SmartFusion2/IGLOO2

Tamper/Tamper2/Tamper3 Core Configuration

Microsemi
a Microchip company

Table of Contents

1 – Configuration Options

Microsemi provides the Tamper core configurator to expose the built-in tamper detection output flags and tamper response inputs to FPGA fabric. The Tamper/Tamper2/Tamper3 core is a Configurator core available in the Libero SoC Catalog for you to instantiate in the FPGA fabric.

The Tamper core comes in three forms: Tamper, Tamper2, and Tamper3. Device support for the Tamper core is shown in Table 1-1.

Table 1-1 • **Device Size and Tamper Core**

Family/Device	Tamper Core Available
SmartFusion2 M2S005/010/025/050	Tamper
SmartFusion2 M2S090/150	Tamper2
SmartFusion2 M2S060	Tamper3
IGLOO2 M2GL005/010/025/050	Tamper
IGLOO2 M2GL090/150	Tamper2
IGLOO2 M2GL060	Tamper3

Note:

1. M2S060 and M2GL060 devices have only one eNVM (eNVM_0).
2. The Tamper2 and Tamper3 configurators support Clock Frequency Error Detection in addition to all the features of the Tamper Configurator.

Depending on the device you select (see Table 1-1) when you first create the project, Libero SoC automatically displays the correct Core (Tamper/Tamper2/Tamper3) in the Catalog for you to instantiate in the fabric.

To configure the options for the Tamper/Tamper2/Tamper3 core, right-click the core in the SmartDesign canvas and choose **Configure** to open the Configurator.

Configuration

Figure 1-1 shows the Tamper2 and Tamper 3 configuration dialog boxes and Figure 1-2 shows the Tamper configuration dialog box.

