Cutter
IT Journal

The Journal of
Information Technology Management

Vol. 27, No. 11
November 2014

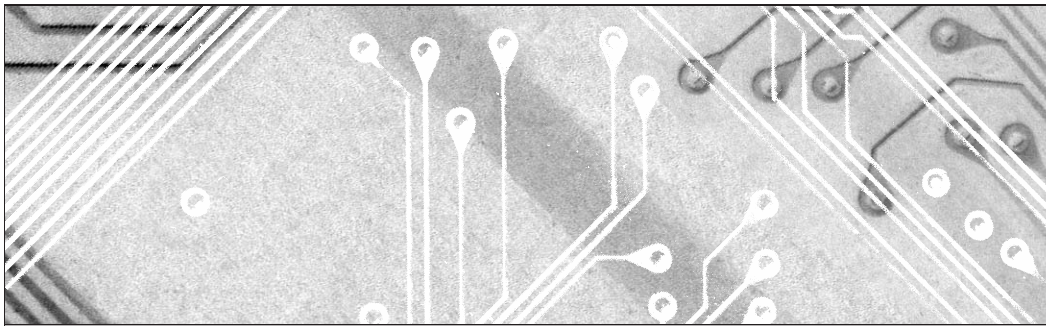
"The IoT should not be viewed as only a technological opportunity. It has the potential to transform how people and business interact in significant ways. Therefore, people must be placed at the center of the IoT conversation."

— Ron Zahavi and Alan Hakimi, Guest Editors

The IoT:

Technologies, Opportunities, and Solutions

CUTTER CONSORTIUM



Cutter IT Journal

About Cutter IT Journal

Part of Cutter Consortium's mission is to foster debate and dialogue on the business technology issues challenging enterprises today, helping organizations leverage IT for competitive advantage and business success. Cutter's philosophy is that most of the issues that managers face are complex enough to merit examination that goes beyond simple pronouncements. Founded in 1987 as *American Programmer* by Ed Yourdon, *Cutter IT Journal* is one of Cutter's key venues for debate.

The monthly *Cutter IT Journal* and its companion *Cutter IT Advisor* offer a variety of perspectives on the issues you're dealing with today. Armed with opinion, data, and advice, you'll be able to make the best decisions, employ the best practices, and choose the right strategies for your organization.

Unlike academic journals, *Cutter IT Journal* doesn't water down or delay its coverage of timely issues with lengthy peer reviews. Each month, our expert Guest Editor delivers articles by internationally known IT practitioners that include case studies, research findings, and experience-based opinion on the IT topics enterprises face today — not issues you were dealing with six months ago, or those that are so esoteric you might not ever need to learn from others' experiences. No other journal brings together so many cutting-edge thinkers or lets them speak so bluntly.

Cutter IT Journal subscribers consider the *Journal* a "consultancy in print" and liken each month's issue to the impassioned debates they participate in at the end of a day at a conference.

Every facet of IT — application integration, security, portfolio management, and testing, to name a few — plays a role in the success or failure of your organization's IT efforts. Only *Cutter IT Journal* and *Cutter IT Advisor* deliver a comprehensive treatment of these critical issues and help you make informed decisions about the strategies that can improve IT's performance.

Cutter IT Journal is unique in that it is written by IT professionals — people like you who face the same challenges and are under the same pressures to get the job done. *Cutter IT Journal* brings you frank, honest accounts of what works, what doesn't, and why.

Put your IT concerns in a business context. Discover the best ways to pitch new ideas to executive management. Ensure the success of your IT organization in an economy that encourages outsourcing and intense international competition. Avoid the common pitfalls and work smarter while under tighter constraints. You'll learn how to do all this and more when you subscribe to *Cutter IT Journal*.

Cutter IT Journal®

Cutter Business Technology Council: Rob Austin, Ron Blitstein, Tom DeMarco, Lynne Ellyn, Israel Gat, Vince Kellen, Tim Lister, Lou Mazzucchelli, Ken Orr, and Robert D. Scott

Editor Emeritus: Ed Yourdon
Publisher: Karen Fine Coburn
Group Publisher: Chris Generali
Managing Editor: Karen Pasley
Production Editor: Linda M. Dias
Client Services: service@cutter.com

Cutter IT Journal® is published 12 times a year by Cutter Information LLC, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA (Tel: +1 781 648 8700; Fax: +1 781 648 8707; Email: citjeditorial@cutter.com; Website: www.cutter.com; Twitter: @cuttertweets; Facebook: Cutter Consortium). Print ISSN: 1522-7383; online/electronic ISSN: 1554-5946.


Opening Statement

by Ron Zahavi and Alan Hakimi, Guest Editors

Both of us work at Microsoft, in particular within its Enterprise Strategy Group in Microsoft Services, where we are involved with strategic Internet of Things (IoT) initiatives internally and with clients. Ron has been involved with the IoT since 2001 at a private equity company and has worked on several IoT solutions and architectures for border protection, bio surveillance, and cities. Alan has worked on systems thinking and complexity theory, focusing on their relationship with the architecture of IoT systems in the petroleum, high-tech manufacturing, and financial industries.

The IoT is difficult to define precisely. The current lack of a standard definition means that each technology vendor or analyst group offers a slightly different interpretation, but conceptually the IoT shares these common elements:

- Physical "things" (active or passive devices with sensors and actuators) that have the ability to be connected to each other, and to the Internet
- Things that have the ability to gather and communicate data collected from both the environment and human input
- Things that may also do some level of "processing" using embedded logic by taking instructions from external sources (human or machine) and storing algorithms, information, software, and configurations

The IoT enables us to develop smarter products and service offerings, as well as to facilitate the creation of cognitive enterprises by harnessing the power of communities of people, digitizing work and life processes, breaking down the silos of information, and building a highly interconnected ecosystem of very diverse things. The notion of "smarter things" encompasses both the public and private sectors with smart government, smart cities, smart public transportation, smart retailing, smart oilfields, smart homes, smart appliances, smart pets, smart logistics, smart hospitality, smart manufacturing, smart vehicles, ad infinitum. This ambient intelligence comes from the convergence of operational and information systems in which the "system" makes recommendations based on context, personal experience, and anticipated actions. The digitization of process will change how organizations interact within themselves and with their customers and suppliers. It will drive efficiency through the elimination of waste and automation of processes, enhance decision-making processes though improved heuristics and insights, and ultimately create a more satisfying experience for all potential IoT stakeholders. All of this is made possible by the technology platforms that offer us ubiquitous computing. The foundation of IoT systems is provided by the highly interconnected global community with its diversity of devices, its highly resilient and flexible information processing data centers that provide fully finished IT services, its application platforms, its infrastructure, and its virtualized computing systems.

The IoT enables us to develop smarter products and service offerings, as well as to facilitate the creation of cognitive enterprises.

While the IoT may seem new due to the current hype, it is not a futuristic technology trend. IoT-like systems have been around for many years in various shapes and forms. What is evolving is that these systems are now taking advantage of ever-present connectivity, new nanotechnology with embedded logic, sensor actuators, and cloud platforms to store and analyze large amount of data. Many transitional SCADA-oriented systems that traditionally utilized proprietary programming interfaces and communication protocols are now moving toward standards based on the new capabilities that the IoT has to offer.

Yet many IoT challenges have not changed. These include security, privacy, and finding the right business model to monetize the opportunity. Many IoT implementers are not the ones to benefit directly, so adoption slows. Another challenge is that the IoT can be very different given different scenarios. It can be consumer-oriented or focused on the factory floor; it can involve a large number of transactions and smart devices or infrequent messages and simple devices. Is the architecture for such differing solutions the same or different, and do standards exist for integrating between different IoT systems from different vendors?

It is important to note that the IoT should not be viewed as only a technological opportunity. It has the potential to transform how people and businesses interact in significant ways. Therefore, people must be placed at the center of the IoT conversation. We need to consider how people accomplish "doing things" whether it is within their work, play, or day-to-day lives.

Although the complexity of the landscape can be overwhelming, there are several things you can do to get started:

- Become educated about the IoT landscape and focus on the conversation you are having. Is it about your customers? Your business? Building technology environments? Your product and service offerings?
- Understand the IoT's potential impacts on people and how this will change your business. Is this an incremental change or potentially transformational in nature?
- Build awareness and develop scenarios that are meaningful to the business and technological leadership within your organization.
- Use a multidisciplinary team to help facilitate innovation brainstorming sessions to elicit and capture viewpoints from a variety of people.
- Experiment through iterative solution development techniques to better understand potential IoT roadblocks and risks, and demonstrate value early and often.

We expect that these highly evolvable IoT systems will create new ecosystems that have the potential to:

- Provide improved offerings through the capture of product and services data
- Provide better customer services and help drive better product and services performance
- Help organizations better understand target markets and improve customer loyalty
- Enable new business models and opportunities for customers, partners, employees, and suppliers
- Monetize organizationally developed heuristics, including information and algorithms developed based on industry expertise

For this issue, we searched for articles that would cover these topics and provide insight into the current state of the IoT and and what is on the horizon.

IN THIS ISSUE

In our first article, Richard Soley, executive director of the Industrial Internet Consortium, discusses the evolution of the Internet from connecting people and systems to connecting things that exchange vast amounts of data. He defines the Industrial Internet as the intersection of the Industrial Revolution and the Internet Revolution and provides several examples of the opportunities it presents. Soley cautions that the transformation will not be without challenges and outlines the business model changes and security, privacy, and interoperability issues that will need to be addressed. Drawing on his many years of experience with interoperability standards at the Object Management Group (OMG), Soley ends with a discussion of the need for a collaborative ecosystem and standardization in order to realize the promised benefits of the IoT.

Next up, Fujitsu's Ian Thomas and Kazunori Iwasa explore the architecture needed for the IoT. They focus on how connectivity and digitization are impacting the way we live at an extremely rapid pace. To figure out how to address the future, they look at three historic perspectives: the Internet as platform; the way that smaller, bottom-up changes form the basis for success and innovation; and (from recent history) how the cloud supports end-to-end solutions. The authors believe that a small-scale approach is a better recipe for IoT success than large, complex monolithic environments. Their article further explores connectivity requirements, protocols, and services, and provides a digital flow example that ties it all together.

Taking a deeper dive into IoT architectures is the author of our third article, Munish Kumar Gupta, a lead architect at Wipro Technologies. Gupta uses a retail example to weave through the customer experience, highlighting how technology needs to come together to produce a reference solution architecture. He explores the in-store components, the gateway that collects the data, the internal enterprise components, and the external enterprise components, which together enable the creation of a rich set of applications and services. Just as critical as the architecture is the point that use cases and real-world scenarios are key to identifying the appropriate IoT business model for an enterprise.

In our next article, Angelo Corsaro, CTO of PrismTech (one of the implementers of the OMG's Data Distribution Service [DDS]), delves into the most common IoT data-sharing and messaging protocols. The article provides qualitative and/or quantitative analyses of four such protocols and lays out Corsaro's view as to why DDS is the best protocol for the industrial and consumer IoT. Of course, IoT users and implementers can deploy IoT solutions on top of many different protocols, and readers should consider which protocol will be most appropriate for their particular application and need.

We close this issue with an article by Adam Justice of Grid Connect, who introduces 10 things to keep in mind when applying the IoT to make products smart. Taking a device manufacturer's perspective, Justice covers various factors that should be considered, such as the device's overall cost, size, and power needs, as well as platform issues such as security, interoperability, and the cloud. He also believes, as most of us do, that the IoT presents many opportunities for innovation. While we may wish to be limited only by our imaginations, we also need to pay careful attention to the design constraints to ensure products are well designed.

IoT OPPORTUNITIES AND CHALLENGES

The articles in this issue highlight the technology enablement of a rich set of new and innovative opportunities. Ubiquitous connectivity, nanotechnology, machine learning, and the cloud, in conjunction with trends like mobility and social networks, provide the underpinnings for solutions that will affect our lives in unimaginable ways. Yet with every new wave of technology come basic challenges that need to be addressed. These include security and privacy, the need to create new business models that generate value, interoperability between differing vendor solutions, and some level of standardization. We hope this issue of *Cutter IT Journal* will better acquaint you with the new IoT opportunities while showing you the steps you need to take to succeed in this new and wonderful world of connected devices.

Ron Zahavi is a Senior Enterprise Strategist with Microsoft and leads Microsoft's Worldwide IoT Architecture Community. Mr. Zahavi has over 30 years of experience in all aspects of technology management and solution delivery, 15 of those related to IoT solutions. Prior to joining Microsoft, he ran his own consulting company and held positions as Chief Business Architect at Unisys Corp. and CTO/CIO, managing technology across several companies and performing due diligence of potential acquisitions. His breadth of experience includes work with startups, large companies, government, and private equity firms. Mr. Zahavi has also worked in several business domains, including healthcare, pharmaceuticals, energy, intelligence, and defense. He is a member of the OMG Board of Directors, has served on the OMG Architecture Board, and is certified as an OMG Expert in BPM. He is the author or coauthor of several books, including Business Modeling: A Practical Guide to Realizing Business Value. *Mr. Zahavi holds a BSEE from the University of Maryland and an MS in computer science from Johns Hopkins University. He can be reached at ron.zahavi@microsoft.com.*

Alan Hakimi has over 25 years of experience in the IT industry. He joined Microsoft in 1996 as a consultant within Microsoft Consulting Services (MCS), where he has advised industry executives from several Fortune *50 companies, delivering innovative business solutions using enterprise architecture. In his current role in Microsoft's Enterprise Strategy Practice, Mr. Hakimi consults with large oil and gas, retail, and high-tech manufacturing companies to improve their business efficiency and effectiveness through the application of technology. He also leads Microsoft's Worldwide Enterprise Architecture Community, helping advance the discipline internally. Mr. Hakimi has architect certifications from Microsoft (MCA-Infrastructure), the International Association of Software Architects (CITA-P), and Open Group as a Distinguished Enterprise Architect; is a member of the Association of Enterprise Architects (AEA) and the IEEE; and sits on certification boards for the Open Group and the International Association of Software Architects (IASA). He has a BS from the University of California at Davis in computer engineering. He and his wife and two children currently reside in the San Francisco Bay Area. In his spare time, Mr. Hakimi enjoys cycling, hiking, making music, cooking, and studying philosophy. He can be reached at alan.hakimi@microsoft.com.*

The Industrial Internet: The Opportunities ... and the Roadblocks

by Richard Mark Soley

In 1999 Bill Gates famously wrote, "A fundamental new rule for business is that the Internet changes everything." Unquestionably, the Internet has revolutionized the way people listen to and record music, the way they communicate, the way they consume news and entertainment, and even the way business collects, processes, and shares data. Yet while it has systemized business automation, there are countless other systems that remain disconnected or even manually driven. Take, for example, discrete programmable manufacturing systems, which have been programmed in the same way since I worked on manufacturing systems in the 1970s, and which continue to resist integration into Internet-based enterprise solutions.

Why? While the Internet connects people and systems, it doesn't (yet) connect *things*. And those things have vast amounts of data to share.

We're now on the cusp of the Industrial Internet, a revolution of truly transformational business changes in which machines, devices, and common objects become identifiable, readable, analytical, actionable, and connected. The Industrial Internet is where the Industrial Revolution meets the Internet Revolution, the revolution in connected devices finally impacting the revolution in manufacturing that began long ago. Integrated computing devices — from the minuscule to the gigantic — interact with machines, devices, and people and feed a continual data stream to which those machines and people can react, thus preempting problems and creating new efficiencies.

