US Headquarters
1000 N. Main Street, Mansfield, TX 76063, USA
(817) 804-3800 Main
www.mouser.com

Technical Article Release

Specialized Devices Promise Greater Clarity in Evolving IoT Vision

by Stephen Evanczuk, Mouser Electronics

With forecasts promising billions of interconnected devices, the Internet of Things (IoT) has captured the attention and imagination of the industry. Although often viewed as a single entity, the IoT is likely to resolve less as a massive, unified system of smart sensors and cloud-based applications than as a richly layered hypersystem. The year two thousand fifteen promises will set the stage for the realization of a complex IoT that resolves into a series of functional layers fractured by vertically integrated solutions. While third-party Software-as-a-Service (SaaS) solutions will likely dominate the upper layers, IoT device manufacturers will rely on specialized hardware solutions for the lowest layers. At its farthest reaches where the IoT reaches into the physical world, the combination of specialized requirements and competitive forces will drive the growing segmentation of hardware systems and semiconductor devices.

For the semiconductor industry, the market potential of the IoT will continue to be a driving force in fueling the emergence of devices specifically designed for IoT applications. In particular, MCU architectures will become highly specialized, segmenting into device classes designed for smart devices and for the hubs that manage them. In fact, one of the most interesting trends expected to gain steam in 2015 revolves around the further differentiation of MCUs targeting smart devices and those hubs.

For designs addressing endpoints of the IoT, engineers will find growing availability of MCUs that combine very low-power requirements with integrated peripherals needed for sensor interfaces, control, and communications. Along with stripped-down versions of existing MCUs, emerging MCUs in this class will differentiate themselves with ultra-low-power management features and strictly limited peripheral sets targeted for specific IoT application segments, such as automotive and industrial, among others.

– continued –

Figure 1 *The Internet of Things will gradually evolve into a richly layered hypersystem driven by IoT endpoints and hubs based on specialized processors. (Source: iStockPhoto.com)*

At the same time, the market's emphasis on both low-power operation and efficient-connectivity options will drive further integration of RF capabilities in these MCUs. For these devices, the combination of a fully supported communications stack utilizing on-chip MAC and PHY capabilities will become increasingly important as designers look to shrink smart-device designs while speeding time-to-market.

In "pure" IoT applications, 802.15.4-compliant radios and even proprietary sub-GHz radios will dominate for this class of devices. For applications targeting consumer smartphones, however, Bluetooth radio will remain a vital requirement. In general, standards-based wireless connectivity will continue to dominate IoT endpoint design. Still, the reduced communications overhead and concomitant power efficiency of proprietary radios will remain an attractive option. The use of proprietary approaches will apply particularly for IoT designs intended for vertically oriented solutions targeting specific application segments such as healthcare or transportation that remain private due to security, licensing, or regulatory concerns.

Between countless smart-sensor endpoints and cloud-based applications, a layer of increasingly sophisticated systems will begin to blend the real-time capabilities of deeply embedded smart devices, the connectivity of conventional routers, and the applications features of higher-level applications. Unlike typical routers, hubs geared to the IoT will support more diverse connectivity options needed to connect to both smart devices and cloud applications. For connecting to IoT endpoints, 802.15.4-based communications will dominate, but hubs designed for proprietary solutions will also support sub-GHz connectivity. For connecting to the cloud, these hubs will more closely resemble conventional routers with support for wide-area-network connectivity but begin to offer support for optional broadband, particularly 4G LTE, and even satellite for remote industrial applications.

The first wave of hub implementations introduced in 2014 presage the emergence of hubs with multiprotocol connectivity. For example, both Wink and Nest support WiFi and ZigBee; Wink goes even

further with additional support for Z-wave and Bluetooth. IoT hubs will bring increasing support for efficient protocols such as MQTT, XMPP, CoAP, and others required for efficient real-time communications between endpoints and the cloud. Moreover, vendors will begin to bring portions of the cloud-based application down to these hubs, effectively short-circuiting the cloud to provide local monitoring and control features when cloud applications are unavailable or unneeded. As a result, hubs themselves will become increasingly intelligent themselves, not only supporting Internet functionality with built-in Web http servers found in conventional routers, but also hosting some software components of the applications themselves.

To provide these diverse capabilities, semiconductor manufacturers will enhance an emerging class of processors that meld traditional real-time capabilities with conventional application-processing features. Designers can find existing hybrid multicore architectures that combine a real-time MCU core, such as the ARM Cortex-R or Cortex-M with an application processor core, such as the ARM Cortex-A. As IoT requirements solidify, manufacturers will respond with hybrid SoCs that exhibit greater specialization for combined requirements including real-time analysis of sensor data from endpoints and high-level application software execution.

Across all layers of the IoT, more sophisticated security mechanisms will be required not only to protect proprietary devices but also to mitigate corruption of trusted data streaming from endpoints to the cloud. In fact, IoT security policies will gain significantly greater attention in the months ahead, and deservedly so. Security breaches dominated international headlines in 2014 and will likely continue into 2015, and while those stories concerned traditional networks, the prognosis for the IoT is much worse. Corrupted IoT devices provide the ultimate “back door” into IoT data networks, so the ability to thwart attacks on trusted devices and networks looms as a major factor in the growth and acceptance of IoT applications.

Semiconductor manufacturers will continue to offer hardware-based features needed not only for the sake of security itself, but also to ensure that execution of security policies does not detract from performance of the application itself. Along with integrated hardware accelerators for encryption and decryption, MCUs and associated ICs will broaden support for more advanced security features able to speed performance and security of higher-level security mechanisms such as challenge-response-based authentication. In turn, to support these capabilities, these devices will include more effective protection features for secure on-chip storage of security keys and certificates. Backed by this combination of integrated features, security features needed to ensure a hardware root of trust now found in specialized security processors will emerge in mainstream IoT MCUs and associated chip sets.

For all the advances in hardware for endpoints and hubs, deployment of sophisticated IoT applications will remain a significant challenge, requiring specialized knowledge from a widening pool of embedded systems, communications, security, and big data experts. As a result, IoT solution providers will find themselves relying on SaaS solutions such as the Oracle IoT platform, Arrayent Connect, and many other emerging commercial offerings as well as open-source platforms such as Contiki and IoT Eclipse from the Eclipse Foundation known for its eponymous IDE.

The IoT offers great potential for new types of applications, but successful deployment requires new classes of solutions at each level of the hierarchy. For engineers, 2015 promises greater clarity in the choice of specialized processors required to meet emerging IoT requirements.