Customer Training Workshop Traveo™ II Protection Units

Q4 2020

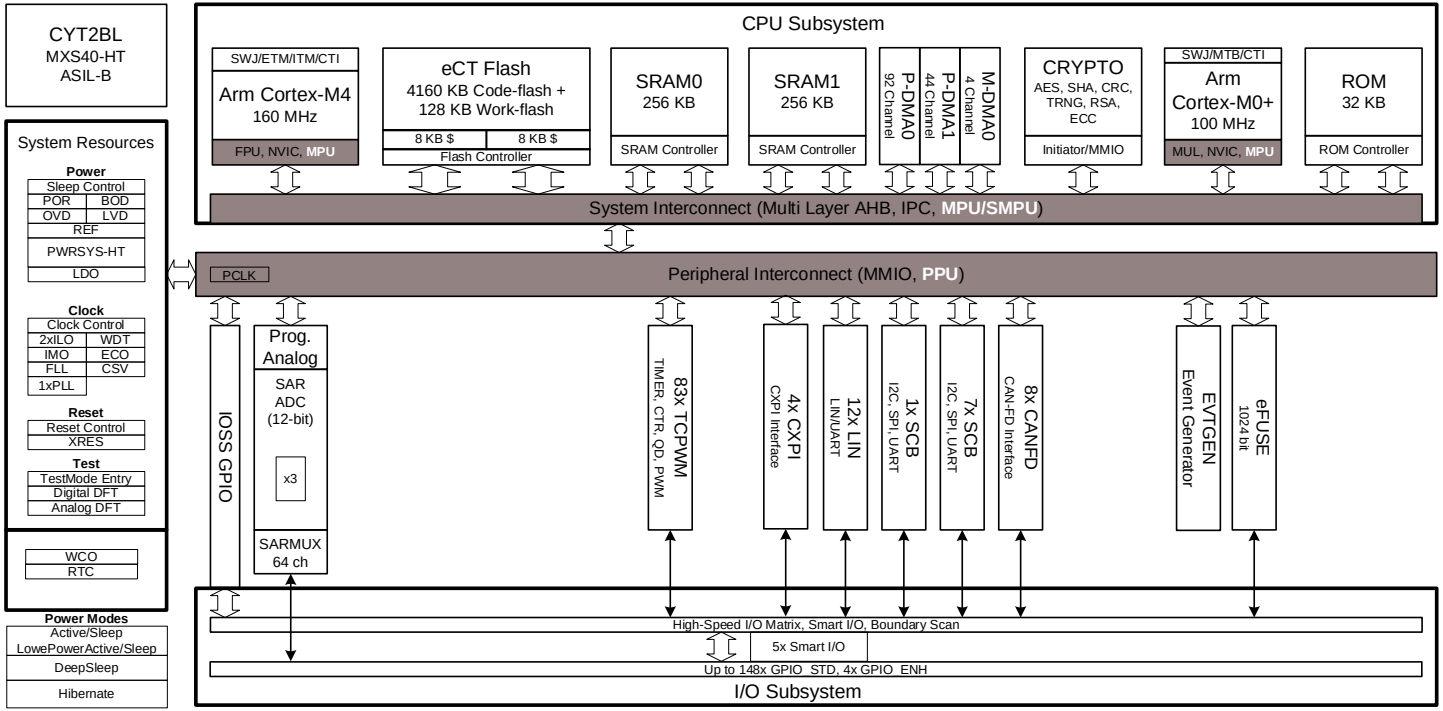
Target Products

› Target product list for this training material

Family Category	Series	Code Flash Memory Size
Traveo™ II Automotive Body Controller Entry	CYT2B6	Up to 576KB
Traveo II Automotive Body Controller Entry	CYT2B7	Up to 1088KB
Traveo II Automotive Body Controller Entry	CYT2B9	Up to 2112KB
Traveo II Automotive Body Controller Entry	CYT2BL	Up to 4160KB
Traveo II Automotive Body Controller High	CYT3BB/4BB	Up to 4160KB
Traveo II Automotive Body Controller High	CYT4BF	Up to 8384KB
Traveo II Automotive Cluster	CYT3DL	Up to 4160KB
Traveo II Automotive Cluster	CYT4DN	Up to 6336KB

Introduction to Traveo II Body Controller Entry

› Protection units (MPU/SMPU/PPU) are in CPUSS and peripheral interconnect

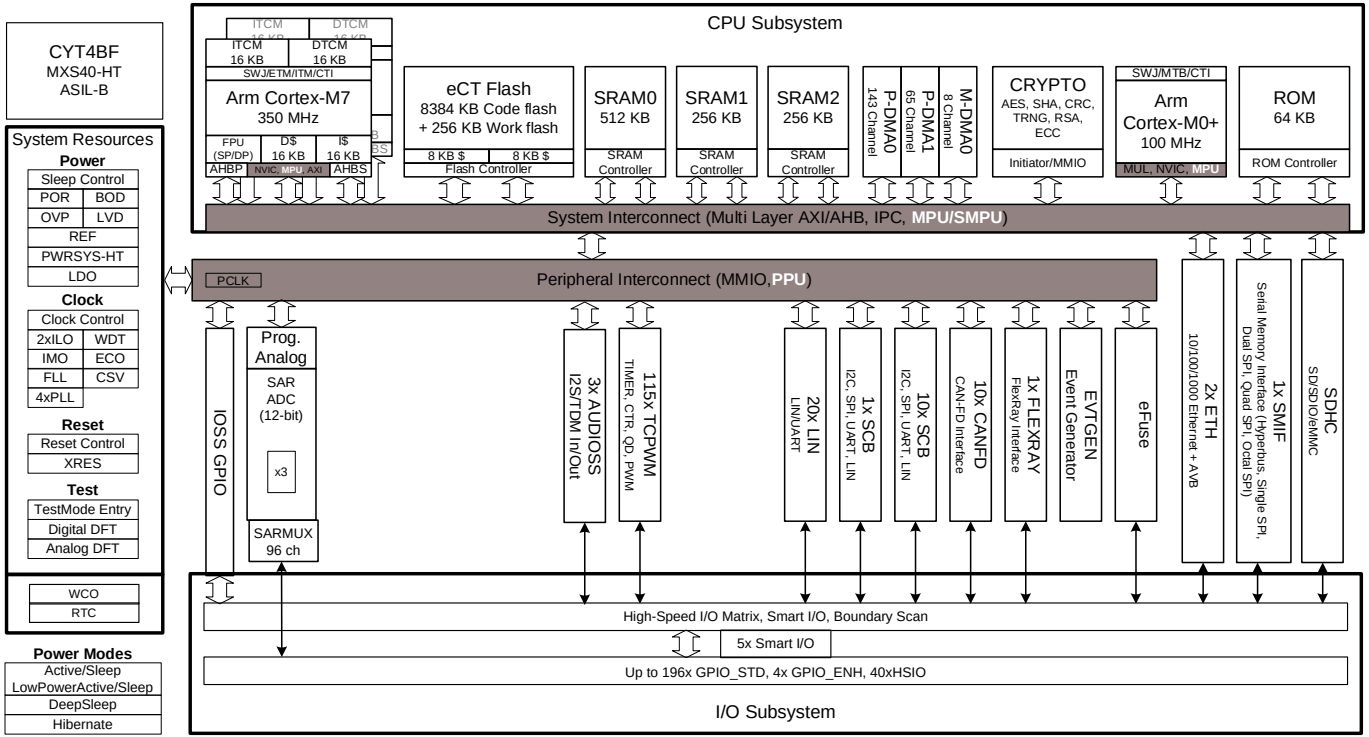


Hint Bar

Review TRM chapter 6 and the Register TRM for additional details

Introduction to Traveo II Body Controller High

› Protection units (MPU/SMPU/PPU) are in CPUSS and peripheral interconnect

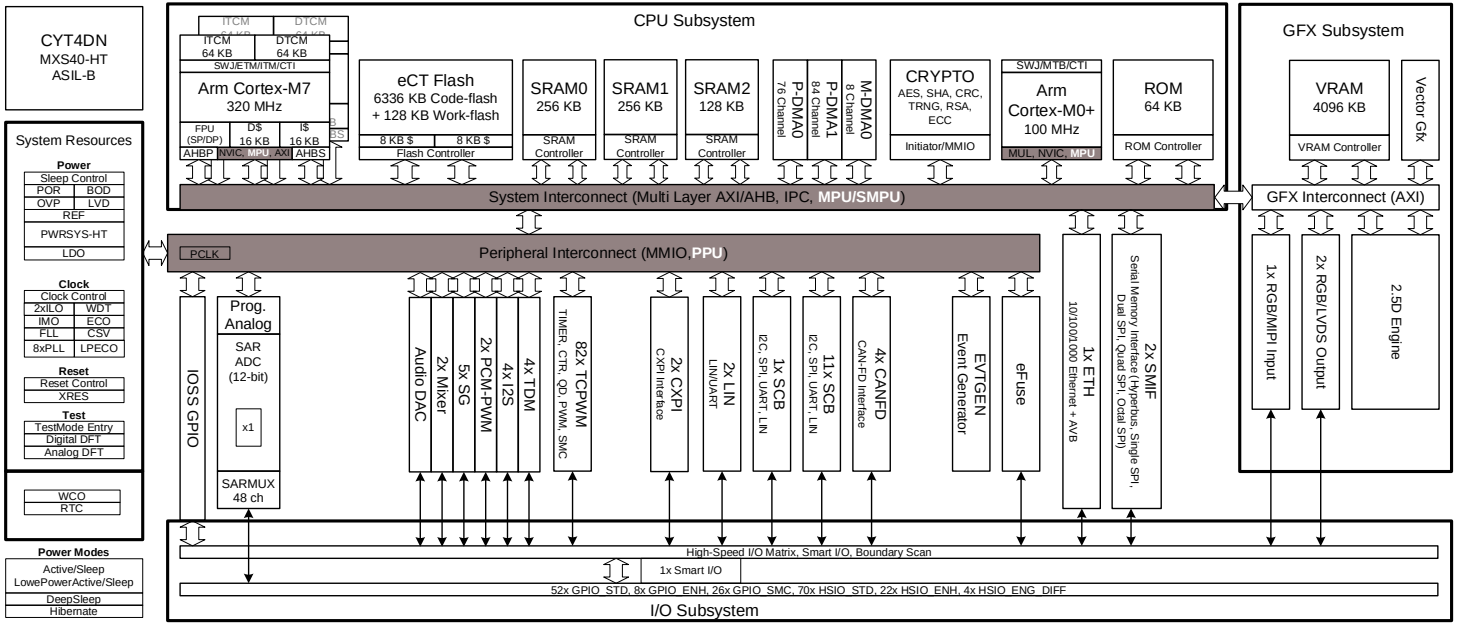


Hint Bar

Review TRM chapter 6 and the Register TRM for additional details

Introduction to Traveo II Cluster

› Protection units (MPU/SMPU/PPU) are in CPUSS and peripheral interconnect



Hint Bar

Review TRM chapter 6 and the Register TRM for additional details

Protection Unit Overview

- Overview
  - Allows/restricts bus transfers on the bus infrastructure
  - Includes four protection units (MPU/SMPU/PPU/SWPU)
- Features
  - Supports various access attributes
    - Address range (Start Address and Region Size)
    - Read/Write
    - Execute (Code or Data)
    - Privileged/Unprivileged
    - Secure/Non-secure
    - Protection context (PC)
  - Protects protection structures
  - Captures protection violations in fault report structure

