Building a gateway from the sensors to the cloud

Texas Instruments

Dung Dang,
SimpleLink™ MSP432™ MCUs
Texas Instruments

Punya Prakash,
SimpleLink™ MSP432™ MCUs
Texas Instruments

By 2025, the Internet of Things (IoT) will comprise as many as 75 billion connected things according to IHS Markit. The IoT market evolution has consistently drawn parallels to the growth of the PC and cellphone markets in late 1900s and 2000s.

Although those markets evolved over time, the foundational requirements were crisp – that is not the case with the dynamic and heavily fragmented IoT space. New connectivity standards continue to emerge with no convergence in sight, while legacy systems with a decades-old infrastructure consisting of mostly wired protocols need retrofitting to interoperate in the new IoT space.

Despite the wild, Wild West of connectivity standards, the number of edge nodes (the things in the IoT) will multiply with a mix of smarter and more intelligent sensors and actuators to benefit the entire ecosystem, including end customers, service providers and original equipment manufacturers (OEMs). In industrial systems, for example, end equipment can communicate with remote sensors, other end equipment and a centralized management console to improve reliability and productivity.

The complex communication standards required to aggregate and connect these sensors to the internet represent the greatest barrier to realizing this +75 billion-unit market, **Figure 1**. The path to creating a ubiquitous cloud requires that devices with varying communication protocols connect and cooperate without full Ethernet, or a Wi-Fi® interface with an accompanying protocol stack. Gateways that bridge devices from local area network (LAN) connectivity out to an internet-connected network

***Figure 1**. Intelligent gateway can help manage and connect the 75 billion edge nodes to the cloud.*

of servers can make this a reality. A gateway can integrate IoT agents to interact with cloud servers via standardized protocols as defined by cloud service providers. In addition, adding intelligence to gateways can simplify IoT device design by providing access to shared processing resources.

While smarter sensing drives the volume behind the IoT trend, this white paper focuses on solving the infrastructure challenges associated with connecting more than 75 billion edge nodes to the cloud by introducing a smart industrial gateway concept. With a robust and interoperable gateway solution, IoT developers can spend more energy differentiating their IoT solutions.

The connectivity challenge

IoT technology has advanced in industrial applications because of the value gained in connecting end equipment for automation, system reliability and centralized management. This progression is evident across different industrial sectors, including both residential and commercial heating, ventilation and air conditioning (HVAC) and building security systems and factory automation and grid infrastructure energy-measurement and monitoring networks.

The greatest challenge in designing for the IoT is connectivity. Implementing robust and secure access to the internet or wide area network (WAN) is outside many designers' experience range. To complicate matters, developers need to support access to multiple devices that are limited in their processing capability and add connectivity in a way that does not adversely impact overall system cost or power efficiency.

The diversity of end points that a gateway must support raises design concerns as well. Directly connecting a simple node like a pressure sensor to the internet can be complex and expensive, especially if the node does not have its own processor. And because different types of end equipment support different interfaces, the collection and aggregation of data from a disparate set of nodes requires a way to consistently and reliably bridge devices with a range of processing capabilities and interfaces.

Gateways offer an elegant way to simplify the networking of "things" by supporting the different ways that nodes natively connect, whether that's a varying voltage from a raw sensor, a stream of data over Inter-Integrated Circuit (I^2C) from an encoder or periodic updates from an appliance via *Bluetooth*®. Gateways effectively mitigate the variety and diversity of devices by consolidating data from disparate sources and interfaces and bridging them to the internet. The result is that individual nodes don't need to bear the complexity or cost of a high-speed internet interface in order to connect.

Figure 2 shows several ways that an industrial gateway can extend connectivity to nodes. In **Figure 2a**, nodes connect to the cloud through a gateway. The nodes themselves are not Internet Protocol (IP)-based and thus cannot directly connect to the internet/WAN. Rather, they leverage existing wired or new wireless technology to connect to the gateway with a cost-effective and

