Design of a Secure Personal Health Monitoring System

Application Example

With growing health awareness and the escalating cost of worldwide medical care, there is increasing emphasis on new and advanced technologies for disease prevention, early diagnosis, and treatment. Personal health monitors and other portable medical devices are making it easier for people to assess their wellness, adopt better lifestyles, and prevent the majority of serious illnesses. These devices also improve the management of existing, long-term conditions outside the hospital environment. Wearable units connected to treatment centers can alert health professionals to problems before they become serious, no matter where the patient is located.

Personal heart monitors, ultrasound devices, defibrillators, and other portable medical devices share common needs. They must ensure effective Data Security (authenticity and confidentiality) so that third parties cannot intercept personally identifiable medical data. In order to provide Data Security the device must also protect the design itself (Design Intellectual Property, or IP), called Design Security, so that the design can't be reverse engineered or tampered with. These types of attacks on the design could allow secure data to be compromised by circumventing any Data Security features. Portable versions of these systems, also need to be small, lightweight, and capable of operating for long periods on a single battery charge. All of these challenges can be met with field programmable gate array (FPGA) technology.

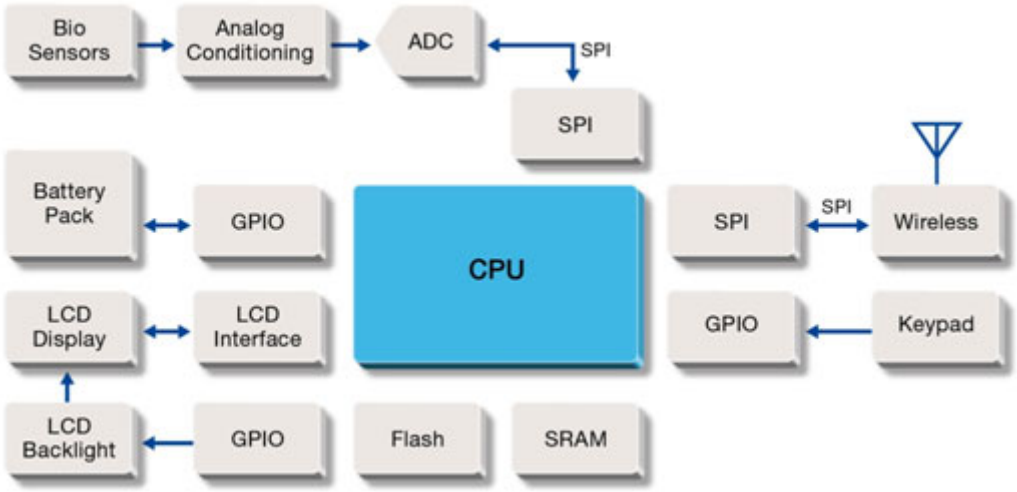

Figure 1: **Example of Personal Health Monitor – Block Diagram**

Example Portable Medical Device

The block diagram for a typical personal health monitor is shown in Figure 1. This monitor controls and reports various medical measurements and could include simple things like pulse rate and blood pressure or more complex measurements, such as those used to detect heart attacks or blood oxygen levels. Usually biosensors are used to capture data through an analog conditioning and conversion front-end. The CPU processes the data, stores key metrics, and displays results on the LCD. The keypad is used to select the desired function to be performed and a wireless connection can be used to send data to a storage or management system. Let's look at the key requirements for a typical system and then at a specific implementation to better understand the design of a typical personal health monitoring system.

Security Requirements for the Example Design

The growing use of portable devices to record, store, and transmit patient data to a central server means that personal health records now extend beyond the hospital or doctor's surgery. These devices need secure ways to transmit recorded data, through Data Security, at high speed to ensure that personal records cannot be compromised at any point. Additionally, it is increasingly important to provide Design Security to protect the design implementation from reverse engineering or tampering that could counter the Data Security of the system. Flash-based FPGAs have several key features that help protect design IP from attack.

