

# MICROPROCESSOR *report*

Insightful Analysis of Processor Technology

## SILICON LABS UPGRADES WIRELESS MCUS

*New EFR32 Series 2 Chips Improve Performance and IoT Security*

By Tom R. Halfhill (June 17, 2019)

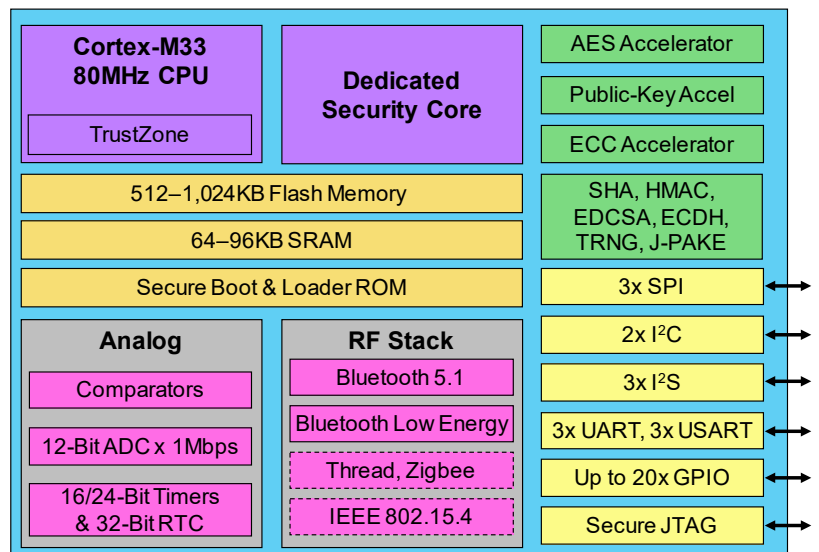
Mindful of the embarrassing security breaches that plague first-generation IoT devices, Silicon Labs is girding its newest wireless microcontrollers with hardier security hardware. Secure boot, cryptography acceleration, side-channel defenses, a secure debug port, and a true-random-number generator (TRNG) are among the improvements. The new EFR32xG21 chips in the Wireless Gecko Series 2 family are also the first Silicon Labs products to adopt Arm’s Cortex-M33, and they have enhanced 2.4GHz radios for popular IoT protocols.

Shipping in volume since April, these 32-bit wireless MCUs target line-powered IoT. The company is also developing plug-and-play wireless modules and battery-friendly models that will inherit the power-saving features of its Wireless Gecko Series 1 family (see [MPR 4/11/16](#), “Silicon Labs Goes Wireless”). Already, the new chips rank among the lowest-power wireless MCUs on the market. In active mode (albeit with their radios silent), they draw only 51 microamps per megahertz. And they’re tiny, cramming all their features into a 4mm surface-mount QFN package with only 32 pins.

As Figure 1 shows, the new chips are essentially 32-bit MCUs with integrated radios for the most popular IoT wireless protocols. The Cortex-M33 CPU implements the Arm v8-M instruction-set architecture, including TrustZone (see [MPR 11/14/16](#), “Cortex-M23/M33 Bolster IoT Security”). By contrast, the older Series 1 employs Cortex-M4F, which lacks those advanced features. The CPU upgrade, plus a dedicated security core and additional acceleration hardware, considerably strengthen Series 2’s resistance to attacks.

Table 1 shows the differences between the EFR32BG21 and EFR32MG21. The former implements the Bluetooth 5.1 protocol, including Bluetooth Low Energy (BLE) and Bluetooth Mesh; the latter implements those protocols plus Zigbee 3.0, Thread, and IEEE 802.15.4. Each design also is available with different integrated power amplifiers. Some can output up to 10 decibel-milliwatts (dBm), whereas others can output up to 20dBm. Silicon Labs claims the latter radios can operate at up to twice the range of competing products.

As usual with MCUs, the on-chip memories also vary. Some models have 512KB, 768KB, or 1,024KB of flash memory and 64KB or 96KB of SRAM. These aren’t the largest



**Figure 1. Wireless Gecko Series 2.** The new EFR32BG21 and EFR32MG21 are nearly identical, except the latter implements the additional radio protocols marked with dotted lines.

