CoreSMIP v2.0

Handbook

Table of Contents

Introduction

Core Overview

CoreSMIP (SMIP = Security Monitor Intellectual Property) can be used to enhance the security of a design implemented in a SmartFusion2 or IGLOO2 device. CoreSMIP can initiate the erasure (or zeroization) of programmed data within a device when any of the following occur:

1. A user requests device erasure by asserting the ERASE_P or ERASE_N input.
2. Some unauthorized activity occurs such as the detection of an attempt to use the JTAG debug port.

Key Features

- Monitors tamper detection indicators within the device.
- Outputs signals corresponding to tamper indicators along with a master alarm signal.
- Outputs a heartbeat signal that toggles continuously.
- Can initiate device erasure/zeroization in reponse to tamper detection or when requested to do so by the assertion of an input.
- The extent of zeroization that occurs is configurable.

  Note: The device can be left in a non recoverable state if CoreSMIP is configured for this outcome.
- A watchdog counter delays the onset of zeroization by 1000 cycles of CLK after a tamper event is detected. The watchdog can be reset by simultaneously toggling the RESET_WATCHDOG_P and RESET_WATCHDOG_N inputs to their active states to extend the time before the initiation of zeroization. This may be useful where a system requires more time to housekeep before zeroization occurs.
- When device zeroization is requested by assertion of the ERASE_P or ERASE_N inputs, zeroization is initiated immediately and the watchdog does not feature.

Supported FPGA Families

CoreSMIP supports the following families:

- SmartFusion2
- IGLOO2

Core Version

This handbook supports CoreSMIP v2.0.

Interface Description

Parameters

The parameters present on CoreSMIP are listed in Table 1.

Table 1 CoreSMIP Parameters

Parameter	Description
ZEROIZATION_LEVEL	Controls the extent of the zeroization that will occur if device zeroization is initiated. Possible settings are: 3 – No zeroization occurs. 2 – Device is erased and left in a “like new” state. The device can be reprogrammed. 1 – Part is erased but can be recovered. 0 (or any value aside from 1, 2, or 3) – Part is erased and cannot be recovered. In the configuration GUI for CoreSMIP, these options are presented in text form as follows: Unchanged (No zeroization occurs.) Like new Recoverable Non recoverable

Ports

The ports present on CoreSMIP are listed in Table 2.

Table 2 CoreSMIP Ports

Port Name	Type	Description
CLK	Input	Clock.
RESET_N	Input	Active low reset.
ERASE_P	Input	Active high device erase request. This input should be asserted for at least two cycles of CLK to cause device erasure/zeroization. The degree of zeroization is determined by the setting for the ZEROIZATION_LEVEL parameter.
ERASE_N	Input	Active low device erase request. This input should be asserted for at least two cycles of CLK to cause device erasure/zeroization. The degree of zeroization is determined by the setting for the ZEROIZATION_LEVEL parameter.
RESET_WATCHDOG_P	Input	Assert this input (high) at the same time as the RESET_WATCHDOG_N input to reset the internal watchdog counter. More precisely, a rising edge on this input should occur within

Port Name	Type	Description
		one quarter of a cycle of CLK from a falling edge on RESET_WATCHDOG_N to reset the watchdog.
RESET_WATCHDOG_N	Input	Assert this input (low) at the same time as the RESET_WATCHDOG_P input to reset the internal watchdog counter. More precisely, a falling edge on this input should occur within one quarter of a cycle of CLK from a rising edge on RESET_WATCHDOG_P to reset the watchdog.
HEARTBEAT	Output	Toggles every 1000 cycles of CLK.
JTAG_ACTIVE	Output	Asserted if the JTAG TAP controller is released from reset.
LOCK_TAMPER_DETECT	Output	Asserted if a parity error is detected on the internal lock data.
MESH_SHORT_ERROR	Output	Asserted if short is detected in the mesh covering the Security Flash.
DIGEST_ERROR	Output	Asserted if a digest request has detected an error.
POWERUP_DIGEST_ERROR	Output	Asserted if a flash digest error is detected at power up.
SC_ROM_DIGEST_ERROR	Output	Asserted if a System Controller ROM digest error is detected.
PASSCODE_ERROR	Output	Asserted if an attempt has been made to match an incorrect passcode.
MASTER_ALARM	Output	Asserted if any of the other error indication outputs are asserted. This signal is essentially the logical OR of the eight signals listed in the rows above, from JTAG_ACTIVE to SYSCTRL_UNRESPONSIVE inclusive. After MASTER_ALARM asserts, it can only be cleared by resetting the core.

Note: All signals in this table are active high unless otherwise stated.

Tool Flows

SmartDesign

Figure 1 shows how the CoreSMIP symbol appears in a SmartDesign design.

