Flash Protection for Stellaris® Microcontrollers

Application Note
Copyright

Copyright © 2007–2009 Texas Instruments, Inc. All rights reserved. Stellaris and StellarisWare are registered trademarks of Texas Instruments. ARM and Thumb are registered trademarks, and Cortex is a trademark of ARM Limited. Other names and brands may be claimed as the property of others.

Texas Instruments
108 Wild Basin, Suite 350
Austin, TX 78746
Main: +1-512-279-8800
Fax: +1-512-279-8879
http://www.luminarymicro.com
Table of Contents

Introduction ......................................................................................................................................................... 4
Flash Block Protection ........................................................................................................................................ 4
Execute-Only Protection ..................................................................................................................................... 4
Read-Only Protection .......................................................................................................................................... 5
Permanently Disabling Debug ............................................................................................................................ 5
Committing Security Settings .............................................................................................................................. 6
Conclusion .......................................................................................................................................................... 6
References ......................................................................................................................................................... 6
Introduction

Code security has become of paramount importance in modern embedded systems. Protection requirements range from marking regions of flash as read-only, to completely blocking accesses to the device from external debug hardware. Stellaris® microcontrollers contain built-in code protection features to address the diverse protection needs of customers. This application note discusses some of these protection features and their limitations.

Flash Block Protection

Stellaris microcontrollers allow software to assign security on a per-block basis (a block is 2 KB in size). The registers that control the security attributes are the Flash Memory Protection Read Enable (FMPRE) and Flash Memory Protection Program Enable (FMPPE) registers, which are located in the System Control address space. Each 2-KB block has a corresponding bit in the FMPRE and FMPPE registers, allowing various security combinations. Flash protection settings can be tested for software debug purposes before being permanently committed.

Table 1. Flash Protection Policy Combinations

<table>
<thead>
<tr>
<th>FMPPE</th>
<th>FMPRE</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td><strong>Execute-only protection.</strong> The block may only be executed and may not be read, written or erased. This mode is used to protect code.</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td><strong>The block may be written, erased or executed, but not read.</strong> This combination is unlikely to be used.</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td><strong>Read-only protection.</strong> The block may be read or executed but may not be written or erased. This mode is used to lock the block from further modification while allowing any read or execute access.</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td><strong>No protection.</strong> The block may be written, erased, executed or read.</td>
</tr>
</tbody>
</table>

For more information about programming the flash protection registers, see the Internal Memory chapter of the data sheet for your specific Stellaris device.

Execute-Only Protection

Execute-only protection prevents both modification and visibility to a protected flash block. This mode is intended to be used in situations where a device requires debug capability, yet portions of the application space must be protected from external access. An example of this is a company who wishes to sell Stellaris devices with their proprietary software pre-programmed, yet allow the end user to add custom code to an unprotected region of the flash (such as a motor control module with a customizable motor configuration section in flash).

Literal data introduces a complication to the protection mechanism. When C code is compiled and linked, literal data (constants, and so on) is typically placed in the text section, between functions, by the compiler. The literal data is accessed at run time through the use of the LDR instruction, which loads the data from memory using a PC-relative memory address. The execution of the LDR instruction generates a read transaction across the Cortex-M3’s DCode bus, which is subject to the execute-only protection mechanism. If the accessed block is marked as execute only, the transaction is blocked, and the processor is prevented from loading the constant data and, therefore, inhibiting
correct execution. Therefore, using execute-only protection requires that literal data be handled differently. There are three ways to address this:

1. Use a compiler that allows literal data to be collected into a separate section that is put into one or more read-enabled flash blocks. Note that the LDR instruction may use a PC-relative address—in which case the literal pool cannot be located outside the span of the offset—or the software may reserve a register to point to the base address of the literal pool and the LDR offset is relative to the beginning of the pool.

2. Use a compiler that generates literal data from arithmetic instruction immediate data and subsequent computation.

3. Use method 1 or 2, but in assembly language, if the compiler does not support either method.

At the time this document was created, C compilers supporting Cortex-M3 do not support moving the literal pool or computing constant data without the DCode bus accesses. Future compiler releases may add these features.

**Read-Only Protection**

Read-only protection prevents the contents of the flash block from being re-programmed, while still allowing the content to be read by processor or the debug interface.

The read-only mode does not prevent read access to the stored program, but it does provide protection against accidental (or malicious) erasure or programming. Read-only is especially useful for utilities like the boot loader when the debug interface is permanently disabled (see the “Permanently Disabling Debug” section). In such combinations, the boot loader, which provides access control to the Flash memory, is protected from being erased or modified.

