EnforcIT
Security Monitor

The Heart of Security

Every system has unique security, power, performance, safety, and business requirements. While many of these requirements can be addressed with the right selection of hardware and software, security is a requirement that spans nearly all parts of a system. Security is therefore both a strategic and technological problem for program managers and developers. Since it is generally unfeasible to solve security problems using a single technology, using mature security products based on established expertise is a far more effective approach.

EnforcIT® Security Monitor addresses complex security, performance, safety, and business requirements by providing a configurable, multi-layered security IP block for Microsemi's SmartFusion®2 and IGLOO®2 field programmable gate array (FPGAs). Built using nearly a decade of FPGA security experience and built into the heart of the lowest-power and most secure FPGAs on the market, EnforcIT Security Monitor allows the end-user to configure additional layers of tamper protections and tamper response penalties through a single soft IP block.

Intelligent Security

EnforcIT Security Monitor is a single, low-resource, soft IP block capable of monitoring and responding to an assortment of internal security flags and system conditions. Taking full advantage of the tamper detectors and responses built into the FPGA silicon, it can report threats, act autonomously, or some combination thereof. Once implemented, it acts as an intelligent security controller for the hardware security mechanisms packaged with the SmartFusion2 and IGLOO2.

When configured for reporting, EnforcIT Security Monitor can report to the FPGA a variety of internal security flags and system conditions. When configured to act autonomously, EnforcIT Security Monitor can respond to FPGA threats and take action, mitigating further attack by protecting or destroying critical data and design.

Configurable Security

The EnforcIT Security Monitor IP block is made up of a JTAG monitoring core, a clock frequency monitor core, a system heartbeat, and a watchdog timer, all working together to ensure the FPGA is not under attack. Each of these four components can emit individual tamper responses. Under tamper, the user can configure various responses up to and including device zeroization.

Each component in EnforcIT Security Monitor can be independently configured for tamper monitoring and customized for response. The entire IP block utilizes less than 5 percent of Microsemi® SmartFusion2 FPGA in a typical configuration and is easily customized by the end-user, minimizing impact to development schedules without compromising on security or performance.

Configurable Security

EnforcIT Security Monitor was built using nearly a decade of FPGA protection development experience. It can be used as part of the layered solution in NSA's Commercial Solutions for Classified Program. This and other Microsemi cryptography, software, and hardware products including WhiteboxCRYPTO™ and EnforcIT are built in the U.S. in one of Microsemi's trusted facilities.

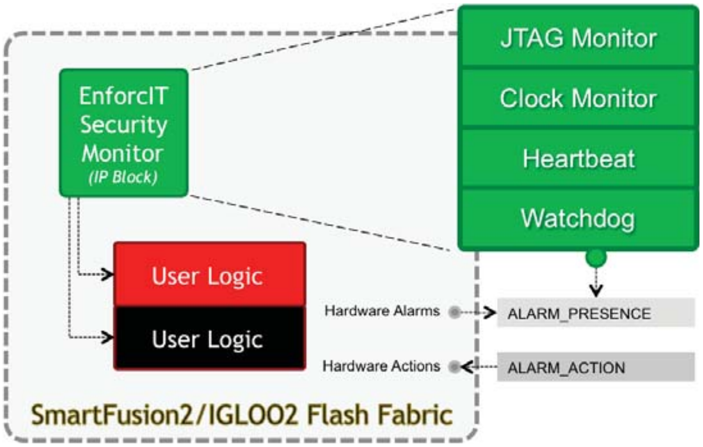

Figure 1: **Security for Critical Data and Designs at Rest and in Motion**

Microsemi Security Solutions

The Microsemi SmartFusion2 and IGLOO2 FPGA families have the world's best suite of complementary security features for implementing protected embedded systems. These FPGAs can implement many security-enhancing capabilities without negatively impacting system requirements. With innovative technology, holistic security conscious device architecture (from the bottom level silicon process all the way up to the target system), simplified design methodology, and extensive support ecosystem, many security capabilities can be implemented without any added system cost, additional power, or increased time to market.

EnforcIT Security Monitor intelligently reports threats, acts autonomously, or some combination thereof allowing the user to find the right balance between security, performance, and safety.

Table 1: Features and Benefits

Features	EnforcIT Security Monitor Benefits
Seamless Interface	Seamlessly interfaces with Microsemi's SmartFusion2 SoC and IGLOO2, the most secure and lowest power FPGAs on the market.
Configurable	Configurable alarm actions include zeroize, lockdown, chip reset, and more.
Safety Controls	Safety controls permit the user to delay or cancel automatic responses.
Customizable Security	Customizable clock, JTAG, and timeout monitoring; Logic integrity and fault detection; Runtime IP version reporting.
Extensible	For advanced security needs, contact sales@microsemi-wl.com about enhancing EnforcIT Security Monitor with additional FPGA security IP cores including FIPS 140-2 certified Suite B cryptography, secure memory controllers, secure logging, authentication, and more.

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer's responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided "as is, where is" and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,600 employees globally. Learn more at www.microsemi.com.

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
email: sales.support@microsemi.com
www.microsemi.com