Hint Bar

Review TRM chapter 6 and Register TRM for additional details

Training section references:
CPUSS

Protection Context

- Protection Context (PC) is an access attribute of the protection units
- The PC prevents erroneous writing from the access with an unintended PC to memory and peripheral
- The PC helps to apply different protection attributes without changing the SMPU, PPU, and SWPU settings
  - Traveo II supports eight PCs
  - Used as the PC attribute for bus transfers
  - Access to memory and peripheral is allowed or restricted by SMPU, PPU and SWPU
  - Changed by reprogramming the PC field in MSx_CTL
  - PC0 and PC1 are hardware-controlled and not available to the user; PC2 to PC7 are available

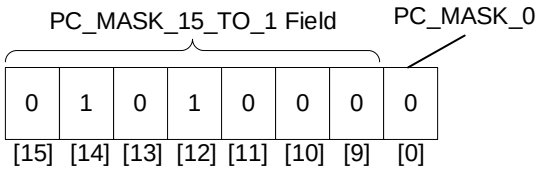
Hint Bar

Review TRM chapter 6 and the Register TRM for additional details

Protection Context Programming and Restrictions

- PC Programming
  - Main CPU[1], secondary CPU[2], and test controller bus master have a PC field[3]
  - A PC attribute is changed by reprogramming the PC field
  - The PC is used as the access attribute for all bus transfers by the master
  - The SMPUs, PPUs, and SWPUs allow/restrict bus transfers based on the PC attribute
- PC Programming Restrictions
  - Changes to the PC can be restricted by the PC_MASK[4] field
  - Controlled by secure CPU (CM0+)

PC_MASK Example[5]



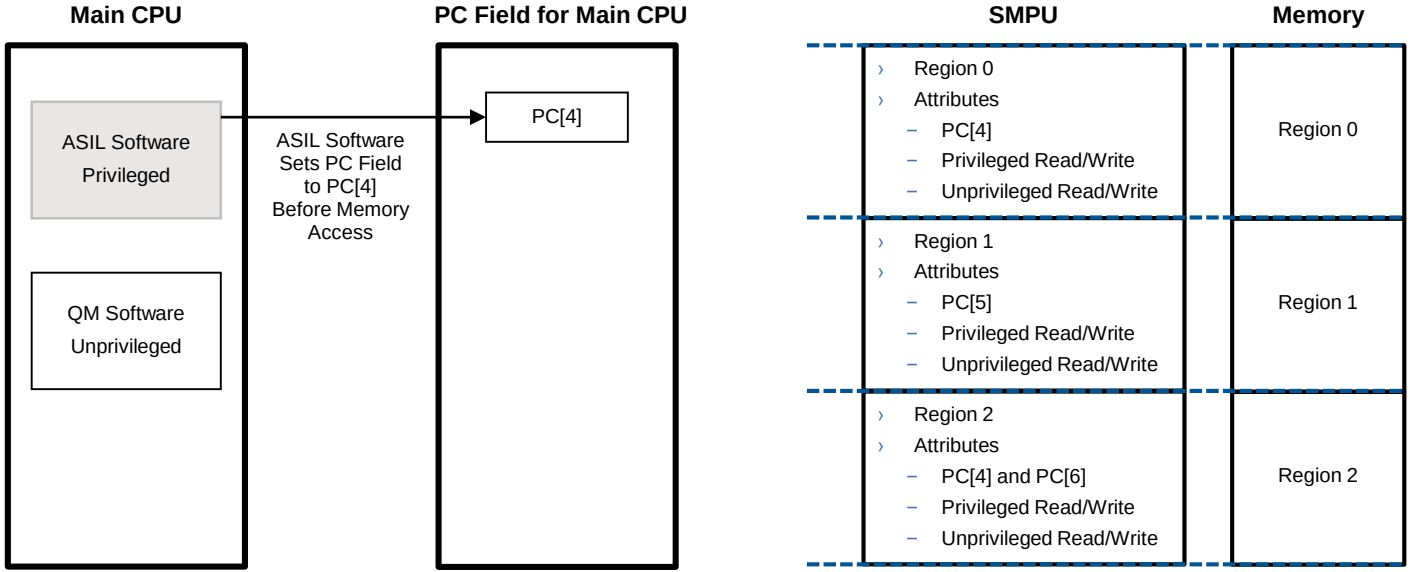
Hint Bar

Review TRM section 6.3 and the Register TRM for additional details

[1] The main CPU refers to CM4 or CM7 CPU in the MCU.
[2] The secondary CPU refers to CM0+ CPU in the MCU.
[3] The PC field is located in the MPU_MSx_CTL register.
[4] PC_MASK field is located in the SMPU_MSx_CTL register. PC_MASK_0 is always '0' and cannot set any master.
[5] PCs 4 and 6 are configurable; other PCs are nonconfigurable.

Protection Context

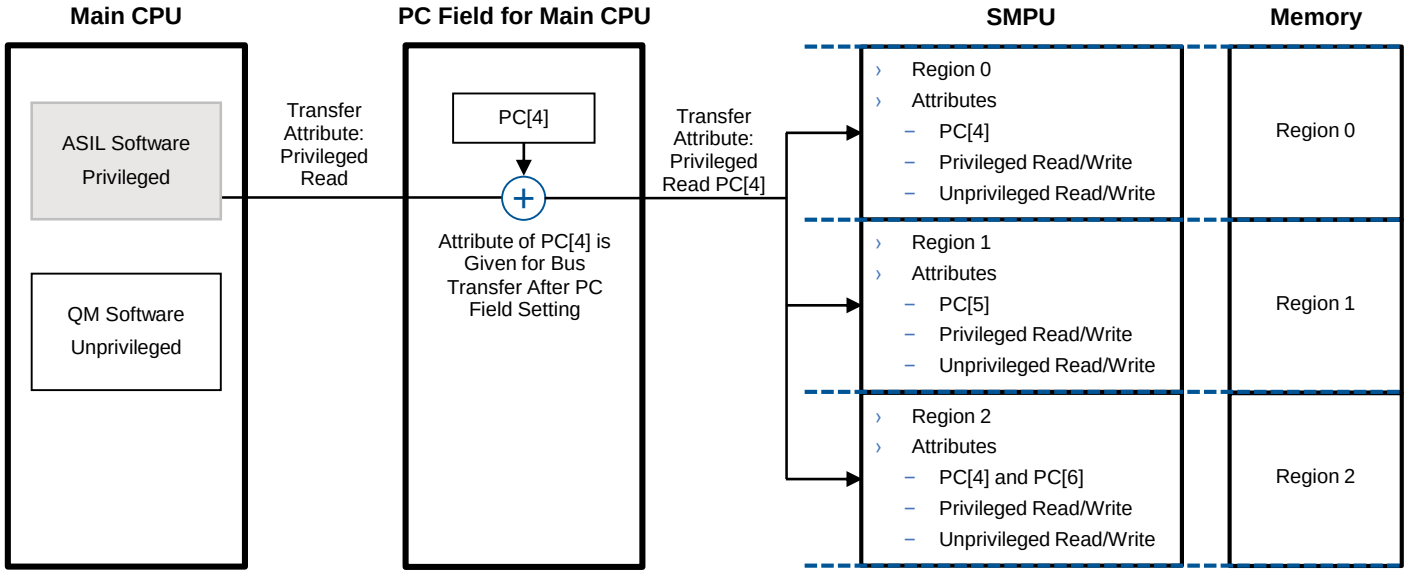
- Software separation between ASIL[1] and QM[2]



[1] ASIL: Automotive Safety Integrity Level. This software function has safety requirements.
[2] QM: Quality Management. This software function does not have safety requirements.