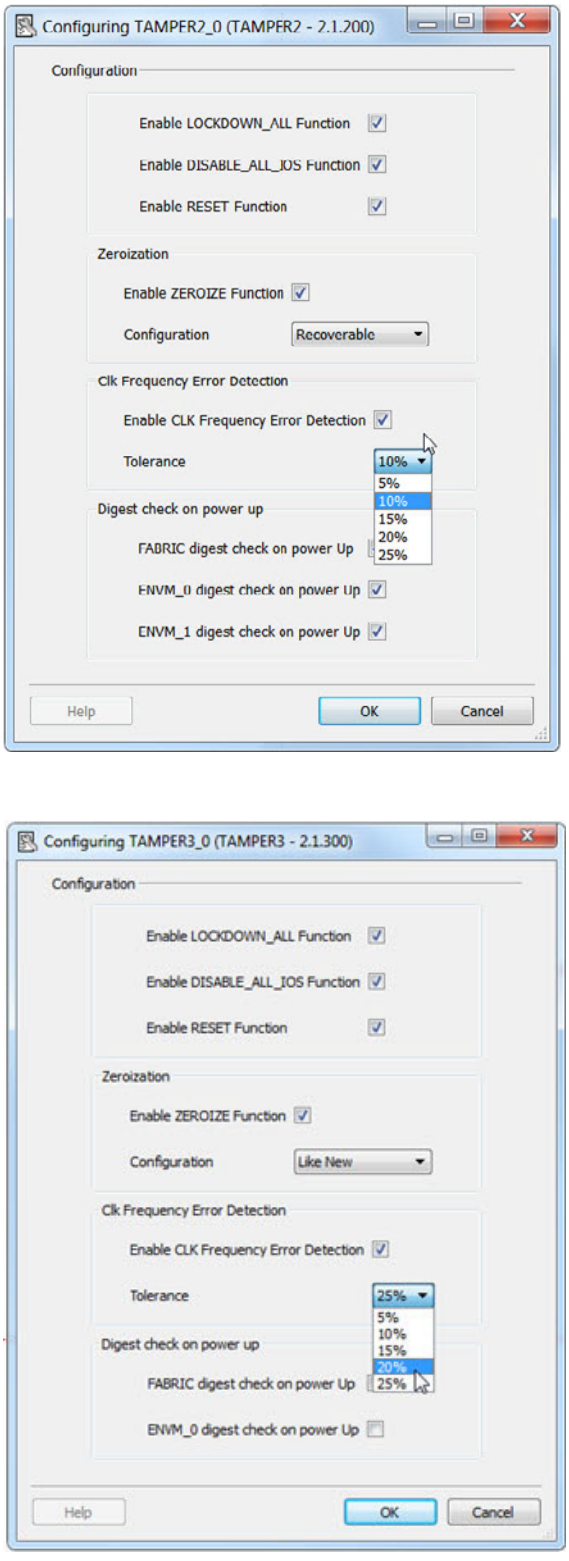

Figure 1-1 **• Tamper2 (Top) and Tamper3 (Bottom) Configuration**

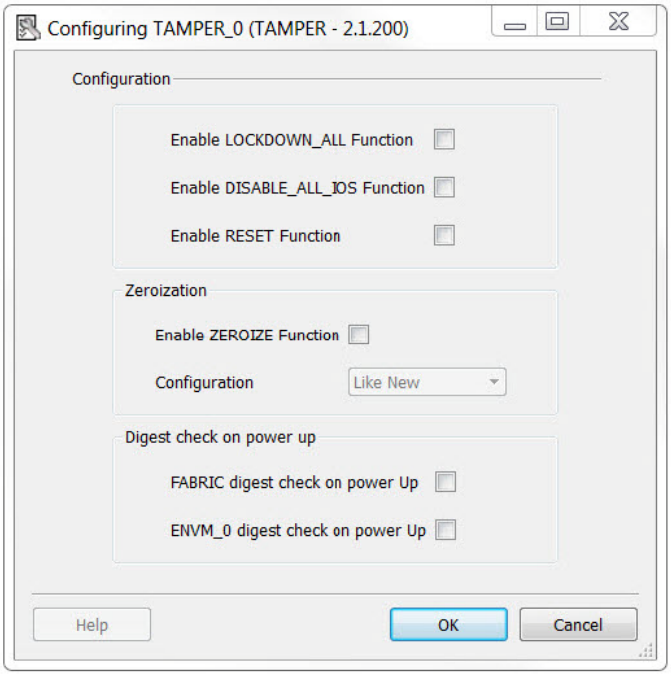

Figure 1-2 • **Tamper Configuration**

The following configuration options are available for the Tamper/Tamper2/Tamper3 core:

- **Enable LOCKDOWN_All Function** - When checked, it exposes the LOCKDOWN_ALL_N (Active Low) input port name for the Tamper core. When asserted, the LOCKDOWN_ALL_N signal activates all locks (Security Policy locks and Hardware Firewall locks) for the device.
- **Enable DISABLE_ALL_IOS Function** - When checked, it exposes the DISABLE_ALL_IOS_N (Active Low) input port for the Tamper core. When asserted (connected to logic 0), the signal disables all I/O functions for the device.
- **Enable RESET Function** - When checked, it exposes the RESET_N (Active Low) input port for the Tamper core. When asserted (connected to logic 0), the RESET_N signal resets the device.
- **Enable ZEROIZE Function** - When checked, it exposes the ZEROIZE_N (Active Low) input port for the Tamper core. When asserted (connected to logic 0), the ZEROIZE_N signal zeroizes the device. Three options are available for Zeroization; refer to "Zeroization" on page 6 for details.

Caution: If you enable any of the above four options, you must ensure that the corresponding input signals are not set to zero inadvertently during normal operation. For example, if the ZEROIZE_N signal is set to zero inadvertently and the non-recoverable mode is selected, your device may enter the non-recoverable state.

In addition, on connecting RESET_N pins to external IO directly, the POWER_ON_RESET, PLL locks can cause an issue. The RESET_N pins should not be connected to fabric logic reset. If connected, this will put the system controller in reset from power up itself. The JTAG programming will not work even when system controller is in reset, thereby bricking the device.

- **Clk Frequency Error Detection (Tamper2 and Tamper3 Only)** - This option is available only on the Tamper2 and Tamper3 cores (M2GL060/M2S060 or larger devices). When enabled, the CLK frequency is monitored and compared to the on-chip RC Oscillator frequency. When the CLK frequency falls beyond the tolerance limit specified by the user, the CLK_ERROR output port signal is asserted. Refer to "Clk Frequency Error Detection (Tamper2/Tamper3 Core Only)" on page 6 for details.
- **Digest check on power up** - When the Digest Check on power up option is checked, the device's System Control reads from the Fabric, eNVM_0 and eNVM_1 blocks to calculate the digest and compares this value with the stored digest value. Refer to "Digest Check on Power Up" on page 6 for details.

Zeroization

Three zeroization options are available, and are described in Table 1-2.

Table 1-2 • **Zeroization Options**

Option	What Stays	Comments
Like New	Factory Keys and Factory Configuration Segments	When configured for this option, the part's eNVM, Fabric, and User Security are zeroized. After zeroization, the part can be reprogrammed like a new part.
Recoverable	Factory Configuration Segments Only	When configured for this option, the part can be recovered in the field with the recovery bitstreams from Microsemi.
Unrecoverable	Nothing stays	All configurations are destroyed and the device is permanently disabled and unusable.

Refer to UG0443: SmartFusion2 and IGLOO2 FPGA Security and Reliability User Guide for details about zeroization procedures and various zeroization modes.

Clk Frequency Error Detection (Tamper2/Tamper3 Core Only)

This option is available only on the Tamper2/Tamper3 core (M2GL060/M2S060 or larger devices).

Enable CLK Frequency Error Detection - When enabled, the CLK frequency is monitored and compared to the on-chip RC Oscillator frequency. When the CLK frequency falls beyond the tolerance limit specified by the user, the CLK_ERROR output port signal is asserted.

