SmartFusion2 MSS

Security Configuration

Microsemi

Table of Contents

Introduction

The SmartFusion2 devices offer extensive configurable access controls to the MSS memory map. These controls can be split into three major categories:

- AHB Bus Matrix Master/Slave Access
- Fabric Master MSS Access
- System Registers Access

This configurator provides three different tabs, one for each category, to configure the MSS access policies.

Reads or writes to areas not allowed cause the AHB bus matrix to complete the transaction with an HRESP error indication. An error bit is set in the SW_ERRORSTATUS field of the MSS_EXTERNAL_SR register. The following types of errors can occur:

- Write by an enabled master to a slave that is not RW
- Write by an enabled master to addresses not corresponding to a slave
- Write by the fabric master to the protected region
- Write by a disabled master to any location
- Read by an enabled master to any slave that is not R or RW
- Read by an enabled master to addresses not corresponding to a slave
- Read by the fabric master to the protected region
- Read by a disabled master to any location

The values entered in the configurator will be exported into the programming files for programming of the flash bits that control this functionality. The flash bits are loaded in the system registers at power up (or when the DEVRST_N external pad is asserted/de-asserted).

For complete details, refer to the Microsemi SmartFusion2 User's Guide.

1 – Configuration Options

AHB Bus Matrix Master/Slave Access Configuration

The master/slave access controls are restricted to those devices offering the Advanced Security Features. For devices offering baseline security only, all programmable accesses are granted and cannot be changed. The controls are grayed out.

The Master/Slave configuration tab defines how masters and slaves communicate and whether it also has write access when a master has read access. The AHB Bus Matrix can be configured to restrict those accesses.

When all the read/write programmable controls are checked in the configurator, you have the default access matrix.

The master/slave access is defined in the matrix as follows:

- - : No access is granted
- R: Only read access is available
- RW: Both read and write access are available

Whenever you restrict a master/slave access by un-checking the Read or Write access for a particular group of masters (masters are organized in three groups with respect to access configuration), the actual access is shown in the matrix.

eNVM blocks have special sectors that can be write protected. The number of special sectors depends on the device selected. The size of each sector is 4KB and the address range for each special sector is shown in blue in the GUI. Check the Use as ROM option to write protect these eNVM regions. Note that the eNVM special sectors are hidden in the matrix when you open the configurator and that you need to click the '+' sign to show these special sectors (Figure 1-1).

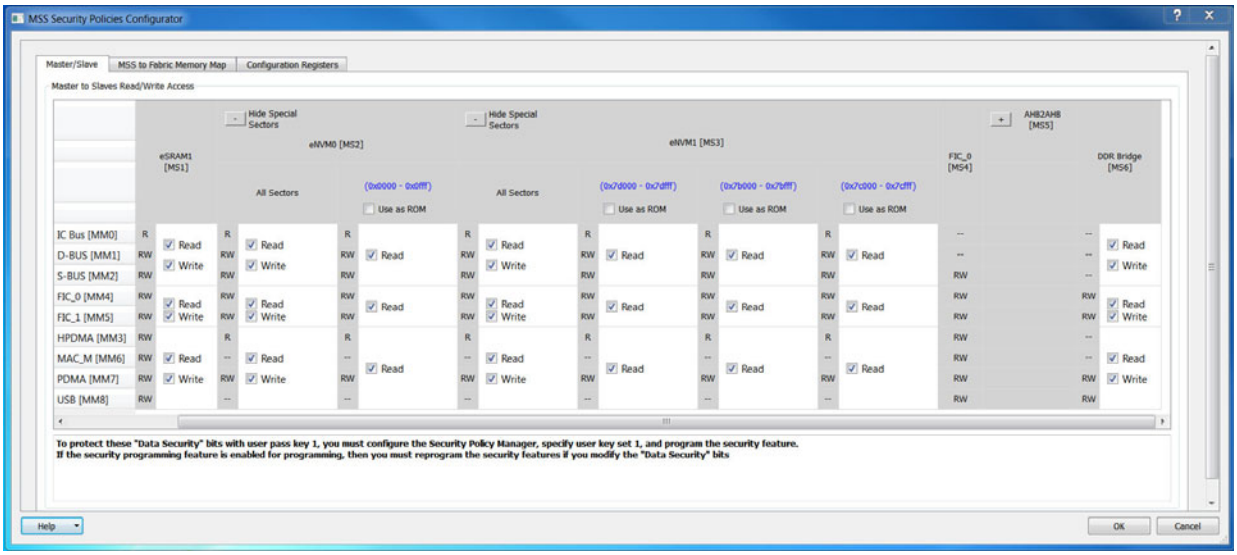

Figure 1-1 • MSS Security Configurator with eNVM Special Sectors

Table 1 shows special sector address ranges.

Table 1 • **Special Sector Address Ranges**

Die	eNVM0 (number of available Sectors)	eNVM1 (number of available Sectors)	eNVM0 (address range)	eNVM1(address range)
M2S150S/TS, M2S100S/TS, M2S90S/TS	1	3	0x0000-0x0fff	0x7d000-0x7dfff 0x7b000-0x7bfff 0x7c000-0x7cfff
M2S050S/TS	2	0	0x0000-0x0fff 0x3f000-0x3ffff	N/A
M2S025S/TS, M2S010S/TS M2S005S	4	0	0x0000-0x0fff 0x3d000-0x3dfff 0x3e000-0x3efff 0x3f000-0x3ffff	N/A

Fabric Master MSS Access Configuration

You can restrict the access to the MSS memory region for any FPGA fabric master attempting to access the MSS through one of the two Fabric Interface Controllers (FIC_0 and FIC_1). To restrict the FPGA master to a particular memory map region, you must:

1. Check the **Restrict Memory Access** check box.
2. Define the size of the restricted region.
3. Define the base address of that region; the base address should be a multiple of the restricted region size selected in the configurator (Figure 1-2).