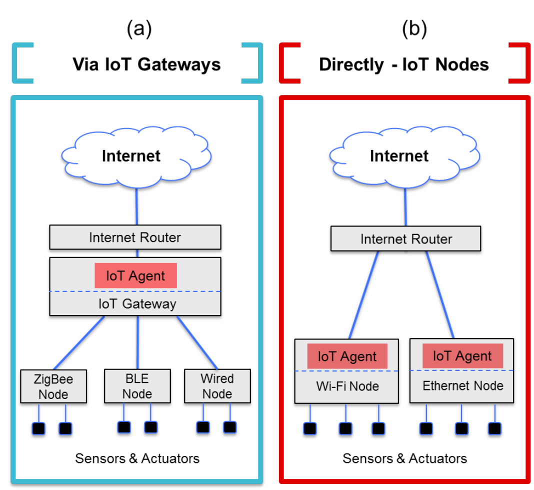

Figure 2. *An IoT gateway can simplify connectivity design for sensor nodes by centralizing IoT functionality in the gateway. Nodes connect to the IoT via a gateway using both wired and wireless technology (a); nodes connect directly to the internet using a WAN connection such as Wi-Fi or Ethernet (b).*

less complex mode of connectivity. The gateway maintains an IoT agent for each node that manages all data to and from nodes. In this case, application intelligence can also be located in the gateway.

In **Figure 2b**, nodes connect directly to the internet using a WAN connection such as Wi-Fi or Ethernet. The gateway serves primarily as a router; in fact, it can actually be a router where the nodes have their own IoT agent and autonomously manage themselves.

Traditional versus intelligent gateways

There are several ways to implement an industrial gateway, depending on the application. Two common approaches are a traditional gateway and an intelligent gateway. Both provide consolidated connectivity by aggregating data from multiple end points. In general, a traditional gateway organizes and packetizes data for transport over the internet. It is also responsible for distributing data back to end points in applications where two-way communications are advantageous or required.

Note that a gateway is different from a router. A router manages similar traffic and connects devices that share a common interface. For example, devices that connect to a home router all use IP. In contrast, because a gateway functions as a bridge, it must be able to route different types of traffic, aggregate data from varying communication interfaces and convert these streams to a common protocol for access across the WAN. Some devices might use IP natively, such as Wi-Fi or Thread, while others might use non-IP-based protocols such as *Bluetooth*® or various Sub-1 GHz protocols. Nodes that are sensors may need to leverage high-precision analog-to-digital conversion (ADC) to convert the raw analog voltage to a digital value before transport.

An intelligent gateway extends the functionality of a traditional gateway by providing processing resources and intelligence for handling local applications. This can take the form of shared processing resources where the gateway performs tasks that would otherwise occur on nodes. For example, an intelligent gateway could evaluate and filter sensor data as well as implement high-level management tasks. For example, after evaluating and filtering sensor data, a gateway could determine the crossing of a critical threshold and trigger an alarm, which is then passed up through the network to alert an appropriate manager.

Having an intelligent gateway can reduce the complexity – and cost – of edge nodes. Consider a security system connected to an array of sensors. Consolidating processing in the gateway enables edge nodes to leverage a shared resource, reduce local processing time and active power consumption, and ultimately increase battery life and save cost.

The same principle holds for enabling connectivity. IP is a complex protocol to implement, with relatively high overhead for more simple IoT nodes. Instead, simple nodes can connect to a LAN using a wired connection such as RS-485 or I^2C, or a wireless interface like *Bluetooth*®. The gateway also connects to a personal area network (PAN) and then bridges each connection to an IP-based WAN interface like Wi-Fi or Ethernet. In both of these cases, savings include lower processing, memory and power requirements. Nodes can be less expensive, as well as more efficient.

Distributed intelligence also accelerates the implementation of new applications.

Enabling intelligence in a gateway addresses interoperability issues on a local level while minimizing the changes required to retrofit existing systems. Instead of requiring full intelligence in each edge node, the gateway can offload some of the heavy lifting and number-crunching. The gateway can also analyze harmonized data from various edge nodes to drive more intelligent decision-making. A gateway can serve as a fabric between co-located nodes when internet access is lost or temporarily interrupted. Ensuring robust local connectivity without the cloud increases the reliability of the local network to maintain its intended functions.

Adding intelligence to the gateway offers another advantage: consolidating management of new features for operators. Rather than integrating and maintaining each edge node individually, technicians and operators can leverage gateways and systems such as a building management system (BMS) for centralized network management. An intelligent gateway also better addresses the issues that arise from connecting disparate nodes, compared to users manually connecting each edge node to the internet.

