Bringing Enterprise IoT to Cable

A Technical Paper prepared for SCTE•ISBE by

John Jason Brzozowski
CTO, Vice President Engineering
MachineQ, a Comcast company
1800 Arch Street, Philadelphia, PA 19103
+1-484-962-0060
john_brzozowski@comcast.com

Table of Contents

Title **Page Number**

1. Introduction

Cable infrastructure is at the heart of voice, video, and Internet services. Subscribership across classic cable services has been evolving rapidly across our ecosystem, which prompted MSOs to invest in the development of new products and services that help enable diversification and initiate new subscriber growth.

As such there is burgeoning demand for enterprise class, wireless-based IoT platforms to enable operators to expand their product and service offerings to address the needs of the enterprise, SMB, B2B2C, and even the consumer market segments. Enterprise IoT platforms in particular are essential to enable adoption, when new, disruptive technologies are involved. The availability and use of DIY (Do-It-Yourself) or BYO (Bring-Your-Own) to support the large-scale enterprise IoT deployments is proving to be challenging, if not an impediment. Forcing or expecting adopters to locate, validate, deploy, and manage all the critical components, securely, slows adoption and inevitably growth. Further, Enterprise IoT platforms are particularly important when adopters require the ability to manage IoT offerings across multiple media, wireless or otherwise. As the IoT landscape evolves beyond devices that leverage broadband connections, facilitating the deployment of and offering a seamless, streamlined customer experience is difficult if not impossible if an operator is relying on a swivel chair approach. Enterprise class IoT platforms must offer the ability to manage the deployment and operations of a vast, virtual IoT network that span multiple geographic regions. A purpose built enterprise IoT platform must truly be an enabler of mission critical use cases across a wide range of verticals.

The vision outlined here is one that envelops the following:

- An Enterprise IoT Platform that enables global adoption and enablement
- Spans multiple media, mainly wireless
- Illustrates the need for scale and performance
- Couples in enterprise-class functionality
- Leverages best in class security

The vision components listed above are the core characteristics of any enterprise IoT platform that intends to fuel adoption and operation at scale, while enabling a broad base of market verticals -- from Quick Service Restaurant (QSR), to asset tracking pharmaceutical manufacturing and laboratories, all while spanning the use of multiple wireless media including LoRAWAN, BLE/Bluetooth, and others. Supporting multiple connectivity methods helps to uniquely address each vertical's specific challenges and operating environments.

The world is changing for MSOs, and so is the definition of IoT. More specifically, Enterprise IoT. How we plan for and build to support, manage, and operate Enterprise IoT is rapidly evolving, in lockstep with the demands set forth by our customers. These requirements range from touchless, automated solutions to enable temperature/humidity monitoring and high value asset tracking, to energy monitoring and management for cable infrastructure.

2. Definition of Enterprise IoT

The IoT (Internet of Things) carries a wide range of meanings and the term continues to evolve on practically a daily basis. For the purposes of this document, IoT will generally refer to the act of connecting or enabling the connection of a device to utilize the Internet or network, with the intent of interacting with a human or consumer. Or, according to Oxford Languages:

"The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data." [1]

Conversely, Enterprise IoT refers to the enabling of machines to interact and exchange data with other machines in a manner that may or may not be usable by a human. Further, the machines in the case of Enterprise IoT are not strictly required to have a direct connection to the Internet. However, the machines may leverage other elements to facilitate communications.

The Enterprise IoT is viewed by some [2] as the "next advancement in technology that enables physical 'things' with embedded computing devices (tiny computers) to participate in business processes for reducing manual work and increasing overall business efficiency."

An example of consumer-grade IoT, generally, is a video camera connected to the Internet or home network using Wi-Fi via a broadband connection that supports two-way video and audio. Whereas, Enterprise IoT is best exemplified by a wireless (not necessarily Wi-Fi) temperature and humidity sensor that transmits data periodically from multiple locations in a QSR to automate food monitoring. The bandwidth, connectivity model, wireless characteristics, and power consumption vary widely across these and numerous other scenarios.

3. Wireless Communication Considerations

Not all wireless communication protocols are created equal, nor do they need to be. Further, it should not be expected that a single wireless communication protocol be able to universally address every technical and/or business use case. Each form of wireless communications carries its own distinct pros and cons. A summary is provided here, as an in-depth compare-and-contrast of IoT wireless protocols is beyond the scope of this document.

