Representing:

Organisation

Organisation (if applicable):

ARM Holdings

What additional details do you want to keep confidential?:

No

If you want part of your response kept confidential, which parts?:

Ofcom may publish a response summary:

Yes

I confirm that I have read the declaration:

Yes

1. IoT definition, applications and demand:

There are many definitions of IoT. We believe that the key point is that objects will be equipped with sensors able to send data about the object or its environment somewhere else. This means they will need to be connected, probably via Internet Protocol. The data is also likely to be able to be stored, processed and analysed in the Cloud.

IoT can be defined as any embedded devices that have connectivity, directly or indirectly to the internet.

A key element is that IoT will focus on receiving and transmitting data without any human intervention.

The applications of IoT are wideranging. They include: industrial production (eg robotic manufacturing), agriculture (e g sensing soil for water /fertiliser content), health (e g remote health monitoring, personal health monitoring), enterprise (e g buildings management, energy management, security), infrastructure (e g smart cities with better traffic monitoring, smart street lighting, water pipe management), consumer (e g white goods energy consumption, heating rates) etc

The application, technical requirements, connectivity types and form factors are all very diverse.

The key requirement will be for sensors which are low cost, low energy, long battery life and secure.

Connectivity

Connectivity will be required at both the Local Area and Wide Area Network levels.

For the Local Area (e g Home Area) we believe that Internet based standards are key. But, unlike the data/telecoms world, most of the devices in an IoT world will have significant constraints: first they will need to use energy very efficiently and run for a long time, so they will probably need to be low power; second, they will not need to send data all the time; third they will not need to be able to receive large amounts of data themselves. Because of this, many IoT devices are known as 'constrained' devices.

This means that the standards used to operate the IoT world will need to be tailored to the characteristics of constrained IoT devices

An Open System
We also believe that the full benefits of IoT will only be reached in a system which is open, ie in which various companies can offer their services and products on a framework which allows them to operate effectively and which does not restrict access to certain entities only.

We believe that the best model for providing basic IoT connectivity which is open to all should be modelled on that of the Internet. The Internet has been hugely successful at establishing key basic technologies and protocols which provide a framework on top of which many organisation and companies have been able to build customised offerings.

In addition, the Internet provides a model for how a system can be designed which avoids technological lock in, ie one company providing a proprietary system for linking objects to the Cloud, which does not interoperate with other systems, effectively locking the customer into using one company's products.

This means providing IP 'to the edge', ie giving devices an IP address which is their unique link to other devices, the Internet and the Cloud.

The Key Standards

Four key standards are at the foundation of the Internet:

- IPv6 (and IPv4) - Everything on the Internet has a unique address.
- TCP - Transmission Control Protocol is the Internet's primary transport layer. TCP handshaking guarantees reliable, in-order delivery of packetized information.
- HTTP - This is the Internet's application protocol. It's how every web page is constructed and it's the foundation of data exchange on the Web.
- TLS - Transport Layer Security provide communication security over the Internet.

It would be great if we could use these standards for IOT. Today, larger devices over fast networks can already participate as full members of the Internet. However, constrained IoT devices cannot use these standards as-is.
Fortunately , the worldwide Internet community has been working on this problem for many years. There is a parallel set of standards that offer services similar to IPv6, TCP, HTTP, and TLS but are applicable to constrained networks and devices.

IPv6 > 6LoWPAN - It's possible (and highly desirable) to use IPv6 to address everything on the Internet including all IoT devices. However, constrained IoT networks such as 802.15.4

have smaller packet sizes and lower bandwidth. Therefore, we need a more efficient protocol that preserves the universal addressing of IPv6 while reducing the protocol overhead so that operation over constrained networks is possible. This is what the IETF standard 6LoWPAN does.

TCP > UDP - Many IoT nodes are heavily power managed. This means that they sleep a lot. Therefore, it's not practical to rely on TCP because the protocol fails when trying to send to sleeping nodes or when packets are dropped. UDP is a much simpler transmission protocol that has no handshaking. It is therefore more suitable for communicating with IoT nodes.

HTTP > CoAP - This is the foundation for data exchange on the Web. It's not suitable for constrained IoT because it requires TCP and it simply has too much overhead. CoAP, the Constrained Application Protocol, is a similar data exchange protocol designed for use with constrained devices over UDP connections.

TLS > DTLS - Transport Layer Security also requires TCP and therefore won't work with UDP. DTLS (Datagram TLS) is designed for UDP and is suitable for securing communications with constrained devices.

All these standards are available today and accessible to anyone.

2. Spectrum requirements :

Many IoT applications can make use of existing approaches to wireless communication:

- 802.15.4 is gaining momentum (including through the Thread network protocol) for home automation. It is arguably also likely to be the default system for buildings and industrial applications. This should be the basis of LAN connectivity.

- Bluetooth LE is also popular mostly because of the wide availability in mobile phones/tablets. Bluetooth has put the focus on 2.4 GHz, (but IoT is also likely to require sub GHz spectrum - see below).

