From January 2006 *High Frequency Electronics*

Zigbee System-on-Chip (SoC) Design

By Khanh Tuan Le
Chipcon

This article describes the Zigbee/IEEE 802.15.4 standard, and the design philosophy used to develop a single-device solution

Addressing the need of low cost, low power radio solutions for fairly simple wireless applications within our homes, offices and the industrial environment, the Zigbee™ wireless technology and the underlying IEEE 802.15.4 standard are specifically designed to provide a cost-effective, standard-based and flexible wireless network, which supports low power consumption, reliability, interoperability and security for control and monitoring applications with low to moderate data rates. The complexity and cost of the IEEE 802.15.4/Zigbee compliant devices are intended to be low and scalable in order to enable broad commercial adaptation within cost sensitive applications. System-on-chip (SoC) silicon solutions for IEEE 802.15.4/Zigbee applications must therefore be optimized to meet the challenging low-cost and low-power targets.

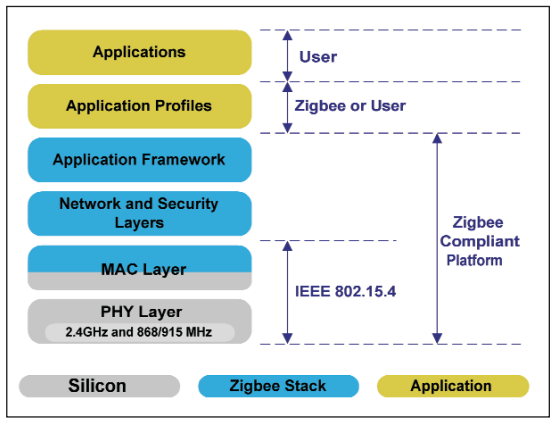


Figure 1 · IEEE 802.15.4 and Zigbee working model.

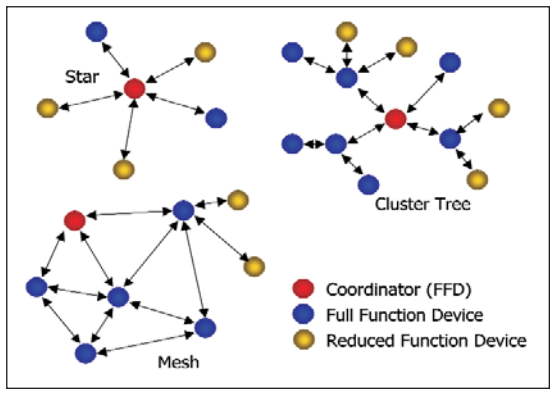


Figure 2 · Zigbee network topologies.

IEEE 802.15.4 and Zigbee Introduction

The IEEE 802.15.4 standard and Zigbee™ wireless network technology, illustrated in Figure 1, are ideal for the implementation of a wide range of low cost, low power and reliable control and monitoring applications within the private sphere and industrial environment.

The IEEE 802.15.4 standard [1], ratified in May 2003, specifies the physical (PHY) and media access control (MAC) layers at the 868 MHz (Europe), 915 MHz (US) and 2.4 GHz (worldwide) ISM bands, enabling regional or global deployment. The air interface is Direct Sequence Spread Spectrum (DSSS) using BPSK for the 868/915 MHz PHY, and O-QPSK for the 2.4 GHz PHY. The main parameters of the IEEE 802.15.4 PHY are summarized in Table 1.

The IEEE 802.15.4 PHY includes receiver energy detection (ED), link quality indication (LQI) and clear channel assessment (CCA). The IEEE 802.15.4 MAC sublayer controls the access to the radio channel using the CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) method, and handles net-

work (dis)association and MAC layer security (AES-128 encryption based). It is also responsible for flow control via acknowledgement and retransmission of data packets, frame validation, and network synchronisation as well as support to upper layers for robust link operation. The IEEE 802.15.4 standard employs 64-bit IEEE and 16-bit short addresses to support theoretically over 65,000 nodes per network.

The ZigBee™ wireless technology [2], ratified in December 2004, specifies the network, security, and application layers upon the IEEE 802.15.4 PHY and MAC layers. The Zigbee Alliance also provides interoperability and conformance testing specifications. The Zigbee network layer is responsible for device discovery and network configuration, and supports three networking topologies: star, mesh (peer-to-peer) and cluster-tree. Zigbee-enabled networks will employ a combination of device types as shown in Table 2. Figure 2 shows the Zigbee network topologies employing these different device types.

Physical device type distinguishes the device hardware complexity and capability:

- Full function device (FFD): Adequate resources and memory capacity to handle all designated tasks.
- Reduced Function Device (RFD): Modest resources and memory capacity compared to FFD.

Logical device type distinguishes the physical devices deployed in a specific Zigbee network:

- Coordinator: Network establishment and control.
- Router: Support data routing functionality; can talk to other routers, coordinator and end devices.
- End device: Can only talk to routers or the coordinator.

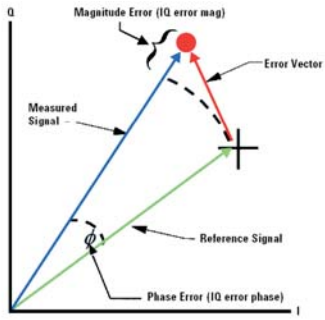
Parameter	2.4 GHz PHY	868/915 MHz PHY
Sensitivity @ 1% PER	–85 dBm	–92 dBm
Receiver Maximum Input Level	–20 dBm	
Adjacent Channel Rejection	0 dB	
Alternate Channel Rejection	30 dB	
Output Power (lowest maximum)	–3 dBm	
Transmit Modulation Accuracy	EVM <35% for 1,000 chips The Error Vector Magnitude (EVM) is the scalar distance between the two phasor end points representing the ideal and the actual measured chip positions, and is equivalent to the residual noise and distortion remaining after an ideal version of the signal has been stripped away. 	
Number of Channels	16	1/10
Channel Spacing	5 MHz	single-channel/2 MHz
Transmission Rates Data Rate Symbol Rate Chip Rate	 250 kb/s 62.5 ksymbol/s 2 Mchip/s	 20/40 kb/s 20/40 ksymbol/s 300/600 kchip/s
Chip Modulation	O-QPSK with half-sine pulse shaping (MSK)	BPSK with raised cosine pulse shaping
RX-TX/TX-RX Turnaround Time	12 symbols	

Table 1 · IEEE 802.15.4 PHY parameters.

Physical device type	*Logical device type*		
	Coordinator	**Router**	**End Device**
Full Function Device (FFD)	Yes	Yes	Yes
Reduced Function Device (RFD)	No	No	Yes

Table 2 · Device types in Zigbee networks.

System-on-Chip Considerations

Implementing true system-on-chip solutions, that is, integrating all operational functions such as radio transceiver, data processing unit, memory and user-application features on one single silicon die, contributes greatly to both performance, cost and time-to-market advantages.

High performance at lower power consumption is achieved due to the intimate interaction of dedicated on-chip functions minimising overhead.

Low manufacturing costs and short time-to-market are obtained by:

- Lowest system bill-of-materials
- Small footprint and small number of components
- Simpler assembly and testing
- Easy and reliable design (single active device)

For a majority of Zigbee-based wireless user applications, optimally designed IEEE 802.15.4/Zigbee-compliant system-on-chip silicon devices will be a critical contributor to successful commercial adaptation by downscaling of application system cost and design complexity without compromising the technical merits of the IEEE 802.15.4/Zigbee technology.

The principal mapping of a SoC to the various layers of the IEEE 802.15.4/Zigbee technology is illustrated in Figure 3. SoC device implementation in general is a tremendous challenging design task and an extremely extensive subject. Focusing specifically on the design of Zigbee-optimized SoC devices, system-level considerations and implementation choices will be highlighted and discussed based on the IEEE 802.15.4-compliant and Zigbee-ready CC2430 SoC from Chipcon.

SoC Design

The CC2430 family is true system-on-chip CMOS solutions specifically tailored to deliver high performance and to satisfy the low cost, low power requirements of IEEE 802.15.4/Zigbee™-based wireless applications at 2.4 GHz ISM frequency band. The 2.4 GHz PHY of the IEEE 802.15.4 standard has huge potential because the globally available 2.4 GHz ISM band with the largest bandwidth promotes worldwide market and flexibility of application designs. The CC2430 combines a proven and high performance 2.4 GHz DSSS radio transceiver design with an industry proven, compact and efficient 8051 microcontroller (µC). Each SoC device

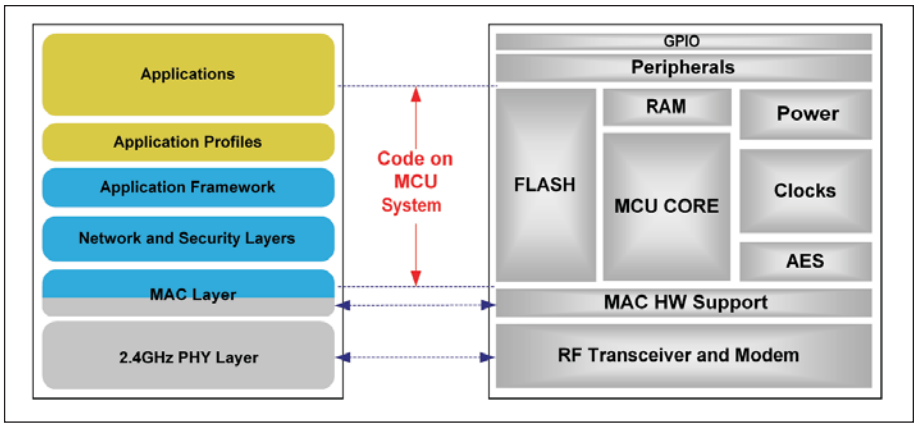


Figure 3 · SoC content mapping.

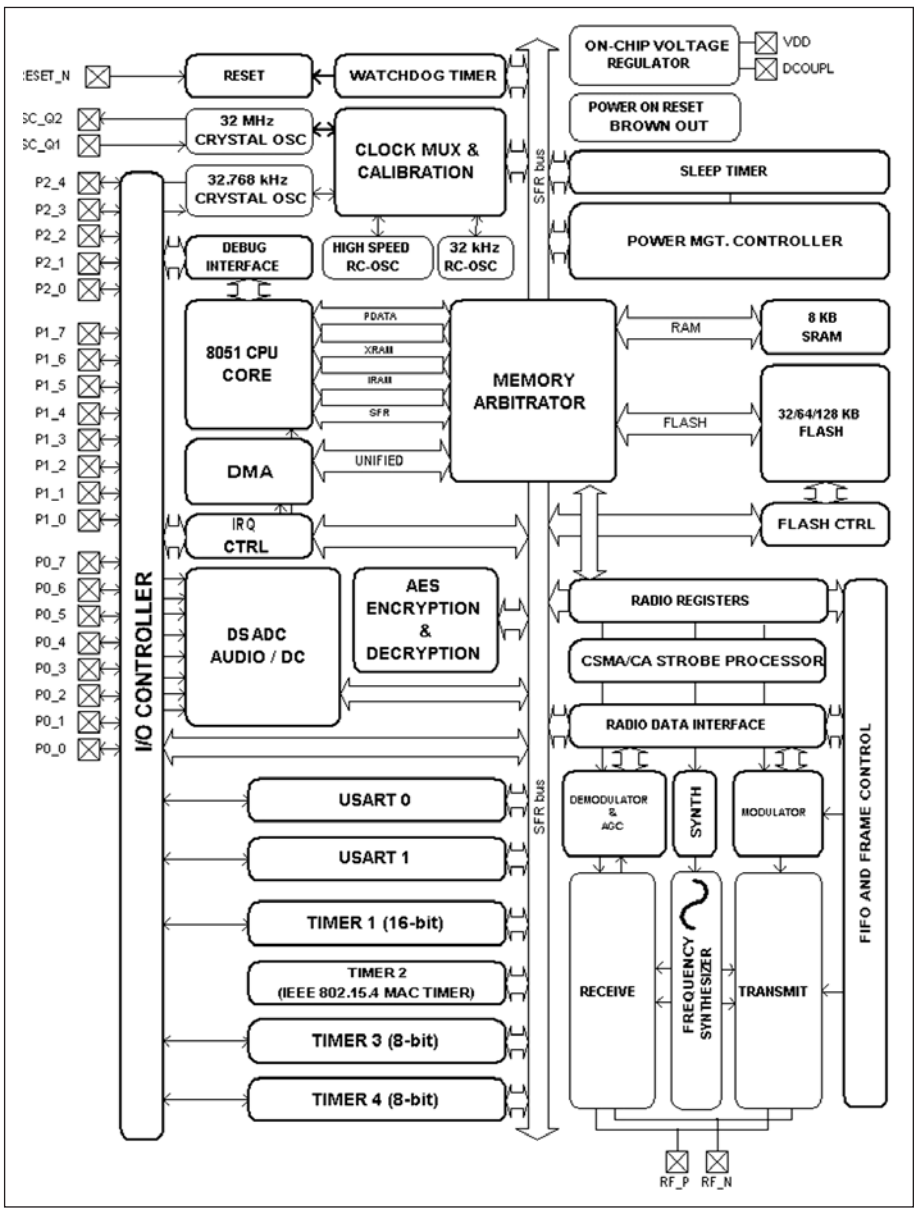


Figure 4 · Block diagram of the CC2430 IEEE 802.15.4/Zigbee SoC.

of the CC2430 family also contains 8K bytes RAM and powerful supporting features, and includes either 32K, 64K or 128K bytes of embedded Flash memory for optimal trade-off between complexity and cost. For example, a device equipped with 128K bytes of Flash and 8K bytes of RAM will be sufficient for virtually all ZigBee wireless network nodes, including coordinators, routers and end devices. The CC2430 solutions are implemented in a mainstream 0.18 µm CMOS technology with embedded-Flash capability, which enables the integration of digital baseband processing, RF and analog circuits and system memory on the same physical silicon. The unparalleled integration capability and low cost of CMOS make it the most viable technology for the implementation of the IEEE 802.15.4/Zigbee compliant SoC solutions.

A detailed block diagram of the CC2430 is shown in Figure 4. The most important subsystems of the CC2430 are the radio transceiver part and the microcontroller unit (MCU) including on-chip memory and peripherals. The remaining modules provide vital functions related to power management, clock distribution and test.

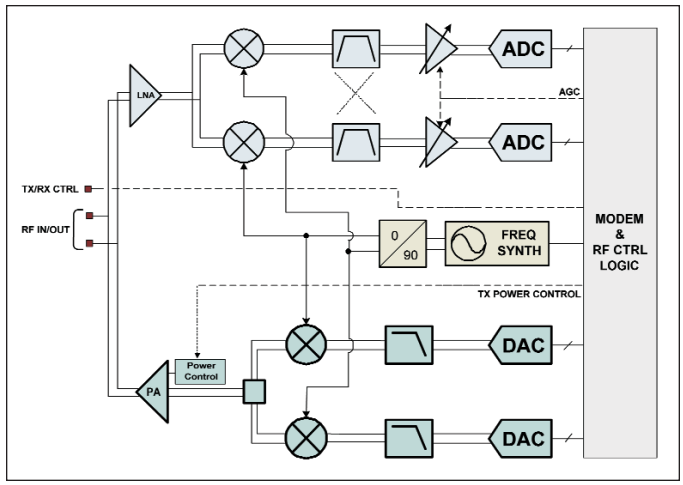


Figure 5 · RF and analog part of the CC2430.

RF/Analog Transceiver

The RF and analog part of the CC2430, as shown in Figure 5, implements the 2.4 GHz PHY-related operations of the IEEE 802.15.4 standard. The transceiver architecture of the CC2430 has been carefully selected to optimize functional performance, power consumption, ease-of-integration, and overall system BOM.

Driving IEEE 802.15.4/Zigbee silicons to the cost level and power performance necessary for mass market of low data rate applications requires pushing the channel filtering function on-chip using a single-conversion receiver architecture at a conveniently low IF. The CC2430 receiver is based on the low-IF architecture, eliminating largely the DC offset and 1/f-noise problems, wherein the received RF signal from the antenna is amplified by the low noise amplifier and down-converted in quadrature to a 2 MHz intermediate frequency (IF). The complex signal at IF is filtered and amplified, and then digitized by the analog-to-digital converters. Automatic gain control, fine channel filtering, and demodulation are performed in the digital domain for high accuracy and area efficiency. The Cyclic Redundancy Check (CRC) of the received data is carried out automatically on-chip, and the CC2430 buffers the received data in a 128 bytes RX FIFO. The relatively relaxed image and neighbouring channel rejection requirements of the IEEE 802.15.4 PHY are surpassed with good margins by the carefully designed low-IF receiver on the CC2430. The integrated analog channel filter enables excellent co-existence with other communication systems in the crowded 2.4 GHz ISM frequency band.

