IHS TECHNOLOGY

IoT platforms: enabling the Internet of Things

March 2016

ihs.com

WHITEPAPER

Sam Lucero
Sr. Principal Analyst, M2M and IoT

Contents

No portion of this report may be reproduced, reused, or otherwise distributed in any form without prior written consent, with the exception of any internal client distribution as may be permitted in the license agreement between client and IHS. Content reproduced or redistributed with IHS permission must display IHS legal notices and attributions of authorship. The information contained herein is from sources considered reliable, but its accuracy and completeness are not warranted, nor are the opinions and analyses that are based upon it, and to the extent permitted by law, IHS shall not be liable for any errors or omissions or any loss, damage, or expense incurred by reliance on information or any statement contained herein. In particular, please note that no representation or warranty is given as to the achievement or reasonableness of, and no reliance should be placed on, any projections, forecasts, estimates, or assumptions, and, due to various risks and uncertainties, actual events and results may differ materially from forecasts and statements of belief noted herein. This report is not to be construed as legal or financial advice, and use of or reliance on any information in this publication is entirely at client's own risk. IHS and the IHS logo are trademarks of IHS.

IoT platforms: enabling the Internet of Things

Sam Lucero, Sr. Principal Analyst, M2M and IoT

Introduction

This whitepaper examines the impact of the Internet of Things (IoT) and analyzes the role that IoT platforms play in enabling the development and implementation of IoT applications and services. The target audience for this whitepaper is first and foremost mobile operators that are assessing IoT platforms for incorporation into their own IoT strategies, but this whitepaper is also intended for IoT application developers and implementers as well.

This report first provides a broad, overarching vision of the role that IoT is playing in industry and society, then examines several key challenges for IoT market development in depth. Following this is the IHS definition of the concept of an "IoT platform" as well as details on how Huawei's Ocean Connect IoT Platform fits within this concept. Finally, this whitepaper examines factors that IoT solution providers, and in particular mobile operators, would benefit from considering in their selection of IoT platforms.

This whitepaper was written from December 2015 to February 2016 and draws upon the research and analysis contained in IHS Technology's IoT Connectivity Intelligence Service, IoT Ecosystem Intelligence Service, and M2M Intelligence Service, including topline forecast data. After reading this whitepaper, the reader should have a solid understanding of the potential for the IoT market at a high level, the challenges facing IoT market growth, the role that IoT platforms play in ameliorating these challenges.

The IoT is transforming industry and society

The Internet of Things (IoT) is a technology concept that is currently transforming and redefining virtually all markets and industries in fundamental ways. The past five years have seen an inflection point in which fragmented efforts to connect machines and sensors in industry-specific ways are now coalescing into a comprehensive vision of connectivity permeating the global physical environment.

This is a shift from the narrow development of new information and communication technology (ICT) systems for specific industries towards the broad view of pervasive interconnectivity of the global physical environment. This includes a continually increasing focus on integrating the massive, new flows of data from machines and sensors with existing and emerging data sources—including enterprise resource planning systems, open government databases, and social media feeds—in order to produce novel and actionable new insights.

An important signpost of the fundamental importance of the IoT concept is the strategic activity of most major ICT vendors in developing IoT offerings. Companies that sit at the heart of the telecom, networking, industrial infrastructure, enterprise system, and cloud computing sectors are converging on the strategy of offering IoT platforms to facilitate the broader economy's transformation to pervasive connectivity. Examples of leading ICT firms that have introduced IoT platforms include: Amazon Web Services, AT&T, Cisco, Deutsche Telekom, Ericsson, Fujitsu, General Electric, Huawei, IBM, Salesforce.com, and Vodafone among others. Huawei's Ocean Connect IoT Platform is an example of a leading IoT platform strategy.

“Datafication” is the new electrification

Although the IoT fundamentally entails universal connectivity, including personal computers and smartphones, the focus of most observers when discussing the IoT is the opportunity to both connect existing machines that were not previously connected (for example, aircraft engines) as well as dramatically expand the number of connected points in the environment through sensors, actuators, and devices that would have never been developed nor deployed without the underlying infrastructure to connect them into a pervasive ICT infrastructure.

IHS views the current push to the IoT as analogous to the transformation of electrical infrastructure from specialized and isolated point systems to a pervasive, commoditized, and essential building block of the modern industrialized world. From the 1880s to the early 1900s, there was not the all-encompassing electrical grid that there is today. Companies and organizations that needed electricity deployed local generators and “Vice Presidents of Electricity” were needed in organizations to oversee the very specialized infrastructure. If electricity needed to be delivered to a new part of a building or facility, the Vice President of Electricity implemented the custom system.

Nowadays, electricity is essentially a commodity service available everywhere in the industrialized world. The pervasive, standardized electrical grid delivers power comparatively much more easily. This type of abstraction—having access to power without having to devote extraordinary resources to sourcing and managing that power—has been a key catalyst to the enormous economic growth that the world experienced in the 20th century. Individuals, companies, organizations, and governments have been able to focus on innovating without the burden and constraint of needing to focus on the fundamentals of powering their innovations as these were developed previously.

