TB3179

How to Configure the Memory Protection Unit (MPU)

Introduction

The Memory Protection Unit (MPU) is an optional component provided by the Cortex®-M7 core for memory protection. It divides the memory map into a number of regions with privilege permissions and access rules. This document is intended to familiarize the user with the configuration of the memory regions of the MPU, which is provided by Microchip's Cortex-M7 based MCUs.

Features of the MPU are as follows:

- Prevents an untrusted application from accessing protected memory regions for the purpose of intellectual property infringement.
- Prevents user applications from corrupting data used by the operating system.
- Separates data between processing tasks by blocking tasks from accessing other data.
- Allows memory regions to be defined as read-only so that vital data can be protected.
- Detects unexpected memory access.

In brief, the MPU provides,

- Memory protection
- Peripheral protection
- Privileged code access protection

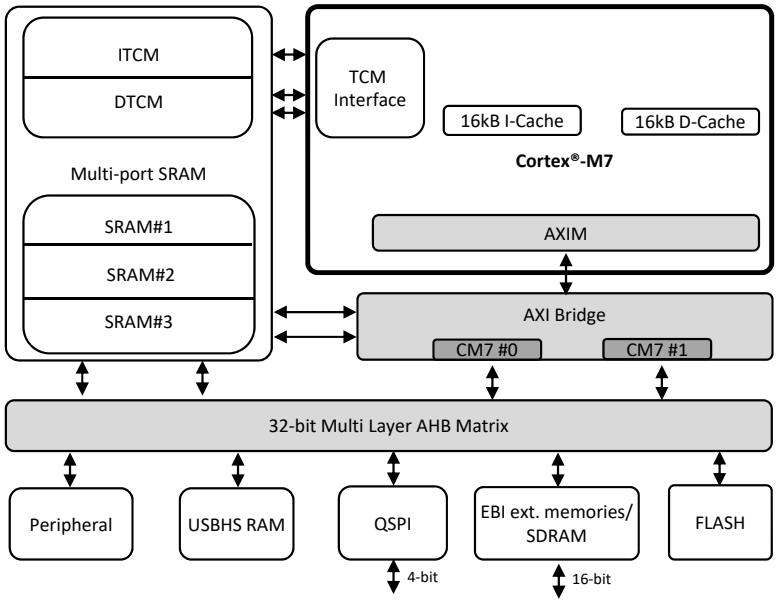
© 2017 Microchip Technology Inc.

1. MPU of the Cortex-M7

The MPU option provided by the Cortex-M7 devices can be used to protect from eight to sixteen memory regions in the system space.

The Cortex-M7 based MCU's memory interface based on the MPU regions is shown in the following figure. For details on the product specific memory mapping, refer to the specific device data sheet.

Figure 1-1. Memory Interface of a Cortex-M7 based MCU



The functions provided with the MPU are based on the memory unit of region. A region is a part of the memory map with individual access rules. The memory type and attributes determine the behavior of the access to a region.

Each memory region can have an independent attribute setting. When memory regions overlap, memory access is affected by the attributes of the region with the highest number (i.e., the attributes for region 7 take precedence over the attributes of any region that overlaps region 7).

The configuration of MPU regions is based on memory types, memory regions, types, and attributes.

The MPU contains a number of registers. For the list of Cortex-M7 MPU registers, please visit: http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.dui0646a/BIHJJABA.html.

© 2017 Microchip Technology Inc.

2. Setting up the MPU in a Cortex-M7 MCU

The system should have the following memory types:

- *Normal*: refers to data or code memory space such as, Flash or SRAM
- *Device*: refers to memory mapped peripherals such as, USBHSRAM
- *Strongly-ordered*: refers to memory whose access always follows the program order (i.e., EBI, TCM)

The memory region should have the following attributes:

- Shareable or non-shareable (S)
- Cacheable or non-cacheable (C)
- Memory access permission (AP)
- Access for Instruction Fetch (XN)
- TEX and B are other bit-fields, which in combination with the above bit-fields, define the memory attribute for each MPU memory region

Figure 2-1. Memory Region Attributes

Memory Region	Memory Access Attribute; Shareable bit	Access Permission; Instruction Access
#1 ITCM	Strongly Ordered; Shareable	RW access from privileged SW only; Instruction fetches enabled
#2 FLASH	Normal; Not shareable; Cacheable; Inner Write back; no write allocate	Read only, by privileged or unprivileged SW; Instruction fetches enabled
#3 DTCM	Strongly Ordered; Shareable	RW access from privileged SW only; Instruction fetches enabled
#4 SRAM #1	Normal; Not shareable; Cacheable; Inner Write back; no write allocate	RW full access; Instruction fetches enabled
#5 SRAM #2	Normal; Not shareable; Cacheable; Inner Write back; no write allocate	RW full access; Instruction fetches enabled
#6 PERIPHERAL	Device; Shareable	RW full access; Instruction fetches disabled
#7 EXTERNAL	Strongly Ordered; Shareable	RW full access; Instruction fetches enabled
#8 SDRAM	Normal; Shareable; Cacheable; Inner write back; write and read allocate	RW full access; Instruction fetches enabled
#9 QSPI	Strongly Ordered; Shareable	RW full access; Instruction fetches enabled
#10 USBHS	Device; Shareable	RW full access; Instruction fetches disabled
#11 SRAM #3	Normal, Shareable, Outer and inner non-cacheable	RW full access; Instruction fetches enabled

For more information on the attribute bit-fields, please visit: http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.dai0179b/CHDFDFIG.html.

