Key Building Blocks of Internet of Things (IoT)

Going Beyond The IoT Hype

IoT is already a reality. Products ranging from home temperature control and entertainment to security and industrial control have already been deployed by the millions. But this is just the beginning of the new IoT age, with its market projected to grow exponentially over the next few years.

The hype around IoT has paradoxically hindered the understanding of how it actually works. Ask a hundred people about what they think IoT is and you might get a hundred answers, with most related to the outward features of common IoT products. However, there is a lot of technology under the covers that makes IoT possible.

This white paper will help you understand the key building blocks of IoT and how they work together. It overviews considerations in validating that a particular IoT product or service is functional, safe, and conforms to industry standards; and the need for ongoing monitoring access of IoT data across the network. The aim is to help you successfully evaluate, design, or deploy the next generation of IoT solutions.
Ecosystems

A better way to visualize IoT is to think of it as a conglomeration of separate but synergistic ecosystems. Each of the ecosystems below has its own specific technology and technical considerations and is independently setup. The ecosystems don’t need IoT to survive, but the sum of all these ecosystems working together is what constitutes IoT.

1. Things

A “Thing” in the context of IoT is any entity that has three characteristics:

- It can be uniquely identified
- It can sense and share information about itself and its surrounding
- Optionally it can receive directives to perform certain actions

These “Things” are what makes IoT possible. They can range from temperature and humidity sensors inside a house, to accelerometers on a car, to proximity sensors at a secured facility, to heart rate monitor on a person. The more varied and numerous the sensors are, the better the value that can be extracted from IoT as a whole.

This is the reason why analysts project the Things to grow exponentially. According to a report from Cisco¹, by 2020 there will be up to 50 billion such connected devices.

¹ https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
2. Access Technologies

Access technologies cover all the different methods used by Things to share their information with the rest of the IoT infrastructure.

The particular method used by the Things to share this information is dependent on multiple factors – distance from nearest access point, projected data rate and throughput, power requirements, and size among others. For example, a Thing that requires battery life of 10 years may not use Wi-Fi for its connectivity needs as Wi-Fi may be too power-hungry for such application. Whereas, a consumer device Thing at home can happily use Wi-Fi as it doesn’t have very stringent battery life need.

3. Network Infrastructure

While not considered essential to IoT, the network infrastructure is one of the key element in the IoT world. The network infrastructure transports Things’ data from the access technologies to the cloud processing ecosystem. Unlike the network infrastructure of the past, to serve IoT data traffic, the networks need to be elastic – grow with the increased traffic and shrink when traffic dies down. This will allow for decreasing the operating expenses for the service providers and cheaper cost for the end users as they are not paying for the network resources they are not using.

In addition, the network infrastructure has to have intelligence to differentiate between and cater to mission-critical and non-mission-critical IoT applications.

If the network infrastructure is deployed incorrectly, it will detract from the value provided by IoT. For example, if a security camera report of a break-in reaches the property owner 10 minutes after the fact, it will offer little value to the customer.

4. Cloud processing

All the data generated by Things is of no use until companies or users store, analyze, and, if necessary, act-upon it. This is where cloud computing comes into the picture. The cloud computing ecosystem is where the smarts in the IoT comes from.

The potentially huge amount of data generated by the Things has to be processed to make sense of and decide if follow up action is needed. For example, a person’s vehicle may report that it is reaching her home in an hour. Based on this information, the home thermostat may need to be ordered to turn on heater so the home is cozy at her arrival. Upon reaching her driveway, the home will sense the proximity of her vehicle and may open the garage and unlock the front door. The aggregation of these disparate Things information and the resultant actionable decisions are all happening in the cloud processing ecosystem.
5. Security

While not an ecosystem itself per se, security is needed across all ecosystems – in sensors that generate data, at the access points connected to sensors, inside the network infrastructure, and at the cloud processing and storage.

Many of the IoT products seem to have been developed without keeping security as a major design focus. This has led to some products being susceptible to attacks. As a result, many end-user companies and customers cite security as the reason why they haven’t fully embraced the IoT concept. Furthermore, the recent news of hackers breaking into vehicle control and industrial systems plays into the hesitation.

To combat this, industry groups are building security into most of their standardization efforts related to IoT ecosystems so that IoT products and solutions are hardened against unauthorized access and control of assets.

Standardization

There is a flurry of parallel standardization efforts taking place to ensure that IoT can be a reliable platform for future products. This standardization would also allow disparate systems to talk to each other.

A good example is the industry agreement to converge on the Narrowband-IOT (NB-IOT) technology that will allow wireless carriers to provide IoT services cost-effectively by piggybacking on their existing installed infrastructure while also allowing for long battery life.

Another example is the convergence between information technology (IT) and operational technology (OT). OT used to be a bastion of proprietary closed systems, but using IT technologies like Converged Plantwide Ethernet (CPwE) would allow OT systems to become more open and provide better insight and value to the user. This results in lower operating cost and higher system knowledge—allowing for strategic solutions that were previously too expensive and too complex to create.

End Goal

When all the ecosystems are working in synergy with each other, the focus will no longer be on any one Thing as it is now. Instead, when you leave work, your car will inform your home of your estimated time of arrival, your home environment system will accordingly ensure that the home is at the right temperature by the time you arrive, upon your arrival your front door will unlock.

---

This synergistic interoperation of different ecosystems will revolutionize industrial, transportation, security, entertainment, and defense sectors.

**Test and Measurement**

A comprehensive test and measurement plan is the key in ensuring IoT devices comply with key operator and industry performance standards, while at the same time also delivering a sustainable, high-quality experience for the end user. In addition, IoT solution creators and their customers can also use the test results to design solutions that ensure optimum use of resources, while at the same time ensuring the safety and security of the important data.

Testing needs to address the following challenges that have different but complementary requirements that you must meet before moving a product or solution to production:

6. **Reliability**

With IoT devices designed for users to keep them powered-on for many years, it is an absolute necessity that they deliver consistent performance under different conditions.

7. **Regulatory**

Bringing new products to the market also requires that these products meet the different industry and governmental regulations and standards.

8. **Interoperability**

With the widespread adoption of common standards across industries, new IoT products need to be able to interoperate with other IoT devices and systems.
Monitoring

As IoT deployment spreads, monitoring “things” on a network will be essential to network administration so they can ensure network reliability to guarantee that important data-flow from Things goes unaffected. They will also need visibility to keep an eye on any security holes these new devices may create.

We have already entered a new era of applied computing technology where it is easier to implement paradigm-shifting applications faster and cheaper than ever before. However, these products need to securely interoperate across the IoT ecosystem without performance degradation. Ixia offers industry-leading test and visibility solutions that can help you create and deploy competitive IoT products that are functional, compliant, and secure.

Learn more at: www.keysight.com

For more information on Keysight Technologies’ products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus