Protection configuration in TRAVEO™ T2G MCU

About this document

Scope and purpose

This application note explains the functionality and how to configure the protection units for TRAVEO™ T2G family MCU. This document serves as a guide to enhance system security based on different operations. It also explains the structure, access attributes, and a few usage examples of each protection unit.

Intended audience

This document is intended for anyone using the TRAVEO™ T2G family.

Associated part family

TRAVEO™ T2G family

Table of contents

Table of contents

1 Introduction

This application note describes the protection units in TRAVEO™ T2G family series MCU. The series includes CPUSS which is based on multiple 32-bit Arm® Cortex® CPUs, enhanced secure hardware extension (eSHE), CAN FD, memory, and analog and digital peripheral functions in a single chip.

Protection units are an important part of security system design and enforce security based on different operations. A protection unit allows or restricts bus transfers on the bus infrastructure based on specific properties. A protection violation is caused by a mismatch between a bus transfer's address region and access attributes and the protection structures' address range and access attributes.

These series have three types of protection units:

- Memory protection unit (MPU)
- Shared memory protection unit (SMPU)
- Peripheral protection unit (PPU)

Memory protection is provided by MPU and SMPU; protection for peripheral resources is provided by PPU.

The MPU, SMPU, and PPU protection structure definition follows the Arm® definition (in terms of memory region and access attribute definition) to ensure a consistent software interface.

If security is required, the SMPU and possibly PPUs registers must be controlled by a "secure" CPU that enforces system-wide protection.

To understand the functionality described and terminology used in this application note, see the Protection unit chapter of the architecture technical reference manual (TRM).

In addition, this application note describes example code with the sample driver library (SDL). The code snippets in this application note are part of SDL. See Other references for the SDL.

SDL has a configuration part and a driver part. The configuration part mainly configures the parameter values for the desired operation. The driver part configures each register based on the parameter values in the configuration part. You can configure the configuration part according to your system. This sample program shows the CYT2B7 series.

2 Protection units

2.1 Location of protection units

Figure 1 shows the locations of MPUs, SMPUs, and PPUs in the CYT2B series.

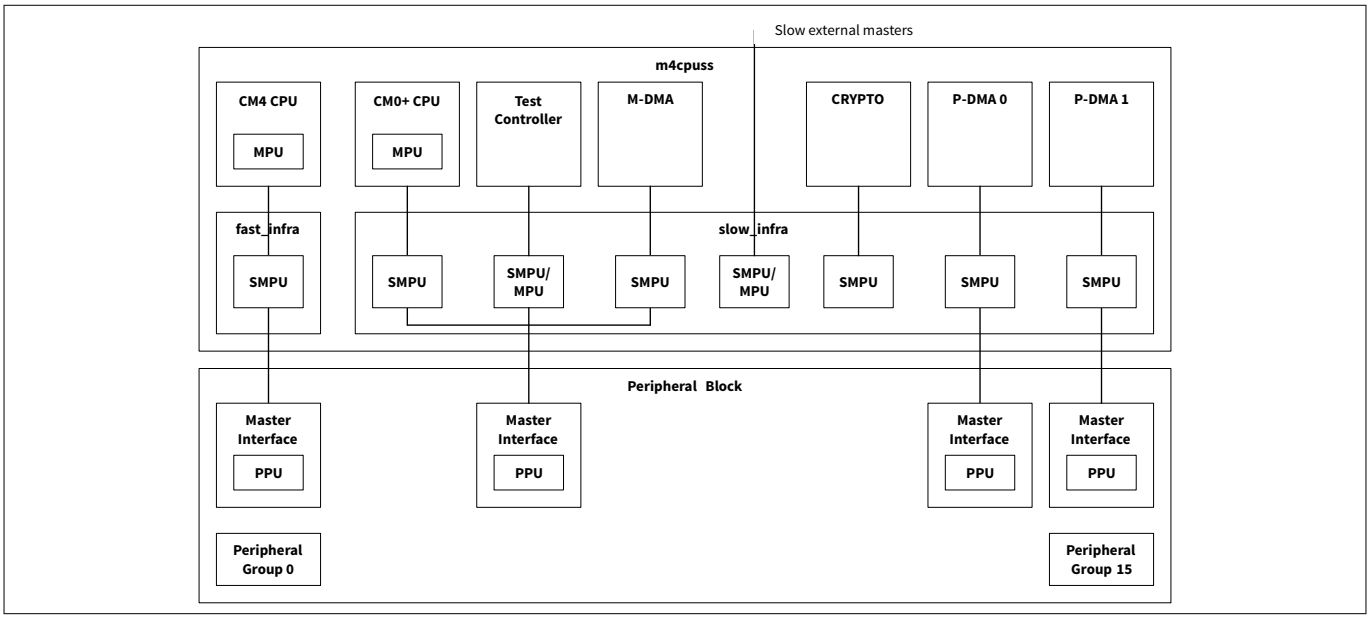

Figure 1 Protection unit locations in the CYT2B series

See the architecture (TRM) for other series location.

