Deloitte University Press

Beyond the dumb pipe

The IoT and the new role for network service providers

An article in Deloitte's series examining the nature and impact of the Internet of Things

About the authors

Philip Wilson is a director in the Telecommunications, Media, and Technology practice at Deloitte Consulting LLP. Wilson has over 25 years of experience in the telecommunications industry. He has developed corporate strategy for over 200 companies in 27 countries, and has taken roles both as a consultant and at a senior level in industry.

Michael E. Raynor is a director with Deloitte Services LP and the Innovation theme leader for Deloitte. He is the author or co-author of four books, most recently *The Three Rules: How Exceptional Companies Think* (May 2013).

Deloitte's Internet of Things practice enables organizations to identify where the IoT can potentially create value in their industry and develop strategies to capture that value, utilizing IoT for operational benefit.

To learn more about Deloitte's IoT practice, visit http://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/topics/the-internet-of-things.html.

Read more of our research and thought leadership on the IoT at http://dupress.com/collection/internet-of-things.

Contents

Introduction

THE Internet of Things (IoT) has become increasingly visible thanks to the rise of intelligent thermostats, interactive fitness trackers, and the promise of autonomous vehicles. Such technologies are compelling because they make the things around us smarter and more interactive. In the words of one commentator, we need no longer settle for dumb tools but can instead look forward to "enchanted objects."[1]

The sensor technologies that make things "smart" are only part of the IoT, however. Connecting all these devices is what turns isolated pockets of technology into a network that generates and pools data in ways that lead to valuable insights.

Thanks to the central role of communications in many IoT deployments, how companies create value is often a function of the interaction between sensor technology and the network layer. Linking new and legacy sensors within an IoT ecosystem often means that companies seeking to realize value from the IoT need to work closely with their communication services providers (CSPs).

Such collaboration is unlikely to come easily to either party. Consumers of communications services can easily overlook the challenges associated with creating the sort of connectivity required to realize the full benefit of IoT technology. With "Internet" in its name, the IoT connotes that the advancing legions of smart devices need simply plug into the existing infrastructure: Just give everything an email address and we're good to go. In this scenario, CSPs aren't indispensable partners—they're mere vendors.

Providers of network services can be expected to have their own biases to overcome. The rise of the Internet separated communications services from the communications network they ride over. There was a tendency among CSPs to resist the claim that they provided little more than "dumb pipes," a term that belied the industry's technological sophistication. Yet the economics of the asset intensity implied by building out near-ubiquitous, high-bandwidth, reliable, and secure wireline and wireless networks rewarded the large-scale deployment of relatively undifferentiated services. Shifting to a more nearly bespoke set of solutions means going against a grain that runs deep.

> In the words of one commentator, we need no longer settle for dumb tools but can instead look forward to "enchanted objects."

To help companies and CSPs think more carefully about how they work together and overcome any legacy of benign mutual neglect, we are well served to consider how sensor technology and network systems relate within different IoT deployments, the nature of the value created, and what that means for the collaboration required.

Sensors and networks: A value-creation framework

THE rise of smart, connected things—from wearable activity trackers to connected cars to the electrical grid—allows companies to compete not only on the functionality and performance of their products or services but also on the information created by the use of these products or services.[2] Where supply chains determine functionality and performance, the value created by information is captured by the Information Value Loop (see inset).

The value loop begins with *creating* and *communicating* information in entirely new contexts. Sensor technology enables actions in the world to give rise to data—the *create* stage. Networks, often provided and managed by CSPs, link *create* and *communicate*, liberating data and enabling the rest of the value loop. It is at the interface between the two that the opportunity for new forms of collaboration arises.

When the Internet emerged, most online services connected people, and there was a relatively high tolerance for low or variable quality because people are good at coping with latency, errors, and/or failure. Unlike people, even smart machines are poorly equipped to deal with these same communication issues. In other words, dumb pipes are sufficient when connecting people; smarter pipes become more important when connecting things.

More demanding still, some companies are deploying a much larger number of sensors—connecting tens of billions of things rather than "merely" hundreds of millions of people—and many companies are placing those sensors in harsh environments or mission-critical situations that put new stresses on how these devices need to communicate. Consequently, there is no one-size-fits-all combination of sensors and network connectivity. What is being connected (that is, the nature of the sensors) and how it is connected (that is, the nature of the network) have a real impact on how value is created. At first principles, the differences turn in many cases on a choice between new and legacy sensors, and between "best efforts" and managed communication.

