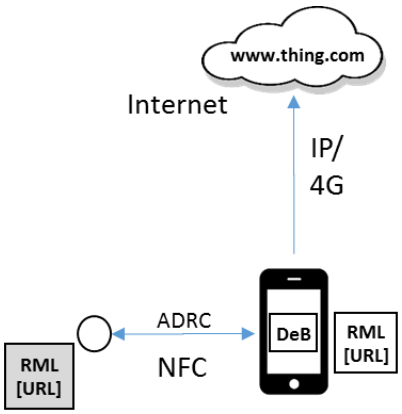

Figure 5 – Connecting Non IP devices to the IoT

Another service that Xped technology can deliver to all Xped enabled IoT "things" is the simplification of the on-boarding process (figure 6). This is traditionally a complicated function for novice users, but also a time consuming task for the expert installer. The ADRC solution allows an off-the-shelf device to associate with the user's smart device via NFC and have the SSID, security key and other options such as desired IP address to be transmitted in a secure manner to the un-configured "thing" via the hub. This then allows the "thing" to become part of the local IP network. The hub is normally a separate device, but the functionality can be included in a specialised smart device if required for standalone on-boarding only.

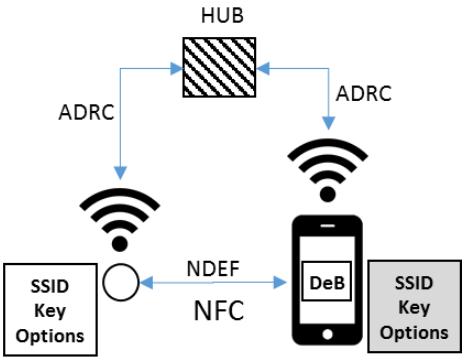

Figure 6 – On-boarding IP-based IoT devices

The Xped business model is to license ADRC in the "thing" in various form factors listed earlier. This relies on embedding a module in the "thing" that interfaces to the application for control of the "thing", and to existing communications via the radio module. The IoT module contains the NFC capability, ADRC protocols, and the storage capability for RML files (figure 7).

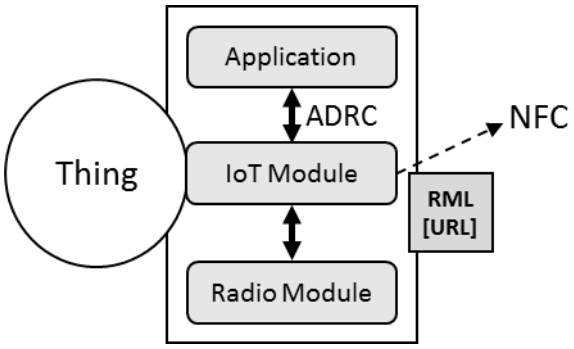

Figure 7 – IoT Module (ADRC) in a Thing

Xped Technology Assessment

This section lists the key Xped technology and competing vendors and technologies.

Dynamic Device Profiles

Described in patent USPTO#2012/0021684

Xped set out to solve the problem of devices needing a base set of common controls and then a set of device specific controls. This then leads to interoperability problems as the specific controls end up being vendor specific. Xped created a novel description language for modelling available resources available in a thing based on XML. It is the Resource Modelling Language (RML). RML files are stored within the "thing" as a descriptor of the complete set of controls available and their current settings. RML files are based on a hierarchical structure which allows the description of multiple "things" within the one unit. An example of this is a TV with an embedded DVD player. Each has its own description in RML and can be controlled separately but be part of the one larger RML file.

Auto-Discovery Remote Control (ADRC)

Patent USPTO#2012/0021684

ADRC is the term given to the process of establishing communications between a smart device and an ADRC enabled "thing". It defines the process of on-boarding the "thing" to the smart device's control software and transferring the specific RML file for the "thing". This enables the smart device to control the "thing". The protocol for transferring RML files is called the Remote Control Protocol (RCP) and is also an invention of Xped. The uniqueness of the Xped patent is the combination of the NFC process with the communications process via the hub.

Other efforts are underway in standards bodies such as the Open Group to create standards for the equivalent of RML[12] and RCP[13]. There is at least one academic paper on the use of

[12] Open Data Format (O-DF), an Open Group Internet of Things (IoT) Standard
[13] Open Messaging Interface (O-MI), an Open Group Internet of Things (IoT) Standard

peer to peer communications describing the security mechanisms for the transmission of information[14] over NFC. There are also patents in a similar field[15] to ADRC.