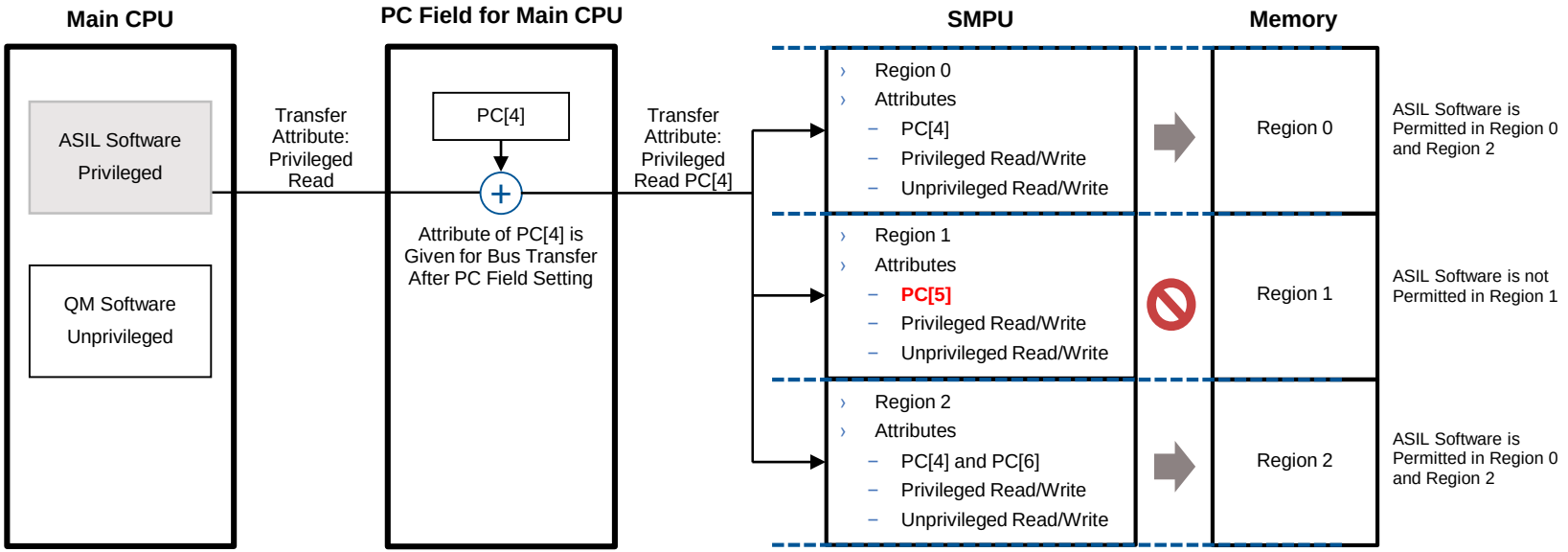
Protection Context

- Software separation between ASIL and QM
- Assign PC[4] to ASIL software



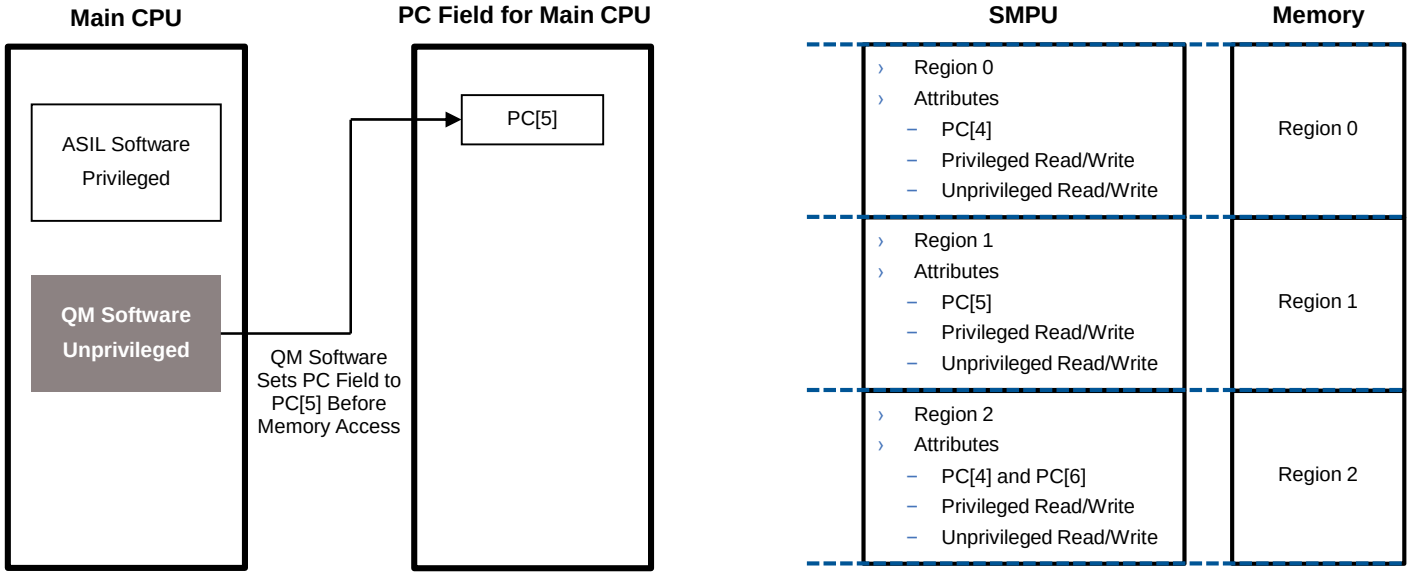
Protection Context

- Software separation between ASIL and QM
- Assign PC[4] to ASIL software
- Restrict memory access between PCs with SMPU



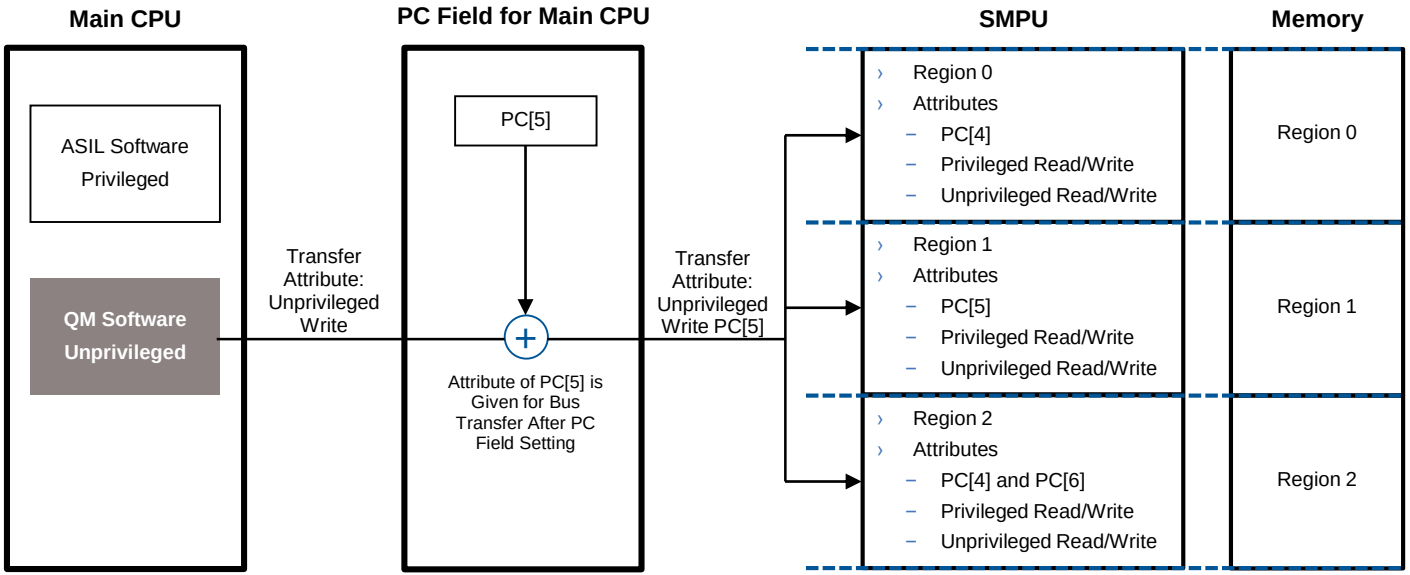
Protection Context

- Software separation between ASIL and QM



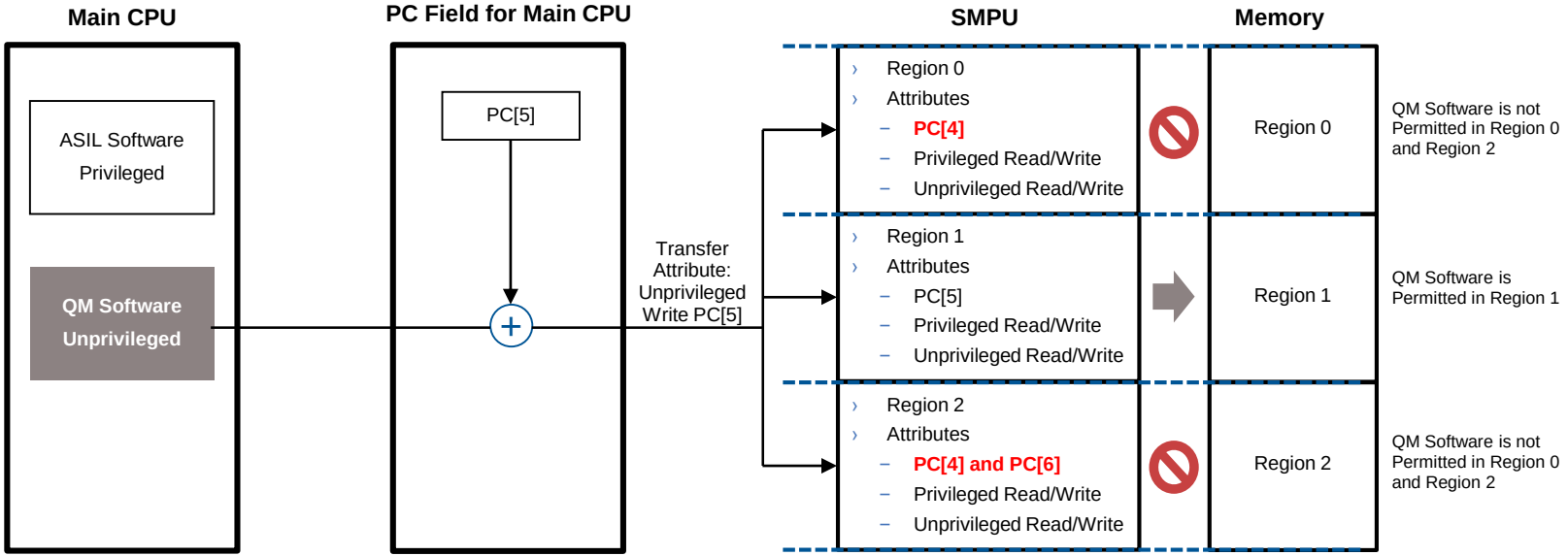
Protection Context

- Software separation between ASIL and QM
- Assign PC[5] to QM software



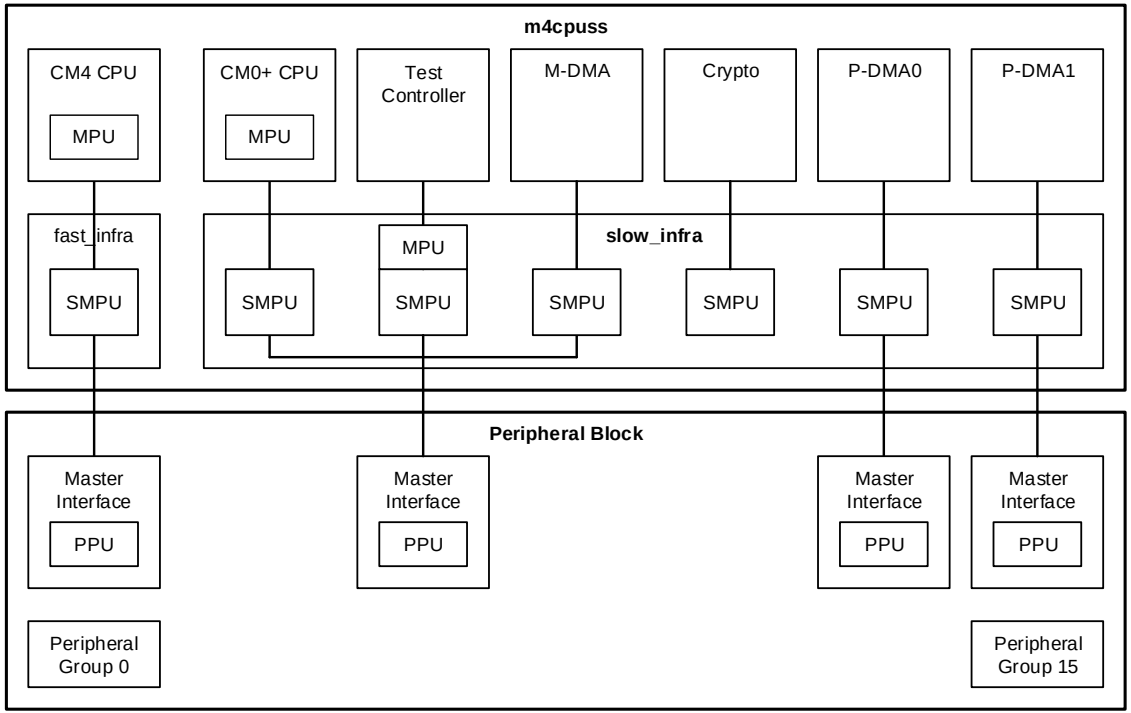
Protection Context

- Software separation between ASIL and QM
- Assign PC[5] to QM software
- Restrict memory access between PCs with SMPU