Sensors: Legacy versus new

In weighing how to incorporate IoT technology and applications, few companies today are starting from scratch. Many industrial activities, for instance, have long had sensors generating data, at central plants and remote locations, at customers' homes and main assembly lines. These sensors, often installed decades ago, typically have limited communication or autonomous operation capabilities— they rely on human operators for activation and data collection—much less the capacity for analysis and action. So the first key decision is whether to augment existing sensors or to replace those sensors with smart, connected devices.

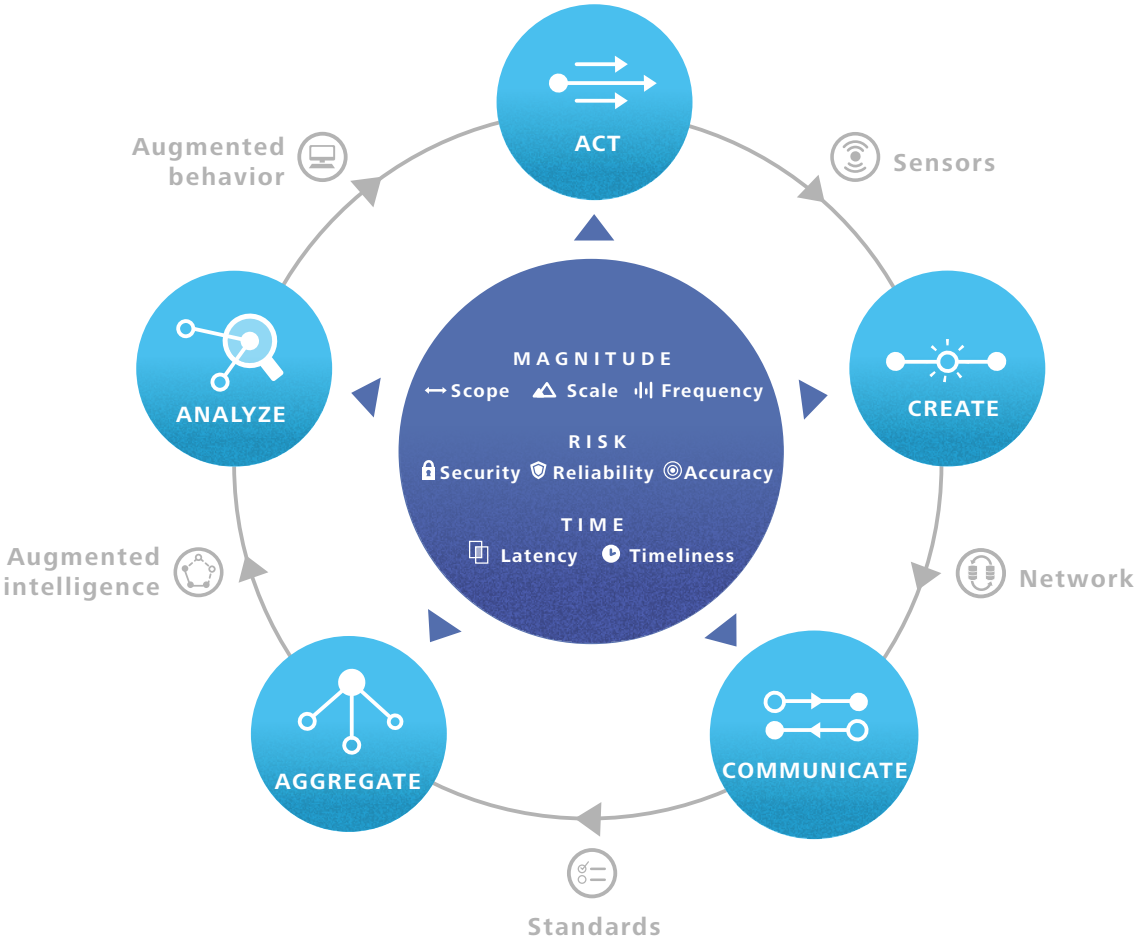
As with many technologies, prices of IoT-enabled sensors are falling. In commercial applications, replacing existing sensors nevertheless can be expensive. More daunting, wholesale replacement can require rethinking a business process. This combination of cost, asset life cycle, and inertia means that many solutions will rely on existing sensors augmented with either communication capabilities or additional sensors. (As a company rolls out new business assets, those can be outfitted with new sensor networks.)

