SECURITY MONITOR IP CORE

SECURITY MONITOR IP

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

Defense contractors and government agencies must address secure, 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 exportable[1] security solution, the Xilinx® Security Monitor (SecMon) IP, meets security needs for both defense 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 8th generation[2] technology is proven and mature.

Xilinx Solution Highlights

- Protection level helping customers meet the stringent design requirements of secure Aerospace and Defense products as instructed by DoD 5200.39
- Commercially viable and exportable solution to safeguard on-device IP
- Mature, proven technology now in its 8th generation[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 place-and-routed design file delivered in the innovative Qualified Bitstream Flow for all available device families through Kintex® & Virtex® UltraScale® devices – source code for Zynq® UltraScale+™ SoC devices)

Post-Configuration Security

The 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.

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, Kintex and Virtex UltraScale, and Zynq UltraScale+ MPSoC and RFSoC & Zynq SoC families today. Contact your local Xilinx FAE for details.

XILINX

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

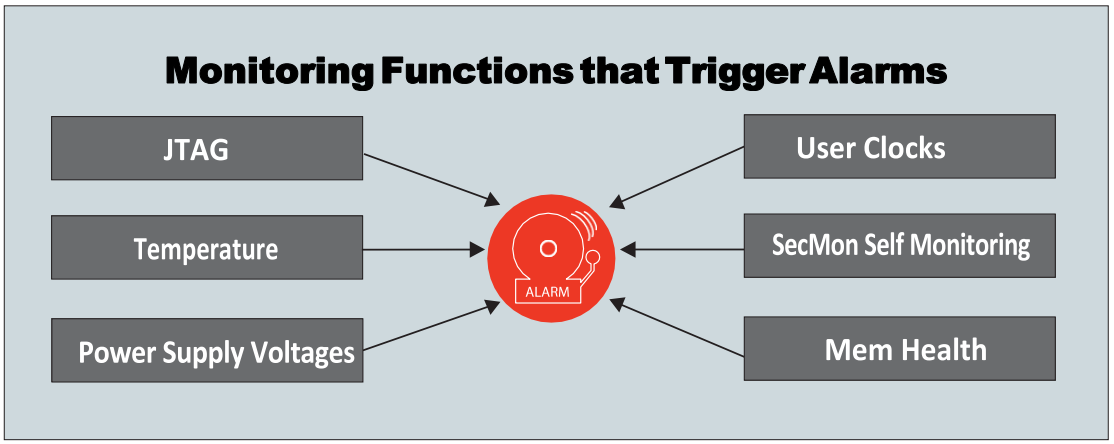
Xilinx K.K.
Art Village Osaki Central
Tower 4F 1-2-2 Osaki,
Shinagawa-ku
Tokyo 141-0032 Japan
Tel: +81-3-6744-7777
japan.xilinx.com

Asia Pacific Pte. Ltd.

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

India

15th Floor, Unit 2A and 2B, Parcel -4,
Octave Block, Salarpuria Sattva
Knowledge City, Survey No. 83/1
Raidurg, Hyderabad, Ranga Reddy
District, Telangana, 500081
Tel: +91-40-6721-4747



Autonomous Monitoring

- Configuration Memory Integrity
- JTAG Activity
- Temperature and Voltage
- User Clocks
- Partial reconfiguration
- Self-monitoring
- Security Critical Register Monitoring
- Processor System Memory Health in Zynq UltraScale+ SoC devices

Configurable Penalties

- Zeroization of FPGA Configuration Memory
- Zeroization of PS Memories and Secure Lockdown in Zynq UltraScale+ SoC
- 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 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 place-and-routed design file for all available device families through Kintex and Virtex UltraScale, 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 can save customers thousands of hours of engineering design and verification effort while upholding strict quality standards.

Delivered as both software and HDL source code, Zynq UltraScale+ SoC Security Monitor is easily integrated using the standard Xilinx tool flows while expanding the provided protection to include the entire Processor System and Programmable Logic. A full documentation suite, including integration instructions, user guide, test plan, and test software, speeds time to market.

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.

Printed in the U.S.A. ww2015