For many applications, an intelligent gateway can eliminate the need for a dedicated on-site management or control end point. For example, with an integrated liquid crystal display (LCD) controller, a gateway can support a user interface that enables users to directly interact with nodes. Alternatively, an intelligent gateway can provide a web-based user interface – accessible through a PC, tablet or smartphone – through which users can easily access additional built-in applications. Thus, the gateway can serve as a flexible and dynamically programmable on-site control point, lowering the installation cost of new systems and enabling third parties to introduce new technology and devices with a significantly lower cost of entry.

Merging wired and wireless connectivity: the SimpleLink™ MSP432E4 Ethernet MCU

With all of the complexities tied into creating an intelligent gateway to meet a wide range of connectivity and industrial requirements, developing a robust and interoperable gateway can appear to be a daunting task. It could take several months or quarters to design and build a gateway and software infrastructure to include security, complete application programming, adapt to currently deployed systems, enhance with new connectivity protocols, and integrate with edge nodes and the cloud.

With the SimpleLink MSP432E4 Ethernet microcontroller (MCU) (explained in **Figure 3**) and the SimpleLink software development kit (SDK), developers can accelerate their intelligent gateway design by harnessing its advanced integration, wireless connectivity plug-ins and unified tool chain.

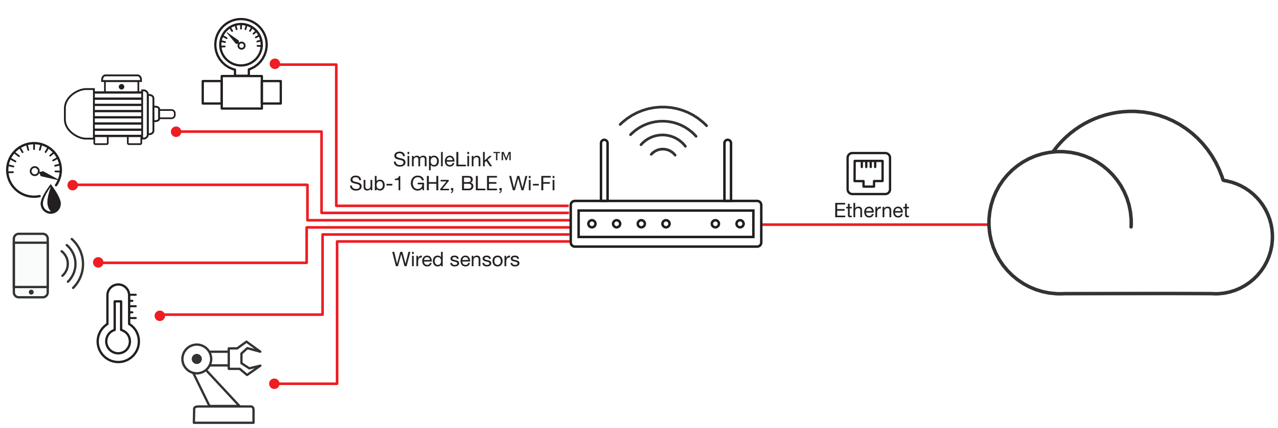

***Figure 3**. SimpleLink MSP432E4 MCUs are the industry's most integrated Arm® Cortex®-M4 MCUs, with an integrated 10/100 media access controller plus physical layer (MAC+PHY) for implementing intelligent gateways.*

SimpleLink MSP432E4 MCUs are based on a 120 MHz Arm Cortex-M4 core with floating-point capabilities that integrate a 10/100 Ethernet MAC and PHY. Bringing the PHY on-chip reduces component count (including passives), simplifies design complexity, provides less noise from external signals and results in an overall lower cost. Designs require less printed circuit board (PCB) space and error-free communications are extended beyond the 100m cable standard. Together, these benefits add up to an appreciable advantage compared to traditional designs using an external PHY.

Ease of design

The value of SimpleLink MSP432E4 MCUs is their integration with TI's extensive software offerings and hardware portfolio. TI's goal is make IoT devices and gateway designs as easy as possible. The SimpleLink SDK provides a comprehensive software framework from foundational levels including the TI real-time operating system (TI-RTOS), functional abstraction with TI drivers, and a multitude of application-level middleware solutions. To learn more about layers of the SimpleLink SDK, read the white paper, "[Simplifying software development to maximize return on investment.]"

