Executive Brief

The Internet of Things: Five Myths and Realities

Exploring the technology's true nature and capabilities

The Internet of Things (IoT) is a concept that describes a totally interconnected world. It's a world where devices of every shape and size are manufactured with "smart" capabilities that allow them to communicate and interact with other devices, exchange data, make autonomous decisions and perform useful tasks based on preset conditions.

It's a world where technology will make life richer, easier, safer and more comfortable. Or is it?

Like many emerging technologies, the Internet of Things is vulnerable to hype and exaggeration. To some people, it sounds like a vague and distant prospect; to others, it sounds threatening and dangerous.

This executive brief will explore five of the most common myths associated with the Internet of Things and shed some light on the true nature of the technology and its capabilities.

Any new technology involves a certain amount of uncertainty and business risk. In the case of the Internet of Things, however, many of the risks have been exaggerated or misrepresented.

freescale™

1

Isn't the Internet of Things a revolutionary vision of a "far out" technology future?

The Internet of Things is simply the logical next step in an evolutionary process.

It's tempting to describe the Internet of Things as a technology revolution. The prospect of millions—or billions of connected devices communicating with each other might seem like a futuristic, and perhaps impractical, concept.

The truth is that the technological building blocks of the IoT—including microcontrollers, microprocessors, environmental and other types of sensors, and short range and long range networking communications—are in wide-spread use today. They have become far more powerful, even as they get smaller and less expensive to produce.

Radio Frequency Identification (RFID) tags, for example, have been refined and miniaturized to the point where they can be used to track and monitor items ranging from railroad rolling stock to supermarket merchandise. Almost any manufactured product, from luxury automobiles to coffee makers, now uses embedded, programmable microelectronics.

The Internet of Things, as we define it, while evolving the existing technologies further, simply adds one additional capability—a secured service infrastructure—to this technology mix. Such a service infrastructure will support the communication and remote control capabilities that enable a wide variety of Internet-enabled devices to work together.

Consider one area where the Internet of Things can put all of these elements into play to solve practical problems: home automation. Widely available technology already supports remote control of lighting, access, security systems and other applications. With the Internet of Things, it becomes possible to add a service infrastructure layer that enables far richer and more complex uses. A combination of sensors and applications, for example, could detect that an older homeowner has spent an unusually long time in the bathroom, call to check on them and, if necessary, summon help if nobody responds. In these and other ways, the Internet of Things will offer new and innovative ways to save lives, time and money.

2

Do the technology and interoperability standards exist to make the Internet of Things possible?

Standards issues pose a challenge, but these will be resolved as the standards process continues to evolve.

The Internet of Things will eventually include billions of interconnected devices. It will involve manufacturers from around the world and countless product categories. All of these devices must communicate, exchange data and perform closely coordinated tasks—and they must do so without sacrificing security or performance.

This sounds like a recipe for mass confusion. Fortunately, the building blocks to accomplish many of these tasks are already in place. These include:

- **Existing standards** such as Bluetooth®, Wi-Fi®, RFID, ZigBee®, Bluetooth Low Energy, Z-wave and IPv6 that provide a ready foundation for robust, highly scalable networking and communications;
- **Open hardware platforms** such as the ARM® architecture that provide a set of shared, baseline technologies for creating intelligent, networking-capable devices;
- **Emerging standards** such as 6LoWPAN, Weightless, 802.11ah, etc., that will support the wide range of communication and networking technologies required for a truly comprehensive Internet of Things;
- **Data standards** such as eXtensible Markup Language (XML) and Resource Description Framework (RDF) that support interoperable applications and devices;
- **Global standards bodies** such as IEEE, International Society of Automation (ISA), the World Wide Web Consortium (W3C), OMA, IETF and IPSO alliance (to name a few) bring together manufacturers, technology vendors, policymakers and other interested stakeholders.

Everybody involved in the standards-making process knows that one size will not fit all—multiple (and sometimes overlapping) standards are a fact of life when dealing with evolving technology. At the same time, a natural pruning process will encourage stakeholders to standardize and focus on a smaller number of key standards.