Block Diagram of Protection Unit

› Protection unit consists of the following components

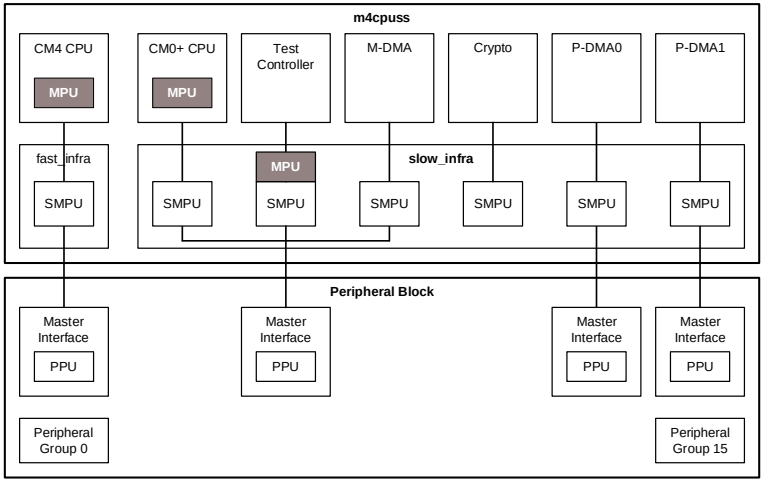


Hint Bar

Arm provides additional supporting material on their webpage at:
http://infocenter.arm.com

Memory Protection Unit Block Diagram

- MPU
  - Provides memory protection
  - Associated with a single master
    - Each CPU can independently give different roles
    - P-DMA, M-DMA, and Crypto inherit the attribute of programmed transfer
  - Up to sixteen regions
  - Two types of MPU:
    - Arm Cortex-M4/7 and Cortex-M0+ CPU
    - Bus infrastructure[1] for the test controller[2]
  - Access restriction:
    - Address range, Read/Write, Execute, and Privileged/Unprivileged
  - The region is equally divided into eight subregions



Hint Bar

Arm provides additional supporting material on their webpage at: http://infocenter.arm.com

Review TRM chapter 6 and Register TRM for additional details

Training section references:
CPUSS

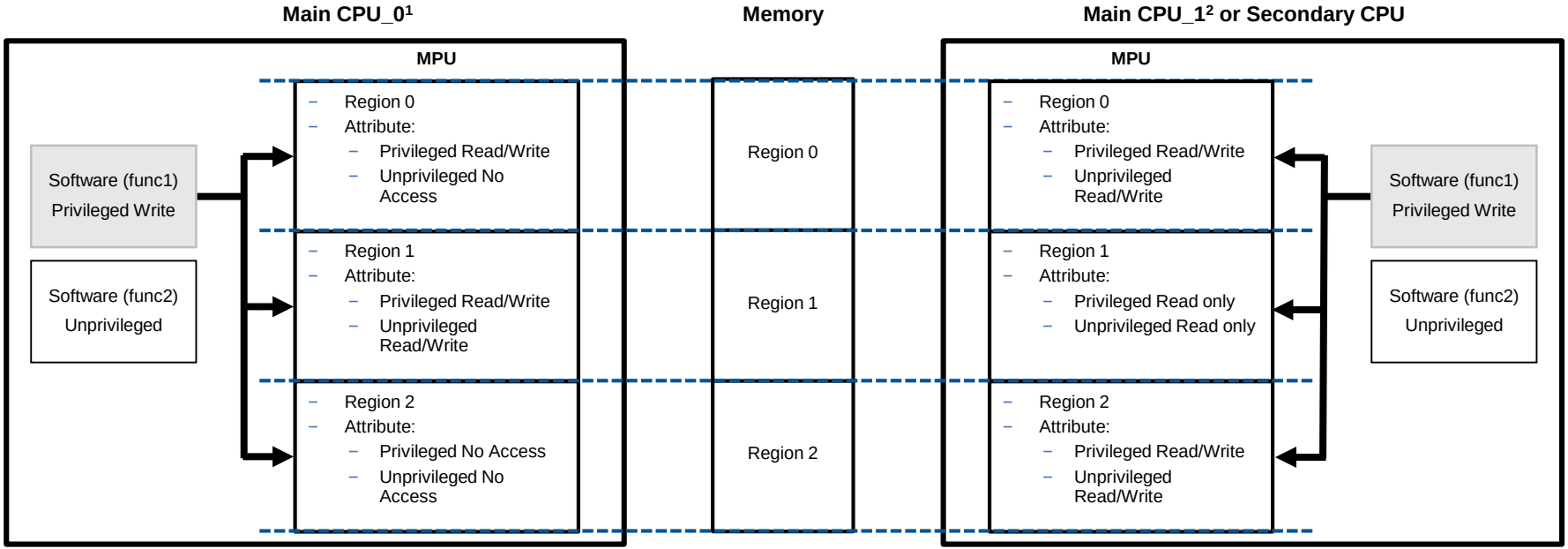
CYT2 series
CM4: 8 regions

CYT3/4 series
CM7: 16 regions

[1] The definition of MPU aspect of bus infrastructure follows the Arm MPU definition.
[2] The test controller is connected to the external debugger.

MPU Protection as Part of CPU

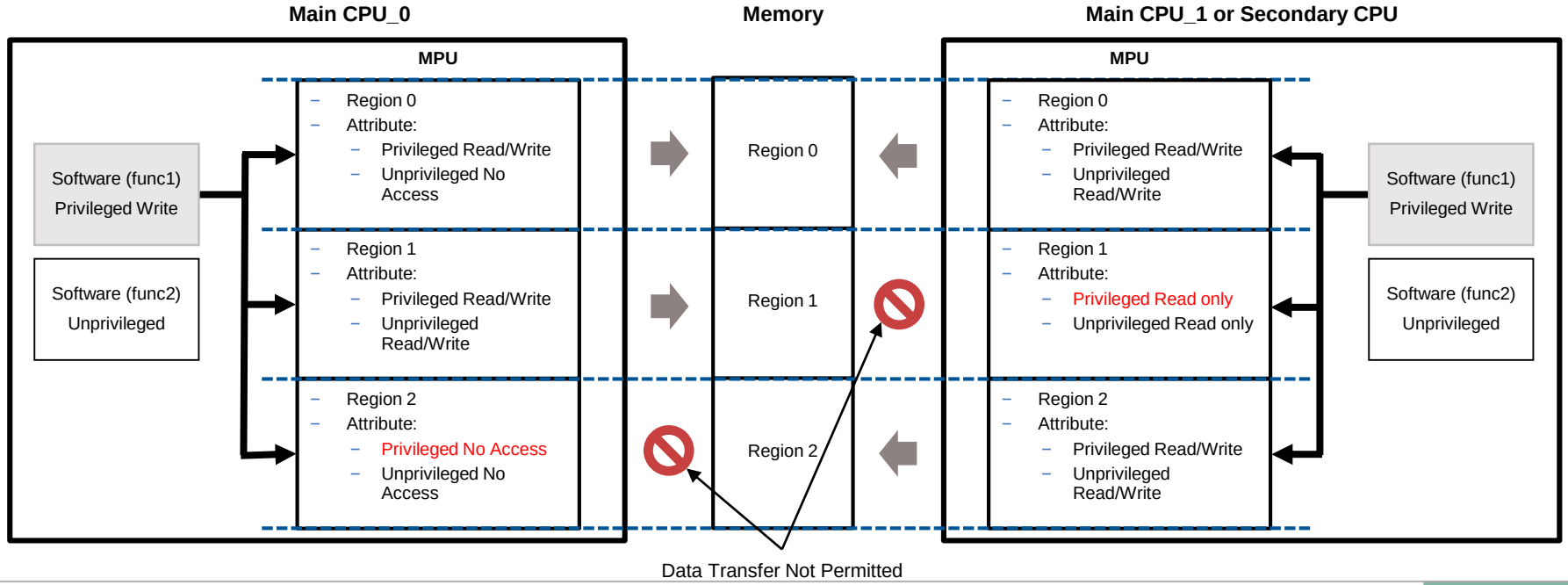
- Use Case 1
  - Software (func1) of both CPUs accesses to memory with privileged write



[1] Main CPU_0 is CM4 or CM7_0 in CYT2 (Entry).
[2] Main CPU_1 is CM7_1 in CYT4BF (High).