In contrast, consumer applications often require new smart sensors—either as standalone additions to an existing asset or to be

THE INFORMATION VALUE LOOP

The suite of technologies that enables the Internet of Things promises to turn almost any object into a source of information about that object. This creates both a new way to differentiate products and services and a new source of value that can be managed in its own right.

Creating value in the form of products and services gave rise to the notion of a "value chain"—the series and sequence of activities by which an organization transforms inputs into outputs. Similarly, realizing the IoT's full potential motivates a framework that captures the series and sequence of activities by which organizations create value from information: the Information Value Loop.



Note first that the value loop is a *loop*: an action—the state or behavior of things in the real world—gives rise to information, which is then manipulated in order to inform future action. For information to complete the loop and create value, it passes through the stages of the loop, each stage enabled by specific *technologies*. An *act* is monitored by a *sensor* that *creates* information. That information passed through a *network* so that it can be *communicated*, and *standards*—be they technical, legal, regulatory, or social—allow that information to *aggregated* across time and space. *Augmented intelligence* is a generic term meant to capture all manner of analytical support, which collectively are used to *analyze* information. The loop is completed via *augmented behavior* technologies that either enable automated autonomous action or shape human decision in a manner that leads to improved action.

embedded in a replacement asset. Current standalone examples include smart thermostats and security systems. Sensors are also being embedded in cars, domestic appliances, and consumer electronics. These solutions' functionality—and business models—are still in flux, leaving similarly undetermined the relationship between the capabilities of the sensors and the networks they require. In other words, consumer-facing businesses don't know yet what IoT-enabled products customers will buy in the coming years, or exactly how those products will function, so it is next to impossible to determine ahead of time what communication networks will be necessary.

Communications: Best-efforts versus managed

In a best-efforts communication network, the customer essentially gets what is available. There are no guarantees on data speed, responsiveness, availability, error rates, or other performance attributes. For some services, such as downloading or streaming content, this can prove bothersome: Almost everyone has experienced delays while the viewing software waits for the missing bitstream to arrive, or been forced to reboot when an Internet-based application freezes. To compensate, many customers end up buying more bandwidth—capacity and speed—than they actually need and hope that in most circumstances this will enable a reasonable service level.

Currently, almost all wireless connections provide a best-efforts approach to communications[3]—in other words, the availability, data transfer rate, packet loss rates, and latency are subject to the vagaries of contention for capacity between users, interference, and radio propagation.

In contrast, a managed-communications solution shifts to the CSP the burden of ensuring a reliable bitstream, opening the door to customer applications that demand reliable real-time or near-real-time connectivity over wide distances or other similarly demanding constraints. The International Telecommunications Union identifies three dimensions of managed services:[4]

- **Grade of Service (GoS)**: This defines the physical connection's availability and performance and measures attributes such as coverage, capacity, and the probability of a network outage.

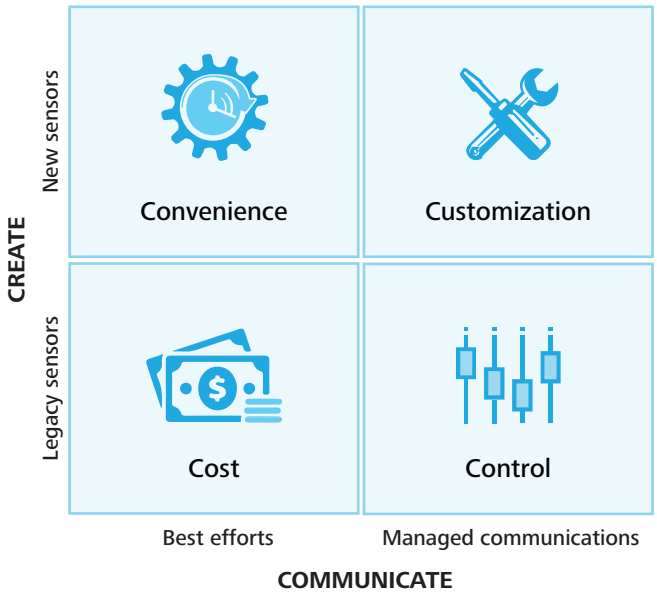
- **Quality of Service (QoS)**: This defines the traffic flow's performance and allows an application to specify its needs according to attributes such as latency, jitter, dropped packet performance, error rates, and guaranteed throughput (bit rate).

- **Quality of Experience (QoE)**: This relates to users' experience of using a service and is beyond the scope of this article. It is a subjective assessment of the end user's experience with the service and thus brings in the communications network, the terminals, ease of use, and so on.