Secure Your Design

Because flash-based FPGAs store the configuration bit files on-chip they are not exposed to 'snooping' during the reset or system power up cycle. SRAM-based FPGAs, on the other hand, must store the configuration file off-chip leaving it easily exposed to copying. Additionally, it is easy to reverse engineer an SRAM-based FPGA design from the captured bitstream so that key design elements or trade secrets can be discovered. Flash-based FPGAs additionally protect the on-chip configuration files by a variety of encryption methods during programming. The capabilities makes it easy to have devices programmed, even in an unsecure contract manufacturing facility without the possibility of reverse engineering or tampering. Using flash-based FPGAs, like those from Microsemi, secures your design even if your manufacturing isn't done in a secure location.

Protect Security Keys

Secure key storage is of critical importance for both Design Security and Data Security—since Data Security depends on security keys to implement standard security functions. It is important that your design uses the most robust security key storage algorithms and design techniques. For example, security keys that are protected from Differential Power Analysis (DPA) (an advanced side-channel attack that uses statistical analysis of small differences in device power use during cryptographic operations to determine security key values) are much more secure.

Support for Standard Cryptographic Functions

Once security keys are protected from attack, a variety of standard cryptographic functions are needed to protect data transferred to, from, or stored within the personal healthcare monitor. Encrypting messages, decrypting messages, and message authentication (proving that the source of the message is from the expected sender) are the most fundamental requirements needed for implementing Data Security functions. Some of the most common requirements include encryption and decryption using AES-128 or -256, SHA-256 for computing message digests, a Message Authentication Code (MAC) function (HMAC based on SHA-256), and a Non-Deterministic Random Number Generator. More advanced functions can include KeyTree Key Derivation (an alternative to HMAC), advanced challenge-response protocols to secure the transmission channel between sender and receiver, and a Physically Unclonable Function (PUF), used to create a physically unique device ID (much like a fingerprint) to support more advanced security capabilities.

Microsemi SmartFusion®2 and IGLOO®2 devices can support all these security requirements, as well as many more.

Portability and Power Efficiency Requirements for the Example Design

In addition to the robust security requirements of a portable medical device, power efficiency is also a key requirement. Portable devices typically run off of batteries and need to stay in service for as long as possible. A typical wearable heart monitor, for example, operates remotely using a battery. The monitor consists of a control unit wirelessly connected to a transmitter that relays heart-rate signals, skin temperature, and other measurements from a chest band or patch. Minimizing the power consumption of these portable devices is critical, and the challenge gets more difficult with the addition of liquid crystal display (LCD) technology and other new peripherals that simultaneously threaten to push system energy requirements even higher.

Many portable ultrasound scanners feature LCDs that support color and high resolution, and can consume as much as 50 per cent of the application's power budget. It is possible to significantly reduce battery drain in these situations by placing the LCD and control logic into power-saving mode whenever possible. This is difficult to do with off-the-shelf application-specific standard products (ASSPs) that are not designed for medical applications.

Minimize Active Time for High Power Functions

Wireless biosensors have the most critical power requirements since they must make measurements, process data, and send results wirelessly to the controller. One power saving approach is to minimize the amount of time the RF transmitter is active, since it can represent a large percentage of the overall power budget. By pre-processing signal data, perhaps using on-chip Digital Signal Processing (DSP) functions embedded in the FPGA fabric, the amount of data that needs to be transmitted can be dramatically reduced. For example, many systems monitor certain conditions (for example, the electrical profile of each heartbeat), that can provide vital information on the progress of a condition and give early warnings of potential problems. If these profiles can be generated locally, a simple summary of key metrics can be sent through the RF transmitter instead of the full data stream. The transmitter can be powered down for longer periods of time, saving a significant amount of energy. SmartFusion and IGLOO devices, with integrated analog capabilities along with FPGA fabric, are an excellent platform for creating intelligent and low power biosensors.

Offload Processing Functions to FPGA Fabric

The control unit can also use several power saving tricks when implemented with advanced FPGAs. FPGA fabric can be used to implement DSP functions prior to use by the control function. For example, a fabric-based pre-processing engine can perform filtering or correlation functions and buffer it prior to use by the control function. The control function need only be activated when the data buffer has reached a certain limit. This dramatically improves power efficiency and extends battery life, since the control function (either implemented in FPGA fabric or through an on-chip embedded processor) is active only a fraction of the time. SmartFusion2 and IGLOO2 devices are a good fit for applications that need a mix of control and DSP pre-processing.