Efficient generation of the transmit signal according to the IEEE 802.15.4 PHY can be achieved by using single-step I/Q-up-conversion, which provides excellent performance and is extremely flexible with respect to supporting relatively high transmission rates and modulation formats of both constant and non-constant envelope nature. The CC2430 transmitter employs a direct-conversion modulator. The device buffers the supplied data in a 128 byte TX FIFO, and the preamble and start of frame delimiter (SFD) are generated in HW. The bit mapping and modulation are performed according to the IEEE 802.15.4 specification. The data bit stream is coded into pre-defined 4-bit symbols where each of the 16 symbols consists a nearly orthogonal 32-chip pseudo-random sequence. The overall data bit to symbol mapping effectively implements a DSSS scheme with a chip rate of 2 Mchips/s from a data rate of 250 kbps. The signal spreading and O-QPSK modulation with half-sine pulse shaping are performed digitally. The modulated and spread I/Q baseband signals are applied to the digital-to-analog converters (DAC's), whose outputs are lowpass-filtered and up-converted directly to RF by a single-sideband modulator. Finally, the RF signal is amplified to a programmable level by the on-chip power amplifier before entering the external antenna.

The RF input and output ports are fully differential and share two common pins. An external TX/RX-switch is not required as the CC2430 handles this switching internally. The chip-to-antenna RF interface effectively implements a balun and consists of a few low cost capacitors and inductors, which also provide impedance matching and slight filtering. Alternatively, a balanced antenna, such as a folded dipole, can be used.

The frequency synthesizer is fully integrated, eliminating any need for loop filter or VCO external passives. The on-chip LC VCO operating at twice the LO frequency range together with a divide-by-2 circuit provide the quadrature LO signals used by the up- and down-conversion complex mixers.

MAC HW Support

Saving processing bandwidth for network and application operations, the SoC design should relieve the mC for MAC-related timing critical operations that could be handled more effectively by dedicated circuitries. Therefore, the CC2430 integrates a significant set of the IEEE 802.15.4 MAC requirements to off-load the microcontroller. These include:

- CSMA-CA coprocessor
- Automatic preamble generator
- Synchronisation word insertion/detection
- CRC-16 computation and checking over the MAC payload
- Clear Channel Assessment
- Energy detection / digital RSSI
- Link Quality Indication

An embedded coprocessor handles the encryption/decryption operations employing the AES (Advanced Encryption Standard) algorithm with 128-bit keys required by IEEE 802.15.4 MAC security, the ZigBee™ network layer and the application layer. This dedicated AES coprocessor allows encryption/decryption to be performed with minimum mC usage.

MCU and Memory

The processing capability for execution of protocol stack, network and application SW of the CC2430 includes an enhanced version of the industry standard 8-bit 8051 microcontroller core with three different memory access buses, a debug interface and an 18-input extended interrupt unit. The enhanced 8051 core uses the standard 8051 instruction set but with typically 8× the performance of a standard 8051 core due to faster execution times and by eliminating wasted bus states.

The CC2430 includes a direct memory access (DMA) controller, which can be used to relieve the 8051 MCU core of moving data operations, thus achieving high overall performance with good power efficiency. The DMA controller can move data from a peripheral unit to memory with minimum mC intervention. At the heart of the system, a memory arbitrator connects the mC and the DMA controller with the physical memories and all peripherals through an SFR bus.

There are 8K bytes of static RAM available on the CC2430. The on-chip Flash block of either 32K, 64K or 128K bytes provides in-circuit programmable non-volatile program memory and is primarily intended to hold program code for the protocol stack, network and user application.

Peripherals and Supporting Features

Well-defined SoC's must also allow easy and flexible implementation of user-defined features. The CC2430 integrates a wide range of peripherals for this purpose.