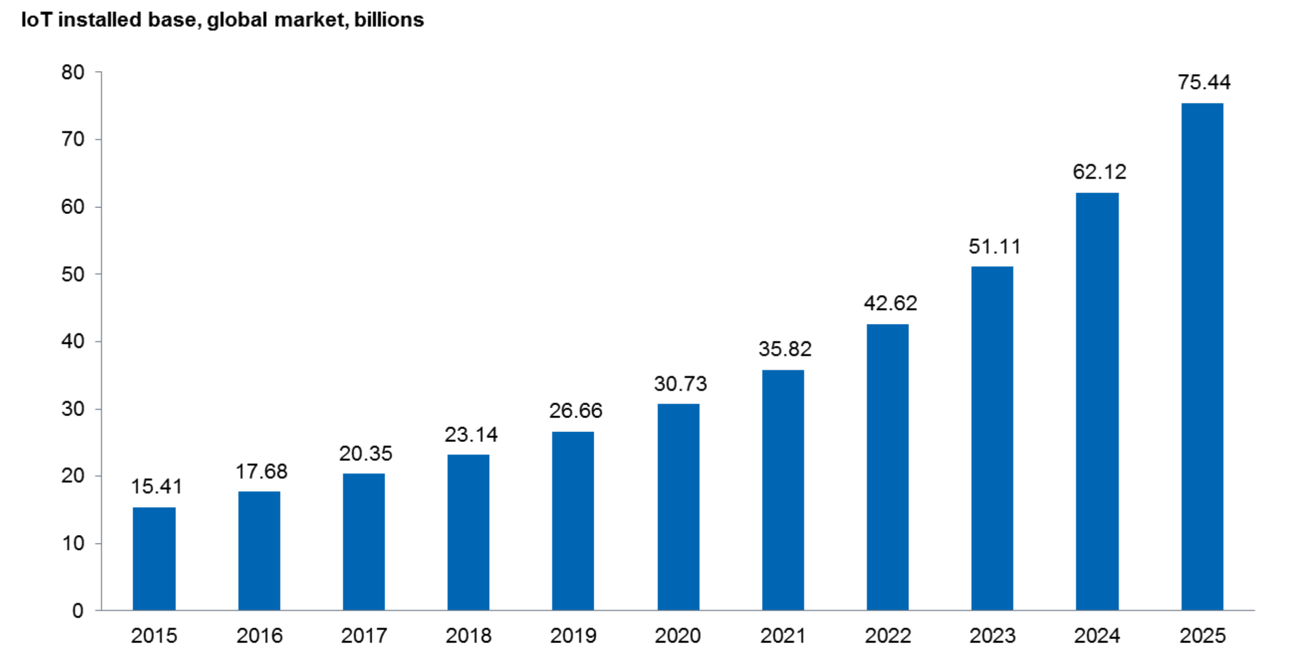
Similarly, through a number of initiatives (including IoT platforms, standards development, regulatory actions, and ecosystem formation) a transformation is underway that will make connectivity pervasive and, more importantly, data from connected machines and sensors available as a fundamental service, almost like a commodity.

Data is much more varied and complex than electricity. IHS recognizes that the “datafication” analogy presented here to the 19th century and early 20th century’s “electrification” transformation is not correlated in every respect, but the analogy does capture the core idea of isolated, complex, and limited systems transforming into a pervasive utility. Electrification had a fundamental impact on most industries and markets in the 20th century. IHS predicts that datafication will have a similar impact in this century.

Forecasting the massive growth of the IoT

IHS forecasts that the IoT market will grow from an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025, as seen below in Figure 1.

Figure 1. The IoT market will be massive



Source: IHS © 2016 IHS

Three key impacts of IoT on industry

Three of the most important means by which the pervasive connectivity of the IoT will affect the economy as well as society are in the areas of automation, integration and servitization. These three features are interrelated in the sense that automation and integration are often employed in tandem to enable servitization. These three factors are explained in more detail below:

- **Automation**: Connecting machines, sensors, and actuators to computing systems enables a large degree of process automation. For example, fleet management systems enable automatic logging of driving parameters such as hours in motion, removing the need for drivers to manually submit this information. Automation facilitates dramatically larger scales of data utilization as well. For example, jet aircraft engines typically produce several terabytes of data per flight on operating parameters. Proactively monitoring this data feed enables faster resolution times in instances of performance faults and minimizes unnecessary maintenance services.

- **Integration**: There are more benefits than simply connecting a machine and automating its performance. Integrating the data from a machine with data from other sources, such as the aforementioned ERP systems, open government databases, and social media feeds, greatly enhances the value derived from connecting the machine. For example, Salesforce.com enables the integration of machine performance and condition data, collected automatically from the machine, to be combined with traditional customer relationship management (CRM) data and social media feeds to improve the organization's customer service by working proactively.

- **"Servitization"**: Together, automation and integration help organizations move from primarily product-centered business models to service-oriented business models, also known as "servitization". Many traditionally product-centered companies are realizing the revenue opportunities offered by developing an ongoing, service-oriented relationship with customers, for example organizing a customer relationship on the basis of a service contract whereby the customer is paying for a negotiated business outcome rather than a piece of equipment. In fact, automakers are increasingly talking about "mobility as a service" as a result of connected, and increasingly autonomous, vehicles as opposed to the traditional vehicle sales model.

Challenges in realizing a pervasive IoT

There are many challenges on the road to a truly pervasive IoT.

Managing complexity

Many of these challenges ultimately flow from the issue of complexity mentioned earlier. This complexity derives from a number of factors, for example:

- **Fragmented supply chains and ecosystems** make it difficult for IoT developers and customers to determine optimal partners and sources for tools, components and supporting services. For example, a product OEM deploying a new connected product service may have to establish new relationships with radio frequency (RF) component suppliers, numerous mobile operators in different countries, and various software vendors to help enable connectivity and data analytics.

- **Diverse standards and technologies** make it difficult to evaluate the multitude of available technology options. For example, depending on the specific applications, a developer may have to consider wired or wireless implementation. If wireless is preferred, a choice must then be made between the use of licensed or unlicensed spectrum, utilizing a public cellular network or deploying a private low power wide area network or short-range wireless mesh network. These are only a few of the possible variants and only consider the physical layer of the communications infrastructure; the task is much more complex than this.

- **The need to change fundamental business or organizational processes** engenders significant uncertainty and risk for traditional organizations implementing IoT initiatives. It is a dramatic change for a business organized on a traditional product OEM basis to adopt the processes needed to successfully implement a successful, ongoing service model with customers.

- **There is a lack of experience in developing connected products and services** on the part of many traditional product OEMs. Continuing on the point above, many traditional organizations lack the experience and expertise needed to successfully integrate connectivity into their products and services. For example, RF engineering alone is challenging, so much so that RF chip supplier Qualcomm provides full smartphone reference designs to phone manufacturers that do not have the in-house expertise to efficiently and economically design their own models. This challenge is amplified for an organization not in the phone business—such as a utility or automaker—to adopt wireless connectivity, especially for a traditionally unconnected product.

- **Occasionally uncertain regulatory environments** exacerbate the potential uncertainty and risk in committing to IoT projects. For example, two major regulatory initiatives concerning connected vehicles—the Contran 245 stolen vehicle tracking initiative in Brazil and the EU’s eCall emergency crash notification initiative—have faced numerous delays in implementation. This has proved problematic for companies trying to plan business initiatives and investment tied to the enactment of these regulations.

- **There is difficulty in determining the return on investment (ROI)** for IoT initiatives due to the underlying complexity mentioned above (which will also be further discussed below). In surveys conducted by IHS targeting IoT implementers, the challenge of determining the ROI of a potential IoT project is often cited as a key barrier to be overcome.