The Design of a Typical Health Monitoring System

Figure 2 on page 4 shows the configuration of a typical health monitoring system. An FPGA is the heart of the control system implementing all the algorithmic, interface, and storage functions. Depending on the specific application requirements different FPGA implementations are possible. For example, if the analog requirements are considerable and the digital control is complex, the Microsemi SmartFusion device can be an excellent fit. It integrates an embedded industry standard microprocessor, flash and SRAM memory, standard peripherals, a wealth of advanced security functions, FPGA fabric, and programmable analog functions (such as voltage, current and temperature monitors; integrated ADC and DAC; analog inputs and outputs; and an Analog Compute Engine to offload the CPU), all on the same chip.

If the analog requirements are simpler, but more digital functions are required, the SmartFusion2 device provides more programmable fabric and additional fixed function capabilities, but doesn't have the on-chip analog capabilities. IGLOO and IGLOO2 devices are most appropriate when computational complexity is low and low-power is more important.

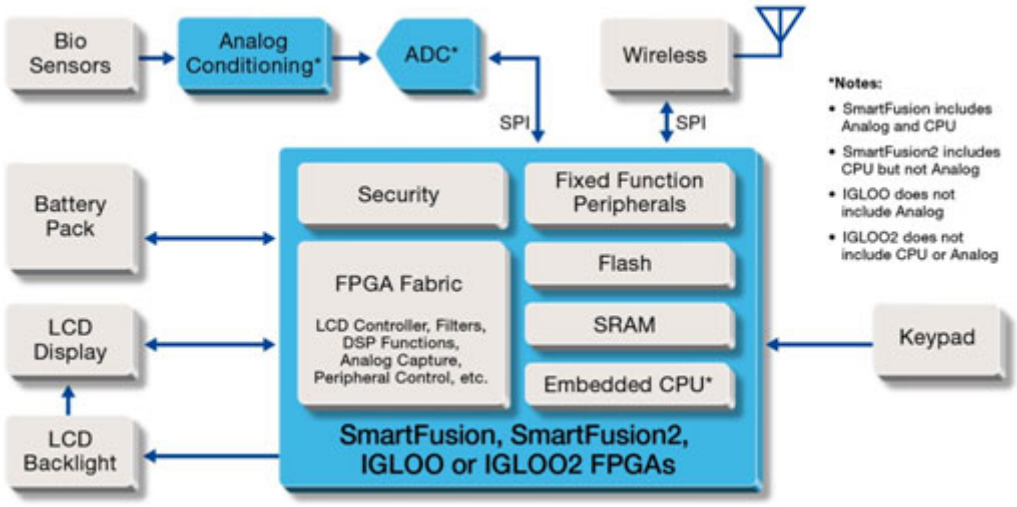

Figure 2: **Block Diagram of the Design for a Personal Health Monitor**

Secure Configuration and Security Key Protection

As previously outlined, the security requirements of the Personal Health Monitor include both Design Security and Data Security. When using Microsemi flash-based devices the configuration bitstream is stored inside the devices, embedded within the FPGA fabric. This eliminates the possibility of 'copying' the bitstream during power-up that SRAM-based FPGAs are subject to. Additionally, because the SmartFusion2 and IGLOO2 configuration bitstream is encrypted, this eliminates the possibility of the design being copied during programming, even at an unsecure contract manufacturing location. Security keys are stored in non-volatile flash memory on-chip and are protected by a variety of DPA attack resistant design and architectural techniques, used under license from CRI. You can explore these techniques in more detail by referring to the articles and videos listed in the "To Learn More" section at the end of this paper under the heading "Protecting Your Design from Side-Channel Attacks".