When connecting sensors to networks—that is, when linking the *create* and *communicate* stages of the value loop—lost information and transmission delays can generate a variety of undesirable outcomes, especially when IoT-generated data are driving the operations of heavy equipment or public utilities. Closer collaboration between network users and network service providers can help avoid such difficulties because the technologies enabling each IoT deployment can be configured to address the specific GoS and QoS performance levels required. (QoE tends to take center stage when we get to *analyze* and *act*.)

On the downside, managed solutions can be comparatively expensive to construct and operate—certainly more so than ad-hoc best-efforts wireless systems—but they can solve legacy issues such as requesting sensor data, managing the relationship between multiple sensor data streams, and understanding whether a sensor has failed or is just unable to communicate.[5] The communications network can take responsibility for managing the

Figure 1. Categories of create/communication combinations and primary dimensions of value for each



Graphic: Deloitte University Press | DUPress.com

collection cycle (a pull approach), providing time and device stamping of sensor information, and ensuring device functionality and security.

Mapping the options for sensors (legacy versus new) and communications networks (best-efforts versus managed) reveals four categories of IoT deployments, each defined by the primary dimension of value most affected by the relationship between the company deploying an IoT solution and its CSP (see figure 1). Locating a given IoT deployment and its associated value loop provides a roadmap for assessing the viability and advisability of evolving current solutions to potentially more valuable—even if more demanding—configurations.

CSPs and the IoT: What's now and what's next

BY examining each quadrant through the lens of a specific use case, we can begin to understand the value that each combination can create, as well as the implications for collaboration between a company and its CSP.

Customization

The current IoT emphasis on cost savings and IP-based solutions, with a heavy reliance on wireless communications (typically a best-efforts network), has resulted in very few examples of customization, which relies on managed communications. Among those that have come closest so far are some industrial point solutions such as German automation manufacturer KUKA's connected robots, part of a 1,444-node network linking around 60,000 devices.[6] One such deployment is in the new Jeep Wrangler production facility in Toledo, OH, where 259 robots are connected through 33 control points and are able to produce 830 car bodies for eight different vehicles every day.[7] The connections between these industrial robots have traditionally been hardwired local area connections.[8] Since each of these solutions has been contained inside a single facility, requiring a full private network, the companies have not engaged CSPs. This self-contained approach is representative of highly customized solutions. IoT systems that require high security, uninterrupted connections, and the latest technology are typically deployed in circumscribed environments running proprietary protocols over a hardwired network.

Such a "closed shop" is unlikely to persist indefinitely, as two forces drive more companies to engage CSPs even when developing customized solutions. First, as firms implement IoT solutions in a wider variety of contexts, the performance benefits of customized sensor/network combinations will become clear, as will the flaws of many work-arounds based on existing best-efforts infrastructure. Early IoT solutions aimed to solve point problems, such as how to make a machine more productive or autonomous; the next step is using the IoT to make a system, with multiple machines, work in concert, and this requires managed communications. Second, the communications technologies required today for customized solutions are likely to follow in the footsteps of previous telecom technologies: falling costs and increasing modularization.[9]

As quality improves and prices fall, more companies will likely find customized solutions, implemented in collaboration with a CSP, increasingly attractive. Consequently it makes sense to explore the other three categories of IoT communication deployment not only in terms of how firms are currently using the technology but also in terms of how companies might migrate their current approaches to this more demanding, but more rewarding, configuration.

Furthermore, since few companies will have the luxury of starting over with their IoT strategies, unencumbered by legacy systems or budget constraints. So, in addition to describing how a company and CSP collaborate in the other three quadrants, we will explore how applications starting in each quadrant can make the migration to customized solutions, with an emphasis on how each application's starting point affects its path forward.

Cost

Unsurprisingly, cost reduction characterizes many companies' current priorities for IoT

deployments, which in many cases consist of comparatively rudimentary sensors linked by a basic Wi-Fi network.[10] Especially with large, established organizations—particularly those with huge investments in existing machinery—we see numerous situations in which equipment is already instrumented but executives have not yet moved to integrate the resulting data into an automated workflow: the value loop's communications, aggregation, analysis, and action stages.