Creating and maintaining reliable connections

Creating and maintaining reliable connections becomes increasingly important as IoT systems become embedded into critical infrastructure and key use-case domains. There are a plethora of connectivity standards and technologies to choose from and this exacerbates the complexity challenges mentioned above. For example, traditional supervisory control and data acquisition (SCADA) systems often use 4-20 mA analog wireline connectivity, while a number of different proprietary wireline and short-range wireless (SRW) technologies exist in the home security alarm space. These are just two of numerous examples of the wide number of technologies used to connect machines and sensors.

Generally, IoT developers and implementers have the following four classes of connectivity technologies from which to choose: **wireline**, **SRW** (including meshing networking), **long-range wireless** (including cellular and low power wide area networking), and **satellite**. Within each class are numerous specific technologies and standards. For example, while 2G cellular technologies (GSM/GPRS and CDMA 1xRTT) have been mainstays in IoT connectivity, the mobile industry is now working to adapt 4G LTE technology to integrate IoT and is looking ahead to how 5G can be optimized to include support for IoT applications from the start. A key, new low power wide area networking (LPWAN) technology under development as part of 3GPP Release 13 is Narrow Band IoT (NB-IoT). NB-IoT should be finalized when Release 13 is frozen in June 2016 and provide a strong additional option for operators in the IoT market.

However, beyond choosing a specific technology there is the challenge of interoperability. Interoperability is not guaranteed simply because two devices use the same standard or technology. Communication standards are typically complex with optional features and implementation choices available to developers. To ensure interoperability, two devices from different manufacturers must undergo interoperability testing and be certified to work together. This increases time to market, development costs, and other market risks. When a key industry player, such as Huawei, creates a formal ecosystem, this greatly helps reduce risk and uncertainty for the developer, implementer or customer. The ecosystem community members can ensure pre-integration of their respective devices to provide guaranteed plug-and-play interoperability and correspondingly reduce the integration effort required of the operator.

Long-range wireless technology, in particular cellular, is becoming increasingly important in the IoT market. Many IoT applications, such as connected cars and various types of remote sensors, are best connected by a long-range wireless technology. However, traditional cellular technology was developed for handsets and has a number of cost and battery life characteristics that are not optimal for IoT applications. Consequently, Huawei, Qualcomm, Vodafone, and others in the mobile industry have spurred the development of NB-IoT in 3GPP to provide a technology better suited to IoT applications requiring longer battery life and greatly reduced cost. Much of the basis for NB-IoT comes from Huawei’s original development of its “Cellular IoT” technology and now has the global mobile industry’s support through the 3GPP process.

NB-IoT does not just reduce device cost and increase device battery life. The technology enables several orders of magnitude increases in the number of devices that can be supported by a single base station, relative to traditional cellular technology. NB-IoT also extends the connection range by 20 dB, enabling connectivity to devices in basements, such as smart electric meters in Europe, or a few feet underground, such as sump pumps. It is important to note that NB-IoT is being standardized in parallel to other LTE evolutions, such as LTE Cat-1 and LTE Cat-M, which are also more optimized for IoT applications, albeit relatively more similar to traditional cellular features and functionality.

In addition to the benefits mentioned above, NB-IoT is designed with the following features:

- Extended battery life from 10 to 15 years.
- Easy deployment with existing network hardware (only requiring a baseband card update at the base station, enabling the reuse of all existing cell site equipment).
- Frequency deployment flexibility in licensed frequency bands. NB-IoT can use re-farmed GSM in-band spectrum in 200 kHz blocks, standalone spectrum, LTE guard band spectrum, and LTE in-band spectrum.
- Low-cost modems (approximately $5 per unit).

However, choosing an optimal connectivity technology is only part of the task in creating and maintaining a reliable connection. The connection must be able to be managed effectively by the operator and customer. Data sent over the connection must be handled correctly and transported to the necessary databases and enterprise management systems. These are part of the functions that are performed by an IoT platform, such as Huawei’s Ocean Connect IoT Platform (and associated ecosystem), which are discussed later.

Ensuring data security and privacy

As IoT applications permeate industry and society, these applications create increasingly critical dependencies. For example, smart electric grids, connected cars, smart homes, and many other “smart” and “connected” IoT applications expose consumers and businesses to malicious attack and exploitation. The hostile parties posing this risk range from adolescents seeking a thrill to highly sophisticated and well-resourced state actors perpetrating cyberespionage.

The risks posed by inadequate IoT security are generally as follows:

- **Theft** of data from the systems or theft of material items as a result of information gained illicitly from compromised systems.

- **Danger to health and safety** from compromised systems not operating in the intended manner.

- **Loss of productivity** from compromised systems not operating in the intended manner.

- **Loss of privacy** from information gained from a compromised system or illicit access to information about a system’s operation.

- **Noncompliance** with laws or regulations as a result of loss of data from a compromised system.

- **Damaged reputation** as a result of losing customers' sensitive data or harm to customers from compromised systems.

IoT security must be implemented at the device level and in the network, cloud, and enterprise back-end systems. Security must be ensured for data at rest (stored data), data in use (on a device), and data in motion (data transported across a network). However, doing so is particularly challenging for IoT applications due to a number of factors:

- **Unattended** remote devices are often physically accessible to an attacker.

- **Low-cost, battery-powered remote devices and sensors** often lack sufficient processing power to host traditional client-server security mechanisms.

- **Inexperienced developers in regards to cybersecurity** best practices, which are prevalent at companies shifting from traditional technological approaches and business models to an IoT model.

- **Proliferating threat vectors** resulting from an expanded attack service as the number and types of remote devices and systems increase.

Encryption forms the primary base on which IoT cybersecurity is implemented. Cybersecurity systems seek to ensure:

- **Authentication** ensures that the device or object is as described.

- **Availability** ensures access to information and services provided by a device.

- **Confidentiality** ensures the privacy of data at rest on a device or in motion between devices.

- **Integrity** ensures that the device is operating and communicating in a trusted manner.

Although cryptography mechanisms can be implemented in the remote device in software, there is growing recognition that software-only systems provide an inadequate level of security. Two primary hardware-based approaches are in use: one is to implement cryptography and other cybersecurity techniques in a standalone security co-processor running alongside the main host processor, and the other is to implement these in hardware circuitry that is designed directly into the host processor.