3.1. 2.4 GHz

Wi-Fi, BLE/Bluetooth, Zigbee all commonly support wireless communications using the 2.4 GHz frequency band. Characteristics include:

- Capable of high bandwidth, two-way communications
- Limited range, limited mobility
- Reasonable propagation for short range wireless communications
- Higher power consumption

3.2. Cellular

- Capable of high(er) bandwidth, two-way communications
- Extend range and mobility
- Reasonable propagation
- High power consumption

3.3. ISM (Industrial, Scientific and Medical) Bands

- Capable of low bandwidth, limited two-way communications
- Extended range, mobility support varies
- Optimal propagation for long range wireless communications
- Low power consumption

Given the nature of this document the above focuses on the technical considerations for each type of wireless communications protocol. Cost, while of out scope, is most certainly an essential detail that must be factored into any wireless protocol evaluation.

4. Enterprise IoT Platform

Most every wireless communications platform consists of one or more of the following:

1. Wireless devices including sensors or endpoints that typically send and/or receive data
2. Wireless base stations or gateways that enable or facilitate communications to and from wireless devices or remote systems
3. Wireless controllers and related sub-systems that govern the wireless communications between wireless devices and base stations

Common misconceptions suggest that one or all of the above adequately provide the tools required to enable Enterprise IoT for an operator or adopter. In fact, regardless of the wireless communication chosen, the attributes listed above only provide the building blocks to enable basic wireless communication for an Enterprise IoT environment. A platform approach supporting any form of wireless communication must minimally account the following:

- Heterogeneity regarding wireless communications as well as from a device and base station perspective
- Operationalization including measurements and monitoring ensuring service quality and reliability

The following sections further delve into key factors that must be considered when evaluating and/or building a platform oriented for wireless, enterprise IoT.

4.1. Integration

Deep integration is essential to ensure the effectiveness of any platform that will effectively be utilized to manage large scale, complex deployments. While integration with internal operational support systems (OSSs) and business support systems (BSSs) is critical, the context here refers to integration with the core hardware elements that truly enable large scale adoption. Wireless communication integration can occur in multiple ways.

First and most common is adherence to a common wireless communication standard. In the case of LoRAWAN® [3], this would imply that a given device or sensor, gateway or base station, and LoRAWAN Network Server (LNS) have all implemented compatible versions of the communication specifications. Compliance at this level simply ensures that elements that are attempting and expecting to interact, can do so.

Alternatively, deeper integration across this confluence of key elements -- where software meets the embedded systems (or hardware) -- affords adopters a “surgical” level control and flexibility. Both matter to confidently, reliability, and seamlessly managing enterprise IoT deployments. This inevitably requires that some form of a platform’s software components reside natively on critical embedded systems. Embedded system integration, in this case, specifically refers to the integration of platform functionality that spans sensors as well as base stations.

4.2. Security

Credible enterprise IoT platforms must tout the ability to secure communications end-to-end. While many of the individual elements available today that can be used as piece parts to orchestrate an enterprise IoT deployment are secure, component-level security does not assure that the concatenation of those elements carries the same level of end-to-end security. Nor does this guarantee that critical aspects have not been overlooked. End-to-end visibility across an entire platform provides security assurance specific to data integrity and communications. Data integrity ensures that the data received is, in fact, the data that was sent, while data communications ensures that the transport mechanisms carrying the enterprise IoT data in uncompromised. Further, control of data encryption by the originator (or customer) from a sensor that is independent of transmission or delivery (by an operator) extends a level of independence that secure, trusted enterprise IoT platforms are expected to support. The capability to securely provision sensor communications while maintaining trust must not be overlooked.

In order to maintain the integrity and value that a secure wireless communications protocol affords it must be coupled with a platform that directly enables its streamlined use. Manual configuration and "swivel chair operations" create process gaps that inevitably result in security challenges.

4.3. Management

Enterprise IoT management, broadly speaking, builds strongly but not solely on the concept of integration and is the backbone for security. The depth of integration is directly proportional to an organization's ability to manage key aspects of their Enterprise IoT deployment. Key considerations include:

- Remote, over-the-air firmware management for both sensors and base stations
- Security management and monitoring
- Configuration management for wireless IoT communications
- Base station backhaul connectivity and configuration management

In a world where new vulnerabilities and viruses are discovered on practically a daily basis, the ability to remotely update your IoT infrastructure on a scheduled, automatic basis is essential to ensuring that your deployment is robust. Updating firmware and configurations over the air (or over any backhaul network) can be a complicated affair. Further, with the rapid evolution across the wireless communication spectrum, where the likes of 5G, Citizens Band Radio Service (CBRS), and Narrowband (NB) IoT are becoming a reality, it is perhaps a forgone conclusion that adopters will require a unified platform to enable the management across any and all wireless communication protocols.

Finally, where adopters are choosing LPWAN alternatives like LoRAWAN, given its favorable performance characteristics over long distances, superior propagation, and optimal power consumption, there are in fact bandwidth considerations that must be accounted for from a management perspective. Namely, facilitating firmware updates over the air for LPWAN must be implemented diligently. In an Enterprise IoT sense, diligence means leveraging partial or delta updates in lieu of full image updates, as a means to dramatically reduce update times, positively impact power consumption, and improve hardware life expectancy.