### Price and Availability

Silicon Labs began shipping the EFR32xG21 Series 2 wireless microcontrollers in April. Distributor prices are generally less than \$5 in 1,000-unit volumes. For more information, access [www.silabs.com/products/wireless/gecko-series-2](http://www.silabs.com/products/wireless/gecko-series-2).

memories in the 32-bit MCU universe, but they're sufficient for typical IoT applications and help to keep the chips small. Except for these features, the EFR32xG21 products are virtually identical. All can operate their Cortex-M33 cores at up to 80MHz, and they share the same integrated peripherals, I/O interfaces, and security features. List prices for 1,000-unit volumes are less than \$5, depending on the radio output power, flash memory, and SRAM.

### Tales From the Crypto

Although the 80MHz Cortex-M33 delivers more than twice the performance of the 40MHz Cortex-M4F in Gecko Series 1, it can't handle complex security functions in addition to the radio protocols. Consequently, a dedicated security core handles the ROM-based secure boot with root-of-trust authentication, the secure loader, crypto acceleration, true-random-number generation, and countermeasures for side-channel attacks. Similar features are appearing in other IoT processors but are less comprehensive in the previous Gecko Series 1 family.

Hard logic accelerates AES (128, 192, 256) and elliptic-curve cryptography (ECC P192, P224, P256); the SHA-1, SHA-2 (SHA-244, SHA-256), and HMAC hash functions; the Elliptic Curve Digital Signature Algorithm (ECDSA);

	Wireless Gecko Series 2 EFR32BG21	Wireless Gecko Series 2 EFR32MG21
Radio Protocols	Bluetooth 5.1, BLE, Mesh	Bluetooth 5.1, BLE, Mesh, Zigbee, Thread, IEEE 802.15.4
Output Power	-20dBm to +10/20dBm	
Receive Sensitivity	-97.5dBm (1,000kbps GFSK)	-104.5dBm (250kbps OQPSK)
Receive Current	8.7mA	9.4mA
Temperature Range	-40°C to +125°C	
Chip Power (active)	50.9µA/MHz (radios inactive)	
Package	4mm QFN-32	
IC Process	40nm CMOS	
Availability	Production 2Q19	
List Price (1,000s)	\$2.55-\$4.65	

**Table 1. Silicon Labs EFR32 Series 2 wireless MCUs.** dBm=decibel-milliwatts; GFSK=Gaussian frequency-shift keying; OQPSK=offset quadrature phase-shift keying. The supported radio protocols distinguish these two otherwise identical products. Each product also has models with different power amplifiers and memories. (Source: Silicon Labs)

and two public/private key protocols: Elliptic-Curve Diffie-Hellman (ECDH up to 256) and Password-Authenticated Key Exchange by Juggling (J-PAKE). The new NIST-compliant TRNG creates the random numbers these operations require. After the chips are deployed in the field, the secure-lock JTAG debug port repels intruders, as do defenses against side-channel attacks such as differential power analysis (DPA).

As noted above, integrated power amplifiers enable the radios to output either +10dBm or +20dBm, depending on the model. When transmitting, the radio draws 426 microamps for each meter of distance to the receiver. This current is in addition to the 51 microamps per megahertz the whole chip draws when fully active. At the full CPU speed of 80MHz, the chip draws about 4.1mA, and the radio would draw a similar amount when communicating with a device 10 meters distant. Another expression of the output power is that the radio draws 33.8mA at 10dBm.

When receiving, the radio's sensitivity is -105.1dBm at 125kbps for Bluetooth Long Range or -104.5dBm at 250kbps for Zigbee and Thread—almost no difference at twice the speed. For Bluetooth at 1,000kbps, it's -97.5dBm. These sensitivity numbers match or exceed those of competitors. In addition, Silicon Labs says these enhanced radios more effectively block interference from nearby Wi-Fi routers operating in the same 2.4GHz unlicensed band, which is increasingly crowded.

Bluetooth 5.1 includes BLE and Bluetooth Mesh, which are marketed to consumers under various other industry brand names (such as Bluetooth Smart). To aid developers, Silicon Labs offers a \$479 mesh-development kit that includes its Simplicity Studio software tools, three wireless main boards, three boards with +10dBm radios, and three boards with +20dBm radios. The radio boards come with a multiprotocol range-test demo and are controllable through a BLE connection using a smartphone (not included). Additional radio boards cost \$49.