Tolerance - Enables you to specify the upper and lower frequency limit (Tolerance) within which the CLK frequency is allowed to go above or below the on-chip RC Oscillator frequency without triggering the CLK_ERROR signal. This field is active only when the Enable CLK Frequency Error Detection is checked. Five tolerance percentages are available:

- 5%
- 10%
- 15%
- 20%
- 25%

Note: An erased device will have the clock frequency error detection enabled with tolerance of 25%.

Digest Check on Power Up

For Microsemi SmartFusion2 and IGLOO2 devices, at the end of the programming step, a digest is calculated and stored for the device's Fabric, eNVM_0 and eNVM_1 blocks.

When the Digest check on power up option is checked, the device's System Control reads from the Fabric, eNVM_0 and eNVM_1 blocks to calculate the digest and compares this value with the stored digest value. This is the digest check process.

- **FABRIC digest check on power Up** - When checked, enables digest check on the device's Fabric (Available on all devices)
- **eNVM_0 digest check on power Up** - When checked, enables digest check on the device's eNVM_0 block (Available on all devices)
- **eNVM_1 digest check on power Up** - When checked, enables digest check on the device's eNVM_1 block (Available only in Tamper2 Core for M2GL090/M2S090 or larger devices only)

Tamper Detection Output Flags

When the Tamper/Tamper2/Tamper3 Core has been configured, input and output ports are exposed based on the configuration you have selected. However, some of the built-in tamper detection output flags are exposed regardless of the configuration. Figure 1-3 shows a Tamper 2 core with all configuration options selected.

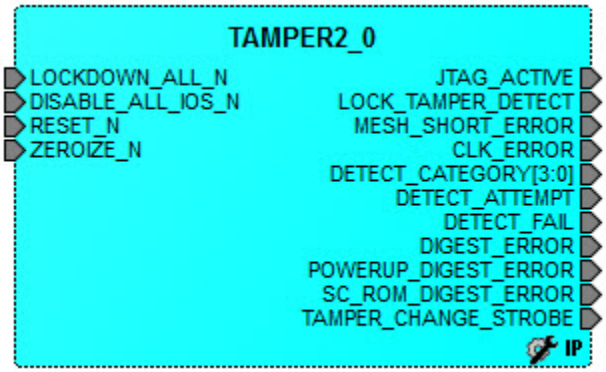

***Figure 1-3* • Tamper2 Core -- All Configuration Options Selected**

Table 1-3 shows the Input and Output ports of the Tamper/Tamper2/Tamper3 core.

***Table 1-3* • Tamper/Tamper2/Tamper3 Input/Output Ports**

Port Name	Input/Output	Description
JTAG_ACTIVE	Output	The JTAG TAP controller has been released from reset (jtag_trstb is '1').
LOCK_TAMPER_DETECT	Output	A parity error has been detected in the security segment where access control configuration bits (Lock bits) are stored.
MESH_SHORT_ERROR	Output	An error has been detected in the metal mesh. This allows protection against invasive attacks, like cutting and probing of traces using focused ion beam (FIB) technology with an active metal mesh on one of the higher metal layers.
CLK_ERROR	Output	A clock monitor that compares the frequency of the two on-chip System Controller clocks (1 MHz and 50/25 MHz). If the discrepancy over a number of clock cycles is too great, this flag is set. (Only on Tamper2 core for M2S060/M2GL060 and Tamper3 core for M2S090, M2S150, M2GL090 and M2GL150.)
DETECT_CATEGORY[3:0] DETECT_ATTEMPT DETECT_FAIL	Output	Ability to detect the programming port activity. Refer to SmartFusion2/IGLOO2 Security User Guide for details.
DIGEST_ERROR	Output	The user-initiated digest request has detected an error.
POWERUP_DIGEST_ERROR	Output	An error has been detected in a flash digest at power-up.

Table 1-3 • **Tamper/Tamper2/Tamper3 Input/Output Ports (continued)**

Port Name	Input/Output	Description
SC_ ROM_DIGEST_ERROR	Output	An error has been detected in the system controller metal mask ROM digest.
TAMPER_CHANGE_STROBE	Output	Active high strobe pulse to indicate state changes of any outputs on the Tamper Macro.
LOCKDOWN_ALL_N	Input	Activate all locking mechanisms (active low)
DISABLE_ALL_IOS_N	Input	All I/Os are disabled and tri-stated (active low)
RESET_N	Input	Reset system controller (active low)
ZEROIZE_N	Input	Destroy stored data as per security settings (active low)

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

For Microsemi SoC Products Support, visit http://www.microsemi.com/products/fpga-soc/design-support/fpga-soc-support.

Website

You can browse a variety of technical and non-technical information on the Microsemi SoC Products Group home page, at 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.

Visit About Us for sales office listings and corporate contacts.

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 Headquarters
One Enterprise, Aliso Viejo,
CA 92656 USA

Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Fax: +1 (949) 215-4996
www.microsemi.com

Microsemi, a wholly owned subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center 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; enterprise storage and communication solutions; 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, California, and has approximately 4,800 employees globally. Learn more at www. microsemi.com.

5-02-00578-5.0/12.19