There are many companies and standards bodies that are working in the field of IoT to develop protocols and standards that might compete with ADRC such as:

- Google with brillo and weave[16].
- Samsung with artik[17].
- Apple with homekit[18].
- ARM with mbed[19].
- Intel with its IoT Platform[20].
- Texas Instruments with ConnectMore[21]
- Phillips, Sony, Faber, Honeywell, HTC, LG and more, with its AllJoyn Framework and the Allseen alliance[22]. An additional 13 members joined this alliance during the writing of this report.
- Qualcomm[23] has a vast range of IoT related products with various protocols and solution architectures.
- 8 standards bodies and 230 hardware and software vendors and service providers are part of the M2M onem2m standardisation effort[24].

The problem with this scenario is that this competiveness often leads to a myriad of new vendor standards, which is no different to the current status quo in remote control technology. This very problem is what Xped and the Open Group is attempting to solve with ADRC. It is interesting to note that one of the largest standards bodies has adopted a similar approach to Xped, which implies that the effort required to align solutions in the future would not be large.

Device Browser (DeB)

Patent USPTO #2014/0154983, #2012/0021684, #2013/176106

Xped have developed a generic device browser that can see, control, and measure device attributes by rendering a common device language (RML) to a smart device or PC browser. This allows a device to have a single browser to control all the things in the home (if they are ADRC enabled).

It is interesting to note that Google has tried to solve the same problem by creating extensions to chrome to allow NFC tags to push information to the browser to share

[14] LLCPS: A New Secure Model For Internet of Things Services Based On The NFC P2P Model
[15] USPTO 8929815 Apparatus and method for controlling functions of a mobile phone via NFC communications with an external reader, USPTO 9042819 Method, system, and apparatus having near field communication (NFC) chip with configurable memory that is updatable via a host processor
[16] https://developers.google.com/brillo/
[17] https://www.artik.io/
[18] https://developer.apple.com/homekit/
[19] https://www.mbed.com/en/
[20] http://www.intel.com/content/www/us/en/internet-of-things/infographics/iot-platform-infographic.html
[21] http://www.ti.com/ww/en/internet_of_things/iot-challenges.html
[22] https://allseenalliance.org/
[23] https://www.qualcomm.com/products/internet-of-everything
[24] http://www.onem2m.org/

information[25]. They call this concept the “physical web”, allowing browsers to talk to physical things, not just other computers.

The Swedish company Linkafy[26] has claimed to develop a single application to talk to IoT “things” via a series of APIs. This is the model of one cloud provider joining other cloud services together as shown in figure 3(a) above. If This Then That[27] (IFTTT) is another example of using a cloud service to solve the unified browser problem. The differentiator is that DeB communicates with the “thing” directly or via the gateway, whereas these other examples rely on a cloud service which is vulnerable to Internet outages. Customers will be hesitant to fully adopt an IoT solution if there are major issues with its operation if their Internet service is interrupted.

IoT is customer facing technology and as such localisation is critical when aiming for global markets. Xped have implemented DeB using extensible language files and have currently successfully tested English and Chinese browser languages.

While most browser concepts are either patented or open source already, Xped have applied for a patent for a unique mechanism that indicates the status of a control action entered on a smart device via DeB. This informs the user whether the action has actually occurred and the current status of the control link to the thing via a blinking coloured dot on the screen.

Embedded IoT Stack

USPTO #2012/0021684

A major part of the Xped business plan is to gain revenue by selling its ADRC protocol stack embedded into multiple types of hardware. This flexibility is critical in the IoT market due to the vast range of devices expected but also due to the varying technical IoT capability of future Xped customers.

There are other examples of similar approaches to the IoT market. DigiKeys Electronics[28] offers development boards for their NFC/IoT solution. ARM offers development boards and embedded chips as part of its eco system to encourage adoption of its ARM chips and IoT software.

Chip manufacturers such as Intel and Qualcomm have solutions for every current IoT vertical. They have products and solutions that work in the application, communication, “thing” and subsystem level.

ADRC Hub

USPTO #2012/0021684

A benefit of the ADRC hub as a standalone product is that the data that is collected via the hub is local and owned by the customer. This allows customers to decide how protect or use their IoT data. IoT solutions which tether directly to cloud services result in the data being

[25] http://blog.chromium.org/2015/04/reaching-and-re-engaging-users-on.html
[26] http://www.linkafy.com/
[27] https://ifttt.com/
[28] http://www.digikey.com.au/en/product-highlight/n/nxp-semi/nfc-for-iot

available to the single cloud application and it can become difficult to export this data to other applications.