The memory mapping of a Cortex-M7 based MCU defines the general memory spaces. Each memory space has a definite memory type in logical operations. This is the default value for the memory type bits in the MPU region attribute register and also the basic design principle of a MPU system.

The basic memory access behaviors for a Cortex-M7 based MCU are listed in Memory Region Attributes. All the region attributes for the memory type must follow this table. For example, the peripheral region can never be set as a non-XN type, and it is always set as device type, non-cacheable, and non-executable.

Software Implementation

© 2017 Microchip Technology Inc.

The MPU registers need to be programmed and enabled before use. This is usually done in the initialization phase of any application running on the target MCU, after the system startup.

The MPU configuration involves the following three-step operation:

1. Select the memory region.
2. Configure the attributes for the selected memory region (TEX, S, C, B, AP, XN).
   – Repeat above two steps for all valid memory regions
3. Enable MPU.

If access is gained to an area of memory without the required permissions, a memory management fault is raised. The memory management fault exception must be set before enabling the MPU module. If any illegal access is detected, the system will enter the memory management fault handler.

The System Handler Control and State Register (SHCSR) of the System Control Block (SCB) is used to enable the MemManage Fault exception. For more details, please visit: http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.dui0646a/CIHFDJCA.html.

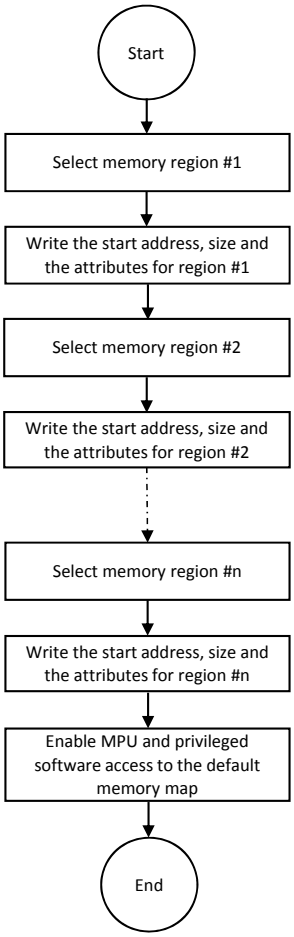
Flow Diagram

The following flowchart briefly explains the steps involved for setting up the MPU regions.

1. Select the MPU region using the MPU->RNR register.
2. Write the base address of the MPU region selected by the MPU->RNR to MPU->RBAR register.
3. Write the attributes of the MPU region selected by the MPU->RNR to MPU->RASR register.
4. Enable MPU in the MPU->CTRL register.

© 2017 Microchip Technology Inc.

Figure 2-2. MPU Configuration Flow



© 2017 Microchip Technology Inc.

3. MPU Region Update

The MPU region attribute can be updated at run-time to satisfy different requirements. To update the attribute of a region, consider the following actions:

- The region must be disabled before changing the attributes.
- To avoid unexpected behavior, the interrupt routine must be disabled before the update.
- The access to the MPU registers should be aligned. A DSB and ISB instruction are required before updating the MPU, which ensures that the outstanding memory transfers are finished. The memory barrier instructions are not required if the update procedure happens in an exception handler, as the memory barrier behavior will automatically take place in an exception entry and return.

© 2017 Microchip Technology Inc.

4. MPU Setup Tips

Tip:

1. The processor does not support unaligned accesses to MPU registers. The MPU registers support aligned word accesses only.
2. If the MPU has previously been programmed, disable the unused regions to prevent any previous region settings from affecting the new MPU setup.
3. Disable the interrupts before updating the attributes of a region that the interrupt handlers might access.

© 2017 Microchip Technology Inc.

5. References

- http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.dui0646a/BIHIIJDC.html
- http://www.microchip.com/design-centers/32-bit/sam-32-bit-mcus/sam-v-mcus
- http://www.microchip.com/design-centers/32-bit/sam-32-bit-mcus/sam-s-mcus
- http://www.microchip.com/design-centers/32-bit/sam-32-bit-mcus/sam-e-mcus
- http://www.atmel.com/Images/Atmel-42128-AT02346-Using-the-MPU-on-Atmel-Cortex-M3-M4-based-Microcontroller_Application-Note.pdf
- http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.dui0646a/Cihegaib.html
- http://asf.atmel.com/docs/latest/samv71/html/mpu_8c.html
- http://asf.atmel.com/docs/latest/samv71/html/mpu_8h.html

© 2017 Microchip Technology Inc.