Using data optimally

A particular area of complexity hindering the IoT market is the optimal management and use of the data flowing from various sources, including connected devices and sensors. This complexity presents itself in seven key areas of data utilization:

- Data security
- Data volume
- Data diversity
- Data velocity
- Data analytics
- Data economics
- Data logistics

Data security involves a range of threats, stakeholders, and applicable technologies. In addition to the technological and business concerns cited above, it is important to emphasize the privacy dimension arising from increasingly pervasive IoT systems.

An interesting case example comes from a 2012 Forbes profile of how retailer Target was able to develop big data analytical techniques that enabled the firm to determine that a teenager was pregnant based on her shopping patterns and sent her coupons for pregnancy-related goods, causing much consternation to her unknowing family. While this is not precisely an IoT application, it shows both the power of big data and at the same time its ability to invade personal lives. More concretely, from an IoT perspective there are concerns that hackers could steal information, for example from smart meters or home automation systems, to determine when house occupants are away from their homes, leading to an increased risk of burglary. There a numerous other examples of how privacy is potentially at risk as IoT applications become more widely deployed.

The issue of privacy in the face of big data and pervasive IoT data collection systems does not have an easy technological solution. There will need to be further development of legal and regulatory systems as well as societal norms around acceptable data collection, storage, and usage.

Data volume in the sense of the need to manage and process very large amounts of data is a well-publicized characteristic of the IoT, though it is not exclusively an IoT phenomenon. It is almost certain that some IoT implementers and customers will encounter the issue of “big data” management, where the sheer volume of the data to be managed is the primary challenge at hand. However, in the near term, and for the majority of IoT developers and implementers, the more pressing challenge is simply moving from less data-intensive processes to more data-intensive ones as data from IoT systems becomes more available.

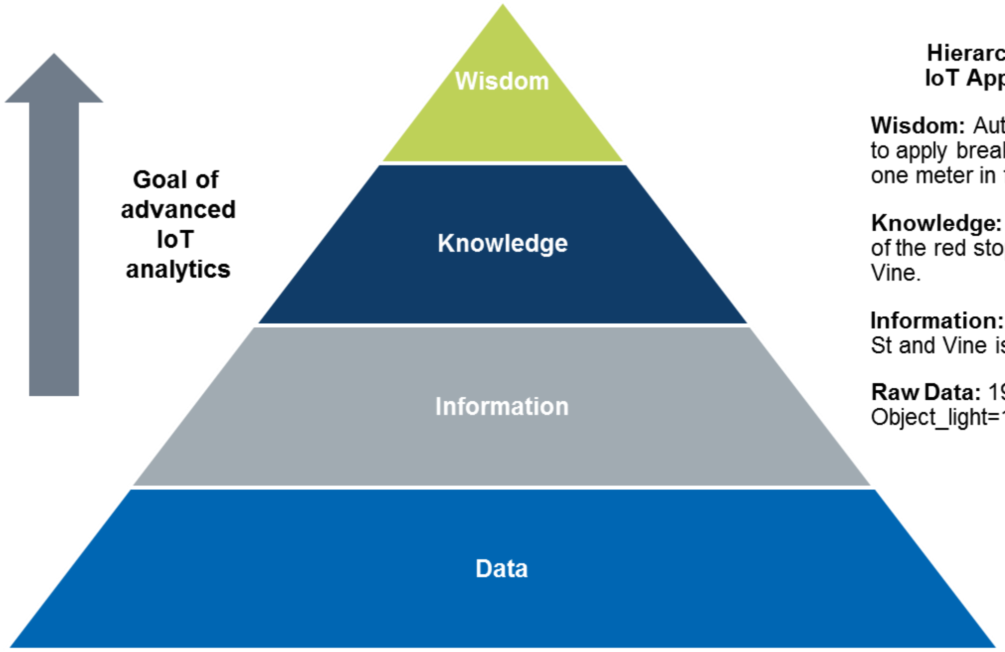
For instance, many utilities have struggled to manage the vastly increased amounts of data resulting from moving from (at the shortest) a once-a-month meter reading schedule to a 15-minute interval smart meter reading schedule. The amount of data in absolute terms is not extraordinary, but utilities have needed to adjust their systems and processes to account for it.

Data diversity entails the widely varied sources and types of data in use. As mentioned above, a key benefit of the IoT is the ability to “mash up” different data sources in new and innovative ways. However, in practice this may entail the need to integrate many different types of data, from structured to unstructured, machine data, and data residing in traditional enterprise database systems.

Data velocity is an aspect of data diversity that bears special mentioning. Unlike the response times to data inputs of most traditional enterprise IT systems, those needed in IoT applications can vary from “none” through varying degrees to “real-time”. Dealing with less time-sensitive systems, such as a weather monitoring station, is a relatively easy task. However, engineering a system that can provide real-time, closed-loop responses, such as those needed for factory automation systems, is a very difficult endeavor.

Data analytics is the means by which raw data is turned into useful information and value. In the context of IoT, the concept of “predictive analytics” is currently experiencing tremendous attention and hype as developers and implementers seek to use automated data to optimally address deficiencies and problems before they occur, leading to increased efficiency and reduced costs. A number of specialist data analytics firms, such as Flowthings.io and Vitria as well as traditional ICT vendors including Huawei, are addressing data analytics. These vendors are seeking to simplify the data analytics challenge for the IoT community as many developers and implementers find that developing robust analytics capabilities in-house, even with the help of “data scientists”, is a challenging proposition. Figure 2 below illustrates the goals of enabling IoT applications with advanced analytics capabilities.

Figure 2. “Hierarchy of Knowledge” as a model for assessing the goals of advanced IoT analytics



Hierarchy of Knowledge
IoT Application Example

Wisdom: Automatically assist driver to apply breaks to gracefully stop car one meter in front of intersection.

Knowledge: I am within 50 meters of the red stoplight at 42nd St and Vine.

Information: The stoplight at 42nd St and Vine is now “red”.

Raw Data: 192.168.7.3 sending Object_light=1

Source: IHS

© 2016 IHS

Data economics is an issue in the IoT market because of the primary/secondary developer structure mentioned above. Primary developers deploy systems in the field and own the resulting data. Secondary developers are third parties that access the data to create new and innovative applications. Incentives need to be created for the primary owners of data to allow access to and use of the data by the secondary developers. Creating and maintaining these incentives over time is potentially a complex technical and business undertaking.

Data logistics deal with the optimal management of data over varying geographic areas and diverse networks. For example, IoT edge routers can typically process some data locally rather than sending it all to the cloud for processing. This data processing model, termed “fog computing”, helps to both increase the speed of response to local events as well as reduce traffic over the network. Additionally, a number of firms, such as PubNub and Wot.io, are creating data exchange services to help manage data flows over large geographic distances. For example, PubNub adds resilience to applications by updating remote devices that have briefly lost connectivity (perhaps to a dropped cellular connection).