Other Technologies

This section discusses the ancillary technology that Xped has developed.
A separate report on Xped technology covers some of these features in more detail[29].

Power Management
Technology that Xped has developed related to patent #2012/0021684

The management of power in the IoT ecosystem is critical with the large number of battery powered devices expected. Xped have invented a power management circuit to monitor local power and have included this status into the RML language so that battery levels (current and historical) can be presented to the user via the DeB.

NFC based coupons
Patent #2013/0176106
This covers the ability of a vendor to push data and triggers to a smart device after it completes a NFC payment cycle during a tap event. As an example, the data now stored on the smart device can be used as vouchers that can be used by the customer next time they shop. The trigger portion of the information can time out the voucher or make it useable after a certain time has elapsed.

Near Field Ping
Patent #2013/0225077
This covers the capability to provide a communications path over near field magnetic induction that has longer range than NFC communications. It also utilises 1/10th of the power of similar technologies to achieve the same outcomes. This is a good candidate for IoT solutions that require low power characteristics.

Wireless Charging
Not Patented – but technology that Xped has developed related to patent #2015/0044966.
This covers the capability to provide wireless chargers and devices that operate in the near magnetic field. This allows devices to charge when sitting on a charge mat while simultaneously providing a data connection for the devices via the same process.

All in one Controllers
Patent #2013/0176106
This covers the ability to provide a controller for devices that integrates smart device and hub capability. This also describes the issues involved in having multiple controllers in any one environment.

ADRC Wand
Patent # 2015/0044966
This covers the ability to provide a wand that can carry out the NFC tap portion of the ADRC process when the smart device does not have integrated NFC capability. Xped could use

[29] Statement of opinion about Xped Corporation, Invertech Electronics, Adelaide, South Australia.

smart watches as the ADRC wand, allowing a new set of use cases to be introduced into the IoT market.

Retail Precincts
Patent #2011/0270712
This covers the ability of a smart device to tap a particular kiosk in an environment (such as smart city or retail) and be automatically logged into the appropriate wireless network for that precinct. This facilitates smart searches of local services. This patent also covers the ability to nest precincts so that searches can be tailored to a specific location (eg. a specific shop) within a larger environment (eg. a shopping mall).

Risk Assessment

The following section describes risks in the technology and the current market that are apparent at the time of review.

Security

The use of IoT technology in itself does not introduce any new risks above what is already present in other IP enabled products. However it can become a problem due to the predicted massive size of the unit numbers and the limited ability to update or patch software and firmware in “things”. Many adopters of IoT devices will get them to work with minimal security settings and default passwords then leave them alone. This means the fine tuning of security parameters, the ongoing monitoring, and patching of the device is unlikely to be a common occurrence. We see this today in many solutions connected to the Internet, for example baby monitors and standalone IP video surveillance cameras where hackers take control of “things” and use them for a multitude of sinister outcomes.

Xped style technology is exposed to security risks on a number of fronts:

- Internet - The Xped hub can be an Internet facing device that is susceptible to hacking.
- Radio – The Xped DeB application, or the IoT stack in the thing, may be vulnerable to NFC related spoofing leading to identity theft. This then opens up the devices and things to unauthorised access.
- Firmware – The process of upgrading the IoT stack in the thing needs special attention as the lack of automated upgrades can lead to out of date and insecure code remaining on a device. On the other hand automated processes can be hijacked to spread non desirable firmware to things in order to take over these devices. A balance is required to provide the optimum security.

Security is normally an afterthought to the design phase. Xped have designed security into the ADRC process, but until a comprehensive investigation (Penetration Test) of the Xped solution is carried out it is hard to declare the effectiveness of security present in the current solutions. After such a test it will be possible for Xped to mitigate against security flaws that may or may not be found. This is planned to occur during the Xped technology development roadmap. The outcome of this test cannot be predicted in this report.

Xped have planned for a separate access control function in their roadmap for ADRC implementation to scale for secure deployments in enterprise or citywide installations.

Initial NFC bump is available as a mechanism to enable a secure key exchange between devices and controllers limited by low power and coverage of NFC. From that point on the ADRC communication uses standards based secure transport methods.

Customer Demand and Return on Investment (ROI)

For any IoT solution to be widely adopted it needs to pass a simple test. It must offer a return on investment on the premium required to buy IoT connected devices. In the home market the return can be in simplicity, functionality or personal health. In other markets it must be tied to reduced expenses, improved productivity or intangibles such as security and employee wellbeing.

