White Paper **WP152016EN**

The Internet of Things and the energy sector: myth or opportunity

Power and Energy Automation Conference
Spokane, WA
March 8–10, 2016

Jacques Benoit
Eaton's Cooper Power Systems

Abstract

Vendors of networking products are claiming that there will be as many as 50 billion devices connected to the Internet by the year 2020. The vision of these devices working together and feeding data to cloud-based applications in order to provide value through Big Data analytics is referred to as the "Internet of Things" (IoT). Because of the large number of Intelligent Electronic Devices (IEDs) being deployed in substations and distribution networks, the energy sector is often presented as a natural target of opportunity for IoT. However, the energy sector poses its own challenges. This paper discusses the technologies and standards on which IoT is implemented, compares them to those already in use in the energy sector, discusses the challenges that have been identified during Smart Grid projects involving large numbers of devices, and identifies some opportunities offered by the IoT and its underlying technologies.

Introduction

While the term "Internet of Things" seems to be the latest technological fad, the term was coined as early as 1999 when researchers envisioned using RFID tags to track large networks of objects[1]. The concept has evolved with the massive introduction of intelligent connected devices and Cisco, a major vendor of networking equipment, now defines the Internet of Things as the point in time where the number of objects, or "things", connected to the Internet exceeded the number of people. Cisco is even predicting that by the year 2020, there will be 50 billion devices connected to the Internet[2].

The vision of these devices working together and feeding data to cloud-based applications in order to provide value through Big Data analytics is what is now widely referred to as the Internet of Things (IoT). While this vision is often associated with connected consumer products, it is also making its way to other domains and we are now hearing about an "Industrial Internet of Things" (IIoT) where the data from thousands of sensors in the field or the plant floor will allow optimized productivity and resource usage in real-time, bringing about "Industry 4.0", the new industrial revolution.

This paper will discuss the promises of IoT, as well as the technologies and standards on which it is being implemented. These will be compared to those already in use in the energy sector, with a discussion of some of the challenges that have been identified during Smart Grid projects. The paper will also discuss how data from existing applications could be retrieved and put to use while still meeting the security and safety requirements of the critical infrastructure.

Defining the IoT

The definition of the Internet of Things suffers from a lot of confusion, as it encompasses a large number of applications and technologies. This is not helped by all the hype surrounding this new commercial opportunity, as every large vendor of networking devices, automation, and software joins the bandwagon. In addition, the description generally remains at a very high level with very little technical discussion on how to build an IoT in order to achieve all the benefits.

Standard Development Organizations (SDOs) have thus formed working groups to provide a formal structure to the IoT. For instance, the IEEE® has launched an IoT initiative and it defines the IoT as "A network of items—each embedded with sensors—which are connected to the Internet"[3]. It has already identified over 140 relevant standards and projects and formed the IEEE P2413 working group to define an architectural framework and identify the various IoT domains, their abstractions and commonalities.

The P2413 working group has identified the following IoT domains: home and building, retail, energy, manufacturing, mobility and transportation, logistics, media, and healthcare. At a very high level, P2413 defines the architecture as three-tiered and consisting of applications, networking and data communications, and sensing[4].

Because of the large number of Intelligent Electronic Devices (IEDs) being deployed in substations and distribution networks, the energy sector is often considered as a natural target of opportunity for IoT. However, the discussion is generally limited to obvious applications such as AMI and "intelligent" thermostat applications. Unfortunately, the fact that the energy sector has gained a lot of valuable experience through work on its own standards-based architecture of connected devices, the Smart Grid, is generally not mentioned.

In the following sections, we will elaborate on the IoT concepts, describe the technologies involved, and put them in perspective with work done through the Smart Grid initiatives.

Networking and data communications

Networking

The fundamental concept behind the IoT is that networks of sensors will feed data to applications in order to generate value for an organization or individual. It is generally assumed that each individual sensor will be assigned its own unique address and that the data will be transported through the public Internet infrastructure to cloud-based applications. However, if there are to be 50 billion devices directly connected to the Internet, this will require a major change in the way devices are addressed.