Data Security Capabilities Support Security Standards

SmartFusion2 and IGLOO2 devices provide a significant amount of Data Security capabilities, typically implemented through service calls to the Security Subsystem. Several industry standard cryptographic functions are supported by simple security service calls including encryption and decryption algorithms such as AES-128 and -256, a Message Authentication Code function (HMAC based on SHA-256), and a Non-Deterministic Random Number Generator (used in some advanced Data Security algorithms to improve secure transmissions by eliminating 'repeated' datasets). More advanced functions include KeyTree Key Derivation (an alternative to HMAC), advanced challenge-response protocols to secure the transmission channel between sender and receiver, and a Physically Unclonable Function (PUF) used to create a physically unique device ID (much like a fingerprint) to support more advanced security capabilities. These are just some of the many Data Security features available on SmartFusion2 and IGLOO2 devices that make them the worlds best platform for implementing secure embedded systems. You can find out more about Data Security by referring to the articles and videos listed in the "To Learn More" section at the end of this paper.

Low Power Capabilities

Once the security requirements are met, the low power requirements of the design must be addressed. Microsemi flash-based ultra-low-power FPGAs can meet the most aggressive power requirements. For example, the Microsemi IGLOO and IGLOO2 devices have been optimized for low power and can push power draw down to as low as 2 µW, when the system is not in active use. IGLOO devices don't include analog functions, but they can support an on-chip processor, so they are appropriate for designs where lower power is critical. IGLOO2 devices don't include analog functions, or an embedded processor (but control functions can be implemented in FPGA fabric), however, they do include several enhanced memory functions for designs with critical data bridging and data buffering requirements. They enable the implementation of a variety of storage and I/O functions that push power draw down to 2 µW when the system is not in active use. This is a vital consideration for systems such as automated external defibrillators, which may be left unattended for weeks or months between tests.

Not all FPGA memory technologies deliver the same levels of power efficiency, however. Today's high-density FPGAs can be based either on static random access memory (SRAM) technology, or non-volatile flash memory technology. The former tend to have high power requirements because a constant current is needed to keep their configuration cells programmed. This limits their deployment in portable or battery-powered medical equipment. In contrast, FPGA-based on-flash memory technology, like those from Microsemi, don't need this additional current. These flash-based FPGAs also have the unique capability of putting the entire device into an ultra-low power state when not in use. For medical devices that often have a low duty cycle and experience long periods between uses or measurements, this feature can make a dramatic difference in battery life.

Improved Integration using Flash-based FPGAs

Flash-based FPGAs also make it easier to squeeze more capabilities into a smaller space. SRAM-based FPGAs may require significant additional circuitry, including a boot read-only memory (ROM) and additional system memory for unsecure configuration code, plus a complex programmable-logic device (CPLD) for system configuration and supervisory tasks. Clock and reset signal generation circuits are also required upon power-up to help initialize components on board. These issues reduce reliability, add complexity and cost to the system design, and slow down the development process. In contrast, flash-based FPGAs are live at power-up, so they don't need this additional circuitry. In addition to improving system operation and reducing power consumption, being live at power-up also gives users immediate access to control functions, which is particularly important for many portable medical devices.

Conclusion

Today's personal health monitoring systems and similar medical devices must use a variety of design techniques to protect the underlying design as well as protect the sensitive data stored within or transmitted to/from the device. Many personal health monitoring devices must also be portable, so they need to be small, lightweight, and low-power. Nonvolatile, flash-based FPGA technology, like those available from Microsemi, deliver the necessary security, integration, and low power consumption to enable extremely compact and energy-efficient system designs that are also extremely difficult to copy or tamper with.

To Learn More

Protecting Your Design from Side-Channel Attacks

1. Protect FPGAs from Power Analysis
2. How Easy is it to Secure Your Designs?
3. What is Design Security in a Mainstream SoC Chalk Talk

Data Security

1. Overview of Data Security Using Microsemi FPGAs and SoC FPGAs
2. SmartFusion2 and IGLOO2 Cryptography Services
3. Overview of Secure Boot with Microsemi SmartFusion2 SoC FPGAs

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo CA 92656 USA
Within the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996

Microsemi Corporation (NASDAQ: MSCC) offers a comprehensive portfolio of semiconductor solutions for: aerospace, defense and security; enterprise and communications; and industrial and alternative energy markets. Products include high-performance, high-reliability analog and RF devices, mixed signal and RF integrated circuits, customizable SoCs, FPGAs, and complete subsystems. Microsemi is headquartered in Aliso Viejo, Calif. Learn more at **www.microsemi.com**.

55900166-0/11.13