What the Internet Revolution hasn't changed, the Industrial Internet will — automatically and rapidly. The Industrial Internet gives us a low-cost, high-value way to integrate information based on widely distributed sensors, smart machines, big data, and real-time analytics.

The Industrial Internet takes us beyond the Internet of Things (IoT). The IoT concept conveys the idea of your refrigerator letting the grocery store know you need more milk, or of self-driving cars. Until recently, applications to industrial systems have been slow to emerge. Now, however, this train is leaving the station, and those on board are poised to gain significant advantage.

Let's take a real-world example. Prorail is the organization responsible for operating and maintaining the Dutch railway network, handling more than 6,000 trains and 1.2 million passengers daily. It uses IoT technology provided by PrismTech to seamlessly and securely share data across sensors, components, and systems managed by the supervisory system that provides overall control and monitoring for the rail infrastructure, thereby ensuring normal operation and monitoring issues that could halt or slow traffic.

The broad economic opportunities of the Industrial Internet are vast, with some estimates putting the value as high as US $32.2 trillion of economic activity, leading to a $10-$15 trillion increase in global GDP over the next 20 years.[1] The Industrial Internet provides enormous opportunities for growth and development, and those who don't use that big data in the next year are in danger of losing market share and momentum. New products and services will create and retain jobs and achieve vast new efficiencies for end users; businesses will increase their market share, profits, and ability to compete; there will be reduced waste in energy, water, and other natural resources; and improvements to healthcare, infrastructure, public safety, and more will improve quality of life for citizens across the world.

THE INDUSTRIAL INTERNET WILL CHANGE YOUR BUSINESS MODEL

> If you went to bed last night as an industrial company, you're going to wake up this morning as a software and analytics company.
>
> — Jeff Immelt, chairman of General Electric, October 2014

For manufacturers, the value of embracing the Industrial Internet lies not only in new products and services, but in avoiding loss of market share.

According to Cisco, roughly 50 billion devices will be connected to the Internet by 2020,[2] and this estimate is on the low side compared to some others. Sensors embedded in machines will skyrocket the value of these machines and industrial products through the advantages provided by extracting the data and using it to increase efficiency, decrease downtime, and integrate with other factory-floor and enterprise data. In healthcare, medical devices (both implanted and external) will be connected to each other and to analytical systems, saving lives and decreasing medical errors and overall costs. Smart cities will oversee and optimize all aspects of city management, including parking and traffic, street lighting, waste disposal, and environmental quality to create greener, more efficient, and more cost-effective cities worldwide.

Manufacturers need to adapt to a new way of thinking: to understand that the value of their products comes not just from their physical attributes, but from their capacity to be networked. The convergence of physical devices and real-time analysis of connected systems and their interactions is what customers want. The data from these connected devices is what creates value in this new world. Companies who can't offer this will be left behind.

If this evolution seems familiar, it's because you've seen it already in something you use every day: your phone. The transition from a basic mobile phone to a smartphone has dramatically increased the value of this device for its user. Now, more than a device for making simple calls, your phone is a connected network of interactive data services that gives you information to act upon: weather, directions, alternative traffic routes around the accident ahead, the location of restaurants and friends in the vicinity, and enterprise information from your company. A continuous stream of updated data, taken in context, has transformed your phone from a device used occasionally to make point-to-point phone calls to a critical personal productivity tool. In the industrial setting, neither machine nor device will stand alone; the way it is choreographed to function in context will increase its value dramatically.

Advances in material science, sensor technology, predictive analytics, and other developments will effectively produce products that, with preventative maintenance and predictive failure replacement, could last forever. Let's take a look at jet engines. The stage is set for even traditional manufacturers to move to being service providers by providing the service of data analytics delivery. Jet engine manufacturers will reduce downtime to zero as real-time engine performance metrics are delivered instantly and compared with benchmarks compiled from hundreds of thousands of statistics to make maintenance decisions before staff members are even aware of potential problems.

For end users, real-time analytics becomes the basis for information-based decision making. Connected global devices continuously send data that is analyzed instantly, replacing the seat-of-the-pants decision making of yesterday. Gone are the USB keys used to extract data from one machine and plug it into a spreadsheet where it can be analyzed further. On factory floors that are already operating at peak efficiencies, preventative maintenance will cause less unplanned downtime, as machines send alerts when key parts are about to fail. Applying connected data to a larger ecosystem — a city, for example — enables the operation of a cleaner, safer, and more efficient environment for its citizens.

Manufacturers need to understand that the value of their products comes not just from their physical attributes, but from their capacity to be networked.

ROADBLOCKS TO THE INDUSTRIAL INTERNET

As with any new disruptive technology, there are roadblocks that will slow down adoption. Security, data privacy, technology, interoperability, and industry fragmentation are all areas to be addressed before the Industrial Internet can reach its full potential. As systems evolve, they will rely less on human decision making and more on computational intelligence based on continuous streams of data. The challenge is to design systems that are dependable, reliable, safe, and secure.

Some security requirements for the Industrial Internet include the systematic application of security measures to existing and future technologies of the Industrial Internet, the identification of existing gaps, and finding a way for systems to automatically identify possible threats as they occur in real time. In order to fulfill these requirements successfully, the industry as a whole needs to come together to construct security requirements to build into architectural frameworks and standards from the beginning, not as an afterthought. Identified best practices will include mitigating controls, countermeasures, and remediation.

Security recommendations should specifically address:

- The steps providers of solutions and their users can take to increase the level of security and privacy to a specified minimum level of compliance
- How solution providers and their users can objectively measure and document the level of security and privacy implemented

The Industrial Internet must have an autonomous end-to-end security capability spanning hardening of endpoints, securing device-to-device communications, and enabling remote management and monitoring. The solution should address both existing technologies and new technologies in order to provide security in all environments.

The vast opportunity presented by the Industrial Internet is, ironically, one of the key inhibitors to its growth.

Security issues always show up at the weakest link. Today, it is fairly easy to find a weak link in the disconnected security components that exist in the many separate efforts across heterogeneous technology environments created by individual vendors. A coordinated approach to these technologies that includes a managed and monitored platform will allow the various components to be secured (on endpoint and via the communications) consistently across the entire environment regardless of make, model, and manufacturer, including both current and future technologies, without altering the actual business process already in place.

Machines and devices need to be able to resist an attack from threats with a configurable array of mitigating controls. The devices themselves would have the ability to deploy countermeasures for security breaches. Ideally, an attack would be communicated to back-end security monitors capable of measuring the risk and notifying the management systems to update policy on the endpoint to mitigate attacks in near real time. Standards to prevent these attacks are now being discussed and hotly debated within broad ecosystems of organizations.

Besides the technologies, there are human and business aspects to systematic security in Industrial Internet applications as well. More than just security controls are necessary to enforce privacy. One option is for businesses to define data privacy policies and establish appropriate ways to handle confidential data.

These systems have to be reliable in all the ways the Web isn't today. Results must be optimized for each individual situation, elements of which may include: a particular machine, a particular "thing" being made or processed, a particular legal environment, a particular owner, and particular goals and desires. This must be done while protecting the network, the machines, the privacy, and the interests of the machine's owners and the data owners from internal misuse or external attack.

The technology itself must evolve. Many companies are investing in Industrial Internet solutions, but the applications created by one vendor do not yet integrate with applications from another vendor. This makes the total adoption of Industrial Internet solutions complicated and less cost-effective, especially if users aren't able to shop around for the best-value application.

Innovative architectures and platforms are needed to support highly complex and interconnected Industrial Internet systems. The development and application of comprehensive architectural frameworks must include both the physical and digital connected elements of the Industrial Internet. New platforms will effectively extract actionable information from vast amounts of raw data. The framework will support the real-time control and synchronization requirements of complex, networked, engineered physical systems. Advances in sensing, control, and wireless communications will enable optimized performance, diagnostics, and prognostics. Systems will "plug and play," self-heal, and be interoperable, and the architecture will adapt in response to constantly changing situations.

AN ECOSYSTEM FOR ALL INDUSTRIAL INTERNET STAKEHOLDERS TO COLLABORATE

The vast opportunity presented by the Industrial Internet is, ironically, one of the key inhibitors to its growth. The business case for change has caused companies of all sizes and in all industries to initiate new IoT projects and departments. They are choosing to work with a few key partners on the development of their Industrial Internet devices, applications, and implementations. This vast number of one-off initiatives is causing fragmentation and confusion on what the standards are, or should be. With fragmented groups working on similar projects, the potential advancements in Industrial Internet technologies are hindered as the knowledge of individuals in the industry is not used collectively.

Work must be done to define and develop common architectures. There are many standards out there, but which ones are best? Prototypes, demonstrations, and testbeds are needed in order to try out ideas; discover disruptive new products and services; select from freely available standards set by open, neutral, international, consensus organizations; and review relevant technologies that compose the ecosystems that will make the Industrial Internet work.

This process can start with groups of Industrial Internet stakeholders identifying industry requirements, technology gaps, and architectural requirements, which can then be tested, proven, and retested against a multitude of use cases to ensure they meet the rigorous requirements across a wide spectrum. Through coordinated efforts and by putting the best minds in the industry to work, these security and technological hurdles will be solved.

One such effort already underway is the Industrial Internet Consortium (IIC), the global not-for-profit organization founded by AT&T, Cisco, GE, IBM, and Intel. The members of the IIC (which number 95 as of this writing) are driving a concerted, systematic, and collaborative approach to the adoption and growth of the Industrial Internet. With the collective knowledge of representatives from large corporations, small industry, academia, and government, large problems will be solved while minimizing duplication of effort. This coming together by technology, communications, and industry leaders brings a wisdom that increases the ability to achieve the true value of the Industrial Internet: transformational business value.

Well before they reach market, new Industrial Internet-enabled products and services need to be conceived, tested for viability through usage scenarios, and then physically brought together in simulated environments. Proofs of concept — or testbeds, as we at the IIC call them — are where new products, processes, and services come together through Industrial Internet ecosystems in unprecedented ways. These testbeds provide the platform for "trying out" large development projects. Testbeds allow for rigorous, transparent, and replicable testing of scientific theories, computational tools, and new technologies. In this development environment, concepts can be freely tested away from the potential pitfalls of a live production environment. Testbed development is a main goal of the IIC, and from these testbeds will come new applications, products, and services.

THE FUTURE IS HERE

While the era of the Industrial Internet is just beginning, there are real-world successes underway today. A quick look at the work being done by IIC member companies provides a glimpse of the huge wave of innovation to come across all industries:

- In energy, Austin, Texas-based National Instruments is helping to prevent oil and gas pipeline failure through remote monitoring of defects and damages. Its stand-alone system collects data from over 250 sensors that report on the health of a pipeline. By collecting, monitoring, and logging this data, oil and gas companies are able to optimize production and minimize pipeline downtimes without stopping the flow and production of oil.[3]
- In healthcare, Sunnyvale, California-based Real-Time Innovations (RTI) is working on connected medical devices that prevent hospital errors that could result in injury or death. By connecting various medical monitoring devices, an alarm will sound only when multiple devices in the system indicate that something is wrong with the patient — thus reducing the number of incidents of false alarms. This technology can connect and integrate the data from all hospital rooms, helping busy hospital staff monitor and keep abreast of all patient conditions.[4]
- In manufacturing, General Electric's factory in Schenectady, New York, is using thousands of sensors to monitor everything from the humidity on the factory floor to the pressure applied by machines. When these data points are compiled together, not only do they form a comprehensive picture of the quality of the products that are being manufactured, but they also allow GE to improve upon efficiency, quality, and cost-effectiveness going forward.[5]
- Another global manufacturer, ThyssenKrupp Elevator, is using the IoT to improve the reliability of its elevators, a top priority for the company's customers. To do this, ThyssenKrupp teamed up with Microsoft and CGI to create a connected, intelligent line-of-business asset monitoring system. By connecting its elevators to the cloud, and gathering data from their sensors and systems, ThyssenKrupp can identify needed repairs *before* an elevator breaks down.[6]

These are just the tip of the proverbial iceberg of innovation that is happening to transform industry today — with much more to come in the months and years ahead.

What is at stake, however, is much greater than corporate opportunity and market disruption. There's no better example of this than what is *not* happening today in healthcare. In hospital intensive care units, patients are tracked by oxygen sensors that run side by side — and separately — from respiration sensors. Nurses who already have a full patient load are manually monitoring this amidst all the beeps of disconnected equipment. Bringing down the cost of *connected systems* will mean we can expect real-time analytics to keep track of all those sensors on those patients' bodies, warn of impending disaster, and automatically trigger a response — ordering the crash cart, alerting the medical team — well before the medical team could even sense Code Blue.

That's why the Industrial Internet matters. It changes software, it changes systems, it changes the way the world is wired, it changes business models, and it changes the workforce. And one day soon, it will save lives.

ENDNOTES

[1]Evans, Peter C., and Marco Annuziata. "Industrial Internet: Pushing the Boundaries of Minds and Machines." General Electric, 26 November 2012.

[2]"Seize New Product and Revenue Opportunities with the Internet of Things." Cisco (www.cisco.com/web/solutions/trends/iot/indepth.html).

[3]Hambardzumyan, Arev, and Rafayel Ghasabyan. "Oil Pipeline Monitoring System Based on CompactRIO." National Instruments (http://sine.ni.com/cs/app/doc/p/id/cs-16372).

[4]"Healthcare Systems Applications." RTI (www.rti.com/industries/healthcare.html).

[5]Ravindranath, Mohana. "GE Brings the 'Internet of Things' to the Factory Floor." *The Washington Post*, 1 August 2014 (www.washingtonpost.com/business/on-it/ge-brings-the-internet-of-things-to-the-factory-floor/2014/08/01/8b78cd74-176c-11e4-85b6-c1451e622637_story.html).

[6]"The Internet of Things Gives the World's Cities a Major Lift." *The Fire Hose* (Microsoft blog), 16 July 2014 (http://blogs.microsoft.com/firehose/2014/07/16/the-internet-of-things-gives-the-worlds-cities-a-major-lift).

Richard Mark Soley is the Executive Director of the Industrial Internet Consortium and is responsible for the vision and direction of the organization. In addition to this role, Dr. Soley is Chairman and CEO of the Object Management Group (OMG), an international, not-for-profit technology standards consortium. A native of Baltimore, Maryland, Dr. Soley holds bachelor's, master's, and doctoral degrees in computer science and engineering from the Massachusetts Institute of Technology. He can be reached at soley@iiconsortium.org.

Leveraging the Internet of Things:
Emerging Architectures for Digital Business

by Ian Thomas and Kazunori Iwasa

Connectivity is the great disruptor. Whether it is the connectivity that containerization brought to physical supply chains or the connectivity that the Internet has brought to digital ones, the ability to reliably and scalably connect things literally transforms the way we think about the world. Connectivity allows us to build on what has been done before, to leverage shared expertise and resources, and to integrate value in new ways to create hitherto unimaginable products and services precisely focused on the needs of our customers.