The Internet Protocol was originally designed as a research project and it used a 32-bit addressing space. At the time, this was not considered a problem. Furthermore, addresses were originally allocated in a wasteful manner with the result that the IP address space is now all used up and there are no more blocks of unassigned public IP addresses with IPv4, the current version of the Internet protocol.

Up to now, this limitation has not prevented the growth of the Internet, as most computers and networked devices do not require a public IP address. Instead, they use private IP addresses and access the Internet through routers that perform Network Address Translation (NAT). In addition to reducing the need for individual public addresses, NAT provides a layer of security as only the externally facing router has a public IP address and the device or computer within the private address range cannot be directly reached from the outside.

Nonetheless, the IoT vision with its 50 billion individually addressable devices is impossible without the use of an enlarged address space. A new version of the standard, referred to as IPv6, uses a 128-bit addressing space that theoretically allows 2128, or approximately 3.4×1038 addresses, more than enough for all foreseen applications.

Modern computer operating systems typically can support both IPv4 and IPv6. But, IPv6 is generally not supported by IEDs used for process control, automation, and protection. These devices are designed to perform a specific task and to meet very challenging cost and environmental requirements. The electronics used to meet these requirements provide limited computing power and memory. Furthermore, device designers focus on the device functionality and often implement only minimal communications and security functions. In the automation domain, networking technology has essentially been used to replace point-to-point wiring. Devices in a system benefit from the network to communicate with each other, but are generally prevented to reach out to the Internet.

While device vendors will eventually migrate to IPv6 addressing in the future, organizations in the critical infrastructure will most certainly continue to control and restrict access to their field devices. Security practitioners generally consider that the use of the public Internet to communicate with field devices raises serious cybersecurity and Quality of Service (QoS) concerns.

Communications

Through substation automation and Smart Grid projects, the energy sector has developed a significant body of experience on communications technology and protocols. At the substation level, communications can be characterized as device-to-device and the key requirements are reliability, low latency, and deterministic behavior. In the energy sector, the IEC 61850 standards have defined an architecture for protection devices based on the use of Ethernet networks to transport sampled values and GOOSE messages. Ethernet can provide fast device-to-device communications with support for priority and QoS. But, even with these capabilities, it remains challenged by some because of its non-deterministic nature.

SCADA/RTU applications can be characterized as device-to-server and have less stringent timing requirements than protection. In the energy sector, this is handled through protocols such as DNP3, IEC 61870-5-101/104, and IEC 61850, over a variety of LAN and WAN communication networks.

Even if it could be characterized as device-to-server, AMI applications have much less stringent timing requirements. One key differentiator is AMI control functions do not typically require a timely response. SCADA is used to control electrical apparatus and thus requires a communications infrastructure that can provide reliable and predictable behavior. On the other hand, an application such as AMI performs very few control operations. The majority of operations will consist of periodic meter readings with very few control requests for meter disconnects. AMI systems have thus typically used a large variety of communications technologies, from Power Line Carrier (PLC) to various wireless approaches, many with high latency and low bandwidth.

Most of these communications technologies are connected to the utility through data concentrators that implement a Field Area Network (FAN) and act as gateways to the utility Wide Area Network (WAN). Again, a variety of standards and protocols, including IEC 61850, have been identified and proposed through the Smart Grid initiative[5].

While energy sector device-to-device and device-to-server protocols have been well defined and are in common use, less work has been done at the level of providing standardized data to business applications. Smart Grid applications typically operate in proprietary vendor silos, even if efforts such as CIM and IEC 61850 have provided the foundations for interoperability.

Protocols

The manner in which data acquisition is performed in the Internet and in automation systems is very different. The SCADA/RTU paradigm still dominates machine-to-machine communications in automation in general. Data acquisition protocols used in the electrical sector typically use a Master/Slave or Client/Server approach. The SCADA master (client) connects to a device and periodically polls for data. Devices such as RTUs and gateways generally concentrate data from a large number of physical points, connected directly or provided by IEDs. Devices implement a slave (server) that listens for incoming connection request, sets up a communications session, and then listens for data read requests and control operations. This is the approach used by all common protocols including Modbus®, DNP3, IEC 61870-5-101/104, and IEC 61850. Modern protocols also support time-stamping, data quality, and unsolicited reporting to reduce latency and bandwidth. Once the communications session is established, the device can report changes to the data between scan operations.