Enabling an open IoT ecosystem

Open ecosystems and cross-vertical, cross-value chain collaboration are crucial in the IoT because much of the proposed innovation and value is due to “mash ups” (e.g. integration) of data from diverse sources, ranging from connected machine and sensor data, social media, and traditional ERP/CRM systems to open government databases.

Traditional models for connected device markets, ranging from SCADA-era industrial automation and proprietary home alarm systems to (until recently) connected car services, face a number of interrelated challenges:

- Such applications and services are typically tightly vertically integrated and in many cases use proprietary technology.
- Data is often isolated and in silos. The developer or implementer is responsible for deploying the application infrastructure and has access to the data only from the application infrastructure.
- The ability to work across industry verticals and enterprise/telecom/government markets is limited due to the need to customize the vertically-integrated application for a specific customer type.
- The pace of innovation is gated by the resources available to the developer.
- Cost declines are often slow as a result of vertically-integrated systems with scale and limited supplier bases.
- Time to market is often long and also gated by the resources available to the developer.
- Security can be problematic. Though “security through obscurity” is in use, it rarely compares well to security mechanisms that have been vetted by a large body of participants in an open manner.

A number of key IoT platform vendors, such as Huawei, are creating open ecosystems along two parallel paths. The first path is via the platform itself, along with related services. Though these will be discussed in more detail below, in short they help to disaggregate application value chains. The second path is through creating formal alliances and partnerships with communities of suppliers at multiple levels of the value chain based on the common use of the vendor’s IoT platform as an anchor. These are “open ecosystems” in a concrete sense of interrelationships in the value chain. Together, these two strategies offer a number of compelling benefits to IoT developers and implementers:

- The pace of innovation increases as the R&D budgets of the entire ecosystem can be leveraged.
- Cost declines are typically faster as competition increases with greater scale and larger supplier bases.
- Time to market is usually faster for the developer as the IoT platform and ecosystem of suppliers take on the burden of many of the development issues.
- Security is typically enhanced as problems are discovered and remedied by a larger body of participants.
- The ability to work across verticals and enterprise/telecom/government markets is greatly increased. The IoT platform and open ecosystem confer an ability to rapidly address new verticals and markets because the bulk of the technical underpinnings of the application is taken away from the developer.
- Assuming security, privacy, and incentive concerns are addressed, open ecosystems enable data to be shared between primary developers/implementers (which have deployed connected machines and sensors and own the resulting data) and secondary developers/implementers (third parties which repurpose data from primary developers/implementers into new applications).
- Suppliers further benefit from participating in a successful, open ecosystem by enjoying a larger potential addressable market than they otherwise might have in trying to offer a vertically-integrated solution on their own.

IoT platforms are a key solution

There are not any quick fixes for the challenges facing the IoT market. Certainly, few companies can affect major regulatory initiatives substantially. However, IoT platforms are a key tool to ameliorate and redress the challenges described in this whitepaper. What exactly is an "IoT platform"? This is a complex question due to the ambiguity of the varied uses of the term by the multitude of players in the IoT market.

IHS defines an IoT platform as "cloud-based and on premise software packages and related services that enable and support sophisticated IoT services". In some instances, IoT platforms enable application developers to streamline and automate common features that would otherwise require considerable additional time, effort and expense. In other instances, IoT platforms enable enterprises to manage thousands, millions, and even billions of devices and connections across multiple technologies and protocols. Finally, in some cases, IoT software enables developers to combine device and connection data with enterprise-specific customer and ERP data as well as data from third-party sources like social and weather data to create more valuable IoT applications.

By analyzing dozens of vendors through primary and secondary research methodologies, IHS has developed a taxonomy of software-related functions comprising what IHS considers to be the entire IoT platform stack. At the highest level, this analysis finds that an IoT software platform will incorporate some combination of the following five functional areas. Each of these must be addressed in order to develop, on board, operate and manage an IoT application:

- **Cloud/data center** services are now a staple of general ICT service delivery as more and more organizations rely on hosted computing and data storage resources. Amazon Web Services, Google, and Microsoft are among the largest cloud computing providers globally. Cloud computing is imperative to IoT applications.

- **Data management** focuses on managing the flows of data between applications and from a geospatial perspective. A key aspect of this relative to the IoT is the "mashup" of data from machines and sensors with data from traditional CRM/ERP systems, open government databases, and social media.

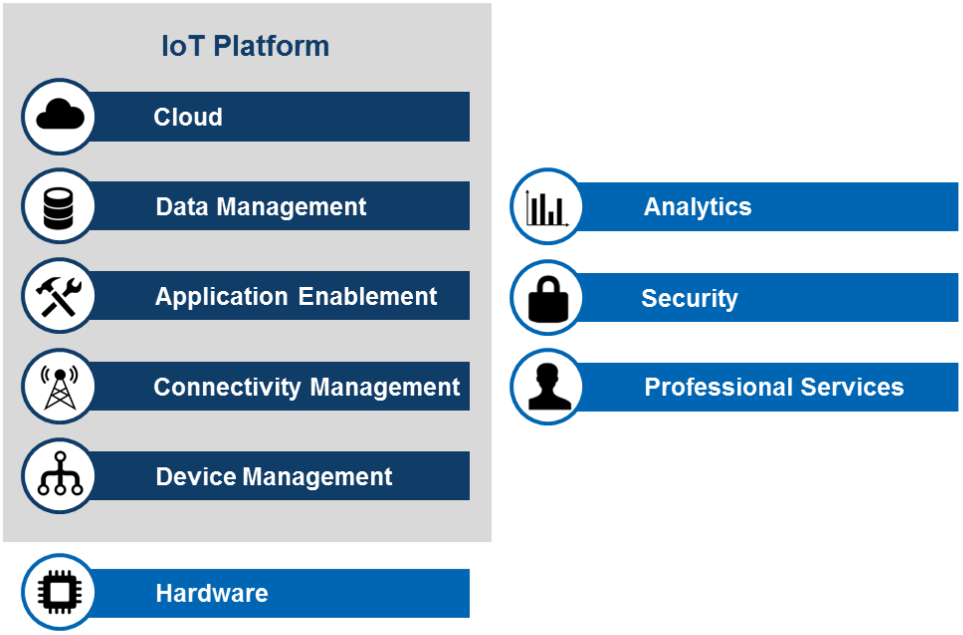
- **Application enablement** entails tools that assist IoT developers and implementers in rapidly and efficiently prototyping, building, integrating, and managing IoT applications. Application enablement platforms (AEPs) are often offered on a standalone basis in addition to being part of a larger IoT platform. They essentially provide business logic, such as the ability to define rules and alerts, which are common to most IoT applications, enabling the developer to focus on the differentiating aspects of the application that are unique to the market.

