JANUARY 2019

FOR PROFESSIONALS MANAGING THE CABLE AND WIRELESS SYSTEMS THAT ENABLE CRITICAL COMMUNICATIONS

Cabling Installation & Maintenance®

WHAT CAN WE DO ABOUT IoT security?

PAGE 5

PRODUCT PREVIEW PAGE 22

A sneak peek at BICSI's show floor

INSTALLATION PAGE 11

Indoor/outdoor cable

DATA CENTER PAGE 15

Multimode: Wavelengths and opinions divided

www.cablinginstall.com

PennWell®

The practical IoT

Planning and designing for the arrival of the Internet of Things.

BY ART KING, Corning

Much has been written about the Internet of Things (IoT) over the last few years, discussing both the explosive growth projections in the number of attached devices and the anticipated value to global business that they will bring. The growth projections alone are staggering. From the chart in this article, you can see that the numerical growth from 2018 to 2019 is 3.52 billion IoT devices globally.

This quantifies what will be asked of IT networking and systems integrators to help attach these devices to various networks, their potential impact, and developing planning guidelines. In the balance of this article, we'll focus on what's important to networking professionals as our business customers ask us to add IoT devices to the infrastructure landscape.

To begin, let's define IoT. IoT is not the desktops, laptops, and tablets we use every day. In general, IoT is the collection of networked devices/applications that are not used by humans, also known as machine-to-machine communications or M2M. They can be sensors that send information, controls that can take action, or both. The devices can operate in homes, office buildings, warehouses, or outdoors from city streets to agricultural fields.

Most IoT devices are standalone and are optimized for their intended usage. To attach an IoT identity to a person, because our smartphones are a "digital mirror" of the owner, there are apps that represent us in the digital space and interact with companion IoT infrastructure. For example, a banking app can be detected when a consumer enters the branch, and the experience with the staff is tailored to them. Finally, there are many apps installed in smartphones that are essentially roving sensors collecting data for much larger IoT platforms.

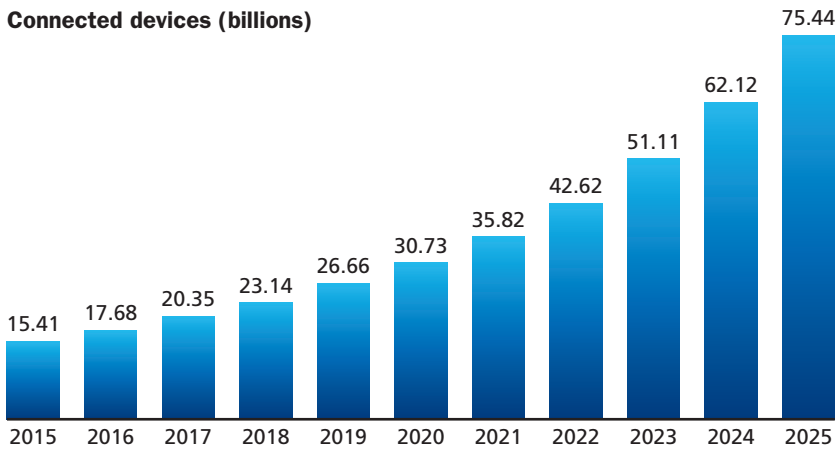
In the infrastructure role of most enterprises, IoT projects will eventually be brought to networking teams by the business units interested in adopting them.

For any IoT usage, there are a few common infrastructure questions to consider:

1. What are the network requirements?
2. Is it "mission critical" to the business?
3. Who manages it?
4. What's the correct security posture?

Network requirements

There is a significant number of network technologies supported by IoT vendors. IoT vendors will offer the best network technology for their systems, ranging from an Ethernet cable down to wireless low-power wide area (LPWA) service. Since IoT devices ultimately connect to an application, the data traffic from the IoT devices will



This market projection from Statista indicates the staggering expected growth in worldwide connected devices through 20215. From 2018 to 2019 alone, the growth will be 3.52 billion devices.

Reprinted with revisions to format, from the January 2019 edition of ***CABLING INSTALLATION & MAINTENANCE***.

travel over an IP network, either private or the Internet, to servers in the enterprise data center or in a cloud service like Amazon AWS or Microsoft Azure.

For every network type, planning is necessary to understand the IoT connectivity needs are fully satisfied.

In planning and budgeting for IoT, the business that is bringing in the service should be budgeting for all expenses necessary to prepare for them. Network assessments of the target networks are used to develop the additional network improvement budget requirements.

Network design considerations:

- Wired Ethernet could require separate Ethernet switches if the IoT devices are unmanaged or connect to an external cloud service.
- WiFi could require a different SSID and authentication method than what is presently in use.
- WiFi engineering assessment for more access points may be required to increase network coverage.
- Cellular coverage assessment on IoT device's service provider/frequency band throughout the enterprise may be necessary to insure network coverage.
- Cellular IoT checks coverage and that the installed base station supporting indoor signal supports the NB-IoT protocol.
- Attempt LPWA network trial connection to insure LPWA network availability before installation.