The Internet itself has been a profound vehicle for increasing connectivity. It has been constantly growing outward from its relatively simple beginnings as a platform for information sharing and linking. Over the last 20 years, we have seen successive innovations — websites, e-commerce, cloud computing, social networks, mobility — drive the influence of the Internet into new areas, connecting new resources, digitizing new interactions, and challenging the underlying beliefs on which a range of industrial and social activities are based. Every additional expansion has brought new industry leaders (e.g., Amazon, Google, Facebook, Uber) that have used greater connectivity to look at the world with fresh eyes, unencumbered by outdated beliefs and practices.

A recent study suggested that the average tenure of companies in the S&P 500 index has dropped from 61 years in 1958 to just 18 years in 2011,[1] something that appears to be moving in parallel with greater connectivity. For CIOs, each successive expansion of connectivity brings new opportunities and challenges. The current disruptive convergence of cloud, mobile, and social technologies is creating so great a demand for digital-fueled change that many CIOs appear to be struggling to adapt.

A RADICAL NEW ERA OF CONNECTIVITY

While today's challenges are already acute, we are on the cusp of an almost unimaginable acceleration of connectivity and digitization. The Internet of Things (IoT) promises to drive the boundaries of the Internet further out than ever before, providing network connectivity to potentially billions of everyday objects.[2] The sensors and actuators these objects embed will enable us to transform our understanding of real-world events and to enact changes simultaneously across digital and physical environments in real time. As IT increasingly merges with life itself, the distinctions between the physical and digital worlds will fade away, leaving technology as an embedded facilitator of everyday life.

The potential for reinvention that this merging creates is literally incredible. As connectivity transforms the potential of even the smallest and most mundane of everyday objects, huge new opportunities to orchestrate value flows across the digital and physical worlds will emerge. The importance of this cannot be overstated. Despite today's huge wave of digital disruption, we are still effectively speaking about resources and activities whose fundamental nature can be converted from analog to digital form — music, books, films, family pictures, status updates, insurance claims, shopping lists, airline bookings, and so on. The opportunity to transform and connect all of these newly digitized assets has indeed been — and continues to be — hugely disruptive, but such assets still only represent a tiny minority of the resources that exist in the real world.

The new wave of connectivity and digitization brought by the IoT will be different. In this case, we are not talking about a conversion of information-based resources from analog to digital form, but rather an ability to extend our digital awareness and control deeply into the realm of the analog world. Such a shift brings disruptive change to the far greater number of activities that are yet to be touched by digitization, offering opportunities to overturn a much wider range of assumptions about the nature of people, places, and things. Once again, as established assumptions break down in the face of increased connectivity, smart start-ups and wily challengers will have an open field to reimagine entire industries.

But how do we become winners in this new environment? We believe that there are a number of historical perspectives that can help to guide us.

LESSONS FROM HISTORY

The Internet Is the Platform

The first perspective suggests that we can only achieve the full potential of the IoT by stressing the "Internet" over the "Things." Despite many waves of technology hype over the years, straightforward connectivity has been the most fundamental driver of transformational change; connectivity allows activities to be broken down, shared, and reconnected in new and often unforeseen ways. Technology optimization can happen later, once we are armed with evidence and an understanding of the necessary performance parameters. In this sense, the most important consideration in creating a viable IoT strategy is not the optimization of wireless networks, the quality of sensors, the extensibility of boards, or the choice of operating systems. Instead, the first and foremost consideration has to be maximizing the ease with which smart objects can be connected to the wider environment.

Consequently, we believe that it is critical to base IoT initiatives on existing standards — or reasonable optimizations thereof — at different layers, leveraging the ubiquitous protocols and patterns of the Internet to maximize connectivity potential.

Think Small to Go Large

The second perspective suggests that innovation on the Internet has rarely been achieved in a top-down, centrally planned fashion. Rather, it has been an emergent property based on the connection of individual ideas, resources, and value into larger solutions. It is the open, chaotic, and Darwinian nature of the Internet that has enabled such a high tempo of innovation, requiring people to conform to some simple standards but otherwise leaving them free to invent and connect anything they want. Many discussions of the IoT, however, start with predictions of huge, complex, and monolithic systems/environments such as smart energy, smart agriculture, smart manufacturing, and so forth, which are on a scale that has little relevance to most people and cannot be grasped in terms of the small, actionable changes that will bring large-scale innovation. Such initiatives are likely to be the preserve of governments and regulated industries that move slowly and have cash to burn.

In our view, the more compelling scenarios are those that find specific, small-scale, and sustainable uses for sensors in improving or transforming a specific product, activity, or process and then connect them together over time. We already see huge bottom-up innovation happening as individuals and companies use sensors embedded within phones, fitness items, or smart watches to connect unrelated devices and services to create higher levels of unforeseen value. As with the Internet, we believe that we will see a gradual layering of value as connectivity builds upward from specific smart objects into smarter processes and ultimately into large-scale connected systems. In this sense, we believe that successful approaches to IoT will need to leverage simple technologies and small-scale approaches that lower the barrier to entry for each individual case.

Connect in the Cloud

Finally, the third perspective suggests that creating systems to orchestrate the end-to-end business flows that connect smart objects with other resources will be best achieved in the cloud. Connectivity of smart objects — while a great enabler of innovation — is only a partial answer. To create end-to-end solutions, we must also connect these resources at scale — both with each other and with information systems and people. We believe that the highly distributed nature of the Internet makes the use of cloud development and integration platforms a highly desirable option for digital process creation. The independent status of cloud platforms — as shared utilities not bound to any particular geography, usage domain, or environment — makes them an ideal candidate for the orchestration and mediation of services and data from many distributed sources. Furthermore, by acting as application-level intermediaries, they can offer a host of useful operational, management, and reporting capabilities that lower the burdens placed on low-power systems at the edge of the network and increase the scale and responsiveness of the overall architecture.

Most importantly, by leveraging the opportunity to consolidate all of the necessary infrastructure, middleware, and operational management within a cloud platform, we can create a high-productivity environment for the rapid creation and scaling of digital processes. The huge explosion in application innovation facilitated by cloud platforms over the last few years has amply demonstrated the power of reducing friction in the development process. We therefore believe that providing higher-leverage tools for the rapid and reliable composition of smart objects at scale within the cloud can likewise accelerate experimentation, testing, and adoption of IoT.

BUILDING THE INTERNET OF THINGS

While there are already highly vertical sensor applications within specific domains (e.g., building automation, industrial machine-to-machine, logistics), they are implemented with a wide range of proprietary and incompatible technologies that are difficult to integrate with each other and with Internet-based services. This tightly constrains them to the use cases for which they were created, limiting their impact and blocking opportunities to reuse them within potentially valuable alternative scenarios. Extending these systems to the Internet requires us to address three highly interrelated issues of scale:

1. Scaling down the cost of connecting individual objects to the Internet
2. Using this reduced complexity to massively scale up the number of connected nodes
3. Connecting information and services from this new ecosystem at scale

Achieving these aims will require us to consider two essential aspects — first, the way in which we connect smart objects to the Internet, and second, the way in which these smart objects communicate.[3]

Connecting Smart Objects

To reduce the costs of smart object connectivity, the IoT aims to use the Internet Protocol (IP) to displace proprietary approaches. Doing so promises to remove translation gateways, increase scalability, reuse network management approaches, and accelerate innovation. But first we need to overcome two major challenges: providing sufficient IP addresses and recognizing the limited capabilities of many smart objects.

Scaling Up IP for the IoT

Achieving the full potential of the IoT requires a unique public IP address for each individual smart object — something that will lead to an explosion in the number of IP addresses required globally. Fortunately, Internet Protocol version 6 (IPv6) enables an almost unlimited number of addresses,[4] putting in place the address space necessary to enable the use of IP as a low-cost and scalable source of connectivity for smart objects. While uptake of IPv6 was initially slow, the demands of the IoT are starting to accelerate its deployment.

Scaling Down IP for Small Devices

Today a range of IP-enabled devices are already being successfully used as nodes within the IoT (e.g., Raspberry Pi), but these devices are the most powerful that fall within the IoT spectrum. To enable us to massively scale the number of connected objects, we need to shrink them and minimize their cost. The majority of devices will likely use cheap 8- or 16-bit microcontrollers and short-range, low-power wireless technology with limited data rates. Such constrained devices lack the powerful processors, operating systems, and TCP/IP stacks required to use traditional IP.

In order to deal with these issues, the IETF created 6LoWPAN,[5] a wireless standard that enables IPv6 to be used within networks of constrained devices. 6LoWPAN deals with compression, data loss, power drain, and device unreliability to enable the efficient extension of IPv6 into the domain of constrained objects. In doing so, 6LoWPAN facilitates the end-to-end IP networking required to bring even the smallest and least powerful objects into the scope of the IoT.

Communicating with Smart Objects

While IPv6 and 6LoWPAN bring connectivity at the network level, they do not deal with the need to create an open architecture at the application layer — a prerequisite to achieving new digital ecosystems. One natural way to unify application-level communication is to reuse existing architectures and protocols such as REST/HTTP. Although this approach simplifies the integration of smart objects with other Internet-based resources, it again only works well for high-capability objects. The performance, memory, and reliability profiles of many constrained devices mean that REST/HTTP is unlikely to be suitable for the whole range of devices that need to be connected.

The IETF has thus been focused on introducing the REST architectural style in a form suitable for constrained devices and networks. The resulting Constrained Application Protocol (CoAP)[6] achieves this by implementing a subset of REST that is common with HTTP but optimized for constrained devices and networks — introducing UDP transport, reduced message overheads, reliable message delivery, and an asynchronous interaction model. At the same time, this approach drastically reduces the complexity of developing Web-based systems that consume smart object resources by establishing a consistent interaction model that is easily mapped to HTTP. Individual resources continue to be identified and addressed via URIs, are able to be represented using arbitrary formats (such as JSON or XML), and can be manipulated using the same methods as HTTP. Finally, security and privacy concerns can be addressed using the familiar DTLS protocol using a range of authentication mechanisms. In this way, the proposals deliver a potentially sustainable basis for communicating with the IoT while simultaneously paving the way for easy integration with broader Internet services.

An Internet of Everything

Together IPv6 and CoAP extend the Internet into the realm of constrained devices and create a broader "Internet of Everything" (see Figure 1). To fully leverage the full breadth of this new environment, however, we still need a way of connecting these services at scale.

CONNECTING DIGITAL FLOWS IN THE CLOUD

We believe that cloud platforms will ultimately consolidate all of the technical and business capabilities required for the rapid implementation of digital solutions spanning the whole spectrum of Internet-connected services, especially given the dependency of such solutions on high levels of adaptability, multitenancy, scalability, and connectedness (see Figure 2).

To facilitate the consistent integration and orchestration of different resource types within our platform (Fujitsu RunMyProcess), we introduced a number of important concepts:

- **Connectors** provide a uniform way to access distributed resources (whether using standard Internet protocols or not).
- **Composite APIs** offer aggregated REST interfaces that compose the outputs of one or more connectors.
- **Business processes** enable the creation of long-running activities spanning any combination of human and system resources.

Given the rapid convergence toward Internet-like protocols, IPv6 and CoAP provided the ideal basis on which to extend our reach into the IoT while preserving the ability to deliver end-to-end service composition.

Extending to the IoT

In order to integrate smart objects alongside other Internet-based services, we extended our range of connectors to include native outbound and inbound CoAP support. These connectors are based on the open source Californium (Cf) framework.

For outbound support, our CoAP connector manages the process of initiating and making calls to CoAP-based resources and of receiving and dispatching the asynchronous response to the invoking client. As with our other connectors, the CoAP connector is configured by specifying, for example, the URL, options, content, and result format within a cloud-based connection wizard.

For inbound support, we created a new gateway that can receive CoAP calls, confirm receipt, and then route them to the appropriate composite API service for processing.

Together, this combination of outbound and inbound integration enables a wide range of digital composition, intermediation, and enhancement use cases within the model already established for other Internet-based services (see Figure 3).

Benefits of Connecting Services in the Cloud

Our experiences suggest that there are a number of additional potential advantages to integrating and orchestrating IoT resources from the cloud.

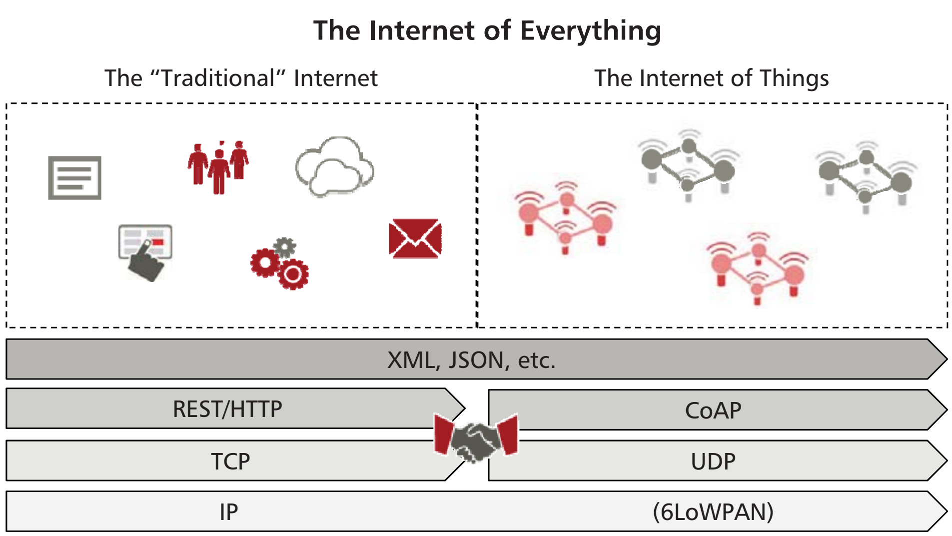


Figure 1 — The Internet of Everything.

Simplification and Externalization of Function

Using the cloud to externalize application logic from individual smart objects where possible ensures they remain simple and focused on their main purpose. This increases the ease of maintenance and adaptability of IoT-based applications by avoiding unnecessarily tight coupling between devices. The removal of overly constraining domain models also encourages new and unforeseen uses.

Composition and Abstraction

Simple resource composition can enable the creation of "virtual sensors," a collection of resources addressed as if they were a single entity (e.g., services that address all lights in a building or gauge mood from sensor data combined with Facebook updates). Such virtual sensors can abstract complexity without removing the flexibility to address individual objects when necessary.