The SimpleLink SDK simplifies connectivity as well, enabling developers new to wireless technology to implement protocols such as *Bluetooth*® and Wi-Fi without any low-level driver development. As shown in **Figure 4**, the SimpleLink SDK provides a software framework expandable via SDK plug-ins to integrate cloud connectivity and IoT agents. These expandable blocks, called SimpleLink SDK plug-ins, are part of the SDK framework and available via TI Resource Explorer.

Accelerate industrial IoT adoption

The IoT evolution is happening at full force across the industrial market. Manufacturers are rolling out IoT networks by adding or retrofitting existing and new buildings, manufacturing plants or grid infrastructure systems with smart sensor networks. The maturity of today's connectivity solutions help developers introduce wireless and wired networks with minimal development effort. The intelligent industrial gateways help developers massively scale the number of networks and edge nodes that can be deployed and effectively managed with the cloud.

TI's SimpleLink MSP432E4 MCUs enable the design of intelligent gateways. The ability to offload data

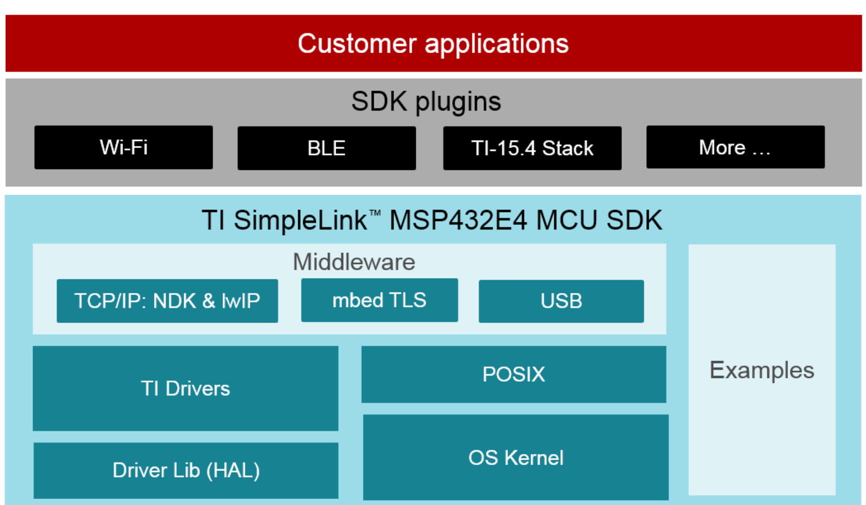

***Figure 4**. The SimpleLink SDK provides a comprehensive application programming interface (API), network services and add-ons via SDK Plugins to significantly simplify the development of core product features.*

processing and IoT management from nodes to a gateway can reduce node complexity, improve power efficiency and substantially lower system cost. In addition, intelligent gateways can actually augment the processing ability of nodes and their applications.

SimpleLink MSP432E4 MCUs make it easier to build gateways that reliably connect devices to the IoT. Developers can confidently design secure gateways that support a wide diversity of end points and interfaces. The SimpleLink MSP432E4MCU family is also designed to minimize energy consumption and reduce system cost while maximizing the capabilities of energy-sensitive systems.

The integration of hardware and software makes it that much easier for developers to connect disparate devices simply and easily without requiring a complete redesign. Backing the SimpleLink MSP432E4 MCU family is a full range of production software as well as wired/wireless communication components. With TI's SimpleLink MSP432E4 MCUs, developers can build robust and interoperable industrial gateways that provide a reliable connection from the edge nodes to the cloud.

Additional resources

SimpleLink MSP432E4 MCU: www.ti.com/product/msp432e411y

Data sheet: www.ti.com/lit/gpn/msp432e411y

SimpleLink MSP432E4 LaunchPad™ development kit (MSP-EXP432E401Y): www.ti.com/tool/MSP-EXP432E401Y

SimpleLink MCU platform: www.ti.com/simplelink

SimpleLink MSP432™ SDK: www.ti.com/tool/SIMPLELINK-MSP432-SDK

SimpleLink Academy training modules for MSP432E4: www.ti.com/simplelinkacademy

SimpleLink MSP432 E2E forum: e2e.ti.com/support/microcontrollers/msp430

To order samples or devices: www.ti.com/product/MSP432E411Y/samplebuy

IMPORTANT NOTICE FOR TI DESIGN INFORMATION AND RESOURCES