As a result, while standards issues pose a short-term challenge for building the Internet of Things, the long-term process for resolving these challenges is already in place.

3

Will the Internet of Things create serious privacy and security challenges?

Security and privacy are major concerns—and addressing these concerns is a top priority.

Inevitably, discussions of an Internet of Things evoke images of a future dystopia where personal privacy—and personal freedom—is a thing of the past. In addition, as a seemingly endless stream of data-breach incidents and hacker attacks proves, stolen or misused digital data is already a very real, and rapidly growing, concern.

These are legitimate concerns. New technology often carries the potential for misuse and mischief, and it's vital to address the problem before it hinders personal privacy and security, innovation or economic growth.

Manufacturers, standards organizations and policy-makers are already responding on several levels:

- Existing privacy enhancing technology (PET) infrastructure standards, such as virtual private networks and DNS Security Extensions, that can be easily adapted to protect sensitive data as it moves between devices or through the cloud.
- Government regulations such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) that mandate the protection of sensitive personal information—no matter where it is stored or how it is transmitted.
- Other security frameworks proposing DTLS secured light CoAP running on UDP, which has also been adopted by ETSI.
- As well as many other activities by multiple members of the ecosystem.

Work remains to be done in other areas related to securing the Internet of Things and protecting user privacy. At the device level, security researchers are working on methods to protect embedded processors that, if compromised, would halt an attacker's ability to intercept data or compromise networked systems. At the network level, new security protocols will be necessary to ensure end-to-end encryption and authentication of sensitive data, and since with the Internet of Things the stakes are higher than the Internet of People, the industry is looking at full system level security and optimization.

Ultimately, the Internet of Things must take a far stricter approach to security and privacy than the existing Internet of People has taken in the past. This is necessary to protect systems and data, and it is also necessary to address the public's concerns that the Internet of Things will create more problems than it solves.

4

With the technology and engineering investments involved, will a few major companies dominate the growth of the Internet of Things?

Open platforms and standards will create a base for innovation from companies of all types and sizes.

The terminology used to describe the Internet of Things—billions of devices, massive data flows, universal networks—can be intimidating. Technology developers and providers may wonder how to translate this concept into tangible products that will generate revenue. Like most consumer-aimed markets, more than 50% of innovations are expected to come from smaller players. Technology buyers, especially those working at smaller firms, wonder whether the Internet of Things will expose them to unnecessary cost or business risk.

- **Open hardware architectures.** Open platforms are a proven way for developers and vendors to build innovative hardware with limited budgets and resources. Hardware based on the open ARM platform, for example, combines low cost with performance, efficiency and flexibility.
- **Open operating systems and software.** The heterogeneous nature of the Internet of Things will require a wide variety of software and applications, from embedded operating systems to Big Data analytics and cross-platform development frameworks. Open software is extremely valuable in this context, since it gives developers and vendors the ability to adopt, extend and customize applications as they see fit—without onerous licensing fees or the risk of vendor lock-in.
- **Open standards.** As we discussed earlier, open standards and interoperability are vital to building the Internet of Things. An environment where such a wide variety of devices and applications must work together simply cannot function unless it remains free from closed, proprietary standards.

Virtually all of the vendors, developers and manufacturers involved in creating the Internet of Things understand that open platforms will spur innovation and create rich opportunities for competition. Those that don't understand this may suffer the same fate as those that promoted proprietary networking standards during the Internet era: They were sidelined and marginalized.

5

Will the Internet of Things be built around smartphones and cellular networks?

The smartphone will play a role in creating the Internet of Things, but it's a supporting player—not the star.

It's not uncommon to hear the Internet of Things tied closely to smartphone technology and cellular data networks. The truth, however, is that the IoT involves more—much more—than just a world full of super-sized smartphone apps.