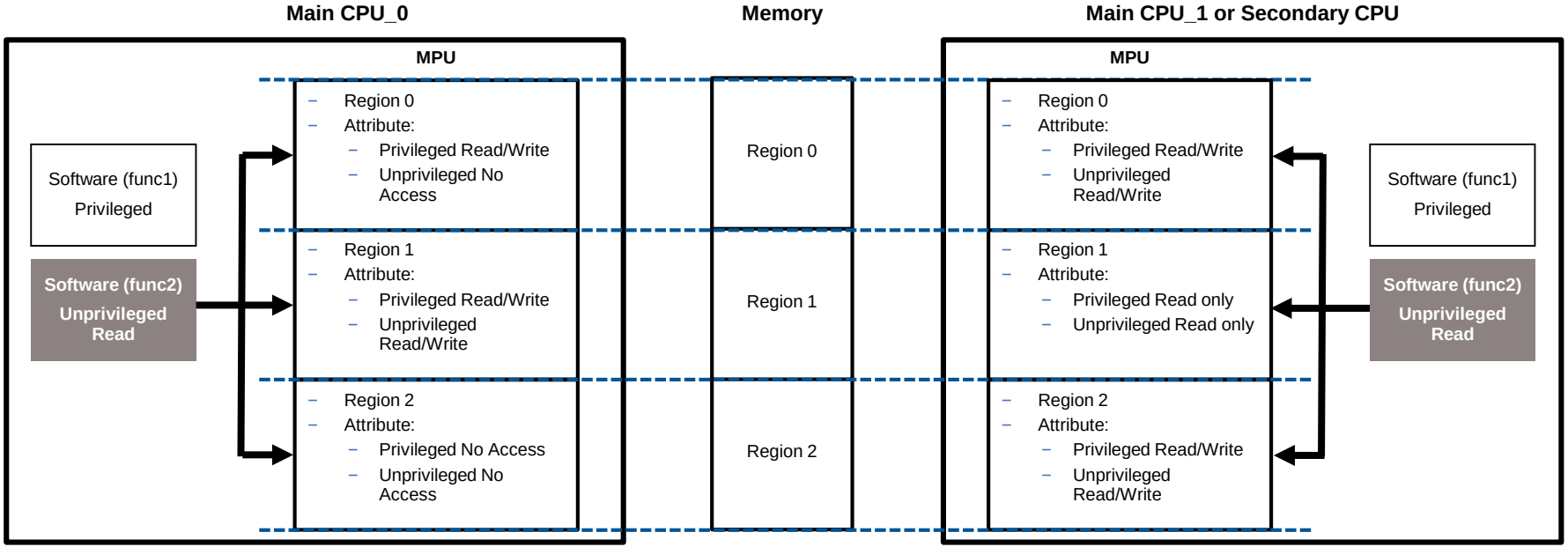
MPU Protection as Part of CPU

- Use Case 1
  - Software (func1) of Main CPU_0 is allowed access to Region 0 and Region 1
  - Software (func1) of Main CPU_1 or secondary CPU is allowed access to Region 0 and Region 2



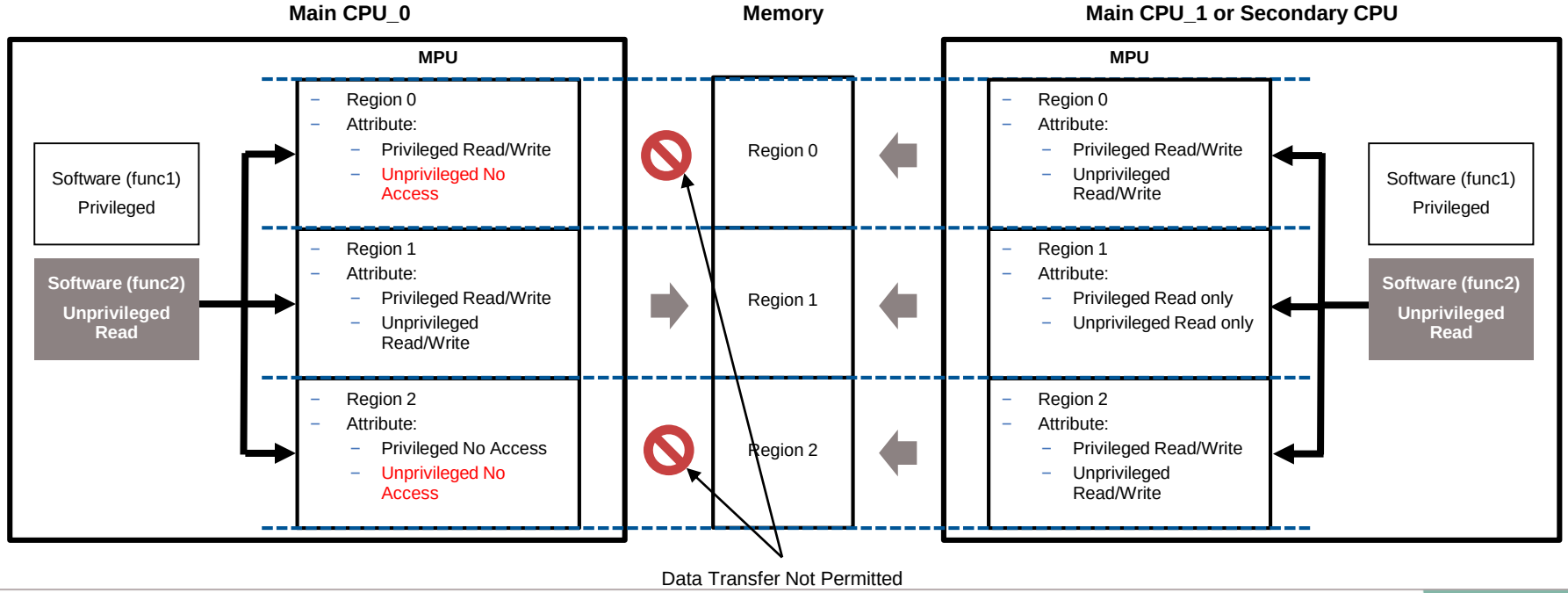
MPU Protection as Part of CPU

- Use Case 2
  - Software (func2) of both CPUs accesses to memory with unprivileged read



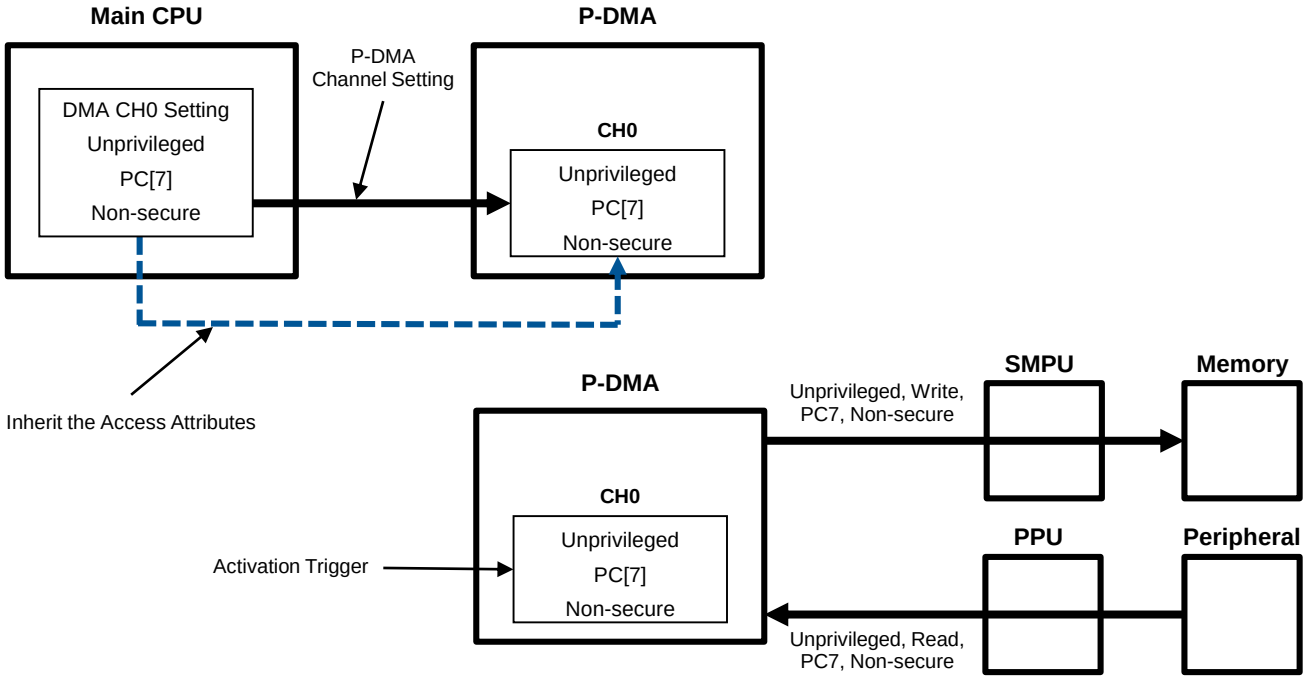
MPU Protection as Part of CPU

- Use Case 2
  - Software (func2) of Main CPU_0 is allowed access to Region 1
  - Software (func2) of Main CPU_1 or secondary CPU is allowed access to all regions



P-DMA/M-DMA/Crypto Access Attribute

- Inherit the access control attributes of the programmed bus transfer for these bus transfer attributes

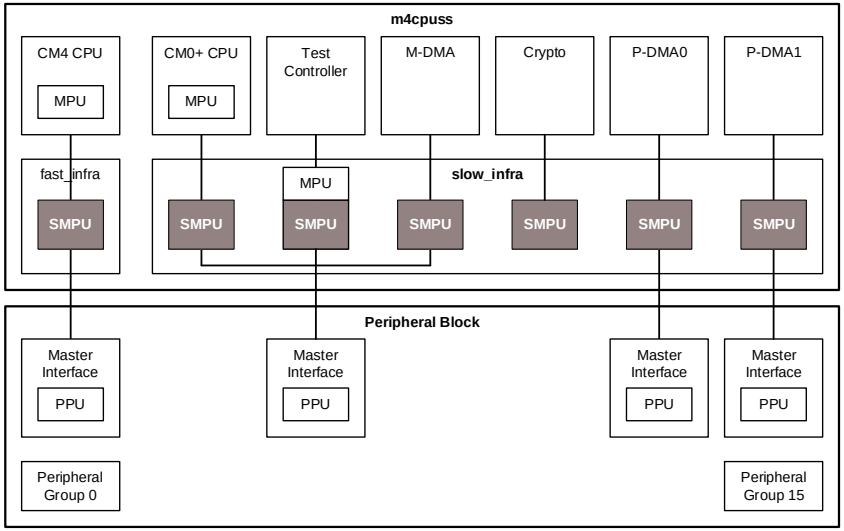


Hint Bar

Review TRM chapter 6 for additional details

Shared Memory Protection Unit Block Diagram

- SMPU
  - Provides memory protection
  - Shared by all bus masters
  - Includes 16 regions
  - Access restriction to:
    - Address range
    - Read/Write
    - Execute
    - Privileged/Unprivileged
    - Secure/Non-secure
    - Protection Context
  - The region is equally divided into eight subregions
  - Protection pair: slave and master protection structures



