Evolving Embedded Wireless Systems with FRAM-Based MCUs

Jacob Borgeson, Texas Instruments, and David Adams, Newark element14

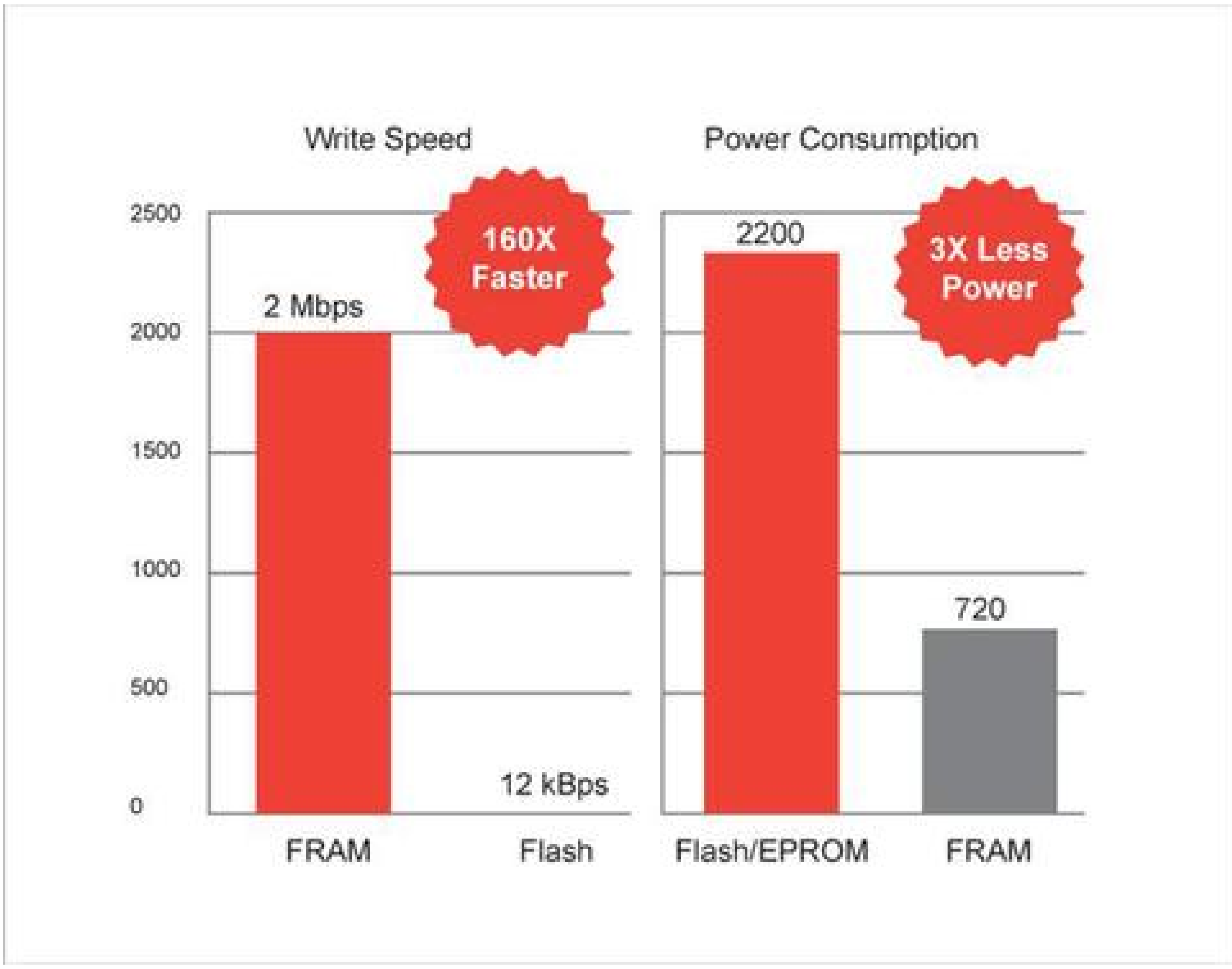
Texas Instruments and Newark element14 explore the design challenges and unique features FRAM offers as a memory alternative for embedded wireless network applications.

Embedded wireless networks are one of the fastest growing applications, outpacing the overall semiconductor industry, due to the rapid uptake of embedded wireless communication in the form of smartphones and portable medical devices. Embedded wireless networks are also found in automobiles, enabling smarter safety features, better engine performance management, and as networked infotainment devices. Future innovation and growth of embedded wireless networks will come from smart buildings, smart grids, and the Internet-of-Things.

Despite the current growth, the full potential of embedded wireless systems has not yet been realized as some fundamental design problems remain unsolved. These challenges are due to limitations in battery solutions, varying memory requirements, wireless security, and reliability.