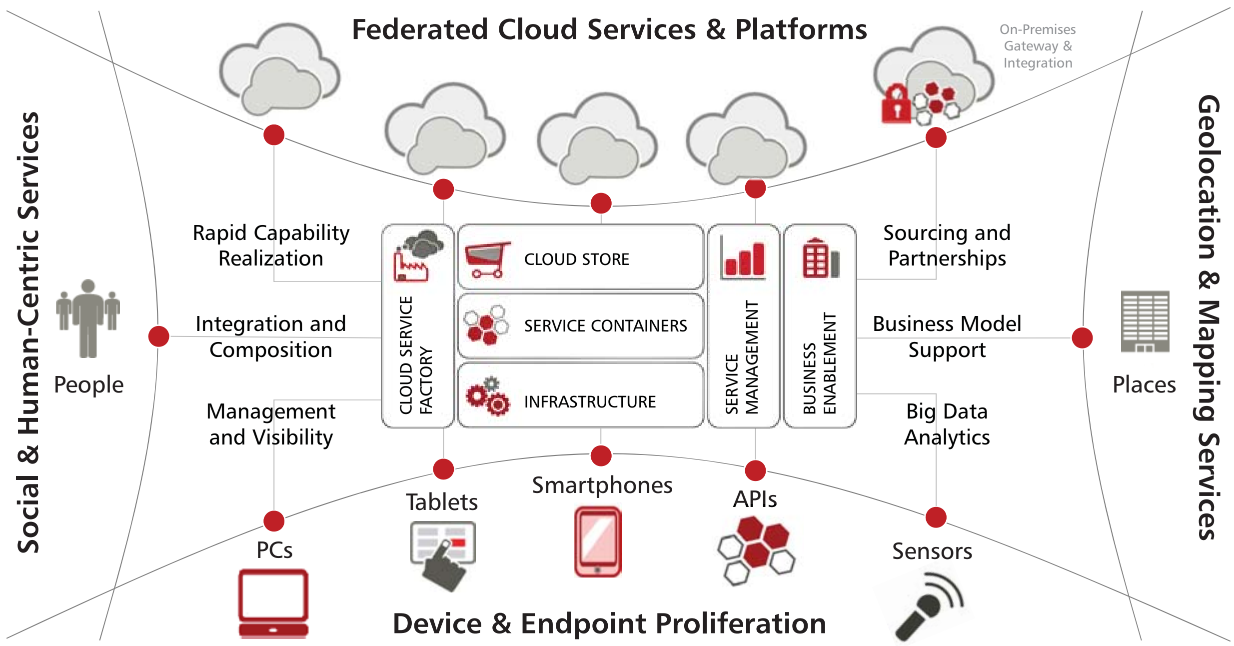


Figure 2 — Connecting Internet services with the cloud.

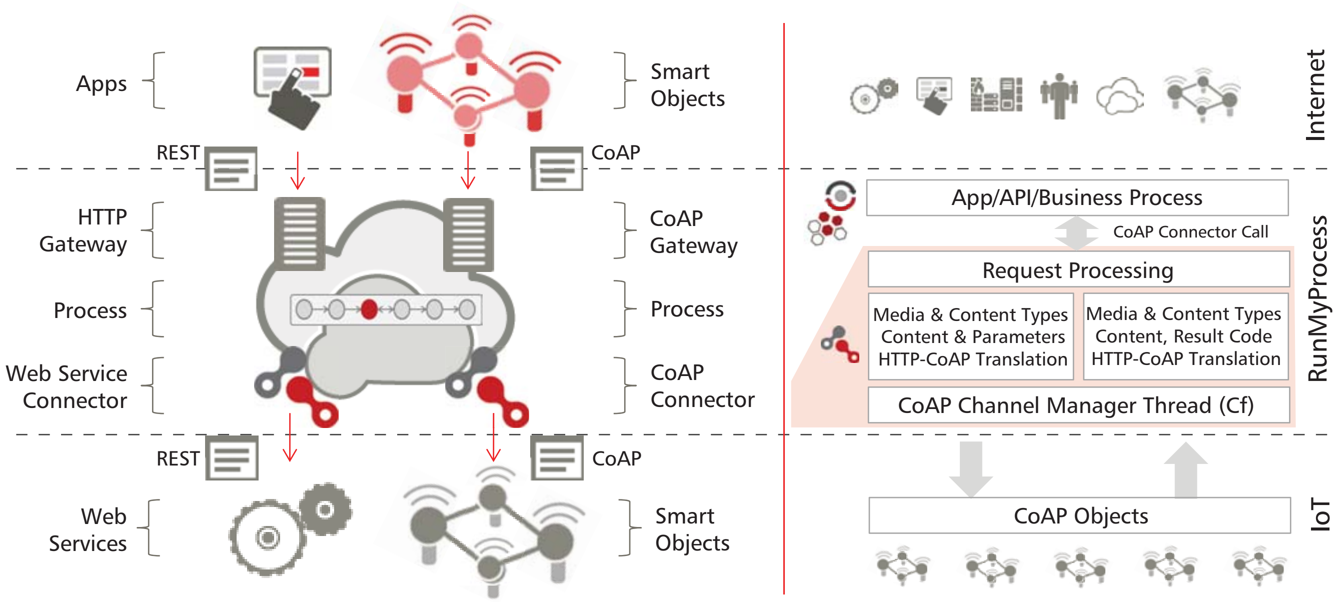


Figure 3 — Extending to the IoT with CoAP.

Resource Management

Uncontrolled usage of constrained devices could quickly lead to performance degradation and/or power issues. Cloud platforms can protect resources from failure by adding throttling, caching, or billing capabilities to shape usage behavior. Without such mediation, resource owners and consumers need to individually manage interactions — a daunting and potentially impractical task.

Service Convergence

Enabling intermediation between smart objects and other Internet-based resources helps to reduce integration barriers between the virtual and physical worlds and encourage the emergence of converged solutions. In this model, digital applications and processes can be created in the cloud that seamlessly span the full range of Internet-connected resources.

Security Adaptation

From a security perspective, an intermediate platform can be used to add security proxies to resources that are insufficiently powerful to process the additional overheads of DTLS communication.

Unified Discovery, Subscription, and Monetization

As the IoT expands, it will become more difficult to find and use appropriate devices. Cloud-based application and API marketplaces that simplify the discovery and consumption of Web-based services could make IoT resources easier to find, subscribe to, and monetize.

Insight and Analytics

Monitoring and managing large networks of devices is likely to be a daunting task, but the use of cloud platforms to intermediate and orchestrate devices could provide valuable insight into their performance and help identify issues. Over time, the analysis of aggregated data could be used to make suggestions on service optimization or to predict failures.

BRINGING IT ALL TOGETHER: A SIMPLE EXAMPLE OF A DIGITAL FLOW

One very simple but illustrative example of end-to-end connectivity has been implemented as part of the IoT6 European project[7] (see Figure 4). In this solution, a presence sensor in an office detects unauthorized persons out of hours. If triggered, an alert is sent to a local control and monitoring system to sound an alarm, and a CoAP message containing a phone number is sent to the RunMyProcess cloud platform. On receiving the alert, RunMyProcess sends an SMS to the transmitted phone number and creates a new incident within an incident management system. The notified user views the incident within a mobile app and can choose to investigate or deactivate the alert. When deactivation is chosen, a CoAP message is sent back to cancel the alarm, and the incident is closed.

While simple in concept, this application demonstrates a number of important aspects of the emerging IoT. First, it shows the viability of rapidly creating low-cost and small-scale systems that address a specific issue in

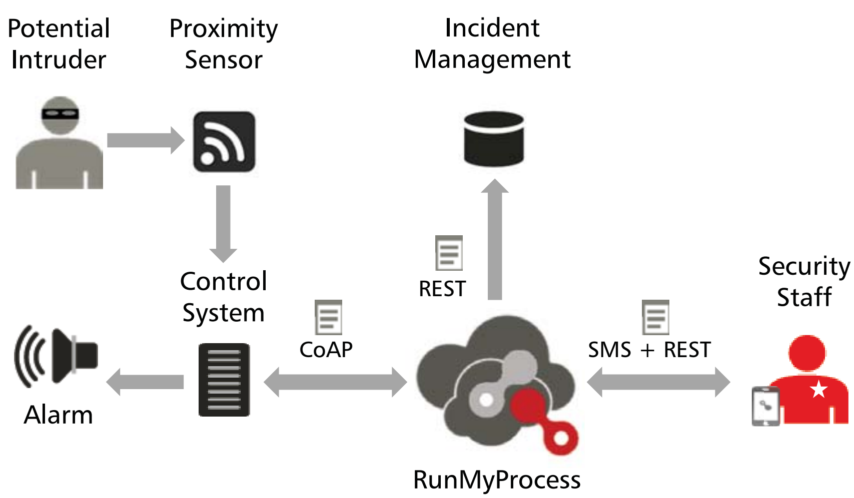


Figure 4 — An end-to-end digital flow.

isolation. In this case, a sensor, an alarm system, and a cloud application are used to protect a single office. Second, it demonstrates the use of IPv6 and CoAP to facilitate connectivity between smart objects and other Internet services, resulting in the straightforward creation of a business process spanning the IoT, the cloud, and a human actor. Third, the speed and low cost with which such a process can be delivered makes a compelling argument for the use of cloud platforms for coordination. Finally, the aggregation of information in the cloud provides a repository of data about patterns of intrusion.

CONCLUSION

In this article, we have described the potential of the IoT as an enabler for new digital business models. We have also outlined the key technologies that are making it real and discussed the use of cloud platforms to simplify the creation of end-to-end solutions. We believe that leveraging these elements together will enable rapid business model experimentation and innovation. We hope that such convergence will accelerate the spread of sensor usage by making it simple to flexibly connect IoT information streams both to each other and to other Internet-connected systems.

The IoT is opening up huge new opportunities to integrate information spanning the physical and digital worlds. While grandiose concepts and highly technical language can make the subject seem overwhelming, simple examples like our office security system demonstrate the viability of starting quickly at a small scale. In fact, many hobbyists and hackers are already using open source software and hardware — such as Arduino — to connect and automate a huge range of activities at extremely low cost.

In our view, the first key step is therefore to actually *take* a first step. The low cost of starting, the immense potential for experimentation, and the importance of gaining insight into this disruptive new area all make it critical to start shaping your future now.

ENDNOTES

[1]"Creative Destruction Whips Through Corporate America." Innosight Executive Briefing, Vol. 10, No. 1, February 2012 (www.innosight.com/innovation-resources/strategy-innovation/creative-destruction-whips-through-corporate-america.cfm).

[2]Evans, Dave. "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything." Cisco Internet Business Solutions Group, April 2011 (www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf).

[3]If we were talking about more passive objects (e.g., tags, near-field communication), then we would need another device such as a mobile phone to act as a gateway. In this article, we are mostly focused on objects that can be both programmed and Internet-connected. In our view, IoT is primarily about smart objects since their connectivity to the Internet is the key dimension — hence they have to be in some sense "smart."

[4]Deering, S., and R. Hinden. "Internet Protocol, Version 6 (IPv6) Specification." IETF RFC 2460, December 1998 (www.ietf.org/rfc/rfc2460.txt).

[5]Kushalnagar, N., G. Montenegro, and C. Schumacher. "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals." IETF RFC 4919, August 2007 (https://tools.ietf.org/html/rfc4919).

[6]Shelby, Z., K. Hartke, and C. Bormann. "The Constrained Application Protocol (CoAP)." IETF RFC 7252, June 2014 (https://datatracker.ietf.org/doc/rfc7252).

[7]IoT6, FP7 European Research Project (www.iot6.eu).

Ian Thomas is a long-time Fujitsu strategist currently working as Chief Marketing Officer of Fujitsu RunMyProcess. Over the last few years, Dr. Thomas has been working on strategy and architecture topics that span the diverse business portfolio of the Fujitsu group, primarily focused on the ways in which technology disruptions are transforming the shape and purpose of enterprises and the societies they serve. He has worked across a broad range of topics, including mobility, cloud, social business, and the Internet of Things and has published a range of papers examining their joint potential in creating radical new business ecosystems. He can be reached at ian@runmyprocess.com; Twitter: @iansthomas.

Kazunori Iwasa is a Principal Engineer in the Software Integration Planning Department, Development Planning Division, Platform Planning and Strategies Unit at Fujitsu Limited. Mr. Iwasa has contributed to various standardization activities within the areas of cloud computing, XML, Web services, and B2B. He is the leading editor of the OASIS WS-Reliability1.1 specification and has contributed to a range of DMTF, W3C, and OASIS standards, including DMTF Cloud Infrastructure Management Interface (CIMI), W3C SOAP1.2, OASIS ebXML Messaging Services 2.0/3.0, and WS-ReliableMessaging 1.1. Through his role as a cochair of the Asia Committee of the Interoperability Task Group in eBusiness, Mr. Iwasa actively promotes interoperability testing for standards. In the wider Japanese economy, he uses his expertise to promote standards within various industry organizations, including JAMA (automotive), JEITA (electronics), and IT (ECOM). He can be reached at kiwasa@jp.fujitsu.com.

Architecting for New Business Opportunities in the Internet of Things

by Munish Kumar Gupta

The Internet of Things (IoT) is creating high expectations from businesses and consumers about the possible ways it can help create new revenue models, increase efficiencies, and enhance customer experience. Businesses are looking to tap into the new business opportunities generated by the IoT, while consumers are seeking intelligent products and services that provide all kinds of insights to help them use those products and services optimally.

Enterprises deal with multiple systems — point-of-sale systems, billing systems, manufacturing shop-floor systems, logistics systems, supply chain systems, financial systems, and so on. If these systems can be connected to the Internet and data can be shared across them, then it leads to new opportunities and new revenue streams, cost optimization, enhanced safety and security on the shop floor, and predictable maintenance. Enterprises want to create a connected, secured ecosystem of intelligent devices/systems that are generating large volumes of real-time streaming data for analysis and actuation.

When enterprises start analyzing the IoT ecosystem, they face a plethora of choices on how to make sense of all the vendors and technologies in the market. Enterprises that want to create opportunities in the IoT ecosystem need to deal or contend with the following:

- **Module manufacturers** make the modules that contain the various sensors (processor chips) for specific applications and connectivity requirements. These modules will typically:
  - Be white-labeled and can be adapted to particular use
  - Support standard data communication protocols
  - Support over-the-air updates
  - Have built-in security modules
  - Include custom module devices based on the underlying systems
- **Software vendors** that develop embedded software, typically focusing on Web services with each new module design, using the SDK provided by the module manufacturers
- **Internet service providers** that will help transmit the data between the IoT devices/sensors and the data consumers
- **Enterprises** that host platforms to offer services to the end user and connected devices

Some of the new opportunity areas that open up because of the IoT are:

- **Operational efficiency.** Connected devices mean that machines, devices, and systems can emit real-time data, which can be used in areas like preventive maintenance, energy use optimization, intelligent operations, and increased asset utilization.
- **Data monetization.** Connected devices generate a lot of data, which can be mined and used for predictive and prescriptive analysis. Generated data can be combined with enterprise data or third-party data for enhanced value for customers.
- **New revenue models.** Designing new business models around connected devices opens up another opportunity for businesses to create value for customers.

Based on the business use cases and new opportunities enterprises identify, they can make the appropriate investments and technology decisions. For present purposes, I will focus on enterprises that want to host and build platforms to make sense of the incoming data and provide actuation services to the devices and consumers.