4.4. Performance

An enterprise IoT offering that cannot perform well impedes adoption and growth. The advent of inexpensive, battery powered devices that can last for 5 to 10 years (or more) introduces many new performance challenges. The need to provision large volumes of inexpensive devices with a lengthy lifetime translates into millions if not billions of sensors that need to be managed over time. This includes high performance provisioning to support rapid deployments and the processing of data from the same. Processing data from an exponentially growing population of enterprise IoT sensors has the potential to yield billions of data payloads -- daily.

Succinctly put, solving problems, creating value, and generating revenue are tightly coupled with the rate at which sensors and base stations can be provisioned and deployed. One of the main purposes of any high-performance enterprise IoT platform is to enable the currency of enterprise IoT, data, to flow as quickly and in as timely a manner possible. The frequency of data transmissions is often a byproduct of the market vertical or use case.

Essential characteristics related to Enterprise IoT performance include:

- Web-scale Application Program Interfaces (APIs) and backend implementations that support large volumes of provisioning events that enable sensors instantaneously
- Intuitive user interfaces allowing for streamlined, high-performance management
- Carrier-grade base station performance and sensor data processing ensuring that payload delivery performance is optimize globally

4.5. Scale

Global scale and locally optimized performance and resiliency are absolute musts for modern day enterprise IoT adopters. Enterprise IoT adopters today have different characteristics and requirements than consumer IoT adopters. Enterprise IoT adopters are multi-national, global corporations that are seeking to form partnerships and build relationships with similarly-sized firms that are able to service their needs around the globe, not just in one region specifically. The scope of scale reaches far beyond, but is anchored in, the scale and performance of an enterprise IoT platform. Scale encompasses service (installation, deployment, etc.), support, and global capacity.

Global scale is, in many ways, a culmination of the characteristics outlined throughout this document. Assembling a platform and business to address the evolving needs of enterprise IoT adopters globally starts with borrowing from the experiences in scaling other businesses, including Internet, voice, and video. Scaling Enterprise IoT, while sharing many similarities with scaling some of the largest data, voice, and video networks in the world, carries many unique nuances. Most Enterprise IoT platforms and networks are designed to support enormous volumes of small payloads originating from sensors across a large heterogenous (global) customer base. Further, ensuring that base stations, which route the lifeblood of most LPWAN networks, have robust, reliable backhaul is essential to every enterprise IoT deployment.

5. Conclusion

Orchestrating a large-scale Enterprise IoT deployment is a complex endeavor. Choosing which wireless communication protocol(s) best address requirements alone is a complex task. Identifying or building a platform that enables an organization to manage it globally increases the sophistication, timing, and investment. Factoring in carrier-class scale, performance, and best-in-class embedded systems like sensors and base stations is also critical to any well-intentioned plan. Ensuring that all embedded systems are qualified regionally, and that all regulatory guidelines are adhered to, are significant tasks.

It is important to not discount the effort involved in operationalizing the use of Enterprise IoT to generate revenue or accelerate cost savings across your own or your customer's enterprise. Implementing an enterprise IoT solution for temperature and humidity monitoring across thousands of locations, globally, or leveraging it to deploy advanced power management and analytics across cable networks for an MSO, are both real and valid use cases. Discounting the need for and the investment required to build a robust, globally scalable multi-wireless media enterprise IoT platform will impose substantial limitations. Limitations that will impact an operators ability to deliver a reliable, future proofed service that will fail to comprehensively and proactively addresses their customers' requirements. Customers' whose revenue relies on you and yours on them.

Abbreviations

MSO	Multiple Services Operator
SMB	Small/Medium Business
B2B	Business to Business
B2B2C	Business to Business to Consumer
IoT	Internet of Things
BYO	Bring Your Own
DIY	Do It Yourself
QSR	Quick Service Restaurant
LNS	LoRAWAN ® Network Server
OSS	Operations Support Systems
BSS	Business support systems
5G	5th generation mobile network
CBRS	Citizens Broadband Radio Service
NB IoT	Narrowband Internet of Things

Bibliography & References

[1] Oxford Languages

[2] http://www.enterox.com/IoT/articles/enterprise-internet-of-things.htm

[3] https://lora-alliance.org/about-lorawan

LoRaWAN® Specification v1.0.2; LoRa Alliance®

LoRaWAN® Specification v1.0.3; LoRa Alliance®

LoRaWAN® Specification v1.1; LoRa Alliance®

What is the LoRaWAN® Specification?; LoRa Alliance®