Consider the mining industry, where most large mine vehicles have been fitted with sensors since before anyone spoke of an Internet of Things. Caterpillar's Vital Information Management System,[11] for instance, collects data on more than 250 attributes such as payload, engine RPM, brake condition and use, structural stress, and replaceable-part condition (for example, air filters) from the massive haul trucks. This information is used to assess the truck's health, increase vehicle uptime, maximize route and payload efficiency, and even provide data on the condition of the haulage road the mining truck is using. Initially, this system was designed to enable data download from the vehicle; now Caterpillar can link it to a system such as MineStar[12] that allows fleet management and vehicle health monitoring over a radio link—usually 802.11 b/g, a best-efforts Wi-Fi connection.[13]

The bottleneck in the *create* phase is the cost and complexity of measuring new vehicle attributes and fundamentally changing vehicle sensors. Since a large mine haulage truck typically costs between $500,000 and $5 million and lasts perhaps 20 years, operators will likely opt, for now, only to augment existing sensor capabilities. But this will necessarily limit the potential value from IoT solutions.

As companies look to exploit IoT capabilities more fully, one way forward is to migrate to more carefully managed networks: With long-lived assets—such as haul trucks, with sensors built into the engine—it is easier to upgrade the network than the sensors. For example, some mine haulage companies are beginning to deploy autonomous vehicles by retrofitting[14] additional sensor systems (collision-avoidance sensors and positioning systems) and networking them through a managed communications system. The companies' CSP partners add significant value and control two bottlenecks: the deployment of managed networks and the ability to manage legacy sensors more effectively to improve asset performance and lower operating costs.

There are already mining applications emerging for which companies are deploying localized managed communications. For example, in many underground situations, companies deploy a wired and wireless data network for telemetry, monitoring, and limited remote operations. But these private networks, while built to a high standard and with extensive redundancy built in, cannot truly offer fully managed communications. As mining moves to more automated solutions, with a shift from simply improving the performance and safety of manned machines (for example, having an operator manage a machine by remote control) to machines working in harmony to create an autonomous mining system, communications networks will require total control, to ensure the system's safety and efficiency. As with other firms and industries with IoT deployments in the *cost* quadrant, mine haulage companies moving toward customization demands both upgrading to new sensors and working with CSPs to implement a managed communications system.

Control

Some companies, working with last-generation sensors installed years ago, have moved to convert their existing connections into IoT functionality by dramatically upgrading the communication links between their sensors, working with CSPs to improve and control communications.

For example, in managing its wind turbines, GE tapped its existing range of sensors, including lasers that measure the wind heading for the turbine and sensors in the turbine linked to others at the wind-farm level, at the storage

system, and in the distribution grid.[15] Using its highly developed communication system to meet demand, the wind farm analyzes information to optimize power production, operations and maintenance costs, and flexibility. The system analyzes tens of thousands of data points every second to integrate hundreds of megawatts into the grid. The GE system has six interconnections that communicate with each other: turbine to turbine, farm to farm, farm to grid, turbine to remote operations center, turbine to battery, and turbine to tech.[16] Through these communications—achieved using reliable fiber and wireless IP communications—the system is able to optimize power output and management for grid operators. These solutions are largely focused on improving the generating capabilities of an individual wind farm.

The next step for GE, and for other companies with legacy sensors and managed communications, is moving to wide-area managed communications and broader sensor networks. Since wind power is less reliable and predictable than traditional fossil-fuel generation, power grids that aim to integrate it often struggle to match supply with demand. Grid operators' technical challenges can result in voltage and frequency management issues: In essence, a grid runs in a situation where demand and supply are exactly balanced; if demand begins to exceed supply, the frequency of the grid will fall, and power-plant operators have a series of approaches to resolve this situation.

Managed wide-area communications will clearly help deal with wind power's unpredictability, but very low latency can enable wind power to play a more significant role in frequency management. The bottom line: As wind power becomes a more significant component of power generation, wide-area managed-control networks will likely be necessary to effectively integrate this new power source.

So in the case of mining operations, the shift to managed communications offers significant benefits; the key tradeoff appears to be deploying a local private network or purchasing managed communications from a CSP. In

the wind-turbine situation, the choices are the same, but the wide-area nature of the communications means that a CSP solution likely makes more sense.

Convenience

Consumer-oriented IoT devices are a recent development, so naturally the sensors at the heart of their functions are more nearly up to date. But since at least some customers will use these appliances across networks managed by different CSPs, the devices' connections can't be as heavily managed as sensors that operate solely within the orbit of a single provider.

An example is the Fitbit fitness band, the latest iteration being the Surge,[17] which measures exercise activities, heart rate, steps, and route information (for example, distance, pace, gain). Usually, it connects via Bluetooth to the user's smartphone and thence to the Internet, updating the user's Fitbit account every 20 minutes or less. This limited communications

does not impede the device's functionality in its current role: primarily, recording exercise data.