This is a complex topic, but it really boils down to two important points:

- **Smartphones work best at the periphery of the IoT ecosystem—not the center.** The Internet of Things combines a number of components. There are sensors, processors and actuators that collect data and perform work; gateways and hubs that aggregate this data and pass it across a network; and applications that can evaluate data and make decisions.

  Smartphones certainly play a role in collecting some of this data and providing a user interface for accessing IoT applications, but they're ill-suited to play a more central role. Consider the example of home automation: It hardly makes sense for critical home-monitoring and security applications, such as those that protect an elderly resident against an accident or illness, to rely upon a smartphone as its decision-making hub. What happens when that person travels and his smartphone goes into airplane mode? Does his home security get interrupted, or home electricity shut down?

  Such examples make it clear that the IoT will, with a few exceptions (such as "wearable" technology and bio-monitoring systems) and some automobile-related applications, rely mostly upon dedicated gateways and remote processing solutions—not on smartphones and mobile apps.

- **The Internet of Things can't—and won't—rely entirely on cellular networks.** Cellular networks are ubiquitous in many areas, and they are increasingly capable of providing the bandwidth needed for modern mobile applications. In the long run, however, even cutting-edge cellular networks can't deliver the bandwidth the Internet of Things will require: By some estimates, by 2020 the IoT will help to drive 22 times as much data traffic as exists today.

  Today, without any IoT services, more than 80% of the traffic over LTE networks goes through Wi-Fi access points. What happens when that data increases by 22 times? In addition, cellular networks and communication devices have serious drawbacks in areas such as cost, power consumption, coverage and reliability.

What's the solution? On a local level, so-called Body Area Network (BAN), Personal Area Network (PAN) and Local Area Network (LAN) communications may adopt a number of current and proposed wireless protocols—each of them optimized for a different mix of power use, bandwidth, cost and reliability. Think Bluetooth Low Energy, 802.15.5 and 6LoWPAN, 802.11n and wireless M-Bus types of low-bandwidth technologies. On a wider scale, Wide Area Networks (WAN) will rely on technologies such as Ethernet (if an access point is available), or up-and-coming technologies such as the Weightless Standard, or even the flavor of Wi-Fi called 802.11ah protocols—the last two being much more optimized for IoT types of applications, with much better ranges, lower cost and lower power consumption. Cellular will certainly have a role for WAN coverage, but only a fraction of the time.

So, will the Internet of Things have a place for smartphones and cellular communications? Absolutely. But in terms of performance, availability, cost, bandwidth, power consumption and other key attributes, the Internet of Things will require a much more diverse and innovative variety of hardware, software and networking solutions.

Conclusion: Seizing The IoT Opportunity

Any new technology involves a certain amount of uncertainty and business risk. In the case of the Internet of Things, however, many of the risks have been exaggerated or misrepresented. While the IoT vision will take years to mature fully, the building blocks to begin this process are already in place. Key hardware and software are either available today or under development; stakeholders need to address security and privacy concerns, and collaborate to implement the open standards that will make the IoT safe, secure, reliable and interoperable, and allow the delivery of secured services as seamlessly as possible.

Given this progress, and given the remarkable opportunity that the IoT represents, the real question is whether businesses can afford not to learn more about their place in this fast-evolving technology ecosystem.

About Freescale

Freescale Semiconductor (NYSE: FSL) is a global leader in embedded processing solutions, providing industry-leading products that are advancing the automotive, consumer, industrial and networking markets. From microprocessors and microcontrollers to sensors, analog integrated circuits and connectivity – our technologies are the foundation for the innovations that make our world greener, safer, healthier and more connected. Some of our key applications and end-markets include automotive safety, hybrid and all-electric vehicles, next generation wireless infrastructure, smart energy management, portable medical devices, consumer appliances and smart mobile devices. The company is based in Austin, Texas, and has design, research and development, manufacturing and sales operations around the world.

freescale.com

For more information about how Freescale is making the IoT a reality, visit freescale.com/intelligence

Document Number: IOTEXECBRIEFWP REV 1
August 2013