The Microchip Web Site

Microchip provides online support via our web site at http://www.microchip.com/. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Customer Change Notification Service

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at http://www.microchip.com/. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: http://www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.

© 2017 Microchip Technology Inc.

- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as “unbreakable.”

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip’s code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer’s risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, AnyRate, AVR, AVR logo, AVR Freaks, BeaconThings, BitCloud, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, Heldo, JukeBlox, KeeLoq, KeeLoq logo, Kleer, LANCheck, LINK MD, maXStylus, maXTouch, MediaLB, megaAVR, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, Prochip Designer, QTouch, RightTouch, SAM-BA, SpyNIC, SST, SST Logo, SuperFlash, tinyAVR, UNI/O, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

ClockWorks, The Embedded Control Solutions Company, EtherSynch, Hyper Speed Control, HyperLight Load, IntelliMOS, mTouch, Precision Edge, and Quiet-Wire are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, BodyCom, chipKIT, chipKIT logo, CodeGuard, CryptoAuthentication, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, EtherGREEN, In-Circuit Serial Programming, ICSP, Inter-Chip Connectivity, JitterBlocker, KleerNet, KleerNet logo, Mindi, MiWi, motorBench, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, PureSilicon, QMatrix, RightTouch logo, REAL ICE, Ripple Blocker, SAM-ICE, Serial Quad I/O, SMART-I.S., SQI, SuperSwitcher, SuperSwitcher II, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2017, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

ISBN: 978-1-5224-2489-5

Quality Management System Certified by DNV

ISO/TS 16949

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: http://www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Asia Pacific Office** Suites 3707-14, 37th Floor Tower 6, The Gateway Harbour City, Kowloon **Hong Kong** Tel: 852-2943-5100 Fax: 852-2401-3431 **Australia - Sydney** Tel: 61-2-9868-6733 Fax: 61-2-9868-6755 **China - Beijing** Tel: 86-10-8569-7000 Fax: 86-10-8528-2104 **China - Chengdu** Tel: 86-28-8665-5511 Fax: 86-28-8665-7889 **China - Chongqing** Tel: 86-23-8980-9588 Fax: 86-23-8980-9500 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 Fax: 86-571-8792-8116 **China - Hong Kong SAR** Tel: 852-2943-5100 Fax: 852-2401-3431 **China - Nanjing** Tel: 86-25-8473-2460 Fax: 86-25-8473-2470 **China - Qingdao** Tel: 86-532-8502-7355 Fax: 86-532-8502-7205 **China - Shanghai** Tel: 86-21-3326-8000 Fax: 86-21-3326-8021 **China - Shenyang** Tel: 86-24-2334-2829 Fax: 86-24-2334-2393 **China - Shenzhen** Tel: 86-755-8864-2200 Fax: 86-755-8203-1760 **China - Wuhan** Tel: 86-27-5980-5300 Fax: 86-27-5980-5118 **China - Xian** Tel: 86-29-8833-7252 Fax: 86-29-8833-7256	**China - Xiamen** Tel: 86-592-2388138 Fax: 86-592-2388130 **China - Zhuhai** Tel: 86-756-3210040 Fax: 86-756-3210049 **India - Bangalore** Tel: 91-80-3090-4444 Fax: 91-80-3090-4123 **India - New Delhi** Tel: 91-11-4160-8631 Fax: 91-11-4160-8632 **India - Pune** Tel: 91-20-3019-1500 **Japan - Osaka** Tel: 81-6-6152-7160 Fax: 81-6-6152-9310 **Japan - Tokyo** Tel: 81-3-6880- 3770 Fax: 81-3-6880-3771 **Korea - Daegu** Tel: 82-53-744-4301 Fax: 82-53-744-4302 **Korea - Seoul** Tel: 82-2-554-7200 Fax: 82-2-558-5932 or 82-2-558-5934 **Malaysia - Kuala Lumpur** Tel: 60-3-6201-9857 Fax: 60-3-6201-9859 **Malaysia - Penang** Tel: 60-4-227-8870 Fax: 60-4-227-4068 **Philippines - Manila** Tel: 63-2-634-9065 Fax: 63-2-634-9069 **Singapore** Tel: 65-6334-8870 Fax: 65-6334-8850 **Taiwan - Hsin Chu** Tel: 886-3-5778-366 Fax: 886-3-5770-955 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 Fax: 886-2-2508-0102 **Thailand - Bangkok** Tel: 66-2-694-1351 Fax: 66-2-694-1350	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4450-2828 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **France - Saint Cloud** Tel: 33-1-30-60-70-00 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-67-3636 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-7289-7561 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820

© 2017 Microchip Technology Inc.