

A Power-Gated Sensor Node Microcontroller for Security Applications

G. Panić, T. Basmer, and O. Schrape

IHP, Im Technologiepark 25, 15236 Frankfurt Oder, Germany

<http://www.ihp-microelectronics.com>

Wireless sensor nodes play important role in power efficient implementation of wireless sensor networks (WSN). In many WSN applications, the content of monitored data is highly sensitive and must be protected from any type of malicious attacks. The security challenges in WSN are mainly driven by limited power and computing resources of sensor node devices, small memory, unsecure radio channels and susceptibility to physical capture. In many applications, commercially available sensor nodes that are entirely built from commodity-of-the-shelf (COTS) components cannot fully answer to specific requirements for low power and high efficiency. Furthermore, those sensor nodes do not provide enough resources to efficiently process security related tasks that employ advanced cryptographic algorithms. The design of an embedded sensor node microcontroller optimized for fast execution of secure crypto algorithms promises the best compromise between power, performance and security.

In this paper we present a low power sensor node microcontroller designed to cope with security problems in WSN. The microcontroller employs a 16-bit processor core supported by 16 kB of RAM and 64 kB of non-volatile Flash memory. It includes hardware accelerators for security related tasks that enable efficient execution of advanced crypto algorithms, AES (advanced encryption standard), ECC (elliptic curve cryptography), and SHA-1 (secure hash algorithm). The chip also integrates a baseband hardware accelerator that supports direct sequence spread spectrum (DSSS) and enables robust wireless communication. Additionally, the chip includes a number of peripherals including an analog-to-digital converter (ADC) that provides an interface to analog sensors, a number of serial interfaces (UARTs and SPIs), four digital IO ports, and two timers. The architecture of the chip is shown in Figure 1.

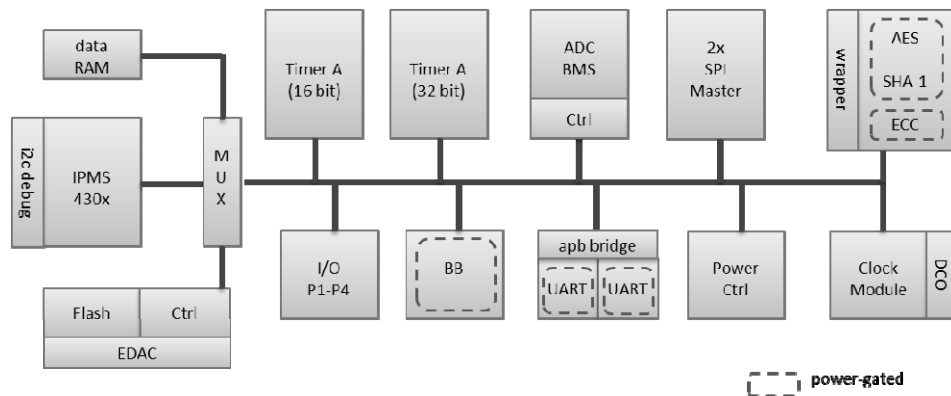


Figure 1. Architecture of sensor node microcontroller.

To enable low power operation, the microcontroller includes five power-gated islands which power supply can be cut-off during the sleep mode. The chip is designed for IHP 0.25 μm BiCMOS technology process, fabricated and successfully tested. The microcontroller runs with maximum frequency of 11.4 MHz and consumes around 10 mW at 1 MHz. The measurements showed several orders of magnitude improvement in the energy consumption of designed microcontroller when executing complex ECC tasks compared to software solutions.