However, those limitations may hamper efforts to integrate the device into a personal health-and-fitness ecosystem. Today Fitbit can be integrated with other analytics and sensors systems, but this relies on the user to create the integration and offers limited increased functionality. For example, a user can manually link her Fitbit to a Weight Watchers, MyFitnessPal, or Endomondo application,[18] or to other IoT devices such as a Withings body analyzer (measuring weight, BMI, fat mass, and air quality). While part of a sophisticated ecosystem of analysis, a Fitbit band is nevertheless hamstrung by best-efforts communication.

With more sophisticated communication links, a Fitbit would be able to interact with other sensors and actuators. In a gym workout situation, it could pass a user's heart rate, exercise levels, and body temperature to smart climate-control systems to modulate the air-conditioning system in real time. Similarly, if multiple gym users are wearing the same technology, their sensors could interact in real time to allow for direct competition or to create overlays of historical data with information from the sensor—for example, overlaying the user's current workout with a historical performance: *How does my time compare to Jesse Owens'*? Finally, the Fitbit could interact with the exercise machine for more sophisticated workouts. Thus it is likely that at least some companies will shift some consumer applications from best-efforts communications to managed situations, allowing for much more complex interactions between devices and for consumer devices to take on more critical functions.

Even so, making such a shift requires careful consideration: for many consumer applications, a shift from best-efforts to high-powered, top-security managed communications would be both impractical and overkill. The basic functionality envisioned for a smart refrigerator or thermostat is not materially compromised by the momentary hiccups and delays of a Bluetooth or Wi-Fi connection, and no hacker would bother attacking such a small target. Also key: Consumer-device manufacturers sell highly standardized products to a global market, with no control over which networks consumers may use for their new IoT devices, making managing those communications problematic at best. Some consumer-facing companies will be able to make the move to the *customization* quadrant; many will not.

The Telcos' role

OBVIOUSLY, companies constitute only half of the partnership that can get them to the *customization* stage, with managed communications to link and draw value from new IoT sensors. CSPs—soon to be tasked with connecting millions of new devices and users, carrying both sensor data and sensitive information[19]—will play an important role, one that both requires more from them than in the past and offers far greater opportunity to create value.

In the IoT world, CSPs' biggest challenge is to shift from an environment in which they charge based on volume of traffic and connections to one in which they charge based on level of performance. These firms, long relegated to a back-office function, will have to take unaccustomed risks to create networks in which they can guarantee that a particular data communication will take place—every time—with the latency, speed, and error rate that the customer has demanded. This represents a major shift, since today, even in managed networks, CSPs either set the bar low on performance guarantees or make only limited, aggregated performance promises.

CSPs also face a major technological challenge, the one that makes high-level IoT applications function: the actual work of collecting and processing information from multiple sensors and devices—and standardizing it, even as technologies continue to evolve. In order to do this, CSPs will need to implement their QoS capabilities in a standardized way that makes it easier for sensors and applications to take advantage of them. This means driving customer loyalty and differentiating their services based on performance, rather than aiming to lock customers into a proprietary interface.

In general, IoT devices generate limited volumes of data traffic, so the capacity of the pipeline is far less important than for, say, streaming video—in the IoT, the relationship *between* traffic flows is where the value lies. In a model where carriers charge for traffic, the revenue uplift from handling IoT-based data will be less than those carriers might hope, especially as data prices continue to fall. Thus, charging for QoS performance and delivering on performance guarantees creates a mechanism by which CSPs are able to grow revenues and sustain investment in their networks. Indeed, the importance of carriers correctly pricing managed services is key—too often, they charge too little to cover the enormous costs of serving clients and prioritize attracting new customers over asking premium prices for premium services.

In terms of the four quadrants:

- For *convenience* and *cost*, standards are key, so CSPs should implement QoS in a standardized form that smoothly links applications and services.

- For companies implementing a *control*-based solution, CSPs need to consider managed services and IoT applications as a way to link the communications network to end-user applications, not just a form of short-term differentiation.

- When defining a *customization*-based solution, CSPs need to understand the benefits of an industrial IoT solution moving to a managed wide-area communications system and, then work with IT services, device providers, and customers to deliver on the plan.