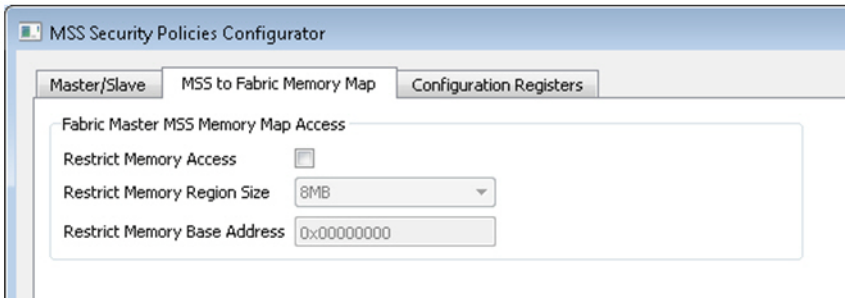

Figure 1-2 • **Fabric Master MSS Access Configuration**

System Registers Access Configuration

You can permanently lock any system register from being changed at run time (typically via firmware) by un-checking any of the checkboxes in this tab. Un-checked registers become Read-only registers (Figure 1-3).

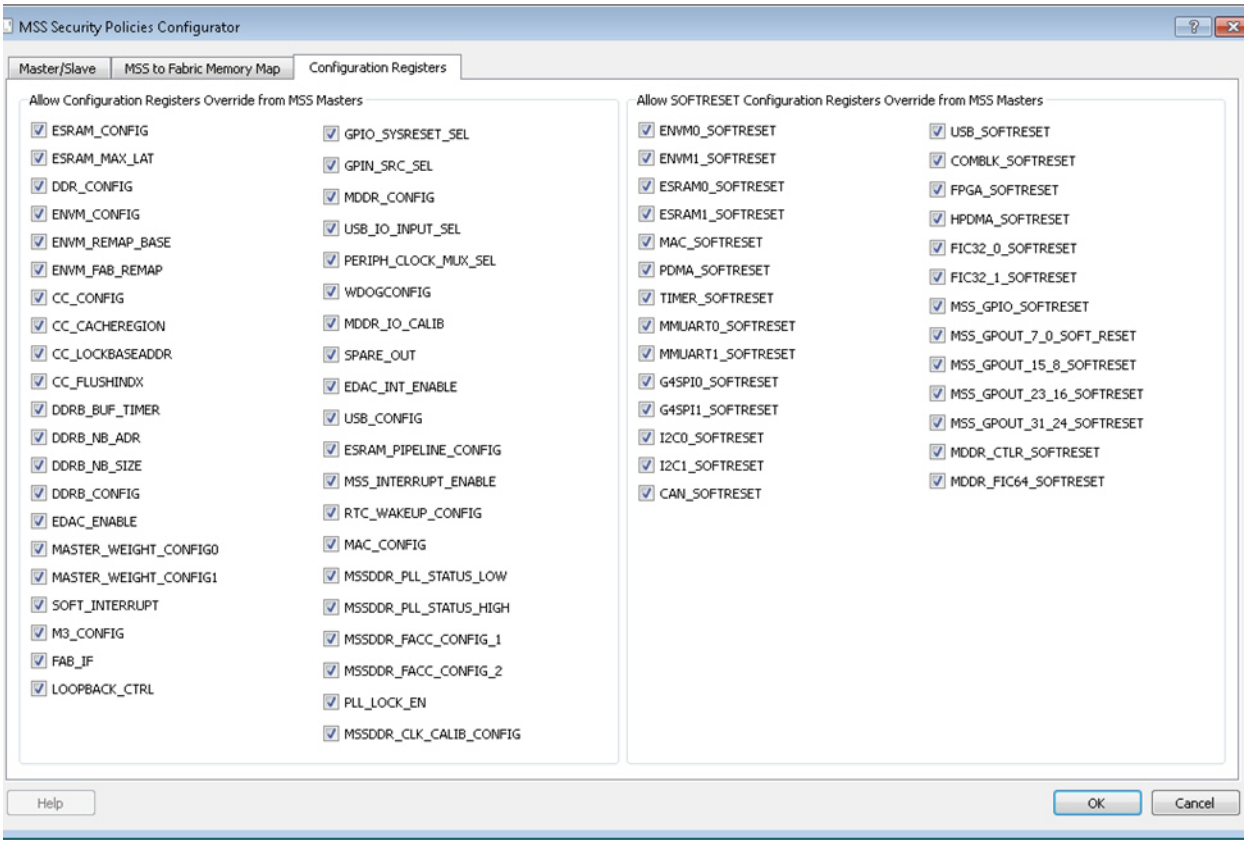

Figure 1-3 **• System Registers Access Configuration**

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, 408.643.6913

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

Website

You can browse a variety of technical and non-technical information on the SoC 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. 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

Microsemi Corporation (NASDAQ: MSCC) offers a comprehensive portfolio of semiconductor solutions for: aerospace, defense and security; enterprise and communications; and industrial and alternative energy markets. Products include high-performance, high-reliability analog and RF devices, mixed signal and RF integrated circuits, customizable SoCs, FPGAs, and complete subsystems. Microsemi is headquartered in Aliso Viejo, Calif. Learn more at **www.microsemi.com**.

5-02-00376-1/08.14