All of the protocols described above have been designed to provide reliable operations under a variety of communications technologies, including low bandwidth and unreliable transports. Modern protocols also provide the capability of exporting the device points list to promote interoperability.

At the industrial level, the OPC UA protocol is replacing legacy OPC and is considered a good candidate for Industrial IoT (IIoT). This client/server protocol is no longer tied to Microsoft® Windows® OS; it provides security, supports a web-services interface and an information model, and is now defined as IEC 62541.

However, none of these protocols are used in IT, web, and Internet applications. These applications use a completely different family of protocols[6][7]. While the web uses a client/server approach, it is based on a different paradigm and the HTTP protocol that it uses is connectionless. The web browser connects to a server, sends a read or write request, and closes the connection. The web server does not keep track of connections. This approach provides scalability and allows a very large number of simultaneous clients.

HTTP and its secure version HTTPS are seeing increased use for machine-to-machine communications through the use of "web services." As a growing number of devices are adding built-in web servers for configuration and monitoring, programmatic interfaces are also being added to support access to the device's data and settings using a Representational State Transfer (REST) interface. This essentially uses HTTP/HTTPS to exchange data structured as XML or JSON messages.

Tightly coupled vs. loosely coupled architecture

The client/server approach is well adapted to automation applications, as the system architecture is well defined and very stable. The SCADA master is pre-configured with the address and points list of the RTU, gateway, and IEDs. RTUs and gateways are pre-configured with the addresses and points lists of the devices. The architecture is thus tightly coupled and all devices can securely and efficiently exchange real-time data. However, adding a new device requires an update to the system configuration.

An alternative to the client/server approach is publish/subscribe. In this type of architecture, devices publish messages in an unsolicited manner whenever they have data or events to report. A special type of server acts as a broker and manages message queues, which it organizes as topics. Client applications subscribe to topics in order to receive data. Using publish/subscribe and messages results in a loosely coupled architecture. A new device can easily be added to a system and start publishing data in a given topic. Client applications will receive the data, recognize that it emanates from a new device, and adapt their architecture accordingly. Obviously, managing a loosely coupled architecture brings its own challenges from the cybersecurity and interoperability perspectives.

The most common vision of IoT is thus for a loosely coupled network of devices and sensors that publish their data through a messaging architecture using web services and messaging protocols such as Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Data Distribution Service (DDS), and Advanced Message Queuing Protocol (AMQP). Besides AMQP, most of these protocols are not yet widely used. The AMQP protocol is used in the financial industry and supports a transactional model, making it more complex and not appropriate for edge devices. To our knowledge, none of these protocols are used in energy sector automation systems and devices.

The use of a messaging architecture has already been proposed as part of the Common Information Model (CIM) for the electrical sector and the IEC 61968 standard. The use of messaging provides a means to create a bridge between devices and enterprise applications that operate in environments with completely different requirements.

One vendor, Intel, is already proposing an IoT gateway development platform that supports a large variety of communications technologies and is provided with software that provides support for messaging protocols and security. Devices such as these may provide a means to bridge these two different environments[8].

However, in order to achieve true interoperability, it is also necessary for devices and applications to share a common data model, and this is what both IEC 61850 and CIM have done for the electrical sector.

Semantics

An important challenge of IoT will be making sense of the large amount of data produced by sensors. Vendors are promoting a vision of large numbers of devices and sensors working together to provide data to sophisticated software applications. However, in order to achieve this vision, applications will need to be able to figure out the meaning of the data, i.e., the semantics. Is the sensor reading voltage or temperature? Is the temperature in Fahrenheit or Celsius? What is the scaling factor?

In order to interoperate, devices will thus need to publish their data model, and software applications will need to configure themselves accordingly, essentially implementing a form of "plug and play."