Toward a new partnership

WE have seen that close connections and structured, predictable relationships between an IoT system's sensors and actuators can allow companies to expand processes' efficiency and capabilities. Take, for example, security. In an IoT ecosystem, security is not a single problem or a single solution—rather, it must be included at each layer of the stack from physical to application layer. The strongest passwords and credentials for an application are useless if hackers can intercept the data as they travel across a network. Researchers have also recently succeeded in wirelessly stealing many decryption keys based only on the emissions from a computer's processor, meaning that devices now too must be designed to strict security standards.[20] To do so, CSPs and their partners at every level must collaborate closely to ensure proper functionality.

However, the challenges for users can be substantial—in particular, the cost and complexity of partnering with CSPs to engineer managed communications networks, especially on a wide-area basis. Without the capabilities of a managed network, companies will find their IoT applications' value generation limited to processes that are not dependent on instant communication and near-total accuracy.

For many IoT deployments, both the key driver of value creation and the main determinant of value capture lie at the intersection of *create* and *communicate*. These stages draw upon sensor technologies and communications networks, respectively. The degree of collaboration with its CSP that a company considers will be a function of the way in which it hopes to create value now and in the future.

When *cost* is paramount, a traditional working relationship can be entirely adequate. CSPs can focus on economies of scale; IoT deployments can exploit well-understood, standardized solutions. Convenience-driven solutions in the consumer sector are largely similar, with the possible exception of a greater willingness by companies to accept lower performance from their CSPs than in commercial applications, in the interest of greater innovation. Exploiting such opportunities requires not so much deep collaboration as sufficient insight into a CSP's technology roadmap so that new functionality can be exploited as quickly as possible.

When *control* is central, companies should at least be open to collaborating more closely, leaning on cutting-edge CSP solutions to compensate for legacy and retrofit sensor technology. Such solutions often create knock-on problems around, for example, security, and CSPs can be well positioned to address such issues.[21] In the early days of such deployments, the CSP may well be relieving the bottleneck to value creation, and so close collaboration might also be key to value capture. However, the CSP should not charge too much for its capabilities, since doing so could create financial incentives for companies to create private networks or stronger standalone capabilities.

Today we have examples in which closed private networks can deliver better results with a similar level of automation: For example, KUKA claims that its factory produces a Jeep Wrangler in 13.57 man-hours, 1.5 fewer than any other Jeep plant. But just imagine what efficiencies could be achieved with wider-area communications enabled by a CSP that link information from point of sale of the vehicle through the entire supply chain. In the case of GE wind turbines, we see how wider-area managed communications can simplify the task of frequency control; in the case of

mining, a wide-area (CSP-provided) solution would allow vehicles to easily move from mine to mine and potentially lower the overall communications costs for many mines. And more examples, both successes and failures, will come forward as more companies expand their IoT deployments.

Whatever the challenges, the opportunities are there for CSPs and companies seeking to capture the full potential of the IoT to become closely aligned partners. It is by deploying managed communications at reasonable price premiums in ways that work today while opening a path to tomorrow that CSPs and companies relying upon them to deploy IoT solutions can move beyond the dumb pipe, creating an IoT that is smart at every level.