2.2 Protection units overview

MPUs are associated with a single master. These are two types of MPUs.

- An MPU that is implemented as part of the CPU: This type is found in the Arm® CPUs.
- An MPU that is implemented as part of the bus infrastructure: This type is found in bus masters such as test controllers.

However, peripheral DMA (P-DMA 0/1), memory DMA (M-DMA), and cryptography (CRYPTO) components do not have an MPU. These masters inherit the access control attributes of the bus transfer that programmed channels or components.

An SMPU is shared by all bus masters. A single set of SMPU region structures provides the same protection information to all SMPUs in the systems.

A PPU is shared by all bus masters. PPU provides access control to the peripherals within a peripheral group. These are two types of PPU:

- Fixed PPU: The address to protect is fixed and cannot be modified by software.
- Programmable PPU: The address to protect is programmable by software.

MPU and SMPU have a higher priority over PPU. In addition, programmable PPU has a higher priority than fixed PPU.

See the architecture (TRM) for more details on protection units.

3 Operation overview

3.1 Protection properties of bus transfer

Protection units identify the following properties of bus transfer:

- An address range to be accessedThe MPU, SMPU, and PPU protection structure definition follows the Arm® definition. Therefore, note the following when setting the region address and region size of the protection unit.
  - The base address of the region address must be aligned to the region size. When the region size is 64 KB, the base address must be aligned on a multiple of 64 KB, for example, at 0x00010000 or 0x00020000. See the registers TRM for details.
- Access attributes such as the following:
  - Read/Write: Distinguish read access from a write access
  - Execute: Distinguish code access from a data access
  - User/Privileged: Distinguish user access from a privileged access
  - Secure/non-secure: Distinguish secure code access from non-secure code access. The non-secure attribute allows both non-secure and secure access.
  - Protection context: Distinguish accesses from different protection contexts

Not all bus masters provide all these access attributes. No bus master has a protected context; Arm® CPUs do not have a secure attribute.

Access attributes not provided by the bus master are provided by the PROT_MPUx_MS_CTL and PROT_SMPU_MSx_CTL registers. These registers may be set during the boot process or by the secure CPU. Figure 2 shows the structure of PROT_MPUx_MS_CTL registers.

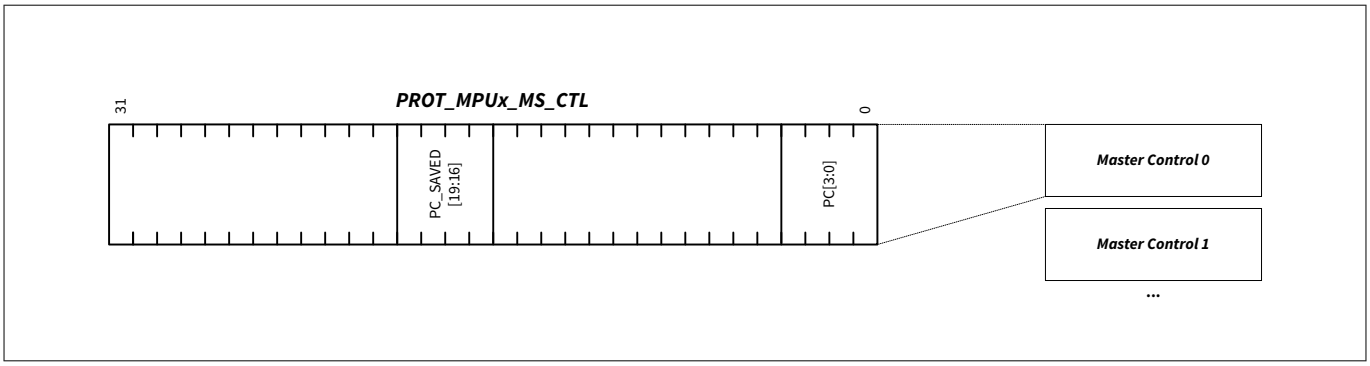

Figure 2 PROT_MPUx_MS_CTL registerPROT_SMPU_MSx_CTL register

This register grants a protection context attribute to its master access.

- PROT_MPUx_MS_CTL.PC: Sets the protection context attribute of its own access
- PROT_MPUx_MS_CTL.PC_SAVED: The boot process sets this field. This field is only present for the CM0+ master.

Figure 3 shows the structure of the PROT_SMPU_MSx_CTL registers.