### Fastest CPU, Smallest Package

The Wireless Gecko Series 2 family joins a growing horde of wireless MCUs for IoT. The largest vendors are NXP, STMicroelectronics, and Texas Instruments, which all have new products. As Table 2 shows, the EFR32MG21 competes with NXP's Kinetis K32W0x-series, ST's STM32WB, and TI's SimpleLink CC1352R (see [MPR 5/7/18](#), "New Wireless MCUs Bolster IoT"). The competing products employ the older Cortex-M4F instead of Cortex-M33 for their main CPU but pair it with a Cortex-M0 or Cortex-M0+ to offload the radio protocols—especially when the chip rests in always-on standby mode. At 80MHz, the M33 is up to twice as fast as the M4F in the other chips, so it needs no extra help for the radios, but it can't match the same low power on standby.

Because these MCUs need help with the compute-intensive security processing, they provide hardware acceleration for the relevant crypto algorithms, hash functions,

and key-exchange protocols. All implement secure boot to protect the chip from loading corrupted or compromised firmware. Silicon Labs, NXP, and ST add protection for user code in flash memory. None of these MCUs have DRAM interfaces, relying instead on their internal memories to store code and data. Silicon Labs generally holds its own in this respect but withholds the ROM size. TI's huge 256KB ROM also stores the low-level 802.15.4 firmware, other low-level drivers, and a TI-RTOS real-time-operating-system kernel, freeing the flash memory and SRAM for user code.

EFR32 Series 2 chips offer the highest ambient-temperature range, which suits them to applications that must withstand extreme heat. In particular, they're designed for "smart" LED lighting. (They're not intended for automotive applications, however.) To squeeze into small light bulbs, they also have the tiniest packages in this group. In fact, their 4mm QFN is slightly smaller than the STM32WB's 4.5mm chip-scale package. To enable its tiny size, the EFR32MG21 omits some I/O interfaces that the other MCUs offer. Most notably, it lacks the USB2.0 and rudimentary LCD interfaces that are standard in the STM32WB and Kinetis chips. The latter adds an SD-card interface and the only digital-to-analog converter (DAC) in this group, which explains its larger packages that bristle with up to 191 pins.

Silicon Labs' active power consumption is among the lowest in this comparison. In stand-by mode, however, the other MCUs can shut off the main CPU and switch to the Cortex-M0/M0+, which drains much less current. In deep-sleep mode, they sip mere nanoamps. By our estimate, the EFR32MG21 can't operate nearly that low, disqualifying it for systems that subsist on small batteries. Silicon Labs plans to sample newer versions with lower sleep power later this year. Its older Series 1 MCUs excel in low sleep power, and the company is adapting the same technology to the new products.

We found 1,000-piece unit prices for the EFR32MG21 similar to those for the ST and TI products. (The price ranges in Table 2 correspond to parts with different memory sizes as quoted on distributor websites.) NXP's Kinetis K32W0x is by far the most expensive in this group. It has the most flash memory and SRAM and more I/O interfaces, including the only DAC. As a result, it has a larger package with many more pins. (The quoted price is for the 9mm VFBGA-176 version.) At less than \$5 for the most full-featured model, the EFR32MG21 competes effectively with the other MCUs in this comparison if the target application is line powered. Although it's compact enough for IoT wearables, it would drain too much power from their small batteries in deep-sleep mode.

## Lizards With Small Footprints

The initial Wireless Gecko Series 2 chips are major upgrades of Silicon Labs' IoT processors. Most welcome are the stronger security features, which we consider mandatory for new IoT designs. Security threats have become too obvious for responsible designers to ignore. Fortunately, the stronger security adds virtually no cost to the chip, and the hard logic consumes less power than implementing the same functions in software. The accelerators also free the Arm CPU to handle the radio protocols, which are complex in their own way.

Another major upgrade is the 80MHz Cortex-M33: it delivers more than twice the performance of the 40MHz Cortex-M4F in the Series 1 family. Both are 32-bit CPUs with an FPU, but the M33 has valuable new features. Mainly, it implements the Arm v8-M ISA, which includes TrustZone security. Unlike the M4F, it can run critical software in a secure partition. And because the M33 is software-compatible with the M4F, Series 1 customers should have little trouble moving up to Series 2.