The energy sector has a strong lead in data modeling and semantics of the "things" in the power network through IEC 61850 and the CIM. However, we can observe that the vision still has not been fully realized and that IEC 61850 provides interoperability mostly between devices from the same vendor.

Cloud computing

In the previous sections we have discussed how devices communicate and produce data to be handled by applications. The benefits promised by the IoT will be achieved through applications which provide use this data to produce valuable information. But, enterprise applications are expensive and organizations are challenged by the very high cost of deploying and maintaining these applications. Vendors are constantly evolving their applications and adding new features to keep up with market and customer requirements, but organizations simply cannot afford to keep up with rapid change. "If it's not broke, don't fix it."

One of the pillars of IoT is cloud computing, which promises to solve many of these challenges. The National Institute of Science and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[9]"

Applications that collect device and sensor data require constantly growing amounts of disk storage. Processing this data to extract valuable information and trends through advanced analytics requires extensive computing capability. Maintaining the applications and installing updates to address bugs or security issues requires IT resources that may simply not be available, even more so for smaller utilities.

Cloud computing platforms provide two types of benefits: managed infrastructure services and a software framework that simplifies the development of large-scale applications. Cloud computing builds on the virtualization capabilities of modern computer systems to provide organizations with on-demand computing and storage capabilities. Through the use of fault tolerant systems and geographically distributed data centers, it can ensure high availability. Most importantly, it ensures that updates and patches can be applied in a timely manner. Cloud computing offers a variety of service models in order to meet different use cases: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Utility applications such as SCADA, DMS, EMS, and FLISR are critical to utility operations, as they operate remote devices that manage the transmission or distribution power system, part of the critical infrastructure. These applications thus have very demanding reliability and security requirements and are generally deployed by utility IT teams in highly secure utility data centers. Cybersecurity frameworks and standards such as NERC CIP require that system operators implement auditable security controls. While deploying and maintaining applications within the utility's data center is more expensive, it provides the utility with fully auditable control on who can use the applications and how access to the data and devices is managed.

Vendors of cloud computing argue that they can provide a level of security that meets all applicable requirements. However, by deploying an application in the cloud, the utility IT and cybersecurity teams become dependent on a third party, and lose part of their control.

Nonetheless, the cloud can provide significant benefits that may outweigh the loss of control for less critical applications and organizations. It can also provide smaller utilities with access to applications that they could not afford to use otherwise.

Utilities may benefit from cloud-based solutions without compromising on security through the use of a multi-layered approach and private clouds. They may choose to manage their own internally hosted data acquisition applications to collect data from their own private network of devices, and use some type of gateway application to push the data to a cloud-based application for processing.

Cybersecurity

Cybersecurity needs to be a fundamental characteristic of the IoT. Nonetheless, security practitioners generally see the IoT as a catastrophe in happening. The vision of 50 billion devices connected to the public Internet raises serious concerns about the widespread distribution of malware, large-scale botnets, and Distributed Denial of Service (DDOS) attacks[10].

Researchers constantly expose vulnerabilities in embedded devices, cars hijacked through their network of built-in computers, compromised pacemakers and insulin pumps, and botnets built out of smart TVs, to name a few. Cybersecurity practitioners blame this state of things on the fact that device manufacturers are focused on delivering product features and still have very limited security skills.

The IEEE P2413 working group has formed a sub-working group to address cybersecurity and realizes the Quadruple Trust: Protection, Security, Privacy and Safety. The group has already identified security in depth as a key principle[4].

Again, the energy sector benefits from a head start. From the very beginning, cybersecurity was a key requirement of the Smart Grid initiative and significant efforts have been invested in defining requirements that have been formalized in reports such as the NIST 7628 Guidelines for Smart Grid Security. While these guidelines do not address the IoT per se, they do define the cybersecurity requirement for applications in the energy sector, from generation plants to customer premises. Furthermore, many utilities are required to meet the NERC CIP cybersecurity standards and have thus acquired valuable experience in protecting their assets. Essentially, critical assets must be isolated in secure network zones and network traffic between zones must be restricted to authorized and authenticated entities; hence, the necessity for a layered defense in depth architecture.