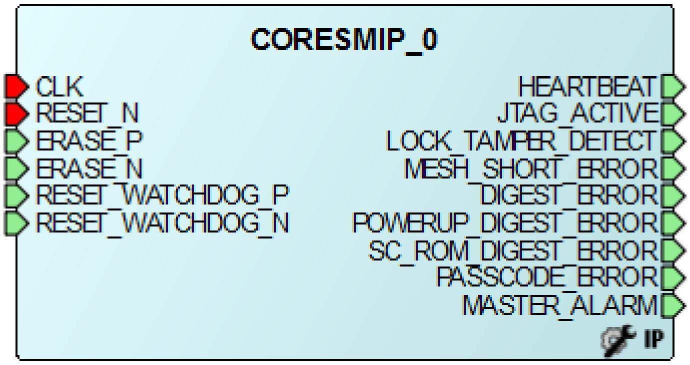
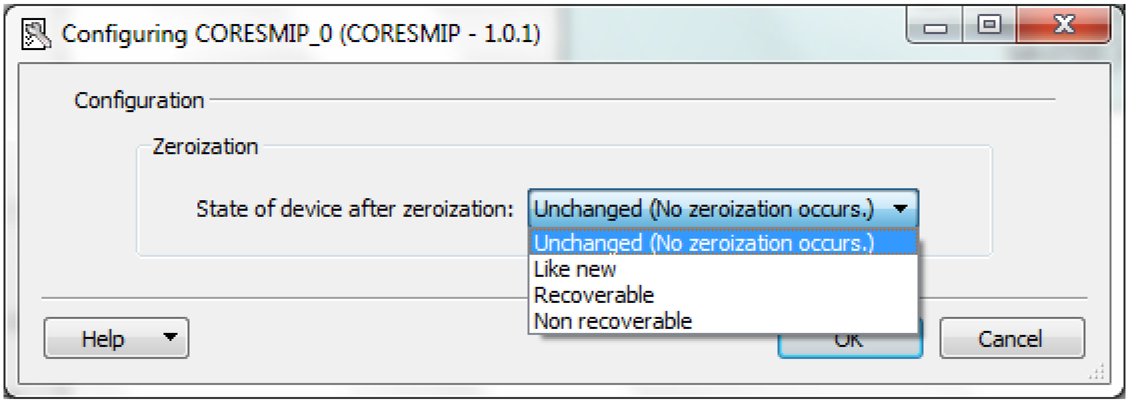


Figure 1 CoreSMIP Symbol

Configuring CoreSMIP in SmartDesign

The CoreSMIP configuration GUI is shown in Figure 2. The only configuration option for CoreSMIP is the level of zeroization that occurs when zeroization is initiated.



Configuring CORESMIP_0 (CORESMIP - 1.0.1)

Configuration

Zeroization

State of device after zeroization: Unchanged (No zeroization occurs.)

Figure 2 CoreSMIP Configuration GUI

List of Changes

The following table lists critical changes that were made in each revision of the document.

Date	Change	Page
August 2014	CoreSMIP v2.0 release	N/A

Product Support

Microsemi SoC Products Group backs its products with various support services, including Customer Service, Customer Technical Support Center, a website, electronic mail, and worldwide sales offices. This appendix contains information about contacting Microsemi SoC Products Group and using these support services.

Customer Service

Contact Customer Service for non-technical product support, such as product pricing, product upgrades, update information, order status, and authorization.

From North America, call **800.262.1060**
From the rest of the world, call **650.318.4460**
Fax, from anywhere in the world **650. 318.8044**

Customer Technical Support Center

Microsemi SoC Products Group staffs its Customer Technical Support Center with highly skilled engineers who can help answer your hardware, software, and design questions about Microsemi SoC Products. The Customer Technical Support Center spends a great deal of time creating application notes, answers to common design cycle questions, documentation of known issues and various FAQs. So, before you contact us, please visit our online resources. It is very likely we have already answered your questions.

Technical Support

Visit the Microsemi SoC Products Group Customer Support website for more information and support (http://www.microsemi.com/soc/support/search/default.aspx). Many answers available on the searchable web resource include diagrams, illustrations, and links to other resources on website.

Website

You can browse a variety of technical and non-technical information on the Microsemi SoC Products Group home page, at http://www.microsemi.com/soc/.

Contacting the Customer Technical Support Center

Highly skilled engineers staff the Technical Support Center. The Technical Support Center can be contacted by email or through the Microsemi SoC Products Group website.

Email

You can communicate your technical questions to our email address and receive answers back by email, fax, or phone. Also, if you have design problems, you can email your design files to receive assistance. We constantly monitor the email account throughout the day. When sending your request to us, please be sure to include your full name, company name, and your contact information for efficient processing of your request.

The technical support email address is soc_tech@microsemi.com.

My Cases

Microsemi SoC Products Group customers may submit and track technical cases online by going to My Cases.

Outside the U.S.

Customers needing assistance outside the US time zones can either contact technical support via email (soc_tech@microsemi.com) or contact a local sales office. Sales office listings can be found at www.microsemi.com/soc/company/contact/default.aspx.

ITAR Technical Support

For technical support on RH and RT FPGAs that are regulated by International Traffic in Arms Regulations (ITAR), contact us via soc_tech_itar@microsemi.com. Alternatively, within My Cases, select **Yes** in the ITAR drop-down list. For a complete list of ITAR-regulated Microsemi FPGAs, visit the ITAR web page.

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
E-mail: sales.support@microsemi.com