A recent revolutionary change in memory technology, highlighted by the release of embedded Ferroelectric Random Access Memory (FRAM), offers developers the best option to tackle these design obstacles. The embedded wireless network application employs distributed rather than centralized processing — a technical evolution central to reducing power consumption.

What is FRAM?



FRAM, like DRAM (Dynamic Random Access Memory), allows random access to each individual bit — for both read and write — and offers considerable advantages over other standalone memory devices. Unlike EEPROM or Flash memory, FRAM does not require a charge pump, special sequence to write data, or a higher programming voltage. FRAM is non-volatile, therefore data is not lost when power is removed, offering more flexibility. All of this combines to decrease power consumption by 250 times per bit when compared to other types of Flash, without wearing out.

Though stand-alone FRAM has been available in the market, its adoption has been limited to general usage in memory storage devices. The recent coupling of FRAM with MCUs has allowed memory to graduate to the next generation of broad applications. Through integrated MCUs, full realization and utilization of the unique memory features in FRAM (universal memory, low-power access, flexibility, high endurance, and reliability) have been missing till now.

Benefits of Embedded FRAM

- Ultra-low-power read/write with increased throughput.
- True unified memory – configurable as Flash or RAM.
- Industry-leading read/write speeds.
- Virtually unlimited write endurance –1015 cycles.
- Inherently robust and radiation-resistant.

Freedom to Design

Wireless communication is characterized by the design freedom it offers in terms of radio parameters, network specifications, and various other protocol-specific requirements. Memory allocation can impact the ability to support multiple standards within the same product when one designs to the specific needs of different wireless applications.

For protocols that are standardized and regulated by governing bodies, as is the case for Wi-Fi, Bluetooth, or Near Field Communication (NFC), the implementations for the same protocol could vary in memory requirements depending on the features present on the chosen MCU platform.

Program space and data space requirements can make a specific MCU unusable in wireless networking applications. Using traditional flash-memory-based MCUs means that the development effort is limited to a few device and memory configurations. The choice of MCU is often restricted due to the program and data space requirements of the desired network protocol. These limitations can often force the designer into a more expensive device, just to get more on-chip RAM or Flash memory. Such an approach is not robust against any major code change that changes memory allocation.

FRAM can function both as storage for program space and RAM for the data space requirements, providing greater flexibility and easier memory allocation to suit the application’s requirements. Multiple networking protocols that were adversely affected by memory allocation can now be implemented in the same device, and this device can be the most cost effective variant. This is of particular interest when looking at the smart grid or smart appliances that will interact within smart buildings in the near-future, and that will need to operate in many different embedded wireless environments.

Better Smart Buildings & Grids

The idea behind the smart grid is to use wireless technology to track electricity use and provide this information to both users and utility companies with an eye toward more efficient delivery and consumption. As the digitally-enhanced smart grid expands, demand for the ability to wirelessly move data between smart appliances and interfaces at very low power will inevitably grow.

The open-nature of wireless communication makes it vulnerable to security threats. A key design challenge is ensuring that the smart grid notes are secure and resilient against attacks. For this to be possible, it is essential that designers and utilities respond in real-time with bug fixes done over the network. Features such as secure-write, high endurance, and ultra-low power consumption make FRAM an ideal choice for enabling security patches and advanced features for smart grids.

FRAM also valuable reduces the system’s complexity and bill of materials; for instance, many of today’s designs include a separate non-volatile memory (either FRAM or EEPROM), which can be implemented inside an integrated MCU with FRAM (like the MSP430FR57xx series from Texas Instruments), and with lower overall system power consumption.

A lot of inherent physical features of FRAM make it favorable for secure applications. With high-write endurance, encryption operations can take place for the foreseeable life of the product without memory write failures occurring. The low-power and fast writes make it difficult to hook up a probe to a chip and sense any of the data, and impossible to open up the chip to read each molecule of FRAM to decode the memory contents. A smart building would be more secure, both from physical hacking, as well as attempts at wireless access to the system data.

With a lower power memory, these designs can be self-contained and sealed for the life of the product. A wide variety of nodes would either need no maintenance or a very simple replacement of the entire node — instead of a more tedious battery replacement. This helps reduce the overall lifetime cost of a smart building system, while also making it more robust to different environmental conditions.

Click here to read the full article [1].

Source URL (retrieved on *03/05/2015 - 1:45am*):
http://www.wirelessdesignmag.com/articles/2013/06/evolving-embedded-wireless-systems-fram-based-mcus

Links:
[1] http://digital.wirelessdesignmag.com/wirelessdesignanddevelopment/may_june_2013#pg1