- **Connectivity management** is particularly applicable in the context of rated cellular connectivity services, but is also necessary in the context of large-scale, private networks. In addition to their role as a part of a larger IoT platform, connectivity management platforms (CMPs) are also deployed on a standalone basis by mobile operators and offered by vendors such as Jasper and Ericsson. Their primary role in a cellular context is to: provide for automated remote bulk provisioning of SIM card-enabled devices directly by the customer, remote troubleshooting, authentication and security, flexible billing and rating, management of thresholds and alerts, management of the connection directly by the customer (e.g. connection turn-on, turn-off, suspension, etc.), and integration of the platform's functionality into the customer's existing enterprise management systems via application programming interfaces (APIs) as well as web-based user interfaces. Additionally, as most IoT connections are to non-cellular devices, the ability to manage technologies beyond cellular will increasingly be a key feature for IoT platforms.

- **Device management/device clouds** are often offered on a standalone basis by IoT devices vendors (e.g. module and gateway/router vendors) to facilitate and encourage adoption of these vendors' devices for IoT applications by customers. Device clouds perform a variety of functions that center on network-centric device control, diagnostics, and optimization.

Figure 3 below places the above collection of software and services that IHS terms an "IoT platform" into the context of the larger IoT ecosystem. It is important to note that IoT platform functionality is not standardized in the market. Some IoT platform vendors offer a number, but not all, of the components listed below. Often, full platform functionality is accomplished with the aid of ecosystem partners contributing important pieces of the puzzle. Additionally, many IoT platform vendors supply the supporting services listed on the right of Figure 2—namely analytics, security, and professional services—but these are also supplied by third-party vendors on a standalone basis.

Figure 3. IoT platform diagram



Source: IHS

© 2016 IHS

The main purpose of IoT platforms is to reduce the complexities discussed above for IoT developers, service providers, and implementers. Think of an iceberg; most of the ice mass is submerged below the waterline. Similarly, many, if not most, IoT applications share a large percentage of core functionality. Functions such as rules for thresholds and alerts, multiprotocol support, over-the-air firmware downloads and remote diagnostics are largely the same whether the IoT application is a fleet management service or a smart meter deployment. Much like the visible tip of the iceberg, the aspects of the IoT application that are truly unique and differentiated are typically quite a small portion of the overall application.

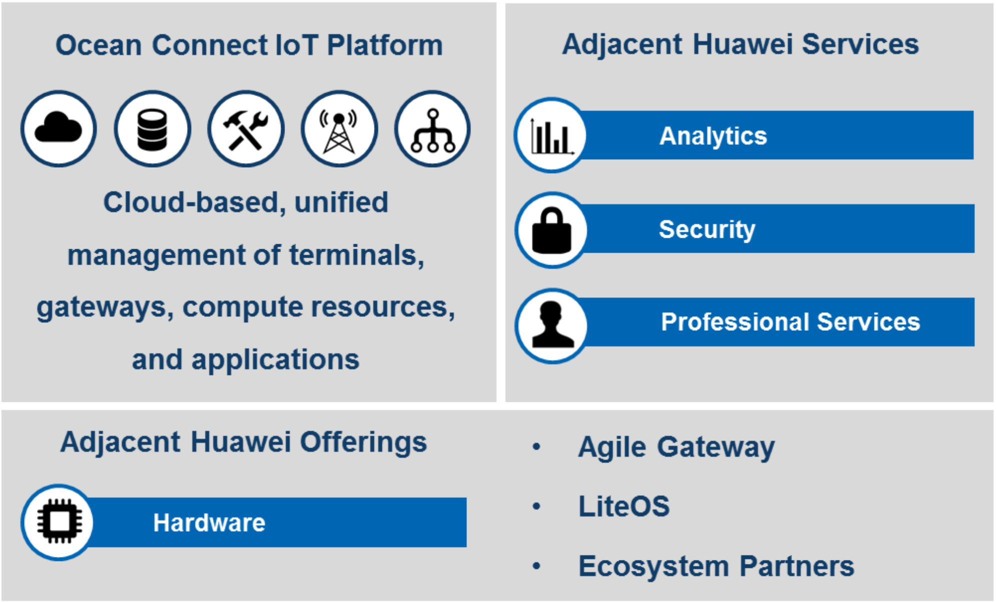
IoT platforms therefore enable the IoT developer to focus on the differentiated and unique value the application provides and outsource common, industry-wide features and functionality. This obviously reduces time to market, needed investment and expertise, and risk.

Huawei's Ocean Connect IoT Platform

Huawei provides a particularly illustrative example of a comprehensive IoT platform. Huawei's offering, which is currently being used in applications ranging from smart meters to connected home appliances, is called the "Ocean Connect IoT Platform". The platform is centered on the five major IoT platform functions described earlier. Huawei also provides closely related offerings, including the "Agile Gateway" (an IoT edge router) and "LiteOS" embedded IoT open-source operating system as well as analytic, security, and professional services. Additionally, a key feature in Huawei's strategy is to foster an open ecosystem of component and hardware partners that leverage the Ocean Connect IoT Platform and thereby help simplify customers' sourcing challenges.

Figure 4 below provides an illustration of the Ocean Connect IoT Platform.