IoT can influence IT network goals. For many enterprises, there are economic benefits to architectural convergence of many physical networks onto individual logical network slices sharing the same physical network; yet, each network slice is not connected to or aware of other slices. This design trend is driving an enormous amount of fiber-optic cable being pulled farther towards the edge of networks to enable this "fiber-deep" strategy. How and where IoT leverages it can affect the implementation costs. Please note, we used network slices here as it is an emergent term in 5G that describes logical network separation.

TABLE 1. IoT use cases and network types

Application	Network Type	Traffic Volume	Comments
Vending machine	WiFi	Low	Unmanaged, not important to enterprise
Security camera	Ethernet cable	High	Managed by security
SCADA PLC	Optical Ethernet	Low	Managed by enterprise, mission-critical
Asset tag	Cellular or WiFi	Low	Unmanaged, important when locating asset
Industrial robot	Cellular	Medium	Managed by enterprise, mission-critical
Ankle bracelet	Cellular IoT	Low	Unmanaged
Field rainfall collector	LPWA	Low	Unmanaged

Mission critical

Industrial IoT applications in manufacturing and distribution centers are considered mission critical. In both of these application areas, the interest in replacing wired cable to robots, programmable logic controllers (PLCs), and other networked manufacturing equipment with wireless services is very high.

Wireless enables flexible configurations of the distribution center's internal conveyor belts that have wired control networks today. High-speed inventory switching is very time-sensitive and requires the high level of network guarantees provided by LTE/5G. Cellular provides time-bound responses, fair access, and quality of service controls.

Wireless enables flexible configurations where the manufacturing line can be reconfigured without the need to restructure wired control networks. Industrial robots that are constantly in-motion and wear out control wiring can have reduced downtime by using LTE/5G for robotic command and control.

Because the downtime in these environments is costly, private LTE or 5G is used to replace the cabling. Private LTE/5G networks are designed to be predictable and don't use public cellular because of the enterprise need for total end-to-end management. When designing IoT networks for these applications, the private LTE/5G network features redundancy in key areas, well-engineered coverage throughout the facility, and the necessary capacity to support the demands.

Management

In the industrial cases just mentioned, IoT is managed by the enterprise. In other applications, the enterprise has IoT devices distributed across the enterprise that connect to a cloud service that the enterprise can log into. In these cases, there is no management responsibility for the service, but there is a requirement to ensure there is adequate network coverage to support IoT devices anywhere they operate in the enterprise.

For example, every clinical device in a hospital or medical campus may have a built-in wireless module for both locating and transmitting patient data. In many cases, WiFi networks can be used to support these needs, but outdoor needs or clinical devices that accompany first responders will support cellular services. In all these cases the IoT will be managed internally to insure patient data-privacy regulations under the Health Insurance Portability and Accountability Act (HIPAA).

Security posture

Unmanaged IoT can pose a threat to enterprises where they use the

enterprise network to connect to their supporting cloud service.

Examples for your consideration:

- Over 100,000 refrigerators were hacked to form a bot-army in 2014 *(Source:* The Hacker News*).*
- 140,000 security cameras and DVRs were hacked to form a bot-army in 2016 (Source: Security Ledger).

All these devices were behind DSL modems, but they were still hacked. Imagine that they were installed on the enterprise network and were connected to the bot army command/control server. What could happen to the inside of the enterprise network in these cases?

Best practices for any devices that are not actively managed by enterprise IT is to never allow them on the enterprise network. This can be done with Ethernet VLANs and multiple WiFi SSIDs technology to create multiple logical network slices sharing the same physical network.

In high-security enterprises, the network policy could override creation of a network slice for IoT and require the creation of a parallel physical network to ensure total segregation.

CBRS is around the corner

In the U.S., the FCC has developed a revolutionary method for enterprises to access cellular spectrum that is called Citizens Broadband Radio Service (CBRS). CBRS sets aside 150 MHz of radio spectrum for use by anyone. CBRS-capable infrastructure requests radio spectrum from a cloud service for use by the enterprise. This access method enables enterprises to build their own private LTE in a building or geographic area without negotiating leased access to radio spectrum from a service provider. Private LTE and, eventually, private 5G offer all the benefits of secure and mission-critical communications while allowing the enterprise the total control required in industrial IoT use cases.

CBRS is close to launching in the U.S., and over the next few years most smartphones and IoT devices are expected to feature CBRS-capable radios. Many enterprises are planning today for CBRS. Information about CBRS can be found at cbrsalliance.org.

The wave of IoT devices and services will drive incremental expansion and capacity increases to existing networks and, in some cases, the creation of segregated IoT overlay networks. Network teams in the enterprise and their systems integrators will be asked to design and plan for the arrival of these IoT devices and networks. A variety of IoT applications may use almost any type of wired and wireless connectivity.

Mission-critical IoT applications will be built and operated by the line of business due to their importance and will open new career opportunities for enterprise IT people. It is a "ground-floor opportunity" to join the transformation. ◆

Art King *is director of enterprise at SpiderCloud Wireless Inc. Corning Inc. acquired SpiderCloud Wireless in 2017. Corning offers innovative connectivity products from optical transport, cellular signal sources, to cellular distribution.*