Bluetooth Low-Energy Differentiation Through Cost Trade-Offs

Emerging NVM will hit mainstream applications before 2020

IoT Security Cannot Afford To Be an Oxymoron
Bluetooth Low Energy (BLE) — or Bluetooth SMART as it’s marketed by most vendors — is rapidly making its way into all kinds of new products. Its adoption has opened the floodgates to a slew of new devices. With support for Bluetooth v4.0, users are no longer required to use expensive authentication processors, lowering costs. Between the low cost and BLE’s low power, new applications such as key-chain finders were born, as were products that weren’t practical before due to Bluetooth’s high power consumption.

Developing products and gadgets depends on selecting the right chipset and ecosystem. More and more vendors are offering Bluetooth chips with varying capabilities and performance. Let’s look at some of the key decisions vendors made when designing their BLE devices, including chipsets from Texas Instruments, Nordic, Dialog, Cypress and CSR.

A few critical design decisions impact cost and power in a BLE chipset. BLE products and applications depend on low power since they operate from a small coin cell battery — the wrong device will consume more current. A key criterion when architecting a BLE chip is cost because most potential applications are cost sensitive.

**Single or Dual Mode**

The first question is what kind of information will be transferred. BLE was designed for low power and low latency. Bluetooth specifications prior to v4.0 focused on sending large amounts of data such as audio, causing them to have a high-connection latency and high power consumption.

BLE, on the other hand, sacrifices high throughput to achieve low power. BLE can’t be used to stream audio or music, but it’s perfect for small amounts of data sent infrequently such as sensor data.

Several considerations need to be made on whether to use just BLE (called Single Mode), Just Bluetooth, or both Bluetooth + BLE (called Dual Mode). The first one is cost. Supporting Bluetooth Classic is usually more complex and costly, but a good choice for:

- Older phones without BLE that have to be supported. The BLE specification isn’t backward compatible. Since BLE began to take off in 2011, supporting old phones requires supporting the older version of Bluetooth, an issue slowly disappearing as more manufacturers add BLE in their devices.
- The ability to stream audio or anything that requires high throughput and low loss.

On the other hand, reasons to use BLE are:

- The product needs to run for a long time from a small battery.
- Only a small or low rate data from sensors or alerts is sent.
- Cost is a concern.

Most developers today are using Single Mode devices supporting BLE only.

A large number of vendors specialize in these chipsets as well because of the number of applications and the Internet of Things. For example, a smart light bulb only needs BLE to send on/off or color commands that allows it to be cheaper.

**Chip Package Is Critical**

Another important aspect of cost is manufacturability. Most BLE devices are offered in two packages: QFN and WLCS. QFN is the standard Quad Flat No Leads package that is easy to use in products. Wafer Level Chip Scale package (WLCS) is the silicon die with solder balls, similar to a BGA. QFN packages cost more and are larger, but are easier to use and can have less issues. WLCS packages are less expensive because they are more basic. They are usually smaller, but require design experience and tighter tolerances. Because the PCB design for WLCS devices requires much tighter tolerances and usually more than two layers, it is more expensive. Ultimately, any saving from using WLCS may end up being offset by higher PCB costs.

**Embedded Non Volatile Memory Choice**

Embedded memory is another critical choice that drives cost. Most BLE devices include embedded flash memory because flash is reprogrammable. However, flash is expensive because it requires many additional semiconductor fabrication process steps and it’s power hungry. Dialog is a relative newcomer to the BLE scene, and it took a different approach. Its DA14580 chipset has no integrated flash memory. Because of this, Dialog can lower its device cost and power consumption. Flash memory requires both specialized circuitry as well higher voltages. Dialog’s device can work off an alkaline battery.

Continued on page 5
Emerging NVM will hit Mainstream Applications Before 2020

By Yann de Charentenay, Senior Analyst, Yole Développement
http://www.yole.fr/

In May, Samsung announced the foundation of the world’s most expensive semiconductor fabrication plant — at more than $14 billion — mostly focused on memory chips. Memory plants are becoming cost prohibitive as the technology’s complexity surges and volumes produced explode.

Indeed, memory chips are one of the electronic devices building blocks increasingly present in our daily life like PCs, cameras, mobile phones, automotive and Internet servers. Thus, the memory business is one of the largest semiconductor market segments, accounting for $78 billion last year for the stand-alone memory market. Embedded memory included into bigger chips like CPU or Microcontrollers (MCU) are widespread in many applications as well. The need for memory will surge in the next few years, especially thanks to the Internet data traffic explosion driven by more connected devices and higher information flow between devices.