IMPROVING THE CUSTOMER EXPERIENCE WITH THE IoT

Let's take a sample retail scenario and see how enterprises can provide services in this model:

1. A customer walks into a retail store and gets a shopping cart with a built-in tablet.

2. The customer taps his mobile device, which pairs the device with the tablet. *(Devices pair using near-field communication [NFC].)*

3. The tablet recognizes the customer and automatically accesses the customer information and current shopping list. *(The tablet uses in-store Wi-Fi to connect to the customer data store and get the customer information.)*

4. The tablet automatically shows the path within the store for picking up all the items. *(The tablet uses inhouse store maps, geolocation and beacons, and path optimization algorithms to distribute traffic among crowded aisles, redrawing the path if the customer takes a deviation.)*

5. As the customer starts pushing the shopping cart based on the assigned path, the tablet recognizes his current location and, based on that location and the customer's past purchase history, can show relevant offers/products. *(The tablet uses inhouse store maps, geolocation and beacons, and past purchase data to make cross-sell/up-sell offers and recommendations to the customer.)*

6. When the customer draws near the relevant aisle or product, the tablet alerts him to the availability of the item. The customer can compare the prices across similar items and different packaging sizes for maximum value. *(The tablet uses inhouse store maps, geolocation and beacons, aisle cameras, and face/eye-level detection to determine the heat map of customer preferences. It can also offer value-added services such as providing information on product contents [e.g., calories, ingredients] and enabling social context [e.g., who among your friends is buying which brands]).*

7. The customer picks the item, scans the bar code with the tablet, and puts the item into the cart. *(The tablet, working in conjunction with the smart shopping cart, enables automated product checkout using QR codes, bar codes, RFID, etc., and simultaneously updates customer preferences.)*

8. The aisle automatically knows an item has been picked and sends a message to update the store inventory. *(Automated inventory information along with the customer profile helps in one-to-one personalization.)*

9. The customer walks through the store, picks up all the desired items, and proceeds to the checkout counter.

10. At the checkout counter, the customer taps on the tablet, which generates the final invoice. He taps his mobile phone for payment, the devices sync together, the customer authenticates the transaction, and the payment is made. *(The tablet enables a self-service model, using a secured payment mode [NFC].)*

11. The customer walks out of the retail store.

In the scenario above, there are number of things that need to work together to provide a seamless customer experience (see Figure 1). As the figure shows, the customer is the center of all attention. Data is collected from multiple sources — social platforms, devices, location, and sensors — and is combined with the transactional customer data available within the enterprise to build a user experience that is omnichannel, contextual, real-time, and scalable.

Enabling such a model opens up multiple avenues for the enterprise to monetize. It is able to understand what products its customers are seeing, what products they are picking, what products they are picking but discarding, and what product sizes they prefer, all of which enables the enterprise to generate a heat map of various customer activities.

This data helps produce operational efficiencies by placing products at the right heights in the aisle, restocking them on a real-time basis, and so on. Restocking of items can even be done using drones that get activated once the stock on aisle goes down below a particular threshold. When a customer wants an item that is not available in the store, the retailer can enable her to place an online order that can be shipped directly to her home later on. All this in-aisle customer data, combined with the customer's purchase history, can provide insights into her choices and preferences, which can be aggregated and sold for use by other product vendors, online channels, and advertisers.

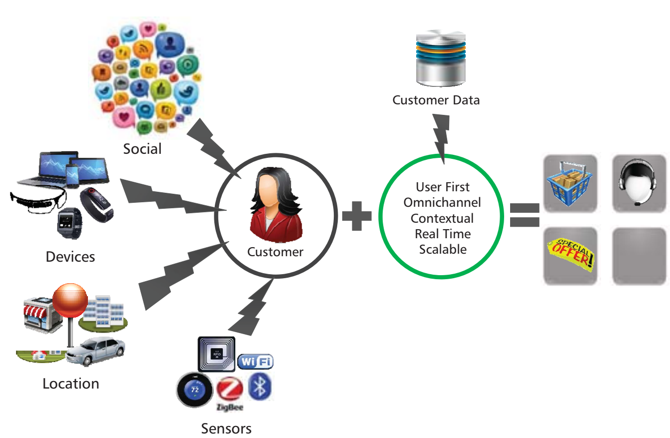


Figure 1 — Connected customer experience.

As we can see, there are numerous ways an enterprise can use connected systems to provide a personalized experience to its customers and at the same time create new opportunities for realizing cost efficiencies and data monetization.

THE TECHNOLOGY BEHIND THE EXPERIENCE

A retailer may have multiple stores, each having its own set of the connected devices that need to process and personalize the experience of customers in real time. From a technology point of view, the enablement of such an ecosystem requires platform thinking. In the above scenario:

- There are large numbers of devices, sensors, and other "things" emitting data on a continuous basis.
- All this data needs to be gathered and stored somewhere.
- Next, all the data needs to be put into a context where it can be integrated, combined, analyzed, actuated, and reported.
- All the collected data needs to be processed, organized, and aggregated for decision making.
- This huge amount of data needs to be processed in real time, providing immediate feedback to users or devices.

Figure 2 touches upon some of the key building blocks that go into the making of the platform.

Some of the key architecture considerations and technology components for enabling the business scenario are discussed below.

In-Store Customer Experience (Things)

This is the most critical part, where the data is collected based on various customer actions and movements and gets transmitted back for analysis and actuation. Data can be collected using:

- **Passive scanner-based devices** that use techniques such NFC, RFID, QR codes, bar codes, or the like to hold the information. When a connected device comes within proximity of these passive scanner devices, they can connect and transmit their data.
- **Active/connected devices** that use protocols like ZigBee, Bluetooth, and Wi-Fi to transmit the data in real time.

For all data, there will localized data collection and storage in every stage of the use case. This is to make sure

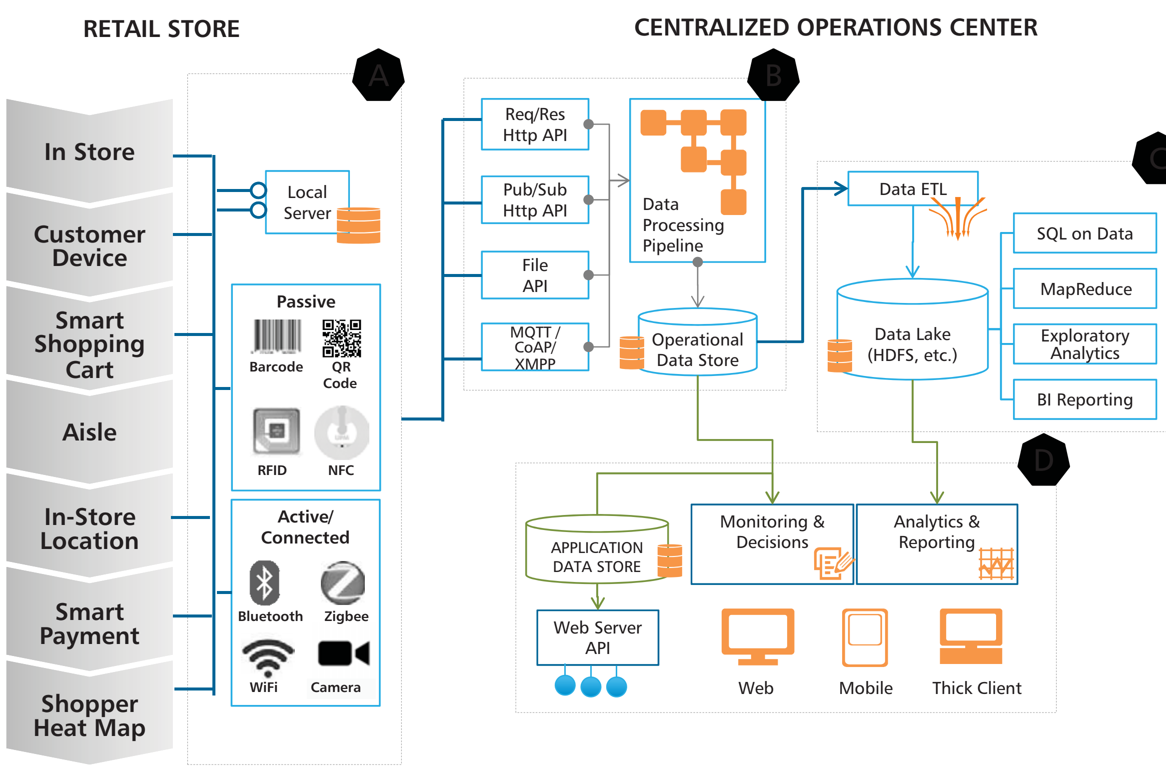


Figure 2 — Reference solution architecture.

no data is lost because of connectivity issues. Another key element in the store is the smart shopping cart equipped with a tablet. The tablet provides the last-mile customer interaction model. The tablet app needs to be well designed and intuitive to use from the customer's point of view. This app holds and stores the data locally for the items the customer intends to purchase, provides the model for advertising (including audio/video), and holds a lot of static data about the product (e.g., product advertisements, pricing/discount offers).

Besides these considerations, system designers must also take into account the following factors:

- Tagging of all incoming data with the current location
- Reliable transmission of data, including handling of failures
- Ability to track the data transfer sequences for failure handling
- Efficient compression and batching for better performance
- Streaming data transfers/keep-alive connections for low latency

Data Collection, Analysis, and Actuation (Gateway)

A retail storefront produces a lot of data. All this data must be collected for analysis. Data coming from different devices needs to be correlated to identify patterns. Based on the patterns, decisions and actions can be defined that will get triggered once all the conditions are met. For example, if a large number of customers are standing in one aisle, the system could reroute the other customers and/or inform the aisle's customer service representative to check if there are any issues. The idea is to enable a lot of analysis at the edge itself, which allows for faster processing and decision making. The customer-specific information needs to be processed in real time and the response sent back to the customer. This module has three key system components:

1. The **API layer** provides two key functions. One is the data collection API, and the second is the actuation API. The first API collects the incoming events using a multitude of devices and protocols. This component must be capable of handling high volumes of data along with high concurrency, as well as providing a subscription-based interface for real-time data streams. Failure handling of data transfers (e.g., retries and missing data requests) is another key feature. The second API, the actuation API, provides the response back to the consumer/tablet/store based on the correlation of the incoming events.
2. The **data processing pipeline** provides the ability to process incoming events that might require in-stream data processing or batch data processing. Incoming events are correlated for pattern identification, SKU/customer tagging, and providing the actuation services. This component needs to be highly scalable and capable of handling very high throughput.
3. Once the incoming events are processed, the **operational data store** captures and stores the derived facts. The data store should handle low-latency writes and reads, support runtime queries, and have the flexibility to store multiple types of data objects (sensor data coming from service providers). This data store provides the information for real-time analysis and actuation services.

Potentially, an enterprise can have multiple instances of this module catering to a subset of retail stores. This model will allow the enterprise to scale out more easily. All components need to be highly resilient and high-performing. The actuation services will rely on split-second decisions based on the incoming data, identified patterns, and decision models.

Enterprise Data Analysis and Storage (Internal Enterprise)

Data from all the deployed operational data stores (as described in the previous section) is aggregated for analysis and storage. This component is the equivalent of the enterprise data warehouse. It should have the ability to handle high volumes of big data, support historical and analytical data, MapReduce jobs for data analysis, and process high volumes of data for simulations and gaining insights. Data collected here can be combined with third-party data for monetization purposes. Data can be anonymized and used to generate patterns and clusters for more targeted personalization and customer targeting.

Applications and External APIs (External Enterprise)

This component provides two subcomponents. The first is the data monetization API for consumption by the external consumers. To support the data monetization API, relevant data needs to be pulled from the operational data stores and big data stores. For data monetization, relevant checks and controls need to be built in (e.g., support for multitenancy to enable the selling of individual pieces of data to different customers, the ability to measure usage and charge customers accordingly). The enterprise should monitor how third parties are using the data and use that knowledge to enhance the monetization capabilities.

The second subcomponent is the internal applications that allow the enterprise to visualize the data coming from the stores aggregated at multiple levels. This data can be integrated with maps APIs (e.g., Google Maps, Bing Maps) for real-time customer/SKU tracking. The application should provide support for rich visualization, have the ability to stream data visualization, and support multiple client types.

Putting It All Together

The above provides an overview of the complexity and various architecture components that go into making the IoT platform. When building an IoT system, all four components will be required to create a cohesive system. Organizations might build some parts of the ecosystem or buy and integrate components from the market. At times, there might be a need to build custom sensors or devices to cater to the needs of the specific use cases.

There are components and products available in the market that can be integrated to build such a system. Many IoT vendors are producing devices that perform certain functions and perform them very well (e.g., wearable devices, beacons, sensors for motion and temperature detection). These devices also provide APIs for consuming the data they are generating. Among the big platform vendors, Amazon Web Services (AWS) has a stream-processing service called Kinesis, and Google has the Cloud Dataflow service that can be integrated to consume large streams of messages for processing and actuation. Microsoft Azure is releasing the Azure Intelligent Systems Service, which not only collects and processes data, but also helps in connecting and managing devices and services. Of course, the IoT ecosystem is still evolving, and technologies to support the ecosystem will continue to emerge.

An enterprise might have legacy systems that need to be upgraded to emit/stream data or to upgrade their existing SCADA (supervisory control and data acquisition) systems, which then can be integrated with the new IoT platform. When building such systems, the nonfunctional requirements — especially scalability, resiliency, and performance — are vital to the success of the platform. As more and more devices are IoT enabled, the amount of data coming in increases exponentially. Having a scalable platform ensures that the application is able to accommodate all this data growth. For the actuation services, real-time performance and subsecond response time in identifying patterns and taking decisions become very important. To enable this resiliency and performance, the ability to segregate noise and take decisions in a time-bound window are critical attributes of the platform.

When enabling large application systems that collect information from multiple sources, data security and user privacy are paramount. In the retail use case, aggregated information about the user categories and preferences can be shared. While sharing information about food purchases isn't nearly as sensitive as, say, sharing medical data, the retailer still needs to be cognizant of what information the consumer might — or might not — feel comfortable sharing. All the collected data belongs to the user, and thus the data needs to be cleansed and anonymized before being shared with third-party service providers. Data at rest needs to be encrypted. Since the IoT is still evolving, regulations have not caught up to all the new devices and systems. In the case of a device/application getting hacked and resulting in an injury/loss to the user, who is liable to pay? Is it the device manufacturer, the data collector/aggregator, the platform provider, the actuator service provider, or the last-mile connectivity provider?

GETTING STARTED

As you begin your IoT journey, you will need to have a cohesive strategy that takes into account all the players. Work with multiple vendors — API, cloud computing, and/or big data — to get started. As you focus on one use case, you will be utilizing your existing customer data and mapping it with context data to create the best possible customer experience, which will result in a business moment for the enterprise. The key is in identifying how to change a product business to a service business. Once the products get connected, the data coming from connected devices will provide immense opportunities for the organization to build service models around them. We need to be geared to align our business models to the possibilities suggested by the ever-evolving IoT.

Munish Kumar Gupta is Lead Architect in the Wipro Technologies Architecture Services Practice. He has extensive experience in digital architectures, emerging technologies, solution engineering, and IT operations management. He can be reached at munish.gupta@wipro.com.

A Comparative Study of Data-Sharing Standards for the Internet of Things

by Angelo Corsaro

The term "Internet of Things (IoT)" was introduced a few years ago to describe applications that connect and allow "things" to communicate and interact through the Internet. Since then, two broad categories of the IoT have emerged:

1. The **Industrial Internet of Things (IIoT)** is an evolution of machine-to-machine (M2M) communication and refers to business-critical IoT environments such as smart grids, smart cities, and transportation.
2. The **Consumer Internet of Things (CIoT)** has enjoyed much of the IoT-related headlines recently thanks to its promise of improving lifestyles through home automation and various wearable technologies.

Although IIoT and CIoT applications tend to require different levels of performance, security, fault tolerance, and safety, they are both data-centric and share the same underlying architectural pattern — the Collect | Store | Analyze | Share pipeline. As a result, data sharing is a crucial architectural element that can make the difference between the success and failure of an IoT application. The challenge for the industry is that there is currently a proliferation of data-sharing and messaging protocols, no set standard, and — until now — no qualitative and quantitative analysis to provide insight and direction.