Endnotes

1. David Rose, *Enchanted Objects: Design, Human Desire and the Internet of Things* (New York: Simon & Schuster), 2014.
2. Michael Raynor and Mark Cotteleer, *The more things change: Value creation, value caption, and the Internet of Things*, Deloitte University Press, May 30, 2015, http://dupress.com/articles/value-creation-value-capture-internet-of-things/, accessed June 24, 2015.
3. Wireless communications have focused on maximizing throughput and have historically set up protocols to give users guaranteed performance in terms of throughput, latency, priority, bandwidth reservation, etc. There have been some niche applications and initiatives here, such as 911 priority for GSM services, but in general the system gives a user the access and bandwidth it is able to, based on the user's request, and does not reserve or manage capacity; Sensors being connected to an aggregation point via a multitude of low-power, short-range wireless systems (such as Wi-Fi, Bluetooth, ZigBee, NFC, HART, UWB, and RFID) will result in best-efforts communications.
4. Brendan Reid, "The networking community's hierarchy of QOS," Exinda blog, Nov. 12, 2012, http://www.exinda.com/wan-orchestration/the-networking-communitys-hierarchy-of-qos/, accessed June 24, 2015.
5. Modern wireless systems such as LTE allow networks to offer managed services less subject to competition, interference, and security issues. While deployment of these capabilities is still at an early stage, many major operators are making investments to allow for managed wireless connections. The initial driver for many of these investments was to enable Voice over LTE, but they are being expanded to create a suite of Quality of Service capabilities. Wired solutions generally offer a managed-communications path, but linking devices using short-range wireless (such as Wi-Fi or RFID) to the wired connection reduces the communications to a best-efforts level. As managed wireless networks evolve and their protocols are used on a short-range basis (e.g., LTE direct), even these aggregation architectures will offer managed communications.
6. Microsoft Customer Stories: "KUKA Systems Group: The Internet of Things transforms a Jeep factory," January 29, 2015, https://customers.microsoft.com/Pages/CustomerStory.aspx?recid=17254, accessed June 24, 2015; "KUKA creates a connected factory," Microsoft, http://www.microsoft.com/en-us/server-cloud/customer-stories/kuka-robotics.aspx, accessed June 24, 2015.
7. "KUKA-Toledo production operations resumes production of Jeep Wrangler bodies," press release, July 6, 2009, http://www.kuka-systems.com/usa_nao/en/pressevents/news/PM_20090702_Jeep_Wrangler.htm, accessed June 24, 2015.
8. The connections include such interfaces as RS-232 and RS-485. For more information, see Lou Frenzel, "What's the difference between the RS-232 and RS-485 serial interfaces?", *Electronic Design*, April 16, 2013, http://electronicdesign.com/what-s-difference-between/what-s-difference-between-rs-232-and-rs-485-serial-interfaces, accessed June 24, 2015; Fiber-based Gigabit Ethernet connections are increasingly being used, running a custom protocol such as Profibus—which can manage industrial operations with cycle times of less than 1ms—to provide the management features necessary for efficient operation. For more information, see Profibus & Profinet International, http://www.profibus.com.
9. Carliss Y. Baldwin and Kim B. Clark, *Design Rules, Vol. 1: The Power of Modularity* (Cambridge, MA: MIT Press), 2000.
10. Sanjeev and Sandeep Sardana, "Is there an app for that? How the 'Internet of Things' is changing the consumer device landscape," *Forbes*, May 29, 2014, http://www.forbes.com/sites/sanjeevsardana/2014/05/29/is-there-an-app-for-that-how-the-internet-of-things-is-changing-the-consumer-device-landscape/, accessed June 24, 2015.

11. "Technology products," section 26 of *Caterpillar Performance Handbook* 41, 2012, http://www.holtcat.com/Documents/PDFs/2012PerformanceHandbook/Technology%20Products%20-%20Sec%2026.pdf, accessed June 24, 2015.
12. "Productivity systems," Caterpillar, https://mining.cat.com/technology/solutions/productivity-solutions.
13. "Infrastructure systems," Caterpillar, https://mining.cat.com/technology/solutions/infrastructure-solutions.
14. Chris Brown, "Autonomous vehicle technology in mining," *Engineering and Mining Journal*, January 20, 2012, http://www.e-mj.com/features/1609-autonomous-vehicle-technology-in-mining.html, accessed June 25, 2015.
15. GE, "The Next evolution of wind is here," https://renewables.gepower.com/wind-energy/overview/digital-wind-farm.html, accessed June 25, 2015.
16. GE Power & Water Renewable Energy, "Digital wind farm: The next evolution of wind energy," 2015, https://renewables.gepower.com/content/dam/gepower-renewables/global/en_US/documents/Digital%20Wind%20Farm.pdf, accessed June 25, 2015.
17. Fitbit Surge, http://www.fitbit.com/ca/surge.
18. Fitbit compatible applications, http://www.fitbit.com/compatibleapps.
19. CSPs are bringing management capabilities to their LTE wireless solutions as they move them from best-efforts to a true managed service; they are also shifting their networks so that over the next five to seven years we will see carriers with as much as 100MHz of spectrum used for 4G and delivering usable speeds perhaps as high as 200Mbps. With industrial customers looking to generate greater benefits from their IoT investments and carriers looking to differentiate and monetize their QoS investments, there is a natural link between the two. See http://www.wirelessdesignmag.com/articles/2013/09/quality-service-over-lte-networks-part-2-3 and http://www.4gamericas.org/en/resources/technology-education/lte-advanced/.
20. Genkin, Pachmanov, and Pipman, *Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation*, Tel Aviv University, March 2, 2015.
21. Irfan Saif, Sean Peasley, and Arun Pernkulam, "Safeguarding the Internet of Things: Security, vigilance, and resilience for a connected age."

Contact

Philip M. Wilson
Director
Deloitte Consulting LLP
+1 415 609 0561
phwilson@deloitte.com

 Follow @DU_Press

Sign up for Deloitte University Press updates at DUPress.com.

About Deloitte University Press

Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.