Figure 4. Huawei's "Ocean Connect IoT Platform" and ecosystem offering


Ocean Connect IoT Platform
Cloud-based, unified management of terminals, gateways, compute resources, and applications
Adjacent Huawei Services
Analytics
Security
Professional Services
Adjacent Huawei Offerings
Hardware
• Agile Gateway
• LiteOS
• Ecosystem Partners

Source: IHS

© 2016 IHS

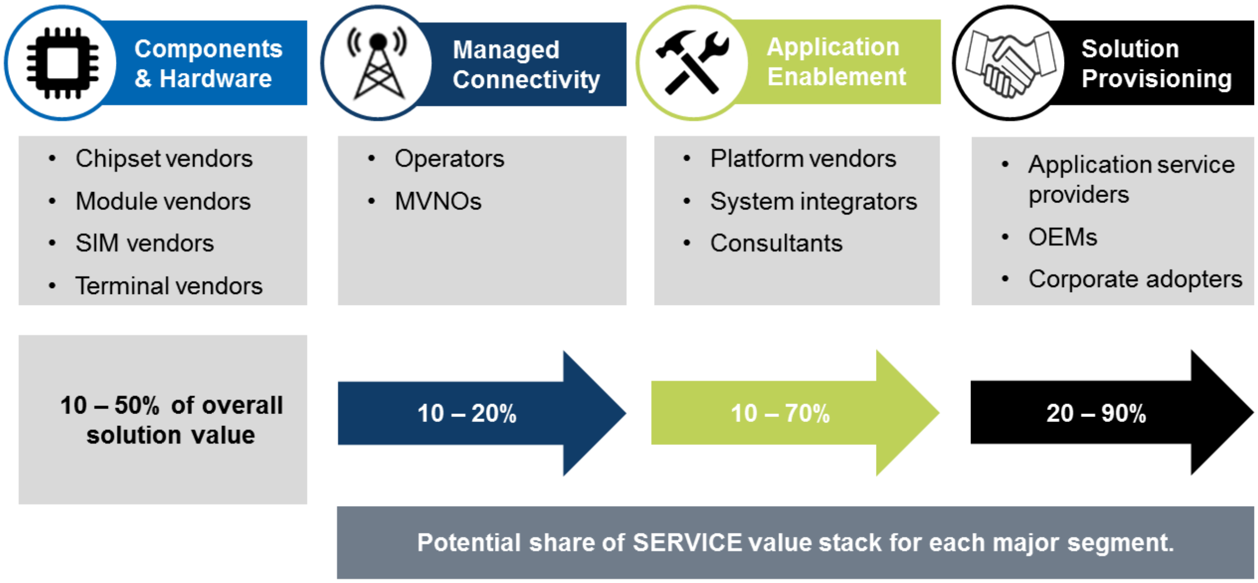
Selecting an IoT platform

Much of this whitepaper has focused on IoT "developers" and "implementers" in abstract, cross-vertical terms. However, both developers and implementers are typically placed within a specific vertical context, such as smart homes, smart energy, or connected vehicles. Equally important are the roles that mobile operators are increasingly playing in the overall IoT ecosystem. These two concepts—vertical specificity and mobile operator activity—are closely entwined.

Globally, mobile operators are taking leading roles in not only providing managed connectivity services for IoT applications but also in moving up the value chain to offer various sophisticated value-added services (VAS) and even complete, end-to-end (E2E) solutions in the market. ("Mobile" operator may be somewhat of a misnomer here as many operators will supply multiple types of connectivity, including wireline and SRW, in addition to traditional cellular mobile services).

Figure 5 below shows a simplified diagram of the IoT value chain and how value is broadly apportioned among the key major segments. Given the wide variability in IoT applications, there is correspondingly large potential differences in the value accruing to each segment for various applications. Components and hardware generally comprise between 10% and 50% of the overall value of an IoT solution. When looking specifically at the service segment of the value chain, the key point to understand is there is generally much more value closer to the end customer. That is, while managed network connectivity services generally comprise only 10% to 20% of the service value stack, platforms and various types of VAS can comprise from 10% to 70% of the service value stack. Likewise, the provisioning of the application to the end customer accounts for 20% to 90% of the service value stack. This is the core reason why operators are seeking to move up the value stack to provide more of the full E2E solution themselves to end customers, typically with the help of partners like Huawei and others.

Figure 5. Simplified value chain segmentation and value apportionment



Components & Hardware

- Chipset vendors
- Module vendors
- SIM vendors
- Terminal vendors

10 – 50% of overall solution value

Managed Connectivity

- Operators
- MVNOs

10 – 20%

Application Enablement

- Platform vendors
- System integrators
- Consultants

10 – 70%

Solution Provisioning

- Application service providers
- OEMs
- Corporate adopters

20 – 90%

Potential share of SERVICE value stack for each major segment.

Source: IHS

© 2016 IHS

Managed connectivity

Managed connectivity forms the basic offering that all operators start with, even if they do not offer more advanced services on top of that. While a full IoT platform is not needed for managed connectivity offers, operators still need specific systems in place to tailor connectivity technology management for IoT use characteristics, as described previously.

A number of operators that entered the IoT market in the last decade built their IoT connectivity management platforms, including Vodafone, Deutsche Telekom, Orange Business Services, and AT&T. This was often done with the help of consultants and system integrators and was a necessity because few alternatives were available. Likewise, several companies have developed merchant market IoT connectivity platforms specifically focused on cellular connection management. These include Jasper (which Cisco acquired in April 2016) and Ericsson. More recently, operators have largely chosen to use third-party platforms, either from telecom equipment vendors or MVNOs that re-sell their platform back to operators. Operators benefit from the research and investment that third-party platform providers can amortize across a larger base of connections. Generally, the underlying trend in IoT platforms is for multi-connectivity management and inclusion of, or connection to, big data analytics capabilities.

Huawei's Ocean Connect IoT Platform provides a robust, multi-technology connectivity management offering with all of the functionalities described above. The Ocean Connect IoT Platform enables management of SIMs, sensors, terminals, and other non-SIM end equipment terminals. This is done in the context of end-to-end policy control and quality of service, with authentication, identity management, and other key aspects of security a key component of the platform.

While the connectivity management functionality could be used on a standalone basis by an operator seeking to offer only IoT managed connectivity services, a key benefit for operators is that the Ocean Connect IoT Platform provides this functionality in the context of not only a full IoT platform software stack but also incorporates closely allied services such as security, analytics, professional services, and a full ecosystem of supplier partners. This greatly increases the flexibility operators have in strategically moving up the value stack in the IoT market.

Application enablement

Operators are increasingly moving up the value stack to provide many additional value-added services to help IoT developers and implementers reduce risks, costs, and time to market. IoT platforms are a key building block in these service offers. Certainly, developers and implementers could source IoT platforms directly from a vendor like Huawei, but by bundling IoT platform functionality with multi-technology network access as well as the full ecosystem that large players like operators can assemble, operators are able provide even greater simplification and risk reduction than is possible through the standalone procurement of an IoT platform.

