Security Supervisor IP (SSIP) for Secure and High Assurance Systems

Why Use Altera's SSIP?

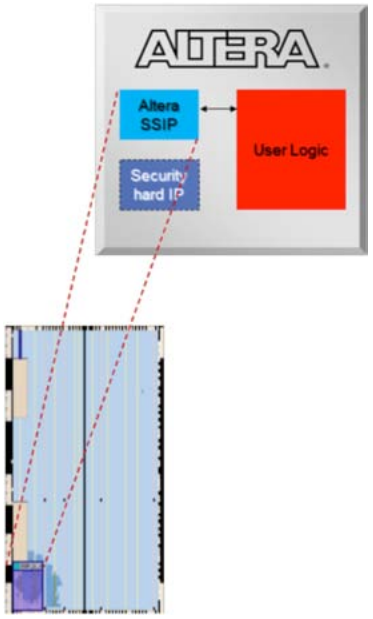
If you are developing a high security or anti-tamper application, Altera's SSIP design block provides all of the configuration settings. In addition, it provides logic to zeroize the device and its configuration registers upon detection of a tamper event.

Multiple security certification authorities are already familiar with Altera's SSIP block and can provide simple direction on how to use the block to ensure system security. This is a key advantage over developing an SSIP of your own.

Additional Features of Altera FPGAs Suitable for Military Applications:

- **SEU Detection and Mitigation** Automatically and continually monitors FPGA configuration RAM for SEU or other errors
- **Extended Life Cycles:** Altera historically provides the longest life cycles of all major FPGA providers, reducing costly EOL risks to program
- **Leaded Packages:** Altera provides leaded package options across nearly all product families
- **Reliable Supply Chain:** Altera maintains a reputation for robust and reliable supply chains
- **AQEC Compliance:** Altera is part of the Aerospace Qualified Electronics Components (AQEC) working group and previous families hold GEIA-STD-0002-01 certifications
- **DO-254 Compliance Solutions:** Combined with certified NIOS® II soft embedded processors and third party assessment partners, Altera has a long history of use in DO-254 applications
- **Advanced Security Features:** Altera has a legacy of security features in all FPGA product families to include bitstream encryption and authentication, anti-tamper and anti-cloning features, and now secure boot and code authentication for Arria® 10 SoC ARM Cortex A9 processors

SSIP is a Logic Locked IP Region



Altera FPGA and SoC products have provided a long history of user accessible and configurable security features for increasingly complex and sensitive logic designs. These designs include early bitstream encryption capabilities in Stratix® II, to more sophisticated static and active features available on modern devices.

FPGA designers have historically been responsible for learning about, testing, configuring, and implementing these security features and capabilities.

Altera's SSIP block, however, provides a single licensable and downloadable logic region dedicated to accurately and correctly setting the security configurations, and providing responses to potential detected attacks.

The SSIP was originally developed as part of a complete high security FPGA solution with the Cyclone® IIILS low power family of devices. Today, however, Altera's entire product portfolio brings these same high assurance and high security features to all of your designs, utilizing the SSIP, and following secure design guidelines provided by authorized government sponsors, will enable faster time to develop, test, and certify system security certifications and requirements for DoD systems.

Use Cases and Scenarios Involving SSIP

The Altera SSIP block operates continuously as part of an overall high security system. It ensures that the FPGA is in a known state upon initialization, ensures that the device remains in the known state, and enables a design to shut down quickly without compromising sensitive data, in the event that an alarm has been triggered.

The SSIP is a logic block that has been designed into a specific logic lock region of the FPGA so that it interacts directly with the device configuration block (DCB). This gives direct and low latency access to device monitors and sensors, as well as the partial reconfiguration control block that is central to the zeroization capability of the SSIP. This logic lock partition is also essential in making sure that a zeroization process overwrites the entire configuration RAM space within the device without impacting its own logic structure and terminating a zeroization event before it is complete.

The SSIP block is designed to allow all permutations of FPGA security features to be implemented in a system. For this reason, it is ideal for use in a product platform where different variants may require different security settings (i.e., domestic military sales versus foreign military sales).

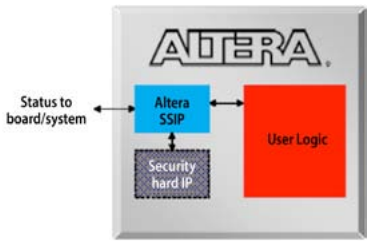
SSIP Features and Functions

	Capability	Benefits to Secure Communications Systems
Monitoring	SSIP Provides Control Block Connectivity, User Settings, and Documentation to Monitor Environment	• Redundant monitoring functions • User Watchdog Timer for command/response awareness • Errors in configuration monitored and reported • Changes in volatile key value or state • Current version (Stratix V) now includes temperature monitor
Status	Continuous Status Register Update	• SSIP heartbeat signal generated and monitored • Alarms and triggers can be set and controlled by SSIP • The current command state and progress of device zeroization
Response	Key Zeroization and Partial Reconfiguration	• User alarms acknowledged • Zeroization of key and entire device configuration RAM through partial reconfiguration • Lock-out of external JTAG access (if not already locked out) • Can tri-state all FPGA I/O

Supported Devices and Resource Counts (Arria V and Stratix V Available Upon Request)

	Estimated Combinational LUTs	Registers	Memory	Support
	979	466	16K	• Available as part of complete certified Cyclone IIILS high assurance solution • Also compatible with design separation flow and monitoring of traffic in red and black FPGA regions • SSIP licensed, delivered, and certified by the United States government • Full documentation and licensing terms available • Solution fielded today in multiple cryptographic modules and systems
	1736	831	14 x M10K	• Based on Cyclone IIILS SSIP but includes new monitoring capabilities • Zeroization of keys, CRAM, and ERAM now accomplished and verified through partial reconfiguration • SSIP supports full range of Cyclone V devices • SSIP support of Arria® V and Stratix V FPGAs available upon request

SSIP Interface to User Logic and Hard Security IP



Learn More About SSIP for Altera Devices

Learn more about SSIP and other solutions for high assurance and anti-tamper systems by visiting http://www.altera.com/end-markets/military-aerospace/secure/mil-secure.html or contact your local Altera representative for additional information about capabilities and licensing information for the SSIP. An SSIP user's guide is available for qualified licensees.

Altera Corporation
101 Innovation Drive
San Jose, CA 95134
USA
www.altera.com

Altera European Headquarters
Holmers Farm Way
High Wycombe
Buckinghamshire
HP12 4XF
United Kingdom
Telephone: (44) 1494 602000

Altera Japan Ltd.
Shinjuku i-Land Tower 32F
6-5-1, Nishi-Shinjuku
Shinjuku-ku, Tokyo 163-1332
Japan
Telephone: (81) 3 3340 9480
www.altera.co.jp

Altera International Ltd.
Unit 11- 18, 9/F
Millennium City 1, Tower 1
388 Kwun Tong Road
Kwun Tong
Kowloon, Hong Kong
Telephone: (852) 2 945 7000
www.altera.com.cn

SS-1058-1.0