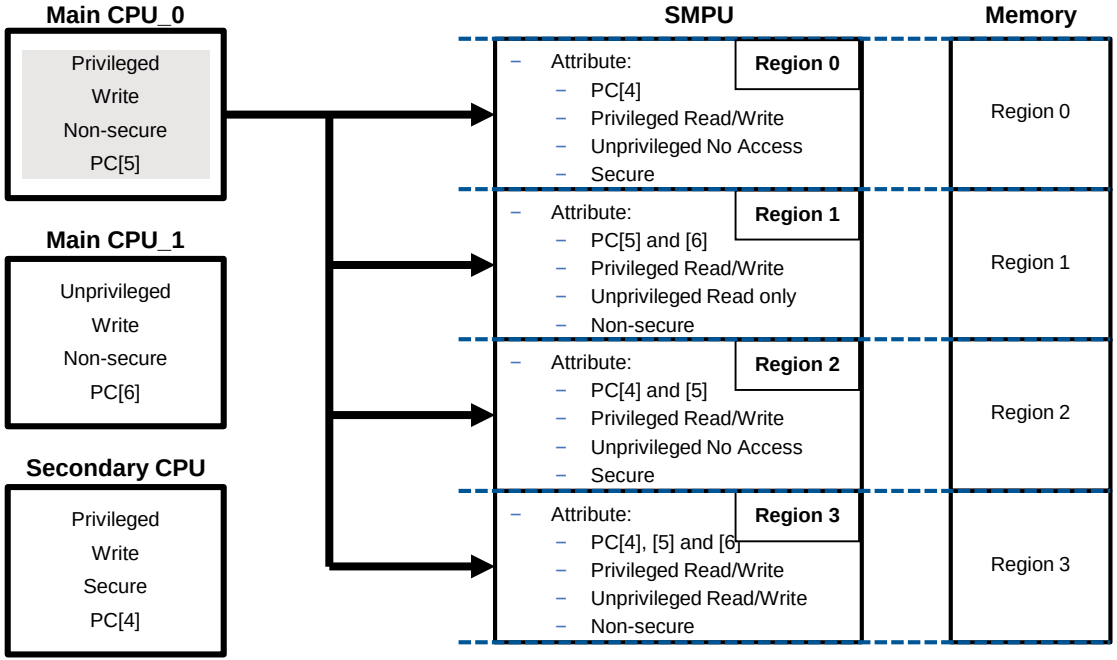
Hint Bar

Review TRM chapter 6 and the Register TRM for additional details

Training section references:
CPUSS

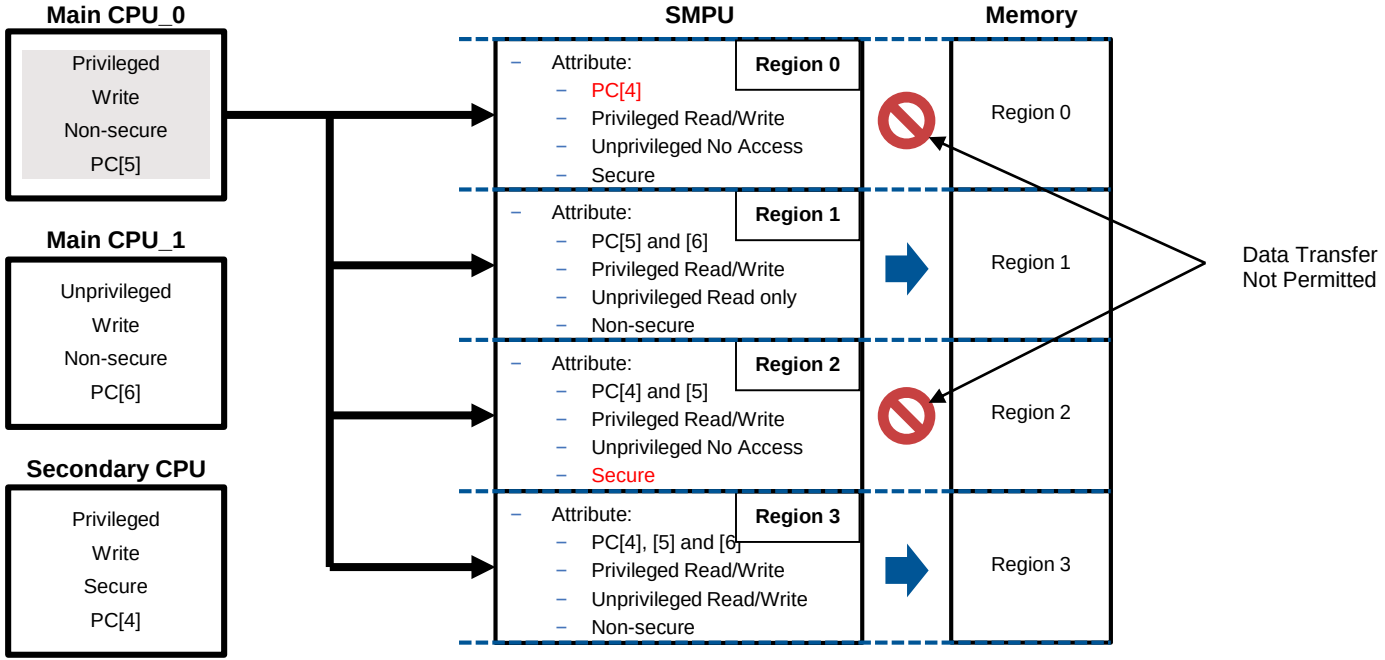
SMPU Protection

- Use Case 1
  - Main CPU_0 software accesses to memory with privileged write, non-secure, and PC[5]



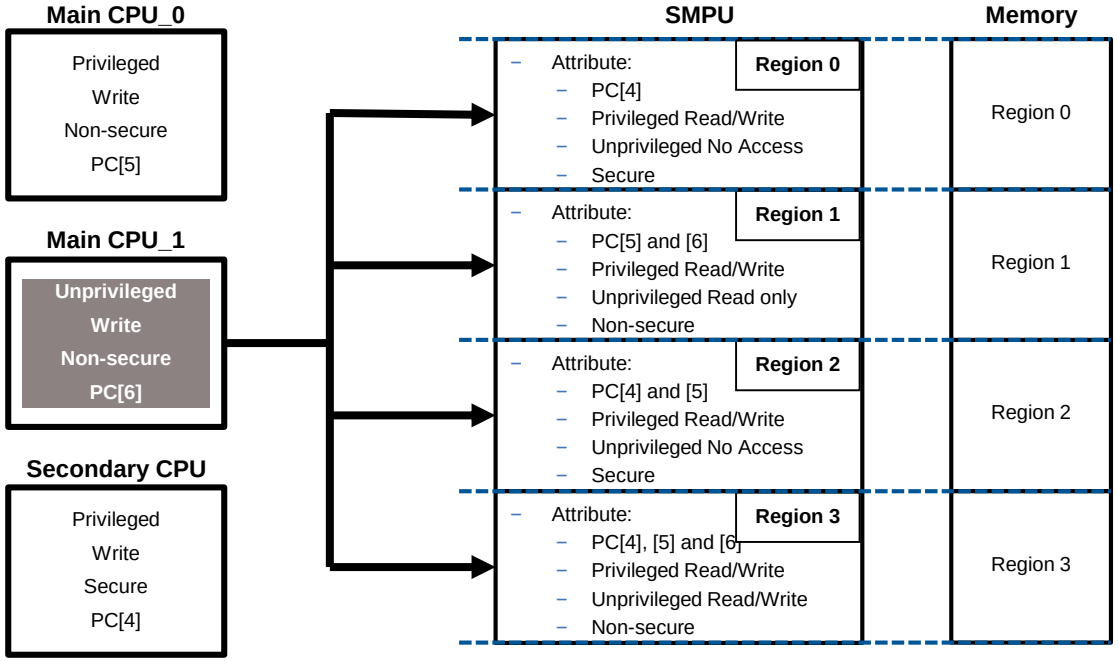
SMPU Protection

- Use Case 1
  - Main CPU_0 software is allowed access to Region 1 and Region 3



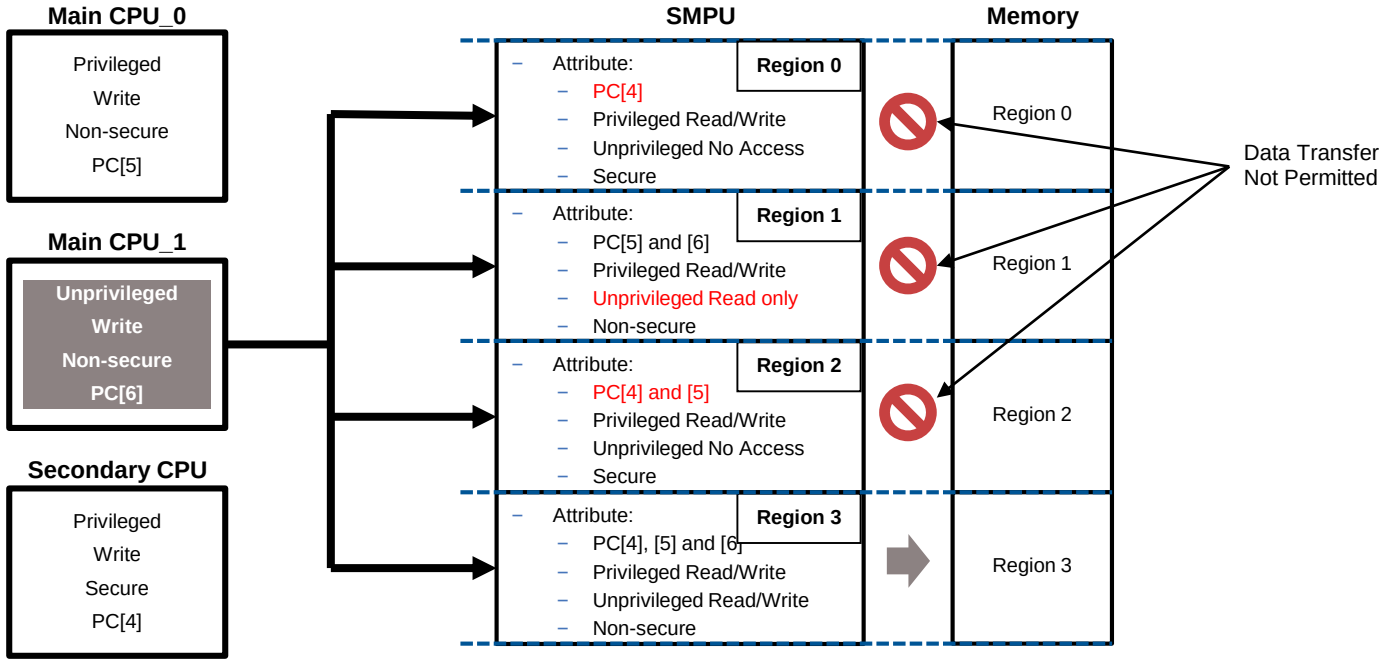
SMPU Protection

- Use Case 2
  - Main CPU_1 software accesses to memory with unprivileged write, non-secure, and PC[6]