This article aims to help IoT practitioners understand the set of data-sharing requirements they must consider and guide them in the selection of viable technologies to satisfy those requirements. To this end, it will:

- Present the key data-sharing requirements of IIoT and CIoT applications
- Provide, possibly for the first time at this level, a qualitative and quantitative analysis of the data-sharing standards proposed for the IoT (specifically AMQP, CoAP, DDS, and MQTT)
- Conclude with a set of recommendations that match the requirements of IIoT and CIoT applications

DATA-SHARING REQUIREMENTS FOR THE IIoT AND CIoT

When comparing and contrasting the fitness of different technologies for a given application domain, it is essential to identify the requirements characteristic of the given domain. Ignoring this step would make the comparison somewhat arbitrary and detached from the problem that needs to be solved. Therefore, the first thing we need to do in order to evaluate the fitness of various standards for data sharing in the IoT is to identify the typical requirements of IIoT and CIoT applications.

IIoT Applications

The Industrial Internet of Things is characterized by industry-oriented applications in which devices are machines operating in industrial automation, transportation, energy, or medical environments.

Individual data volumes and rates range from sustained to relatively high, and low and predictable latencies are key for a relatively large class of IIoT applications. Data sharing has to operate efficiently across low-bitrate and high-bandwidth networks for device-to-device (D2D), device-to-cloud (D2C), and cloud-to-cloud (C2C) architectures. Applications are mission- and, at times, safety-critical; the failure of a smart grid, for example, can have severe impact on life and the economy, while the malfunctioning of a smart traffic system can threaten drivers' safety. Security in IIoT applications needs to extend well beyond the network transport to address confidentiality, integrity, fidelity, and access control at a data level. Finally, IIoT applications target industrial platforms characterized by highly heterogeneous deployments, spanning from embedded devices running real-time operating systems to enterprise, mobile, Web, and cloud applications.

CIoT Applications

The Consumer Internet of Things represents the class of consumer-oriented applications in which devices are consumer products, such as smart appliances (e.g., refrigerators, washers, dryers) and personal gadgets (e.g., fitness sensors, Google Glass).

Individual data rates are relatively low, and data is not subject to strict temporal constraints. Applications are not mission- or safety-critical; the failure of a fitness gadget will make you, at worst, upset, but it won't cause any significant harm. Security, although heavily underplayed,[1] is required at least at a transport level. Finally, CIoT applications target consumer platforms that, while presenting a good level of heterogeneity, are in general less exotic than some of the platforms found in IIoT applications.

Figure 1 shows the list of data-sharing requirements characteristic of IoT applications along with a measure of their relative importance for IIoT and CIoT applications, respectively. This figure is key in evaluating the criticality of requirements for IIoT and CIoT applications as well as measuring the fitness of a given technology for IIoT and/or CIoT.

Finally, to avoid any kind of confusion, it is important to understand that when I refer to "individual" data flows, I mean the volume of data produced by a device. One of the main differences between IIoT and CIoT is in the latency, temporal determinism, and throughout relative to the data produced by a given device. More specifically, IIoT tends to consist of devices that produce higher volumes of data and require dissemination with low latency and high determinism. In contrast, CIoT devices often produce low to moderate data rates that have low to moderate requirements with respect to latency and determinism. That said, in spite of the difference in individual data flows, both IIoT and CIoT systems have to deal with massive aggregated volumes of data.

DATA-SHARING STANDARDS FOR THE IoT

With a rising awareness of the importance of data sharing in the IoT, there is an increasing number of technologies that are being proposed as the "right" solution for this task. In this section, I first introduce the four prominent IoT standards — AMQP, CoAP, DDS, and MQTT — and then analyze how they address the various IoT requirements. In this article, I will limit my analysis to standard-based technologies, as I firmly believe that the IoT cannot reach its full potential without standardization. The essence of the IoT is open exchange between connected devices, and the level of seamless connectivity the IoT requires can only be achieved through the standardization of protocols and data models.

Current IoT Standards

Advanced Message Queueing Protocol (AMQP)

The Advanced Message Queueing Protocol (AMQP) was originally defined by the AMQP working group as

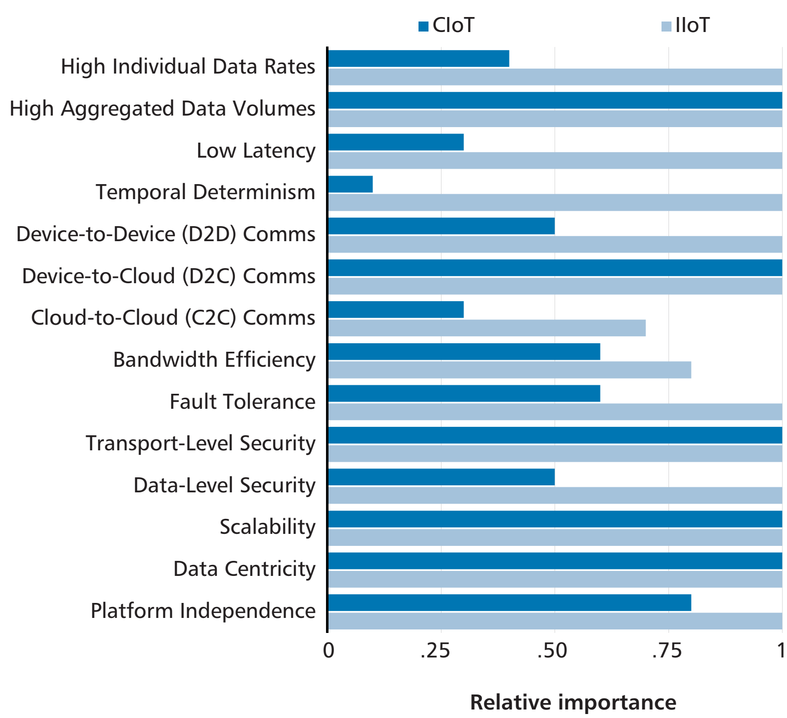


Figure 1 — Relative importance of data-sharing requirements for IIoT and CIoT applications.

a messaging standard that addresses the financial and enterprise market. AMQP, now managed by OASIS, is a standard that defines an efficient, binary, peer-to-peer protocol for transporting messages between two processes over a network.[2] Above this, the messaging layer defines an abstract message format, with concrete standard encoding. It is important to note that the AQMP specification went through major revision in its scope as well as messaging model when moving to version 1.0. The scope was revised to address the "link" protocol for exchanging messages between two nodes, where nodes could be applications, brokers, or message routers.

Constrained Application Protocol (CoAP)

The Constrained Application Protocol (CoAP) is an Internet Engineering Task Force RFC defining a transfer protocol for constrained nodes and constrained networks, such as 8-bit microcontrollers with small amounts of ROM and RAM, connected by 6LoWPAN, a low-power wireless protocol.[3] The protocol is designed for M2M applications such as smart energy and building automation. CoAP provides a request/response interaction model between application endpoints, supports built-in discovery of services and resources, and includes key concepts of the Web such as URIs and Internet media types.

CoAP is designed to easily interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead, and simplicity for constrained environments.

Data Distribution Service (DDS)

The Data Distribution Service (DDS) is the OMG standard for high-performance and secure data-centric publish/subscribe.[4] DDS is based on a completely decentralized architecture and has a built-in dynamic discovery service that automatically establishes communication between matching peers. DDS has a rich set of Quality of Service (QoS) capabilities that provide control over every aspect of data distribution, such as data availability, resource usage (network, memory, etc.), and traffic prioritization. DDS defines standards for communication, platform-independent extensible data encoding, and data representation. The DDS standards family has recently been extended with specifications for RPC, security, and Web integration.

Message Queueing Telemetry Transport (MQTT)

The Message Queueing Telemetry Transport (MQTT) protocol was originally defined by IBM in the mid-1990s as a lightweight protocol for telemetry.[5] MQTT supports a basic publish/subscribe abstraction with three different levels of QoS. MQTT has recently gained much attention as a potential candidate for data sharing in the IoT.

Qualitative Analysis

As providing a detailed overview for each of the IoT standards would require an article for each of them, I have summarized the key features each standard supports (see Figure 2). This list of features reveals how CoAP and MQTT focus on a subset of the IoT data-sharing problem (namely, D2D and D2C, respectively), while AMQP and DDS address the entire IoT design space. When compared to AMQP, DDS has better applicability to the IIoT because of its support for real-time data distribution. It also supports UDP/IP unicast and multicast, which helps to control data timeliness as well as completely avoid TCP/IP head-of-line blocking

	Transport	Paradigm	Scope	Discovery	Content Awareness	Data Centricity	Security	Data Prioritization	Fault Tolerance
AMQP	TCP/IP	Point-to-Point Message Exchange	D2D D2C C2C	No	None	Encoding	TLS	None	Impl. Specific
CoAP	UDP/IP	Request/ Reply (REST)	D2D	Yes	None	Encoding	DTLS	None	Decentralized
DDS	UDP/IP (unicast + multicast) TCP/IP	Publish/ Subscribe Request/ Reply	D2D D2C C2C	Yes	Content-Based Routing, Queries	Encoding, Declaration	TLS, DTLS, DDS Security	Transport Priorities	Decentralized
MQTT	TCP/IP	Publish/ Subscribe	D2C	No	None	Undefined	TLS	None	Broker is the SPoF

Figure 2 — Qualitative comparison of IoT standards.

issues. Figure 3 shows the degree to which the four standards cover the various IoT requirements identified previously.

Finally, Figure 4 provides a normalized standard applicability obtained by adding across all requirements the product of the level of coverage of a requirement provided by each standard with the relevance of the requirement as shown in Figure 1. This sum is then normalized, dividing it by the score of an ideal standard that would score 1 for every single requirement. Based on Figure 4, it appears that DDS is the standard that best covers the IIoT and CIoT requirements.

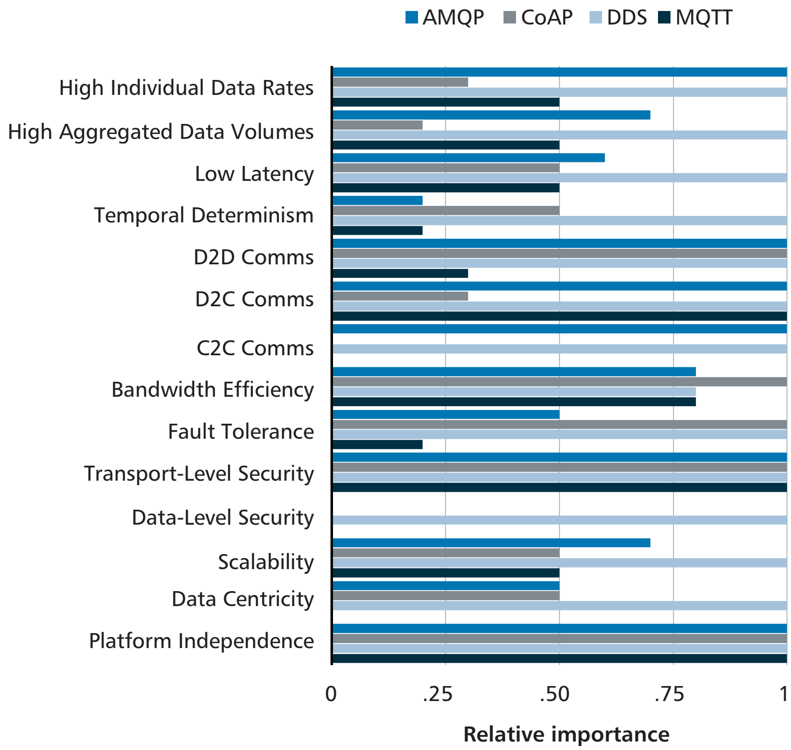


Figure 3 — Coverage of IoT requirements by IoT standards.

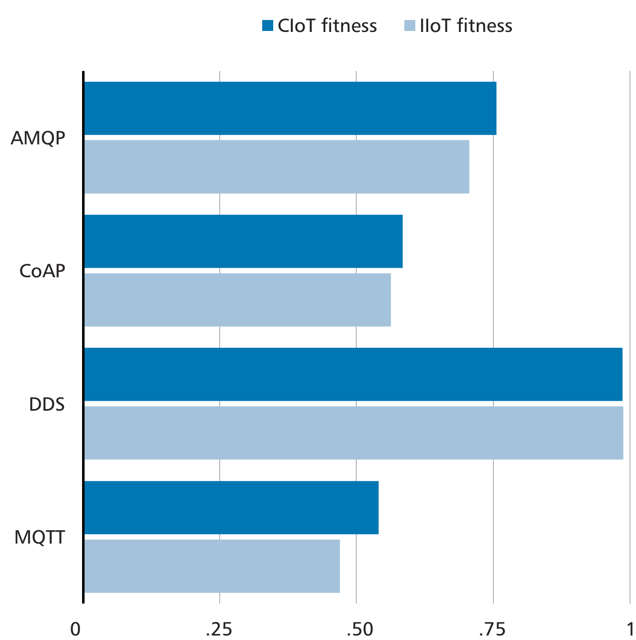


Figure 4 — Applicability of IoT standards to IIoT and CIoT.

Quantitative Analysis

Many of you may be surprised by the fact that DDS — a standard you've not heard of much before — is the one that scores best for IoT applications. Perhaps you have heard a lot about MQTT and its simplicity, wire efficiency, and performance. After all, Facebook has adopted MQTT for its chat application, thus it should be good for everyone, no? Well, not really. As we have seen before, IoT applications have to deal with a set of requirements that go well beyond that of a chat.

To provide empirical evidence to the qualitative analysis performed in the previous section, I will now compare and contrast the wire efficiency and latency of the two standards I feel are most often discussed for CIoT and IIoT applications: DDS and MQTT.

Wire Efficiency Evaluation

When evaluating the wire efficiency of a protocol, there are several aspects that come into play, yet as engineers know, what matters in performance is the common case. To evaluate the relative wire efficiency of DDS and MQTT, we will be looking at the structure of a data message for the two protocols. To put it another way, we will be estimating the protocol overhead as the number of bytes that are used to send user data, over and above the user data itself. Clearly, the lower the size of the protocol data (aside from user data), the more efficient the protocol will be.

The structure of an MQTT publish message is shown in Figure 5. The actual size of the message depends on the QoS that is used for the message delivery. The options are QoS=0 for at-most-once semantics, QoS=1 for at-least-once semantics, and QoS=2 for exactly once semantics.

Figure 6 shows the structure of a DDS (DDSI-RTPS to be precise) message that contains a DATA submessage. In the efficiency analysis, we will consider the case in which individual DDSI-RTPS messages are sent and the case in which a DDSI-RTPS message is streamed over TCP/IP. In the latter case, the header is sent only once, and for each data sample only a DATA submessage is sent.