Incumbent memory technologies are well established — non-volatile NAND flash and volatile DRAM, for example — but their scalability is becoming increasingly complex and problematic. As a result, new non-volatile memories have been developed over the last decade in order to supplant incumbent technologies. Those are RRAM, MRAM, STTRAM, PCM and FRAM. In the last two years, RRAM and STTMRAM have taken a leading position, whereas PCRAM has fallen from grace. (Source: Emerging Non-Volatile Memory (NVM) Technology & Market Trends report, Jan. 2015 edition)

Emerging NVM sales, including MRAM/STTMRAM, are still moderate — below $100 million in 2014 — and limited to niche markets, such as industrial and wearables, due to the limited density available. Indeed, MRAM/STTMRAM new product availability has been delayed by Everspin, Crocus technologies and Avalanche technologies. Micron’s PCM sales have declined sharply due to the collapse of the entry-level phone market.

However, on the bright side, several alliances targeting STTMRAM development have driven progress in structuring the ecosystem/ Panasonic and Adesto are introducing new RRAM products. And last but not least, Micron, the second memory market leader, has officially announced the introduction of two new memory chips for 2015 and 2018.

Improving scalability and, therefore, price/Gbit is the key to having access to mainstream NAND and DRAM applications. Current limitations of the emerging NVM density increase the price per Gigabit to several hundred dollars per Gbit, a limiting factor for a memory mass market adoption. Dominant NAND and DRAM technologies are below one dollar per Gbit.

In the next five years, scalability and chip density of new memories will improve, and this will open up many new applications:

• Enterprise storage will be the killer market for emerging NVM in 2020 because new technologies will improve data center storage system performance, where requirements are intensifying with the data traffic explosion.
• Embedded MCU for wearable, smart card and other markets increasingly will adopt emerging NVM because embedded MCU flash scalability is running out of steam, especially after 2018 at the 28 nanometer node. In the short term, emerging NVM will be rapidly adopted in the wearable and smart card markets thanks to its low-power consumption and higher density chips.
• Mass storage is currently served by NAND memory, but 3D NAND scaling is expected to slow down by 2020. In the meantime, 3D RRAM scalability is expected to surge thanks to big memory makers’ efforts and a new entrant, Crossbar, targeting an aggressive time to market for a 1Tb chip, expected in 2018.

Overall, the global emerging NVM market is expected to reach $7 billion by 2020 for an impressive growth of +118% per year. However, this business will represent less than 10% of the total 2020 memory market. The complete substitution of NAND and DRAM still has a long way to go.

###

About Yann de Charentenay

Yann de Charentenay has worked for Yole Développement in the field of MEMS, materials and compound semiconductors since 2003. He has contributed to more than 60 marketing and technological analysis reports.
IoT Security Cannot Afford To Be an Oxymoron

By Bruce Kleinman, Principal, FSVadvisors
http://fsvadvisors.com/

Securing the Internet of Things (IoT) presents opportunities and challenges. IoT security has seen far more press coverage, to date, than actual delivered solutions. The dearth of secure IoT solutions may severely hinder IoT growth. Imagine the impact of one or two well-publicized IoT security breaches: cyber-attacks compromising credit card and personal records are scary enough; cyber-attacks that jump into the physical world will have a far more chilling influence.

First, a bit of context setting — the term “IoT” is used to describe everything from smart (using the modifier loosely) toothbrushes to complex M2M systems. This article puts gadgets aside and focuses on user-less networked devices in settings such as home, office, factory, and metro environments.

At a fundamental level, the very nature of IoT devices presents good news and bad news:

• The good news: User-less IoT devices do not run mainstream operating systems and have little (if any) user interaction; therefore, they are relatively immune to the most common attack vectors, such as spear phishing messages and email attachments infected with malware.

• The bad news: These user-less IoT device do not run anti-malware protection and are patched far less frequently than a phone or tablet or PC; furthermore, many of the telltale signs of malware infection (for example, erratic performance) may be overlooked for long periods of time.

The most likely attack scenarios will take advantage of the weak points in both user devices and IoT devices on the same network. We’ve learned a tremendous amount about advanced persistent threats (APTs) in 2015. The Carbanak APT* installed malware on PCs, providing the attackers with months of invasive surveillance; based on the collected intelligence, the attacks were launched against financial servers and even cash machines. The Equation Gang APT platform** employed even more sophisticated methods of cyber-espionage and -attack, including kinetic (physical) elements.