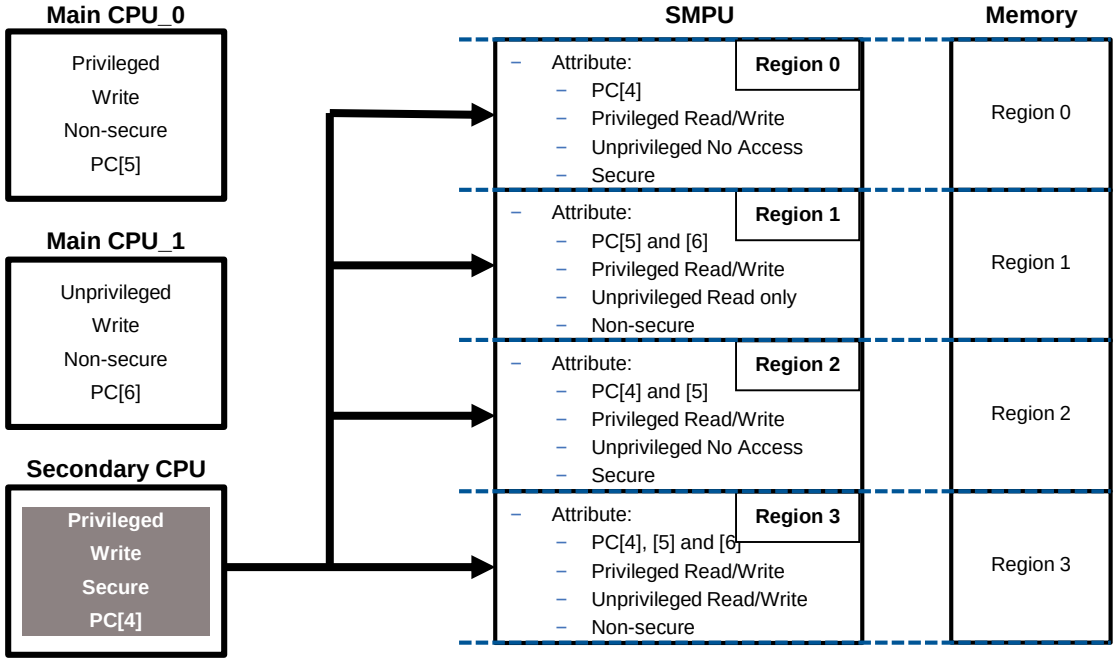
SMPU Protection

- Use Case 2
  - Main CPU_1 software is allowed access to Region 3



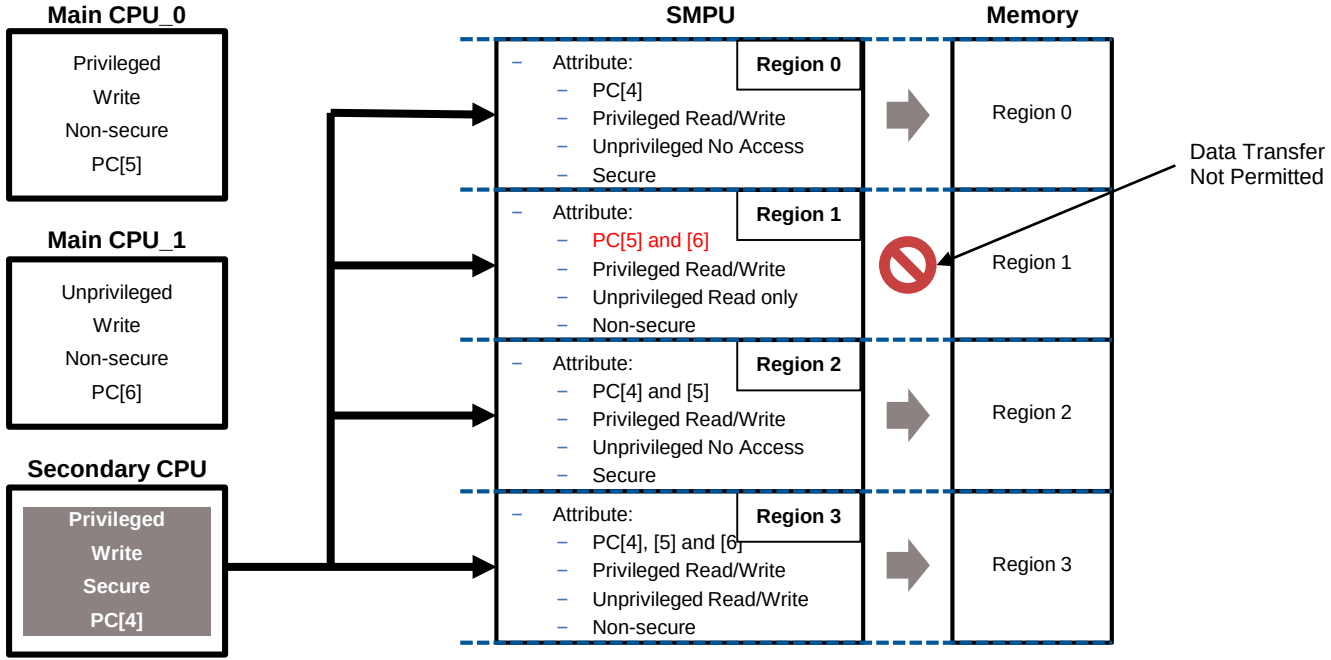
SMPU Protection

- Use Case 3
  - Secondary CPU software accesses to memory with privileged write, Secure, and PC[4]



SMPU Protection

- Use Case 3
  - Secondary CPU software is allowed access to Region 0, Region 2, and Region 3

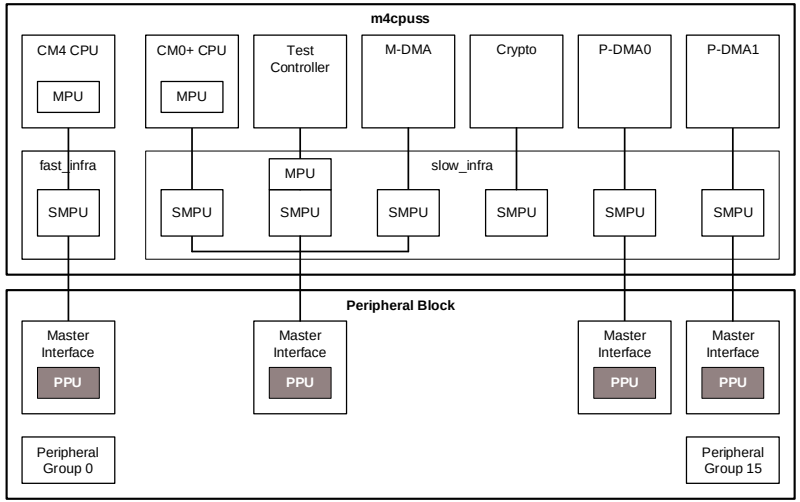


Hint Bar

Non-secure attribute allows both non-secure and secure access

Peripheral Protection Unit Block Diagram

- PPU
  - Provides peripheral protection
  - Shared by all bus masters
  - Two PPU types:
    - Fixed PPU structure[1]
    - Programmable PPU structure[2]
  - Access restriction to:
    - Address range (restricted to programmable PPU)
    - Read/Write
    - Privileged/Unprivileged
    - Secure/Non-secure
    - Protection Context
    - Applies different setting for each PC
  - Protection pair: slave and master protection structures
  - Protection information uses a single SRAM with ECC



Hint Bar

Review TRM chapter 6 and Register TRM for additional details

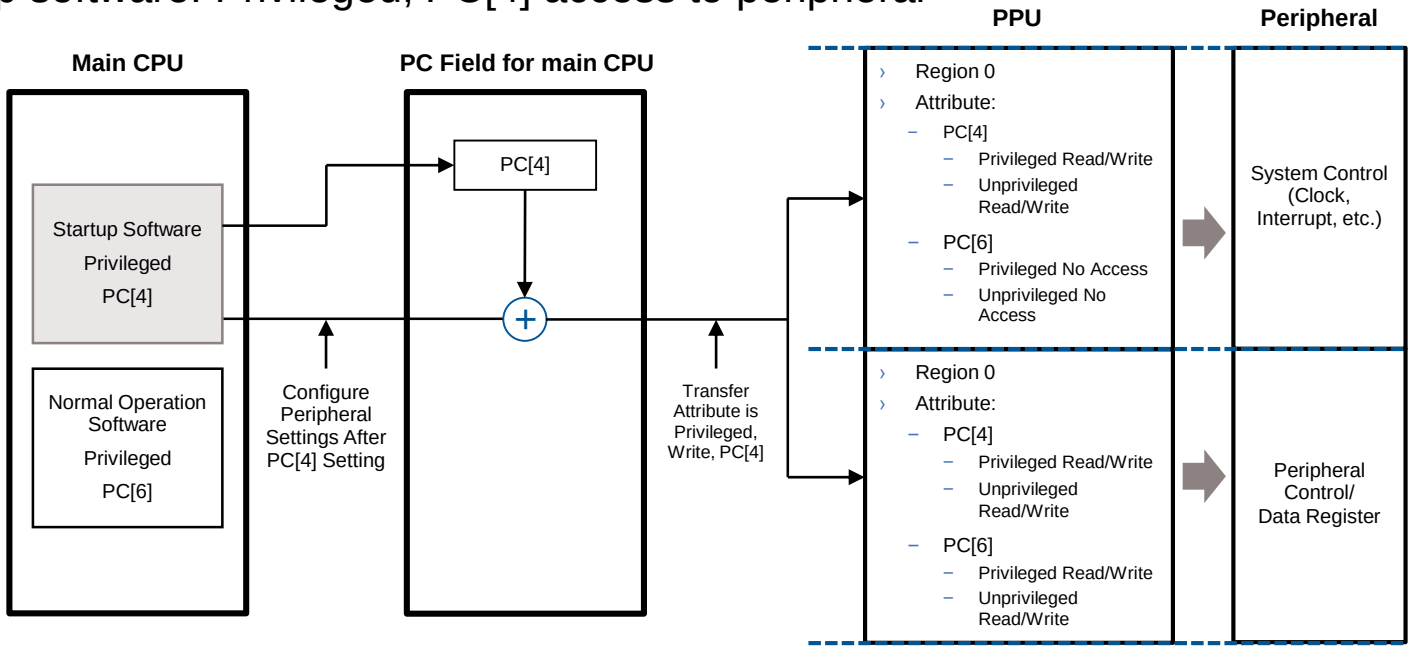
Review TRM section 6.4.7 for details of SRAM and ECC