We can imagine licensed and unlicensed IoT bands working alongside each other. Licensed may be needed for critical IoT applications. But it is limited, and probably doesn't permit the scale necessary for all IoT applications.

For WAN connectivity, we need accessible, low power WAN spectrum. The work of the 'Weightless' consortium has been stalled for a few months, but it could still have a role in standardising a sub GHz ultra narrow band spec. It is looking at sub GHz ISM bands.

Various other companies are making progress in this area, but many of their networks are proprietary. Nevertheless it shows the demand there is for ways to get data over distances of say 5km.

For IoT we will probably need spectrum between 400-900 MHz to provide for small bursts of data at modest bandwidth speeds. The Mobile players are not interested in sub 600 MHz. Maybe in an ideal world we could set aside 470-500 for IoT related WAN.

Dynamic Shared Access is likely to be key to IoT spectrum management : we now have the ability to build 'listen before talk' mechanisms for dynamic shared access. Fixed duty cycles are therefore not necessarily required any more.

Global harmonisation is important. The sensors which are the basis of IoT are likely to be a global commodity business because they will need to be low costs, and hence low margin. One approach to spectrum harmonisation might be to try to get the US and key Europeans to agree first and then others might come along too. Some international coherence around using the 470-500 MHz range might be possible.

The key point is that devices have to be able to connect to the cloud using the best means available to them.

3. Network-related issues:

Heterogeneous networking will be essential to avoid the risk of closed proprietary systems choking connectivity.

The Mobile network can only cover a small part of the IoT application space. Think of having billions of IoT End Points (e.g. sensors) in a smart city - the mobile phone network is not designed for that. It is essential to have multiple wireless mechanisms for different IoT applications. As indicated above, IP 'to the edge' via 6Lowpan is important.

As indicated above we are in favour of open standards wherever possible. These stimulate innovation and competition etc Some closed networks may emerge 'naturally' (eg in industrial internet).

Today, open standards are gaining more attentions as companies realize their importance in driving IoT. But, the software ecosystem for open standards for IoT is only just forming and it is going to take time.

4. Security and resilience:

We fully agree that security will be paramount, including simple authentication for some applications. There are established security models for IoT applications (e.g. TLS and DTLS are open standards). But for many software developers getting this right is a challenge. A reference software platform would accelerate the adoption process.

And of course, in addition to communication level security, there are other aspects of security (e.g. chip device level, product physical level, server level, and data management in the clouds are also important areas).

5. Data privacy:

We believe that data usage will drive IoT and will be the most important added value from IoT. Confidence in how data is transmitted and handled is therefore key . Given that IoT devices will not always have an accessible User Interface, the privacy issues already highlighted by the Internet will be magnified.

We believe that any approach to this has to start with the principle that consumers own their own data. This means giving consumers greater control over how their data is used. In turn this means simpler Terms and Conditions. But it will be important too that any system acknowledges that data has uses beyond what the consumer sees.

Technology has an important role to play in helping to ensure the security of data (ie from unauthorised interception). Security by design has to be built into the IoT.

We would like to see Industry come together around a framework designed to give consumers confidence.

We have produced a couple of papers on further ideas on this topic (attached).

6. Numbering and addressing:

We believe IP addresses will be important and that therefore, faster roll out of IPV6 is needed.

We also need to promote the available open standards. CoAP, DTLS, 6LowPAN are all standard protocols.

7. Devices:

We have mentioned above the fact that sensors will need to be produced at low cost.

Advanced process nodes remains a bit expensive at the moment. Low power non volatile memory is also a challenge as traditional flash memory is costly and power hungry. There are new memory types in research stage.

We believe that existing Linux system is not ideal for low power IoT devices. It requires lots of memory and anything that requires external DDR memory won't last long with a small battery. New OS specially development for low power IoT devices might be the solution. IoT will not need a rich OS.

8. Digital literacy:

The comments above on data privacy and better information for consumers are relevant here. Consumers will not necessarily need to have vastly better digital understanding: the public took to pc's, and then mobile phones easily without wide knowledge of the technology underpinning these devices. But consumer in confidence in how their data is protected and handled will be important. Once consumers have confidence they may be more willing to share their data, particularly once they understand the benefits of doing so.

9. Data analysis and exploitation:

Data will probably drive IoT. The key value (as said above) is in the data. Data Brokers have begun to operate in the US.

10. International developments:

Right now there are many bodies looking at various possible IoT standards. The problem with this is that until the key standards emerge, some developers will hold back from producing new products and services. So we need coalescence around some key standards. We believe the Thread approach (see above) is a good place to start to encourage standards at the bottom end of the stack.

We do not see a role for Governments in designing standards.

Ideally we need to aim for global standards wherever possible. We cannot exclude risk of 'regional' standards: competition among standards bodies to get critical mass.

11. Ofcom’s role :

Ofcom has played an important role in putting a focus on the spectrum requirements of IoT. There is an opportunity for the UK to lead in this area.

12. Additional comments:

we are sending additional papers referred to above to Gary Clemo.