The latter often requires that IoT solutions be tied to a change in business process in order to obtain the promised ROI. IoT solutions sold just for technologies sake are likely to fail in the long run due to the increased operating costs incurred without the realisation of the associated savings.

For Xped technology to be widely adopted it needs to be associated with the correct mix of partners who can deploy IoT into an environment and assist the end customer enact the business process changes accordingly.

Architecture, Technology and Standards

As there are numerous technologies involved in the creation of a complete IoT solution, there are many different standards that need to be observed. This is complicated by the fact that currently there is no agreed upon overseer of architecture framework for IoT solutions. For example chip manufacturers could adopt one standard, communications companies another, and the home product vendors yet another standard. Add to this the fragmentation of the M2M standards bodies competing with the IoT standards and the picture is more complex.

Whilst the claim that ADRC is a valid option for a future standard for IoT, there are many other standards efforts under development. Whilst some standards seem compatible with ADRC such as the Open Group standards, many others are not as similar. There is a risk that Xped may not gain the traction it desires with ADRC if a suitable pathway to standardisation is not found.

Market Fragmentation and Sales

As mentioned earlier, the IoT market ranges from the home, to transport, to smart cities, to the human body, to food production, and finally to industry. Each of these verticals are large enough to support their own standards as they so often have in the past. However a significant part of the appeal of IoT is the inter-connectedness of all “things” and smart

devices to unlock new services and unleash productivity gains. If a comprehensive single set of IoT standards is developed, then the solutions will fragment along market lines.

A fragmented market is far more complicated to sell into, and the end market for Xped is then limited to the market segments that evolve around ADRC solutions.

Partnering and Revenue Sources

The IoT market is segmented into cloud, communications and “thing” providers. Additionally there are those who can provide the intelligence to the “things”. Any successful business model will need to have partners in most of the areas to succeed. The current IoT partner environment can be characterized as follows:

- standalone powerful vendors with their traditional existing partners (Apple, Google, Samsung)
- large groups teaming to provide ecosystems (Allseen Alliance, ARMs Mbed, Open Group,OneM2M). Allseen currently lists 185 partners, mbed lists 50 partners and M2M 230 partners.
- and individual small players.

Xped will need to find a way to influence standards in the IoT area that can compete with these existing efforts. It is possible that the unique NFC based ADRC approach may be able to influence the development of future IoT standards.

Much of the revenue planned for Xped is based around the selling or licensing of embedded devices. This requires Xped to partner with chip or microcircuit manufacturers in order to bring their solutions to market within the appropriate price, size and power constraints. The inability to find and maintain these relationships are a risk to success.

Cost margins are hard to predict. IoT devices can command a premium at first for the early adopters. However if the features become common place and the functionality doesn’t provide a real ROI, then there will be market pressure to integrate IoT at reduced cost. The IoT stack will then be seen as an expense that can be trimmed, hence pressure for reducing margins on the devices or licenses.

The IoT is the opportunity for chip manufacturers to move up the value chain and start to offer end customer solutions (refer to AMDs standardisation effort). Conversely it’s the opportunity of consumer product manufacturers to create standards and offer embedded solutions to other vendors to attempt to promote their IoT standards. This implies that companies that traditionally are in separate ecosystems (hardware, microchips, software, services, communications, etc) are now in competition for IoT mindshare. It is also not uncommon for companies to be involved in multiple standardisation efforts simultaneously.

Xped will need to join an existing standardisation effort, or build an ecosystem of their own.

Technology Shortcomings and the Hype Cycle

The market for IoT devices is predicted to be huge. It must be said however that many of the early adopters of IoT technology have been disappointed with the current state of the Internet of Things. High additional cost for IoT aware products, lack of integration to other IoT devices, security concerns, the burden of ongoing maintenance, the lack of failsafe operation when communications or power is down are all dampeners on the demand of IoT products. It is hoped that the second generation of IoT products that are produced as part of the newly formed standards bodies will address some of these issues. However IoT technology is still seen by many as too early or too risky for prime time adoption. It is up to industry to solve these problems and repair perceptions if the market is to truly embrace IoT and deliver the large sales numbers as predicted.

References

Patents

US Patent 2012/0021684, Arrangement for managing wireless communication between devices
US Patent 2011/0270712, Arrangement for managing mobile device access to precinct regions containing services and products and information
US Patent 2013/0225077, Wireless device detection and communication apparatus and system
US Patent 2015/0044966, Method and apparatus for forming association and communicating between devices
US Patent 2014/0154983 Remote Control Arrangement
US Patent 2013/0176106 Remote Control and Remote Control Systems