APT exploit kits are flowing down the food chain to the broad hacker community. “Today’s top-secret programs become tomorrow’s Ph.D. theses and the next day’s hacker tools,” notes renowned security expert Bruce Schneier. He makes the essential observation that the attack-defense balance is not a level field: “Attack is easier than defense. It’s not just the complexity of modern computer and internet systems — fundamentally, it’s easier to break into one of these systems than it is to prevent others from doing so.”

User-less networked devices in many applications — automotive, energy, factory floor, medical, and others — face the additional challenge of long field deployments. These systems must operate for five to 10 years; they do not have the luxury of a consumer two-year replacement cycle. The lengthy deployment cycles of such IoT systems presents the additional challenge of defending against “unknown unknowns” with threat profiles that do not yet exist.

Now for the positive news: strong cryptography provides the tools needed to transform the field and exponentially favor defense over attack, enabling provable security for decade-plus horizons. Proven standards such as public key cryptography (using RSA-2048) and authenticated encryption (using SHA-256 and AES-256), for example, can construct extraordinarily robust end-to-end security.

Public key cryptography (PKC) is built atop the public-private key pair, and in the context of the applications cited above, every IoT device will have its own key pair or (quite likely) multiple key pairs. Absolute security of the private keys is the cornerstone of system-level security, and this absolute security must endure throughout the lengthy deployment cycle.

All of the major microcontroller vendors introduced families focused on IoT in 2014 and 2015. In all cases, the feature sets are tuned for various IoT applications; in some cases, complete radio subsystems have been added. Unfortunately for the topic under discussion, in few instances do these IoT microcontrollers integrate the security features required to address the threat environment described above. Microcontrollers must evolve to include a cryptoprocessor subsystem, or alternatively, we need new cryptoprocessor devices to complement the microcontrollers.

Continued on page 5
Bluetooth Low-Energy Differentiation Through Cost Trade-Offs...Continued

Gustavo Litovsky, Chief Executive and Founder, Argenox Technologies

Dialog replaced the embedded flash with a One-Time Programmable (OTP) memory. OTP is just that, programmable once. For development, the user application and stack are loaded into memory via JTAG. The device can connect to an external memory via SPI or I2C to load firmware. Although not as flexible as having flash on-chip, it can alleviate issues with firmware updates. Dialog’s BLE chip is one of the parts with the lowest current consumption currently on the market. It is attractive for low-power products needing to run for many years.

Conclusion

BLE has created a way for vendors to develop low power and cost efficient devices, but selecting the right chipset and ecosystem is critically important. At Argenox, we have customers designing with the Dialog BLE chip containing OTP due to cost.

IoT Security Cannot Afford To Be an Oxymoron...Continued

By Bruce Kleinman, Principal, FSVadvisors

Absolute security of the private keys dictates that they must be stored on die. Kilopass XPM one-time programmable memory is an ideal solution. XPM provides the physical security of permanent storage with the flexibility to program the keys during (a) silicon manufacturing, (b) product manufacturing, or (c) system deployment. Some security architectures may, in fact, program different keys during all three stages.

Absolute security of the boot loader is another foundation of system-level security. XPM is superior to mask-programmed ROM for this purpose as it provides the flexibility to tailor the boot loader during (a) silicon manufacturing or (b) product manufacturing. With the private keys and boot loader securely enconced on-die, the rest of the software stack may be digitally signed and stored off-chip. At boot time, the entire software stack is authenticated before normal operation commences.

XPM enjoys excellent density and compatibility with process nodes from 180nm down to 28nm (and soon 20nm and FinFET). XPM natively provides a high degree of security, and additional measures can be taken to protect against side-channel and de-layering attacks. XPM is an enabling technology, helping to build cryptoprocessor devices (and subsystems) that provide robust and durable defenses for the Internet of Things.

About Bruce Kleinman

Bruce Kleinman is the founder and Principal of FSVadvisors, a consultancy providing marketing, business development and sales services. He has 30 years of marketing, business development and sales experience with a broad knowledge of security, networks, systems, hardware, semiconductors, software and algorithms. IoT, security, and IoT security are frequent topics on his FromSilicon Valley blog- http://fromsiliconvalley.com/