By analyzing Figures 5 and 6, we can easily derive the overhead associated with sending user data. Figure 7 shows the protocol overhead formulas for both DDS and MQTT. It is worth noting how MQTT's overhead depends linearly on the length of the topic name as defined by the user. This dependency is quite critical, as MQTT topic names encode hierarchy and are used to do hierarchical subscriptions. As a result, the length of a topic name is usually several tens of bytes.

```
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
+---+---+---+---+---+---+---+---+
| message type  | DF|   QoS | R |
+---------------+---+-------+---+
~  Remaining Length (1-4 bytes) ~
+-------------------------------+
|   Topic Name Length MSB       |
+---+---+---+---+---+---+---+---+
|   Topic Name Length LSB       |
+---+---+---+---+---+---+---+---+
|                               |
~           Topic Name          ~
|                               |
+---+---+---+---+---+---+---+---+
|       Message ID MSB          |
+---+---+---+---+---+---+---+---+
|       Message ID LSB          |
+---+---+---+---+---+---+---+---+
|                               |
~           Payload             ~
|                               |
+---+---+---+---+---+---+---+---+
```

Figure 5 — An MQTT publish message.

```
                    1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      'R'      |      'T'      |      'P'      |      'S'      |
+---------------+---------------+---------------+---------------+
|    ProtocolVersion version    |      VendorId vendorId        |
+---------------+---------------+---------------+---------------+
|                                                               |
+                                                               +
|                    GuidPrefix guidPrefix                      |
+                                                               +
|                                                               |
+---------------+---------------+---------------+---------------+
|  DATA         |X|X|X|X|X|D|Q|E|     octetsToNextHeader        |
+---------------+---------------+---------------+---------------+
|  Flags        extraFlags      |     octetsToInlineQos         |
+---------------+---------------+---------------+---------------+
|           EntityId            readerId                        |
+---------------+---------------+---------------+---------------+
|           EntityId            writerId                        |
+---------------+---------------+---------------+---------------+
|                                                               |
+           SequenceNumber      writerSN                        +
|                                                               |
+---------------+---------------+---------------+---------------+
~           ParameterList       inlineQos       [only if Q==1]  ~
+---------------+---------------+---------------+---------------+
~  SerializedPayload  serializedPayload  [only if D==1 || K==1] ~
+---------------+---------------+---------------+---------------+
```

Figure 6 — A DDS (DDSI-RTPS) message, including used-to-send data.

To evaluate the impact of topic name length on the protocol overhead, Figure 8 shows the DDS and MQTT overhead for various topic name lengths. From the figure it is evident that, for small topic names (e.g., 8 bytes), MQTT is slightly more efficient than DDS. For topic names of 32 bytes, MQTT is already less efficient than DDS, and it gets worse as the topic name length increases.

Latency Evaluation

Aside from the protocol overhead analysis, latency is another useful metric for evaluating the efficiency of a communication standard. I therefore evaluated DDS

	Message Size (bytes)	IPv4 Headers (bytes)	Total Size (bytes)
MQTT (QoS = 0)	(2 to 5) + 2 + length(TopicName) + length(Payload)	IP: 20-40 TCP: 20-40	min = 20 + 20 + 4 + length(TopicName) + length(Payload) max = 40 + 40 + 7 + length(TopicName) + length(Payload)
DDS	44 + length(Payload)	IP: 20-40 UDP: 8	min = 20 + 8 + 44 + length(Payload) max = 40 + 8 + 44 + length(Payload)
DDS Streaming	24 + length(Payload)	IP: 20-40 TCP: 20-40	min = 20 + 20 + 24 + length(Payload) max = 40 + 40 + 24 + length(Payload)

Figure 7 — DDS and MQTT protocol overhead.

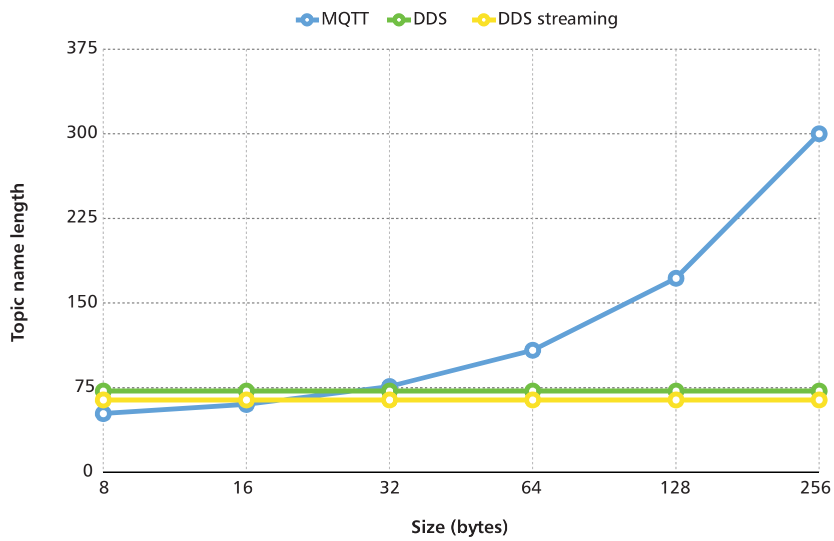


Figure 8 — Protocol overhead as a function of the topic name length.

and MQTT latency using equivalent implementations of a ping-pong distributed application. In this distributed ping-pong, the ping application sends data to the pong application, which immediately responds by sending back the received data. The latency is then estimated as the time required to perform this ping-pong divided by two.

To evaluate DDS latency, I used the Vortex platform.[6] More precisely, I used Vortex OpenSplice, Vortex Café, and Vortex Cloud. Vortex OpenSplice is a C/C++ implementation of DDS, while Café is a pure Java implementation. Vortex Cloud is a PaaS/MaaS implementation of DDS. To evaluate MQTT latency, I used the Mosquitto Broker[7] in combination with the Paho MQTT client library.[8]

Figure 9 shows the latency for both DDS and MQTT (QoS=0) when conducting the test on Intel i7 machines running Linux and connected by a 1Gbps network. Notice that the results were measured with an out-of-the-box configuration for both Vortex and Mosquitto. This will be evident for those familiar with Vortex, as when it is configured for optimal latency, it can deliver latency as low as 30 microseconds.

The results showed latencies close to 40 milliseconds. I had two teams conduct independent validations of these results across machines, and I also tried to validate the behavior by using a different MQTT broker.

From Figure 9, we can see how Vortex OpenSplice and Café exhibit lower latencies than Mosquitto, with the difference growing significantly with the message size. Overall, DDS shows peer-to-peer latencies that are up to three times better than MQTT. If we consider instead the latency when going through the DDS MaaS implementation, namely Vortex Cloud, we see that DDS and MQTT latencies are quite close for small messages but then start diverging for data sizes of 4,096 bytes or more. The results show that Vortex Cloud has a higher per-message cost of routing, but at the same time it is more efficient in dealing with larger data. This is not surprising, since along with supporting content routing, Vortex Cloud is elastic and fault-tolerant. As a consequence, it has a little more work to do for each incoming data message, especially when compared to an MQTT broker like Mosquitto, which is neither elastic nor fault-tolerant.

Finally, it is worth noticing that the tests were performed with the first release of Vortex Cloud; so we

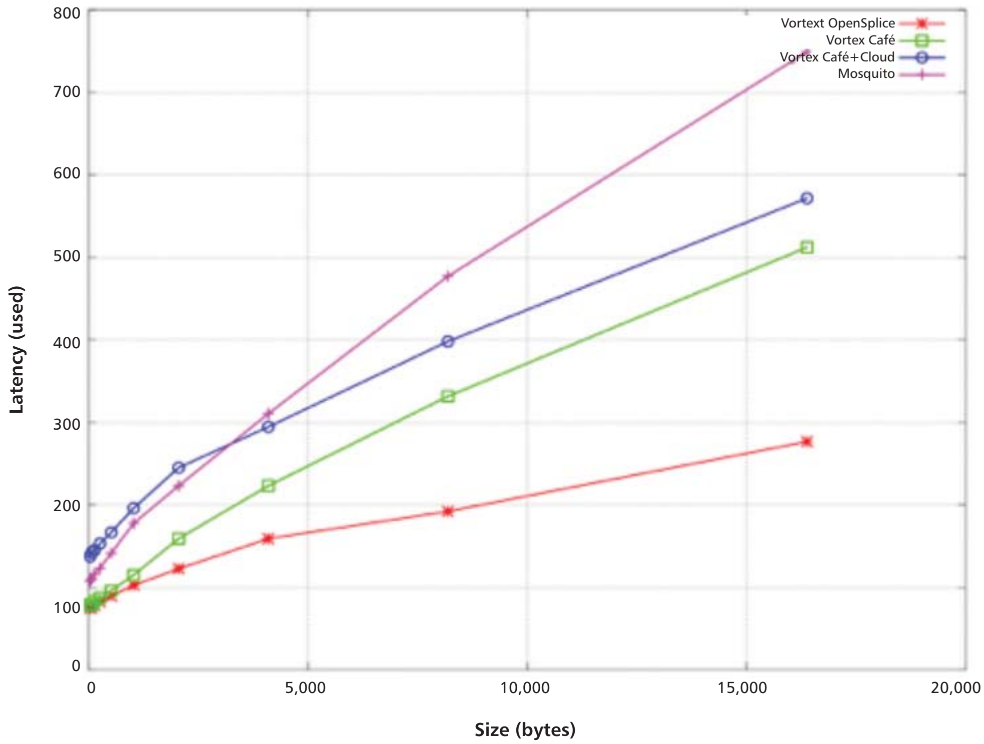


Figure 9 — DDS vs. MQTT latency.

can imagine that the per-message processing overhead will be further improved in coming releases. On the other hand, Mosquitto is a mature broker that has been around for some time.

CONCLUDING REMARKS

In this article, I have sought to provide IoT practitioners with an improved understanding of the set of data-sharing requirements they have to consider when developing IoT applications, along with an assessment of how existing standards address these requirements. I have also provided a framework practitioners can use to reason about and quantitatively evaluate IoT requirements as well as technology applicability.

Based on my findings, the DDS standard seems to provide the best starting point when trying to address IIoT and CIoT data-sharing requirements, with AMQP being the second-best option.

ENDNOTES

[1]"Internet of Things Research Study." Hewlett-Packard, 2014 (www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf).

[2]OASIS Advanced Message Queuing Protocol (AMQP) (www.oasis-open.org/committees/tc_home.php?wg_abbrev=amqp).

[3]Shelby, Z., K. Hartke, and C. Bormann. "The Constrained Application Protocol (CoAP)." IETF RFC 7252, June 2014 (https://datatracker.ietf.org/doc/rfc7252).

[4]Data Distribution Services (DDS) (www.omg.org/dds).

[5]OASIS Message Queuing Telemetry Transport (MQTT) (www.oasis-open.org/committees/tc_home.php?wg_abbrev=mqtt).

[6]Vortex (www.prismtech.com/vortex).

[7]Mosquitto (http://mosquitto.org).

[8]Paho (www.eclipse.org/paho).

Angelo Corsaro is CTO at PrismTech, where he directs the company's technology strategy, planning, evolution, and evangelism. He also leads the strategic standardization at the Object Management Group, where he cochairs the Data Distribution Service (DDS) Special Interest Group and serves on its Architecture Board. Dr. Corsaro is a widely known and cited expert in the field of real-time and distributed systems, intelligent data-sharing platforms, and software patterns; has authored several international standards; and has more than 10 years of experience in technology management and design of high-performance, mission- and business-critical distributed systems. Prior to joining PrismTech, he served as a Software Scientist within the SELEX-SI Strategic and Technological Planning Directorate. He earned a PhD and an MS in computer science from the Washington University in St. Louis, Missouri, and a laurea magna cum laude in computer engineering from the University of Catania, Italy. He can be reached at angelo.corsaro@prismtech.com, Twitter: @acorsaro, SlideShare: http://slideshare.net/angelo.corsaro.

Thinking About Making Your Product Smart?
Keep These 10 Things in Mind

by Adam Justice

All eyes are on the Internet of Things (IoT), which offers the ability to connect and control smart devices remotely via the Internet. Cisco recently predicted that the public- and private-sector economic value created by the "Internet of Everything" will reach US $19 trillion in the next decade.[1]

As the cost of networking devices falls, the number of smart products continues to rise and capture the attention of both consumers and businesses (see Figure 1). At Grid Connect, we expect the largest growth areas will be in transportation, industrial automation, medical devices, and the connected home, while Cisco sees additional opportunities in energy and retailing.[2]

Making products that can connect to the Internet is one way that manufacturers are staying competitive within their industry. Adding IoT capabilities gives consumers more features and allows manufacturers to stay connected with their customers while discovering new uses and applications for their products that can create new revenue streams.

In fact, manufacturers are gearing up for the IoT phenomenon by developing "ghost" devices — IoT-enabled devices without a current application. The idea is that when the application is developed, the product will be ready.

Figure 1 — The rise of smart products.

Designers are working feverishly to add connectivity to products, weighing the potential value to users, as well as risks. For example, the capability exists today to make toilets smart, but is there really a need for a toilet that can be flushed remotely? On the other hand, a smart oven can be triggered remotely to heat up by the time you return from work. It could be a great time saver, but is it a fire risk?

As designers grapple with these questions, there are also a host of design issues that they must keep in mind before jumping on the IoT bandwagon. The top 10 design considerations are:

1. FEATURES

The IoT allows companies to add features to their product that were never possible before. These features have a wide range of benefits and functions including automatic (over-the-air) software updates, smart home and office connectivity, reminders for maintenance, special offers, recall notices and upgrades, and remote or local access and control. It is important for designers to work with marketing teams to ensure the features marketing desires are not limited by the hardware and networking technologies the engineers select.

2. SIZE

Many manufacturers start testing the IoT waters by modifying their existing product designs to add networking technologies. Fortunately, there are a number of compact networking modules available that will fit in a manufacturer's existing products. We are seeing new "smart" features appear in refrigerators, stoves, washers, dryers, and many more products.

IoT products will require some design modifications. Some networking modules are surface mount, others are through-hole or pin-header, and some still use a specialized mating connector. Also, the way the network connector or antenna connector is integrated into the product varies from module to module. Designers must consider the space they have available on their circuit boards and in the product's enclosure to allow whatever technology is selected to be used in existing designs.

3. COST

Connected devices come with higher manufacturing costs than non-Internet-enabled products, but they can be sold with a higher price tag as well. Wi-Fi and Ethernet connections can be added to products for a material cost of less than US $10. Other technologies, such as ZigBee, Z-Wave, and Bluetooth, can be added for a lower price, but they may require a separate router or gateway device to connect to the Internet. Manufacturers must decide if consumers will pay the added cost. For example, adding wireless connectivity to a $20 or $30 lamp could add $10-$15 to the cost. Will customers be willing to pay a 50% premium for the convenience?

Manufacturers may be able to defray the cost of adding connectivity by monetizing the information smart devices gather. A good example is a connected washer and dryer. By gathering usage data, manufacturers can discover which of the 20 functions owners actually use, thereby helping with future product development. Sensors in the appliances can also trigger alerts when a component is about to fail, allowing customers to set up service calls proactively. Since people hate being inconvenienced when an appliance is on the fritz, this capability can boost customer loyalty. Customer usage information about the amount of detergent or other additives used in washes, water temperature preferences, and wash cycle choices could be packaged and sold to detergent companies as consumer insight.

4. POWER

Power use needs to be taken into account when making a product smart. Consider where the product will be used and whether untethering it from a wall outlet makes the product more useful. Manufacturers of products that don't use a wall outlet will have to consider how the power source will affect their product's design.

The power source generally can be decided based on the power needs of the device. If the device needs to be "on" constantly, a traditional battery won't work because it will drain quickly. Many connected products, such as motion sensors, are able to sleep and wake, reducing power consumption and enabling the device to be battery-powered.