The enhanced radios offer a +20dBm option for longer range, allowing customers to choose the appropriate power

	Silicon Labs EFR32MG21	NXP Kinetis K32W0x	ST STM32WB	TI SimpleLink CC1352R
<b>CPU (main)</b>	80MHz M33	72MHz M4F	64MHz M4F	48MHz M4F
<b>CPU (radio)</b>	None	72MHz M0+	32MHz M0+	48MHz M0
<b>Flash Memory</b>	512–1,024KB	1,280KB	256–1,024KB	352KB
<b>SRAM</b>	64–96KB	384KB	128–256KB	88KB
<b>ROM</b>	Undisclosed	48KB ROM	48KB ROM	256KB ROM
<b>RF Protocols</b>	BLE, Zigbee, Thread, IEEE 802.15.4			
<b>Basic Security</b>	Secure boot, ECC, TRNG			
<b>Other Security Features</b>	AES-256, RSA, SHA-1, SHA-2, code protection, secure debug, side-channel defenses	AES-128, RSA, SHA-2, flash-access control	AES-256, RSA, code protection	AES-256, SHA-2 to SHA-512
<b>A/D and D/A Converters</b>	12-bit ADC	12-bit ADC/DAC	12-bit ADC	12-bit ADC
<b>Display I/O</b>	None	FlexIO	LCD 8x40	None
<b>USB</b>	None	USB2.0 FS	USB2.0 FS	None
<b>Common I/O</b>	I <sup>2</sup> C, UART, SPI, GPIO			
<b>Other Features</b>	Comparators, timers, I <sup>2</sup> S	Comparators, timers, audio, FlexIO, SDHC	Quad SPI, audio	Comparators, I <sup>2</sup> S
<b>Temp Range</b>	–40°C to 125°C	–40° to 105°C*	–40° to 105°C	–40° to 85°C
<b>Active</b>	51µA/MHz	76µA/MHz	50µA/MHz	59µA/MHz
<b>Standby</b>	4.5µA	2.1µA	1.8µA	0.8µA
<b>Deep Sleep</b>	4,000nA+	300nA	<50nA	105nA
<b>Package</b>	4.0mm QFN-32	5.9mm x 5.8mm CSP-191	4.5mm CSP-100	7.0mm VQFN-48
<b>Production</b>	2Q19	3Q18	2H18	1Q19
<b>List Price (1ku)</b>	\$3.78–\$4.79	\$7.89	\$3.50–\$4.69	\$4.58

**Table 2. Four wireless MCUs for IoT.** The EFR32MG21 has the smallest package, tolerates the widest temperature range, and leads in processor speed. NXP's Kinetis K32W0x-series offers the most memory. The STM32WB consumes the lowest power in active and deep-sleep modes. TI's chip provides the most ROM and the lowest standby power. \*Chip-scale package limited to 85°C. (Source: vendors and distributors, except +The Linley Group estimate)

profile and wireless range for their system design. According to Silicon Labs, the radio's selectivity is also better—an improvement users will appreciate as more wireless devices jam into the 2.4GHz band. In addition to the usual traffic from Wi-Fi routers, radios must enhance their ability to reject unwanted signals from drones, walkie-talkies, cordless phones, microwave ovens, baby monitors, and numerous other consumer devices that employ this unlicensed spectrum.

Packaged in a 4mm QFN-32, the new Series 2 chips are the smallest wireless MCUs in their class. The tiny package is necessary for diminutive line-powered IoT products, such

as LED bulbs, and they pave the way for similarly compact models that are suited to battery-powered designs. Their unusually high temperature range fits them for devices that either generate high heat or must operate in hot environments.

By sacrificing USB and LCD interfaces, however, the new Wireless Geckos limit the scope of applications they can address without help from peripheral chips. Many IoT devices have a small display, and some have a USB port for battery charging, so future Wireless Geckos may add those features. Nevertheless, the initial Series 2 chips are competitive alternatives to rival products. ♦

To subscribe to *Microprocessor Report*, access [www.linleygroup.com/mpr](http://www.linleygroup.com/mpr) or phone us at 408-270-3772.