The incentive for operators to move beyond managed connectivity offerings is clear: there is much more value—and revenue—to be had further up the value stack, i.e. closer to the end customer. IHS estimates that managed connectivity accounts for roughly 10 – 20% of the IoT service stack. Meanwhile, various types of value-added services comprise an additional 10 – 70% of the IoT service stack; the more services the operator provides to enable developers and implementers, the greater the value and revenue.

As with managed connectivity, operators typically rely on third-party IoT platforms to develop their value-added service offerings rather than developing in-house. A key reason for this is that an IoT platform can help reduce costs and risks for the operator. An IoT platform, like Huawei's Ocean Connect IoT Platform, provides a number of important features and functionalities in this regard. Many of these have been highlighted above, but special mention should be made of service orchestration and automated business logic.

Service orchestration and automated business logic are vital because different sensors and equipment produce very different types of data and communicate in different ways. Service orchestration and automated business logic help to enable configurable rules and actions to be developed to make use of these data. "Configurable" is a key term because a main strength of the Agile IoT Solution is to obviate much of the need for additional custom programming to enable case-specific functionality; even end users should be able to configure specific actions in an “IFTTT” model. This is an important feature because different customers need to be able to define rules, and operators need to be able to provide this capability to these customers. An additional aspect of Huawei’s IFTTT model is that it applies to existing network services (such as “initiate voice call” and “send video to mobile phone”) as well as IoT services, thereby integrating the existing human-centric operator network functions with the IoT capabilities of the platform.

Solution provisioning

Solution provisioning occurs when the operator provides a complete, end-to-end solution or application directly to implementers and end customers. Examples of operators already offering such solutions in the market include: AT&T Digital Life (AT&T’s home security and automation service), Vodafone Automotive (Vodafone’s connected car and fleet management service), and Telefonica Smart Cities (Telefonica’s smart cities offering to municipalities).

Solution provisioning follows the same strategic rationale for operators as providing IoT application enablement services to developers and implementers: greater value and revenue resides closer to the end customer. In the case of providing full end-to-end solutions, IHS estimates that the value of “owning” the end-customer relationship is worth approximately 30% of the entire service value stack. This is on top of other pieces of the solution the operator provides as part of the solution (taking into account that revenue will be shared with suppliers and partners).

Providing a complete, end-to-end solution is challenging for even very large operators. In addition to other challenges already addressed previously in this whitepaper, there is the challenge of developing vertical market expertise. Some of this challenge can be reduced through partnerships with application service providers (ASP) that are structured as a re-sale of the ASP’s solution by the operator, but this is not a full solution offering by the operator, and a significant share of revenue goes to the ASP’s partner.

Operators may also acquire ASPs in order to reduce or eliminate their learning curve (and increase their revenue share). This is what Vodafone accomplished in acquiring Cobra Automotive Technologies to form the basis of Vodafone Automotive. However, the acquisition route entails challenges in terms of both substantial upfront financial costs and well as integration risks.

IHS considers the use of IoT platforms and related ecosystem services and partnerships to be an optimal way for operators to target full solutions in select vertical IoT markets. IoT platforms can greatly facilitate market entry of operators just as they do for IoT developers and implementers directly, for all of the reasons cited above. However, all IoT platforms are not created equal; while horizontal functionality is important, some platforms are, or can be, precisely tuned to meet the needs of specific vertical markets and applications.

To date, several operators have developed (often with partners) their own “tuned” vertical-specific platforms. For example, AT&T worked with Ericsson in the development of AT&T’s Drive Studio connected car platform. Telefonica has likewise developed its Thinking Cities smart cities platform with features and functionality suitable to the smart cities market, including compliance with the developing European FIWARE open-source platform protocols that are geared toward the smart cities market.

Huawei’s Ocean Connect IoT Platform provides preconfigured business logic tuned for a number of key IoT verticals, especially smart homes, smart energy, and connected cars. Equally as important, the Ocean Connect IoT Platform can be personalized with specific functionalities chosen by the operator to differentiate its service and rapidly configured to enter new verticals as an operator expands its market. This agility is on top of a robust, multi-connectivity technology base that enables the operator to utilize whatever connectivity technology or protocol is optimal for a given offering.

Finally, Huawei does not offer applications directly in the market; it is a benefit to an operator not to have to compete with its suppliers (like Huawei) in supplying end-customer solutions.

Conclusion

As industry and society change in fundamental ways as a result of the “datafication” enabled by the Internet of Things, IoT platforms, such as **Huawei’s Ocean Connect IoT Platform**, will play a key role in ameliorating the challenges to realizing this vision. The IoT market is transitioning from isolated point solutions to a pervasive and common data infrastructure. Enterprises, telecoms, and government entities are all leveraging the new capabilities and functionalities of IoT applications to increase efficiencies and provide new value propositions.

IoT platforms serve to remove the complexity in developing, deploying, and managing IoT applications over the application lifecycle from the developer or implementer (whether an enterprise, government entity, or operator). Moreover, IoT platforms provide operators flexibility to choose various strategic approaches to the Internet of Things beyond simple managed connectivity offers. IoT platforms help operators to offer various types of value-added services to developers and implementers as well as complete, end-to-end IoT solutions in the market directly.

Huawei’s Ocean Connect IoT Platform is a key example of a major telecom equipment supplier offering a comprehensive approach in the IoT platform market. Not only is the Ocean Connect IoT Platform a complete IoT platform, it is offered to the market in the context of a complete IoT ecosystem comprising allied services, such as analytics, security, and professional services as well as an IoT edge router (**Agile IoT Gateway**), device software (**LiteOS**), and community of component and terminal supplier partners. The full offering from Huawei, including its extended ecosystem of partners, offers operators, in particular, a means to rapidly, flexibly, and robustly target multiple IoT vertical markets.

Contacts

Sam Lucero
Sr. Principal Analyst, M2M and IoT
Sam.Lucero@ihs.com

Josh Builta
Assoc. Director, M2M and IoT
Josh.Builta@ihs.com

Bill Morelli
Director, IoT and Connectivity
Bill.Morelli@ihs.com

John Byrne
Sr. Principal Analyst, M2M and IoT
John.Byrne@ihs.com

Jeffrey Song
Sr. Account Manager, APAC
Jeffrey.Song@ihs.com

IHS Customer Care:

Americas: +1 800 IHS CARE (+1 800 447 2273); CustomerCare@ihs.com
Europe, Middle East, and Africa: +44 (0) 1344 328 300; Customer.Support@ihs.com
Asia and the Pacific Rim: +604 291 3600; SupportAPAC@ihs.com