SECURITY MONITOR IP CORE

SECURITY MONITOR IP:

Industry-Leading Programmable Device Security Protecting IP and Mission Critical Data

Defense contractors and government agencies must address secure and complex specifications to deliver solutions with Information Assurance (IA) and Anti-Tamper (AT) support. In commercial markets, solution providers put high priority on safeguarding their business-critical on-device intellectual property.

An agency-evaluated and exportable[1] security solution, the Xilinx® Security Monitor (SecMon) IP meets security needs of both defense-related and commercial projects. The fully autonomous soft core continuously monitors for signs of post-configuration tampering and can carry out penalties that render designs inaccessible. The mature, proven technology is now in its 6th generation of development[2].

Xilinx Solution Highlights

- Level of protection to help customers meet the stringent design requirements of secure Aerospace and Defense products as instructed by DoD 5200.39
- Commercially viable and exportable solution for safeguarding on-device intellectual property
- Mature, proven technology now in its 6th generation of development[2]
- Autonomous and self-contained; does not require off-chip control or support (e.g. no need to load external bitstream during zeroization)
- Extensive monitoring functions: integrity of configuration memory, environmental conditions, JTAG status, and more
- Partial Reconfiguration Support / Monitoring
- User-customizable penalties and automatic tamper responses to attempted attacks or “hackers”
- Easy design integration (fully placed-and-routed design file delivered in the innovative Qualified Bitstream Flow)

1 Xilinx SecMon IP has been approved by the U.S. Department of State for export (January, 2012).

2 Available for Virtex®-5, Spartan®-6, Virtex®-6 and 7-Series & Zynq® All Programmable SoC families today. Development in progress for UltraScale™ Kintex® and Virtex devices, with Vivado® Constraint Files (.XDCs) available upon request for planning purposes (includes definition of SecMon reserved pins and FPGA logic). Contact your local Xilinx FAE for details.

XILINX
ALL PROGRAMMABLE™

Corporate Headquarters

Xilinx, Inc.
2100 Logic Drive
San Jose, CA 95124
USA
Tel: 408-559-7778
www.xilinx.com

Europe

Xilinx Europe
One Logic Drive
Citywest Business Campus
Saggart, County Dublin
Ireland
Tel: +353-1-464-0311
www.xilinx.com

Japan

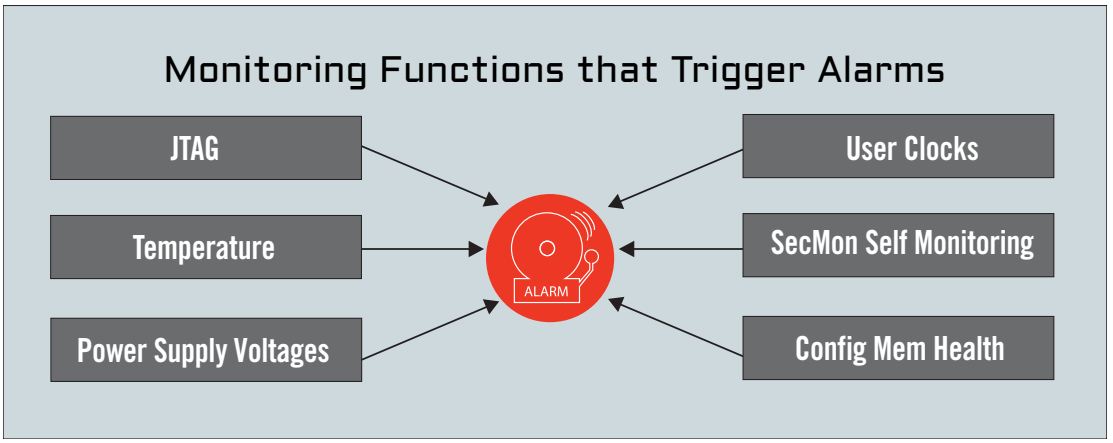
Xilinx K.K.
Art Village Osaki Central Tower 4F
1-2-2 Osaki, Shinagawa-ku
Tokyo 141-0032 Japan
Tel: +81-3-6744-7777
japan.xilinx.com

Asia Pacific Pte. Ltd.

Xilinx, Asia Pacific
5 Changi Business Park
Singapore 486040
Tel: +65-6407-3000
www.xilinx.com

India

Meenakshi Tech Park
Block A, B, C, 8th & 13th floors,
Meenakshi Tech Park, Survey No. 39
Gachibowli(V), Seri Lingampally (M),
Hyderabad -500 084
Tel: +91-40-6721-4747
www.xilinx.com



Post-Configuration Security

SecMon IP core operates completely independent within an FPGA/SoC design to augment existing silicon security features with post-configuration Anti-Tamper protection. The power draw (60mW, worst case) and resource impact (approximately 1% to 8% on the largest to smallest supported FPGA/SoC) are minimal.

Autonomous Monitoring

- Configuration Memory Integrity
- JTAG Activity
- Temperature and Voltage
- User Clocks
- Partial reconfiguration
- Self-monitoring

Configurable Penalties

- Zeroization of FPGA Configuration Memory
- Zeroization of AES Bitstream Key
- Global 3-State
- Global Set/Reset

System Extensibility

- Penalties can be asserted due to off-chip events at the system level
- Alarm limits (e.g. temperature and voltage) are user-configurable; Programmable alarm responses, with delays for accommodating related “housecleaning” events
- Custom tamper conditions (monitor system loops, voltage, etc., via analog input pins)
- UltraScale-based SecMon IP (currently under development) allows multiple SecMon IP cores to be connected together to act as a single functional anti-tamper unit. This provides a solution for both board level (device-to-device) and stacked silicon interconnect (SSI) devices with multiple instances of the SecMon IP.

Revolutionary Delivery Innovations

Delivered as a fully placed-and-routed design file, the SecMon IP allows developers to import Anti-Tamper capabilities into designs with much shorter customer verification and certification times. Xilinx also offers an industry-first automated Bitstream comparison capability for customers that require maximum verification of the integrated security solution. The Xilinx Qualified Bitstream Flow speeds time to market, and potentially saves customers thousands of hours of engineering design and verification effort while upholding strict quality standards.

Take the NEXT STEP

For more information about Xilinx SecMon IP supported devices and availability, please contact your Xilinx sales representative or a local Xilinx office.

XILINX
ALL PROGRAMMABLE™

Printed in the U.S.A. ww2015