Achieving the NIST Quadruple Trust of Protection, Security, Privacy and Safety will require the use of cryptography with all the key management challenges that this raises. The increasing availability of distributed on-demand computing resources raises concerns that encryption keys could be broken through brute force attacks, requiring the use of even stronger keys, and hence more powerful devices. Again, the solution may also reside in isolating devices in private networks.

Managing the device lifecycle

As the author has discussed in a previous paper[11], the management of networked devices continues to be a challenge that needs to be addressed. Developing applications and strategies to support the complete device lifecycle is a necessity in order to reduce the Total Cost of Ownership (TCO) of all these connected "things". Currently, many of the operations from provisioning, to commissioning, updating, and disposal, still need to be performed manually, by highly qualified personnel.

The IT world on which the IoT is being built has a strong lead in this area. Vendors of networking devices offer Network Management Software (NMS) to support their devices. However, this type of software is generally designed to support devices from a single vendor, and which perform very well defined functions. Efforts are being made to define standard interfaces through which devices can publish their capabilities and be programmatically managed. However, the development of a universal management platform remains a challenge, and may not even be economically feasible.

Conclusion

In this paper we have tried to provide an overview of some of the technologies that are being used to implement the IoT and how this relates to efforts already underway in the energy sector.

The IoT is here to stay. Referring to the Gartner Hype Cycle, we can state that the IoT vision was triggered by the widespread adoption of the Internet and the multiplication of connected devices based on a common networking technology. The IoT is thus now at the "Peak of inflated expectations" phase. All major vendors in the industrial and electrical sector are now launching IoT initiatives and promoting their vision.

We have seen how the IoT ties in naturally to efforts already underway in the energy sector. Devices and sensors are being deployed in large numbers to help manage the power infrastructure. While these devices will most probably never be networked through the public Internet, their data can be structured and modeled using IEC 61850 and CIM, and exchanged at the enterprise level using messaging technology and web services. Advanced software applications can be developed by leveraging the functions provided by cloud-based platforms in order to provide utilities with valuable information to optimize their operations. However, these solutions will most probably be based on private clouds, with a subset of the data made available to the public through secure web interfaces and web services–based APIs.

References

1. Internet of Things, Wikipedia, retrieved from https://en.wikipedia.org/wiki/Internet_of_Things
2. D. Evans, "The Internet of things: How the next evolution of the Internet is changing everything," Cisco Internet Business Solutions Group (IBSG), White Paper, April, 2011. Retrieved from http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
3. IEEE, "Towards a definition of the Internet of Things (IoT)". Retrieved from http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf
4. Oleg Logvinov, "Standard for an Architectural Framework for the Internet of Things (IoT) IEEE P2413" Retrieved from https://grouper.ieee.org/groups/2413/Intro-to-IEEE-P2413.pdf
5. V. Cagri Gungor et al., "A Survey on Smart Grid Potential Applications and Communications Requirements", IEEE Transactions on Industrial Informatics, Vol. 9, No. 1, February 2013.
6. Stan Schneider, "Understanding The Protocols Behind The Internet Of Things", Electronic Design, Oct 9, 2013. Retrieved from http://electronicdesign.com/iot/understanding-protocols-behind-internet-things
7. Aron Semle, "IIoT Protocols to Watch", Automation.com, October 26, 2015. Retrieved from http://www.automation.com/library/white-papers/iiot-protocols-to-watch
8. Intel Gateway Solutions for the Internet of Things. Retrieved from http://www.mcafee.com/ca/resources/solution-briefs/sb-intel-gateway-iot.pdf
9. P. Mell, T. Grance, "The NIST Definition of Cloud Computing". Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
10. The Economist, "In the nascent "Internet of things", security is the last thing on people's minds". Retrieved from http://www.economist.com/news/science-and-technology/21657766-nascent-internet-things-security-last-thing-peoples
11. Jacques Benoit, "Managing the Smart Grid Building Blocks", Proceedings of the Power and Energy Automation Conference, March 2014, Spokane, WA.
12. The Gartner Hype Cycle, retrieved from http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Publication No. WP152016EN / Z18183
May 2016

Powering Business Worldwide