**Permanently Disabling Debug**

*Note:* This section applies to all Stellaris family devices, excluding early silicon revisions. This information does not pertain to revision B or revision C0 Sandstorm-class devices. Please check the relevant data sheet for your device and silicon revision.

For extremely sensitive applications, the debug interface to the processor and peripherals can be permanently disabled, blocking all accesses to the device through the JTAG or SWD interfaces. With the debug interface disabled, it is still possible to perform standard IEEE instructions (such as boundary scan operations), but access to the processor and peripherals is blocked.

In Sandstorm-class devices, the two most-significant bits of the **FMPRE** register are the **DBG** bits, and control whether or not the debug interface is turned on or off. Since the **DBG** bits are part of the **FMPRE** register, the user loses the capability to mark the upper two flash blocks in a 64 KB flash device as execute-only.

In Fury-class devices, the dedicated **User Debug (USERDBG)** register controls whether the debug interface is turned on or off. The **DBG0** and **DBG1** bits of the **USERDBG** register function the same way as the **DBG** bits in the Sandstorm-class devices. Since the **DBG** bits are in a dedicated register in the Fury-class devices, the **FMPRE** bits are not affected.
The debug interface should not be permanently disabled without providing some mechanism—such as the boot loader—to provide customer-installable updates or bug fixes. Disabling the debug interface is permanent and cannot be reversed.

**Committing Security Settings**

Once the final security configuration is decided, the settings are permanently written to the device by performing the commit sequence described in the data sheet.

**Important:** These settings can only be written once (one time for FMPPE and one time for FMPRE), meaning that if the debug interface is disabled, in addition to having any of the FMPRE bits set, all changes to the FMPRE should be written at the same time.

As described in the “Permanently Disabling Debug” section of this document, security settings should be committed during the manufacturing process by loading the commit routine into the device's SRAM and executing the sequence.

**Conclusion**

Stellaris microcontrollers offer various flash protection options to help address diverse customer needs. The combination of the block-level access control and ability to completely disable debug access to the processor and peripherals enables customers to protect their application code from both malicious and accidental access or modification.

**References**

The following document is available for download at [www.luminarymicro.com](http://www.luminarymicro.com):

- Stellaris® Family data sheet, Sandstorm-class, Publication Number DS-LM3Snnn (where nnn is the part number for that specific Stellaris family microcontroller)
- Stellaris® Family data sheet, Fury-class, Publication Number DS-LM3Snnnn (where nnnn is the part number for that specific Stellaris family microcontroller)
Important Notice

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and applications using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI products or services with statements different from or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

TI products are not authorized for use in safety-critical applications (such as life support) where a failure of the TI product would reasonably be expected to cause severe personal injury or death, unless officers of the parties have executed an agreement specifically governing such use. Buyers represent that they have all necessary expertise in the safety and regulatory ramifications of their applications, and acknowledge and agree that they are solely responsible for all legal, regulatory and safety-related requirements concerning their products and any use of TI products in such safety-critical applications, notwithstanding any applications-related information or support that may be provided by TI. Further, Buyers must fully indemnify TI and its representatives against any damages arising out of the use of TI products in such safety-critical applications.

TI products are neither designed nor intended for use in military/aerospace applications or environments unless the TI products are specifically designated by TI as military-grade or "enhanced plastic." Only products designated by TI as military-grade meet military specifications. Buyers acknowledge and agree that any such use of TI products which TI has not designated as military-grade is solely at the Buyer's risk, and that they are solely responsible for compliance with all legal and regulatory requirements in connection with such use. TI products are neither designed nor intended for use in automotive applications or environments unless the specific TI products are designated by TI as compliant with ISO/TS 16949 requirements. Buyers acknowledge and agree that, if they use any non-designated products in automotive applications, TI will not be responsible for any failure to meet such requirements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

Products
- Amplifiers: amplifier.ti.com
- Data Converters: dataconverter.ti.com
- DLP® Products: www.dlp.com
- DSP: dsp.ti.com
- Clocks and Timers: www.ti.com/clocks
- Interface: interface.ti.com
- Logic: logic.ti.com
- Power Mgmt: power.ti.com
- Microcontrollers: microcontroller.ti.com
- RFID: www.ti-rfid.com
- RF/IF and ZigBee® Solutions: www.ti.com/prf

Applications
- Audio: www.ti.com/audio
- Automotive: www.ti.com/automotive
- Broadband: www.ti.com/broadband
- Digital Control: www.ti.com/digitalcontrol
- Medical: www.ti.com/medical
- Military: www.ti.com/military
- Optical Networking: www.ti.com/opticalnetwork
- Security: www.ti.com/security
- Telephony: www.ti.com/telephony
- Video & Imaging: www.ti.com/video
- Wireless: www.ti.com/wireless