Interrupts are useful for interfering with the normal program flow in case of important external or internal events that need immediate attention. Interrupt control together with incorporated sleep modes are very useful for saving power. The CC2430 interrupt controller services a total of 18 interrupt sources, divided into six interrupt groups, each of which is associated with one of four interrupt priorities.

The debug interface on the CC2430 implements a proprietary two-wire serial interface that is used for in-circuit debugging. Through this debug interface it is possible to perform an erasure of the entire flash memory, stop and start execution of the user program, execute supplied instructions on the 8051 core, set code breakpoints, and single step through instructions in the code. Using these techniques, it is possible to elegantly perform in-circuit debugging and external flash programming.

An I/O-controller is responsible for flexible assignment and reliable control of the 21 general-purpose I/O pins.

The CC2430 integrates four oscillators: a high-frequency 32 MHz crystal oscillator, a 16 MHz high-frequency RC-oscillator, an optional crystal oscillator, and an optional RC oscillator both at 32.768 kHz. The CC2430 uses one internal system clock, either by the 32 MHz crystal oscillator or the 16 MHz RC-oscillator. The choice of oscillator allows a trade-off between high-accuracy in the case of the crystal oscillator and low power consumption when the high-frequency RC oscillator is used. The system clock also feeds all 8051 peripherals, and operation of the RF transceiver requires active 32 MHz XOSC.

Four timers are available on the CC2430: one MAC timer, one general 16-bit timer, and two general 8-bit timers. The MAC 16-bit timer is mainly used to provide timing for IEEE 802.15.4 CSMA-CA algorithms and for general timekeeping in the 802.15.4 MAC layer. The other three timers support typical timer/counter functions such as input capture, output compare and PWM functions.

CC2430 has a built-in watchdog timer providing recovery mechanism in case of an out-of-control microprocessor, for example, due to software upset. To provide stable and robust operation, the CC2430 includes a power-on-reset and brown-out detector to protect the memory contents during supply voltage variations and provide correct initialisation during power-up.

The CC2430 also includes an eight channel, 8-14 bit delta-sigma ADC, a real time clock with 32.768 kHz crystal oscillator and two programmable USARTs for master/slave SPI or UART operation.

Tailored for Cost, Performance and Power

The CC2430 device [3] surpasses the IEEE 802.15.4 specification and delivers excellent RF performance in terms of selectivity and sensitivity for better co-existence

in the 2.4 GHz ISM band, and longer range and more reliable communication, respectively.

The CC2430 achieves ultra low power operation by combining low power consumption of the integrated circuitries, four operating power modes with different power profiles and by fast operating mode transition times. In the digital part, clock gating is employed to reduce dynamic power consumption, while ultra-low static (leakage) power consumption is obtained by turning off the power supply of modules that are not active.

The CC2430 is also equipped with sufficient processing bandwidth and memory for virtually all ZigBee and similar wireless network nodes, including coordinators, routers and end devices. The CC2430 can also be used as a general 2.4 GHz DSSS device for a number of proprietary or IEEE 802.15.4 compliant solutions not using ZigBee.

Conclusion

SoC devices tailored for IEEE 802.15.4/Zigbee applications, such as the CC2430, can deliver high and robust performance at low power consumption to a wide range of applications, including building automation, industrial monitoring and, and wireless sensor networks. These devices are extremely cost-effective and also enable the application design with the lowest bill-of-material. SoC devices will enable the end-users to develop complex wireless network products quickly, easily and reliably with one single active device in the system, thus reducing both time to market and production cost to the minimum. System-on-chip solutions, such as the CC2430, have arrived and will contribute to the envisioned ubiquity of Zigbee.

References

1. IEEE standard 802.15.4 - 2003: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)

2. www.zigbee.org

3. CC2430 datasheet, downloadable at www.chipcon.com

Author Informtion

Khanh Tuan Le is a senior RFIC system architect at Chipcon in Oslo, Norway, working on CMOS radio transceiver and system-on-chip solutions for WPAN, and related IPR matters. His previous working experience includes research and development of cellular and satellite mobile phones. Khanh can be reached at khanh.tuan.le@ ieee.org.