There are a variety of batteries to consider: alkaline, lithium (rechargeable), and coin. There also are a variety of battery sizes to choose from. Another source of power for Ethernet-based devices is Power-over-Ethernet (PoE). This technology is popular for low-wattage Internet Protocol (IP) phones and security cameras. Recent advancements and new switching technology are pushing the wattage available through PoE to new levels, thus opening up new possibilities for more power-hungry applications and devices.

Once a manufacturer knows how long and how often a device will be connected and which wireless network has been chosen, a proper size and type of battery can be selected. In some cases (e.g., smart meters), the product may be able to connect to the city's grid. Some products may require gasoline engines to provide power to sensors, such as those used in remote areas for border detection.

5. USER INTERFACE

Making a product smart requires designers to approach the user interface with new thinking. Customers will need to interact with the smart device for programming, updates, and other reasons. There are different ways to do this, which entail varying degrees of difficulty, so it's important to understand what the customer is capable of or willing to do in order to program a device.

The type of product and its possible uses are important considerations when designing a product that can communicate information to its user. The product can have a visual interface or display, or it can be controlled through the Web or via an app. If there is no visual interface, consider how the customer will know if a device is "on." It may be necessary to add an "on" light to a product that previously didn't have one. Also, think about whether the device should have a manual on-off switch.

Apps to monitor and control connected devices can be Web-based, available as smartphone apps, or both. If designing a mobile app, hire pros who are well-versed in mobile design.

Finally, consider whether the IoT device can act as a soft access point (soft AP) to allow a user to "join" its network using a smartphone, laptop, or tablet. Soft APs — available only if the product uses Wi-Fi to connect to the Internet — make product LED/LCD displays unnecessary, since the screen of the connected device will serve the same purpose. This dual mode is very attractive because the user can access the product both remotely and locally, depending on the features and uses of the product.

6. NETWORK

There are a number of network connection standards being used to connect devices to the Internet, each with its own pros and cons. Some devices can be directly connected to the Internet using existing networks, such as Ethernet and Wi-Fi, which are based on the Internet Protocol suite (TCP/IP). Other standards require a "gateway" to convert the network to either Ethernet or Wi-Fi, which adds cost and one more potential point of failure.

The easiest devices to connect will use Wi-Fi, Ethernet, cellular, or Bluetooth. Wi-Fi and Ethernet are ubiquitous in most homes and businesses, and Bluetooth connects through smartphones and tablets using their existing cellular network. None of them require the addition of hardware or gateways.

ZigBee and Z-Wave are short-range wireless technologies used for remote monitoring and control. They both require users to buy their own hub or gateway to enable them to communicate with different devices.

Thread is a new protocol that turns IP into a mesh network to optimize coverage. It is based on 6LoWPAN, a low-power wireless protocol. The advantage with Thread is that if the Internet or network goes down, devices can still talk to each other.

7. ANTENNA

The wireless technologies used to make a device smart will impact the type and number of antennas needed. Module manufactures often provide multiple options for antennas, such as on-board chip or ceramic antennas. They may also offer a wire (or "whip") antenna, a "trace" antenna, or a "pin-out" so the manufacturer can add their own antenna (either an internal or external connector elsewhere on the circuit board).

In addition, manufacturers may offer U.FL (also called IPEX) connectors for external use, which use a short coaxial "pigtail" that mates the U.FL connector on one end with the antenna connector on the other. The costs of the pigtail and antenna are often overlooked but need to be included in a manufacturer's cost of materials.

When selecting between internal and external antennas, designers must consider the material (metal, plastic, etc.) of the housing and the potential placement of the product within a home or business. If a product is placed behind a couch or under a desk, for example, it may have difficulty getting a wireless signal from the nearest gateway, access point, or router. Metal housings almost always require an external antenna design because the metal in the housing greatly diminishes the quality of radio frequency (RF). The type of antenna chosen will also depend on your audience and application. People typically don't want their home devices to have unsightly antennas. In IT and industrial environments, this is more acceptable and usually where such antennas are needed.

8. CLOUD

Most IoT applications include some cloud-based component. Many manufacturers entering the IoT space are new to cloud development, which makes decision making for cloud applications, such as how and when a product will connect to the cloud, difficult.

How an IoT-enabled device communicates with a cloud application depends on which protocol is used to communicate with the cloud. Many early IoT implementations followed a proprietary protocol, where the device manufacturer implements its own protocol to communicate with cloud applications. Recently, more companies have become aware that a standard protocol is needed for IoT communications to be successful and have started providing third-party, end-to-end solutions with platforms to develop and host applications.

When an IoT device connects to the cloud refers to the frequency of data exchange with the cloud application. Devices that are always on (connected to a power supply) can easily stay connected to the cloud constantly. This improves the ability to be "near real time" when communicating with the cloud application. Always-on devices are seen in critical applications such as temperature monitoring, where real-time data is critical for monitoring food, drugs, and other temperature-sensitive goods. Battery-powered devices often only connect to the Internet intermittently, sending data periodically in order to conserve battery life. In this case there may be a delay, as the device has to reestablish its connection to the wireless router and then to the cloud server.

Battery-powered devices should be designed to wake periodically. This "heartbeat" allows the cloud application to know the device is still online and has power or battery-life remaining to be used when an event does occur. Battery power is often seen in "edge"-type devices that are difficult to get power to, such as door locks, windows, water sensors, motion sensors, and the like.

9. INTEROPERABILITY

As more manufacturers enable their products for the IoT, consumers of their technology will be faced with many different cloud apps from various devices and manufacturers. Devices should support more than one of these standards to ensure they will be able to work with and communicate with other manufacturers' products. This makes operating many IoT-enabled devices together simpler and more convenient, while opening up new uses and features that the original manufacturers never dreamed of.

For example, one day it might be possible for a consumer to simply say, "Good night, house" to their app, and the app will turn off all of the main house lights and televisions, turn on the outside lighting, alarm the house, set the alarm clock for the morning, and trigger the coffee pot to start brewing at a preset time. In this example, each device might be produced by a different manufacturer, but since they all support the same standard, the application knows how to talk to them all and create new service offerings. The same advances that are being seen in the home will also apply to IT and industrial offerings. New IoT standards are going to allow communication between devices on the factory floor as well as in autos and traffic lights.

Some of the emerging interoperability standards include:

- **Thread —** supported by the likes of Google/Nest, Samsung, and more
- **HomeKit —** supported by Apple
- **AllJoyn —** supported by Microsoft, Sony, and Panasonic, part of the AllSeen Alliance
- **IETF —** an Internet standards body
- **ETSI —** a European-based standards organization, primarily in the telecom domain

The standards landscape is changing rapidly, and manufacturers need to adapt their products to work with these standards as they are consolidated and settled in the future.

10. SECURITY

As the IoT continues to grow, there is an increasing focus on the security of information. New IoT products are introduced daily, and many transmit personal and sensitive information; for example:

- Medical devices can monitor and transmit patient health information to the hospital or doctor's office.
- Home thermostats provide clues about when a home owner is away at work.
- Today's cars are equipped with connected devices that, if hacked, could create a dangerous situation.
- Video surveillance products can be hacked.

It's important to understand how data can be compromised and what the potential outcomes are if data is breached. It's also important to protect the IoT ecosystem. For example, is there a way for the electrical grid to be compromised via an IoT sensor?

Implementing high-cost security into every product is ideal; however, it is not very economical. Manufacturers must keep in mind the risks associated with a breach, then determine the proper security measures for each of their IoT solutions while keeping costs in check.

Product manufacturers must employ best practices and security protocols to ensure the safety of data. In addition, users need to know where they are vulnerable and take appropriate steps. For example, some home automation and security sensors allow users to receive alerts via Twitter, which could widely broadcast sensitive information. Also, users need to take appropriate precautions to secure their IoT apps on smartphones and tablets.

CONCLUSION

The IoT is still new, but it has gained significant attention in a relatively short time. The only limit to new smart products is our imagination. These 10 design considerations will help ensure that new products are well-designed and that users will continue to demand more.

ENDNOTES

[1]"Internet of Everything." Cisco (http://internetofeverything.cisco.com).

[2]Cisco (see 1).

Adam Justice is VP and General Manager of Grid Connect, a manufacturer and distributor of the ConnectSense product line of wireless sensors. He can be reached at adamj@gridconnect.com; Twitter: @adamjustice.

Cutter Consortium

ACCESS TO THE EXPERTS

Cutter Membership

The ultimate *Access to the Experts*

With unlimited access to Cutter's research, inquiry privileges with Cutter Senior Consultants and Fellows, regular strategy meetings for your team with a Cutter Practice Director, virtual roundtables with Cutter experts and peer-to-peer networking, free or discounted admission to events, and more, your Cutter Membership opens up multiple avenues to interact with Cutter's experts to brainstorm and gain guidance aimed at boosting success.

Like everything IT, one size does not fit all. That's why we encourage you to choose the Membership level that's right for your organization:

Full Membership

Best for organizations seeking personal, real-time guidance on the full gamut of business technology and software engineering issues and dedicated to investing in the career development of their entire staff.

Business Technology Strategies

Best for organizations developing operationally sound strategies and plans that link and align business and IT, and harnessing the latest leadership and management techniques to ensure IT is furthering the mission of the business.

Agile Product & Project Management

Best for software and product development organizations that are seeking to create and capture lasting value through end-to-end Agile initiatives.

Business & Enterprise Architecture

Best for organizations interested in using architectural approaches to manage the complexity and cost of IT and to pave the way for strategic planning and portfolio management.

Data Insight & Social BI

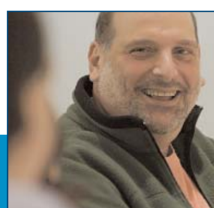
Best for organizations challenged with data collection, analysis, and integration

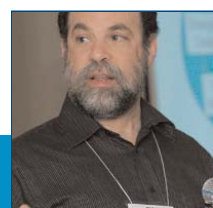
"I am amazed that this venue exists; that I can listen and interact with these individuals. I am more amazed that I have not done this before."

— Mark Rubin,
Fidelity Investments,
USA

"Cutter seems to be unique in consistently providing information one can immediately put into action or clarify one's thinking on day-to-day problems. The service provides tremendous value for the money."

— Lloyd Fletcher,
Information Systems Manager,
Institute of Physics Publishing,
Bristol, UK



as well as internal- or external-facing information sharing via social, mobile, or legacy apps.

CIO Add-On

Ongoing, one-to-one relationships with seasoned expert mentors; research and analysis specially curated to support high-level decision making; peer-to-peer networking.

Membership Benefits

- Continuous flow of advice, insight, and answers via enterprise access to written and multimedia research from Cutter's top experts
- Priority Access to the Experts: get near-real-time answers to your questions
- Regular strategy sessions with Cutter Practice Directors or Senior Consultants
- Admission to client-only online Q&A sessions
- Participation in peer-to-peer discussions led by Cutter's experts
- Cutter events
- Add-on options for consulting and training offerings

And more ...

To arrange for a free trial membership or to discuss how Cutter's consultants can help your organization, contact our team today: sales@cutter.com or +1 781 648 8700

What's Unique About Cutter?

- Cutter's internationally recognized expert practitioners provide all of Cutter's research and analysis. You get to tap into this brain trust whose written words have been likened to a "consultancy in print."
- Without exception, every single inquiry is fielded by a Cutter Senior Consultant, Fellow, or Practice Director.
- Cutter approaches every consulting or training assignment as unique, requiring a tailor-made solution, and creates a team for you that includes only its best-in-class experts. We focus on knowledge transfer, so you can leverage our work together and move forward on your own.
- With Cutter, you get cutting-edge thinking from multiple viewpoints so you can determine what's best for your situation.
- Emphasis is on strategies and processes, so you can be sure your success is not dependent on vendor/product detail.
- Cutter is unique in having no ties to vendors. Rest assured that the advice you get is unbiased and in the best interest of your organization alone.
- Focus includes the business management of IT — you're plugged into the research from top business thought leaders.

"I have personally been able to leverage Cutter's services since 1999. Among the attributes that differentiate Cutter from other firms, two remain at the top of my list — *Thought Leadership* and *Real Value* — executed in a practical way.

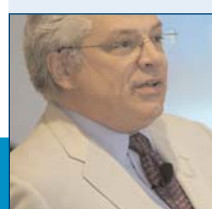
Thought Leadership is driven by Cutter's experts. The advantage is that Cutter doesn't pitch a single best practice for a given area. Instead, Cutter provides multiple good practices/options that come from both academic rigor as well as on-the-ground experience. This provides several benefits for Dairy Farmers of America:

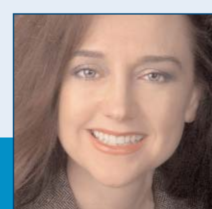
- Exposure and awareness of proven good-practices — particularly for IT, but also for overall business leadership and management
- A finger on the pulse of emerging good practices and IT-impacting trends
- Options for improving our performance
- The opportunity to develop relationships with the experts

The last, 'Access to the Experts,' drives the *Real Value*, letting us go beyond just understanding the options. We can develop relationships with the experts and tailor the options so that they can be quickly and practically executed within our organization, enabling our Business Technology team to continually improve, engage, and contribute to business growth."

— Doug Mikaelian,
VP Business Technology,
Dairy Farmers of America








About Cutter Consortium

Cutter Consortium is a truly unique IT advisory firm, comprising a group of more than 100 internationally recognized experts who have come together to offer content, consulting, and training to our clients. These experts are committed to delivering top-level, critical, and objective advice. They have done, and are doing, groundbreaking work in organizations worldwide, helping companies deal with issues in the core areas of software development and agile project management, enterprise architecture, business technology trends and strategies, enterprise risk management, metrics, and sourcing.

Cutter offers a different value proposition than other IT research firms: We give you Access to the Experts. You get practitioners' points of view, derived from hands-on experience with the same critical issues you are facing, not the perspective of a desk-bound analyst who can only make predictions and observations on what's happening in the marketplace. With Cutter Consortium, you get the best practices and lessons learned from the world's leading experts, experts who are implementing these techniques at companies like yours right now.

Cutter's clients are able to tap into its expertise in a variety of formats, including content via online advisory services and journals, mentoring, workshops, training, and consulting. And by customizing our information products and training/consulting services, you get the solutions you need, while staying within your budget.

Cutter Consortium's philosophy is that there is no single right solution for all enterprises, or all departments within one enterprise, or even all projects within a department. Cutter believes that the complexity of the business technology issues confronting corporations today demands multiple detailed perspectives from which a company can view its opportunities and risks in order to make the right strategic and tactical decisions. The simplistic pronouncements other analyst firms make do not take into account the unique situation of each organization. This is another reason to present the several sides to each issue: to enable clients to determine the course of action that best fits their unique situation.

For more information, contact Cutter Consortium at +1 781 648 8700 or sales@cutter.com.

The Cutter Business Technology Council

The Cutter Business Technology Council was established by Cutter Consortium to help spot emerging trends in IT, digital technology, and the marketplace. Its members are IT specialists whose ideas have become important building blocks of today's wide-band, digitally connected, global economy. This brain trust includes:

- Rob Austin
- Ron Blitstein
- Tom DeMarco
- Lynne Ellyn
- Israel Gat
- Vince Kellen
- Tim Lister
- Lou Mazzucchelli
- Ken Orr
- Robert D. Scott