Fixed structures take precedence over programmable structures

[1] Protects address range of known resources
[2] Protects address range of specific resources

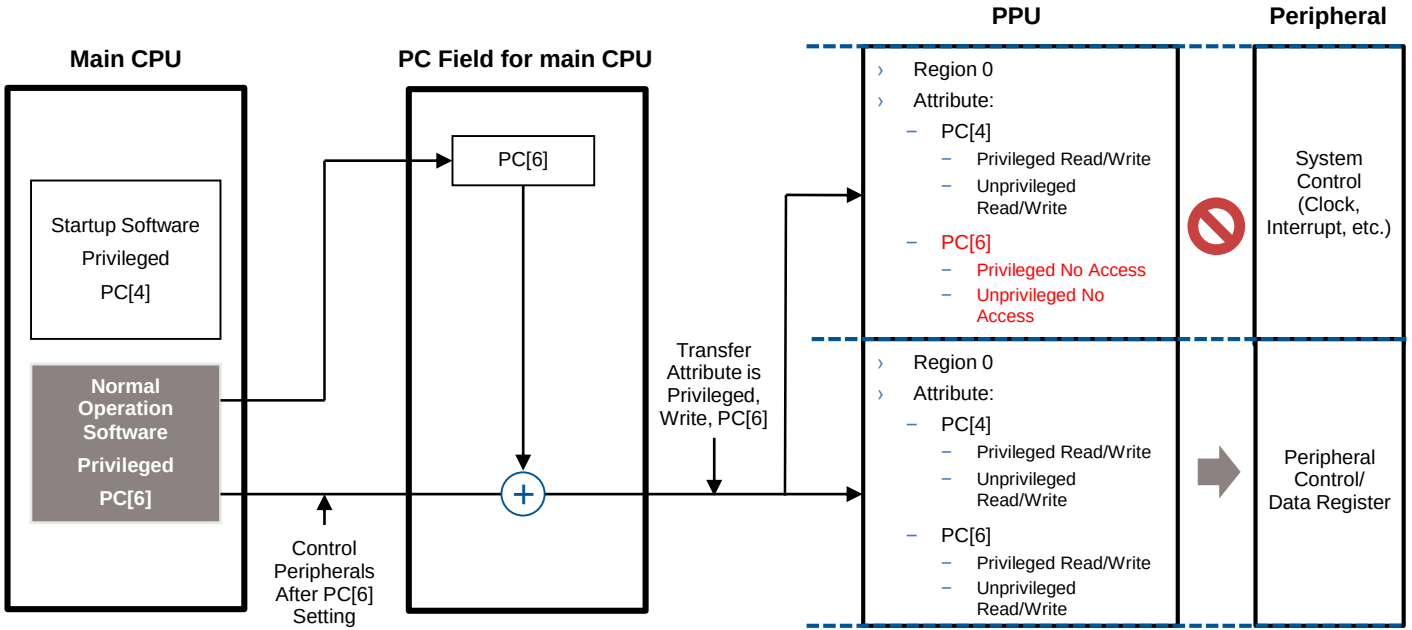
PPU Protection

- Execute system settings such as clock and initial setting of peripheral in startup software at power-up
- Startup software: Privileged, PC[4] access to peripheral



PPU Protection

- Transfer to normal operation software after initial setting and startup software is not executed
- Normal operation software: Privileged, PC[6] access to peripheral



Hint Bar

Advantage:

Prevents erroneous change of system setting by applying different access attributes between initial setting and normal

SWPU

- SWPU is used to access restrictions to flash (write[1]) and eFuse (read/write)
  - SWPU prevents malicious or unintended access of flash or eFuse.
  - SWPU has three Protection Units:
    - FWPU: Flash Write Protection Unit. (Up to 16 regions)
    - ERPU: eFuse Read Protection Unit. (Up to 4 regions)
    - EWPU: eFuse Write Protection Unit. (Up to 4 regions)
  - SWPU has two configuration parts:
    - Boot protection: It cannot be updated.
    - Application protection: It is additional access restrictions specific to the application.
  - SWPU is read during boot process from SFlash, and stores them in RAM
  - Access restriction to:
    - Address range
    - Read/Write
    - Privileged/Unprivileged
    - Secure/Non-secure
    - Protection Context
  - Protection pair: slave and master protection structures

Hint Bar

Review TRM section 6.5 for additional details

[1] Program and Erase

SWPU Structure (Application Protection)

SWPU is stored in SFlash

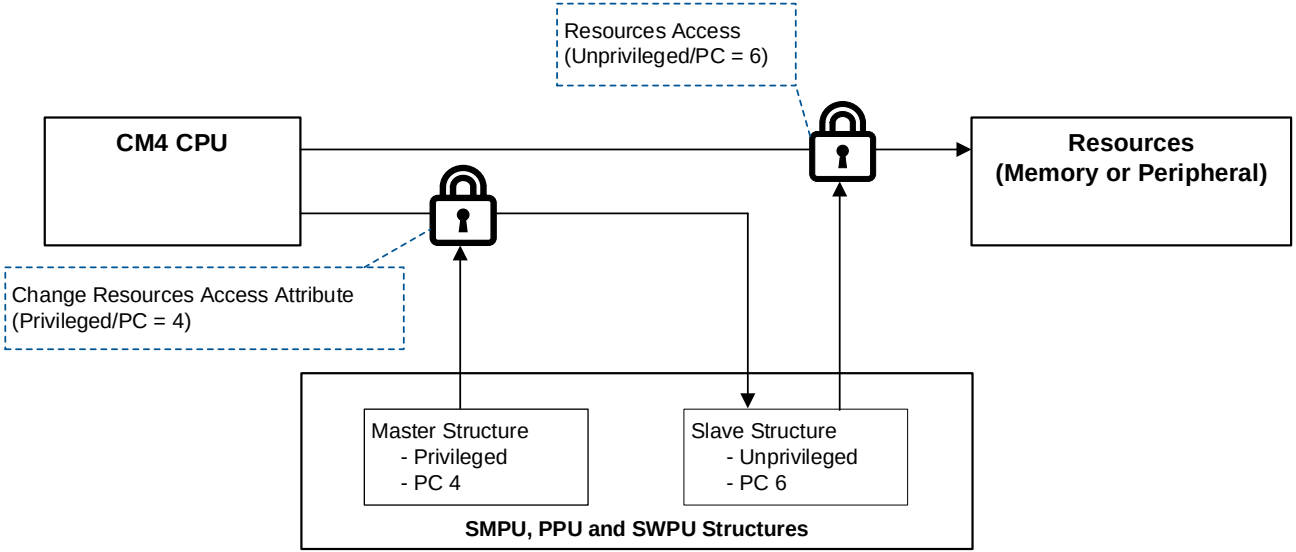
SWPU	Field Name	Size	Description
	Object Size	4 bytes	Number of configured elements
FWPU	N_FWPU	4 bytes	Number of FWPU objects. Up to 16 regions
	FWPU0_SL_ADDR	4 bytes	Configures the FWPU0 base address
	FWPU0_SL_SIZE	4 bytes	Configures the FWPU0 region size and FWPU0 enable
	FWPU0_SL_ATT	4 bytes	Configures the FWPU0 slave attribute
	FWPU0_MS_ATT	4 bytes	Configures the FWPU0 master attribute
	:	4 bytes	
ERPU	N_ERPU	4 bytes	Number of ERPU objects. ERPU has up to four regions.
	ERPU0_SL_OFFSET	4 bytes	Configures the ERPU0 base address offset
	ERPU0_SL_SIZE	4 bytes	Configures the ERPU0 region size and ERPU0 enable
	ERPU0_SL_ATT	4 bytes	Configures the ERPU0 slave attribute
	ERPU0_MS_ATT	4 bytes	Configures the ERPU0 master attribute
	:		
EWPU	N_EWPU	4 bytes	Number of EWPU objects. EWPU has up to four regions.
	EWPU0_SL_OFFSET	4 bytes	Configures the EWPU0 base address offset
	EWPU0_SL_SIZE	4 bytes	Configures the EWPU0 region size and ERPU0 enable
	EWPU0_SL_ATT	4 bytes	Configures the EWPU0 slave attribute
	WPU0_MS_ATT	4 bytes	Configures the EWPU0 master attribute
	:		

Hint Bar

Review TRM section 6.5 for setting example

Protection Pair

- SMPU, PPU, and SWPU have a protection pair for protection of protection structures
  - Master structure: Protection of slave structure
  - Slave structure: Protection of resources
  - Change slave setting attributes by master setting attributes



Protection Violation

- MPU, SMPU, and PPU detect a restricted transfer; the bus transfer results in a bus error
  - Access is evaluated by each protection unit in the following order:
    - MPU (High) > SMPU > PPU (Low)
  - The slave address regions in programmable PPU may overlap with other slave address regions. In this case, access is evaluated by the PPU in the following order:
    - PPU master structure (High) > Programmable slave structures > Fixed slave structure (Low)
  - The bus transfer will not reach its target
- Violation information is reported to the fault reporting structure
  - Violation address
  - Bus transfer attribute
  - Accessed bus master

Hint Bar

Training section references:
Fault Structure

Advantage:

Prevents erroneous writing by not allowing transfer

Possible analysis of violation transfer

Part of your life. Part of tomorrow.

Revision History

Revision	ECN	Submission Date	Description of Change
**	6138645	04/17/2018	Initial release
*A	6346788	12/10/2018	Added slide 2. Updated slides 3, 4, and 5. Revised description on slides 10 and 11 from Privileged to Unprivileged In all slides, changed CM4 and CM0+ to main CPU and secondary CPU, and added notes 4 and 5 on slide 8 Changed slides 22 – 27
*B	6633371	7/22/2019	Added slide 5. Updated slide 2, 18.
*C	6825576	03/06/2020	Changed document title from PROTECTION UNITS (M4CPUSS_VER2/M7CPUSS) to TRAVEO(TM) II PROTECTION UNITS (M4CPUSS_VER2/M7CPUSS)
*D	7060711	01/06/2021	Updated Slide 2, 3, 7, 8, 16, 29, 34 Added slide 32, 33