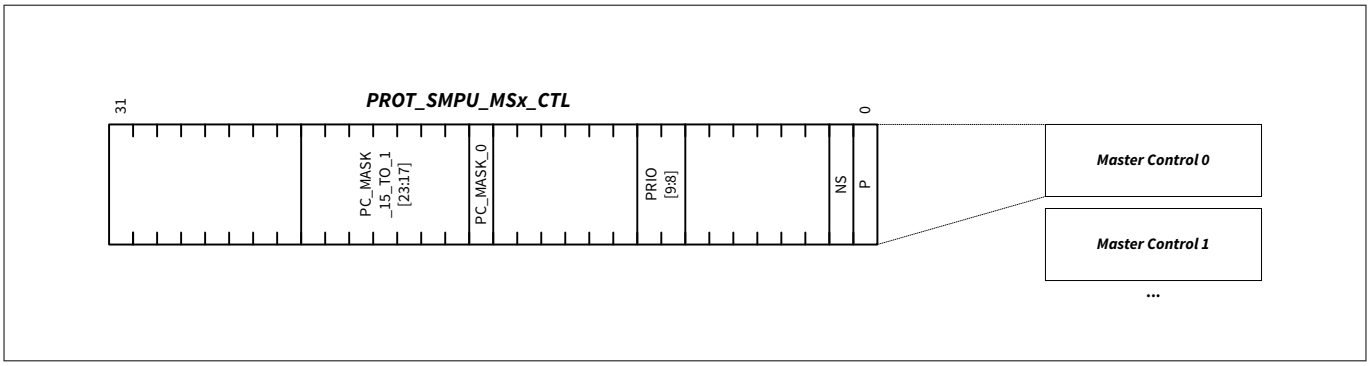

Figure 3 **PROT_SMPU_MSx_CTL register**

This register grants the following attributes to its master access.

- PROT_SMPU_MSx_CTL.P: Provides the User/Privileged attribute for masters that do not provide their own attribute.
- PROT_SMPU_MSx_CTL.NS: Provides the Secure/Non-Secure attribute for masters that do not provide their own attributes.
- PROT_SMPU_MSx_CTL.PC_MASK_15_TO_1 and PC_MASK_0: Restricts the protection context that the bus master can set to MPUx_MS_CTL.PC.

Note: *When one of the bits CPUSS_CM0_PC_CTL.VALID[3:1] is 1 (the associated protection context handler is valid), write transfers of the application software to the associated bits of PROT_SMPU_MSx_CTL.PC_MASK_15_TO_1[19:17] always writes 0. This ensures that when valid protection context handlers are used to enter protection contexts 1, 2, or 3, the application software cannot enter those protection contexts. Also, the application software should clear the relevant bits of PROT_SMPU_MSx_CTL.PC_MASK_15_TO_1[19:17] when CPUSS_CMx_PC_CTL.VALID[3:1] bits are set to 1. See registers TRM for more details.*

- The PC_MASK_0 field is always 0. This means that bus masters cannot set the PC = 0 attribute.
- PROT_SMPU_MSx_CTL.PRIO: Sets the bus arbitration priority.

However, not all bus masters have these register fields. Table 1 shows the relationship of registers for each master.

Table 1 **Register field provided to the master**

Register field	CM0+ CPU	CRYPTO component	P-DMA 0	P-DMA 1	M-DMA	CM4F CPU	Test controller
PROT_MPUx_MS_CTL.PC	Yes	–	–	–	–	Yes	Yes
PROT_MPUx_MS_CTL.PC_SAVED	Yes	–	–	–	–	–	–
PROT_SMPU_MSx_CTL.P	–	–	–	–	–	–	Yes
PROT_SMPU_MSx_CTL.NS	Yes	–	–	–	–	Yes	Yes
PROT_SMPU_MSx_CTL.PC_MASK_15_TO_1 and PC_MASK_0	Yes	–	–	–	–	Yes	Yes

(table continues...)

Table 1 (continued) Register field provided to the master

Register field	CM0+ CPU	CRYPTO component	P-DMA 0	P-DMA 1	M-DMA	CM4F CPU	Test controller
PROT_SMPU_MSx_CTL.PRIO	Yes	Yes	Yes	Yes	Yes	Yes	Yes

P-DMA0/1, M-DMA, and CRYPTO components do not have MPU. Therefore, these peripheral functions do not have fields to set attributes.

Each master has an associated SMPU MS_CTL register. However, in secure systems, this register can be typically controlled only by the secure master (CM0+) to prevent a master from changing its own privileged setting, security setting, arbitration priority, or enabled protection contexts.

3.2 Attribute inheritance

As mentioned earlier, P-DMA, M-DMA, and CRYPTO components inherit the access control attributes of the bus transfers that programmed the channels and components. The inherited access attribute is allowed/restricted by SMPU and PPU.

Figure 4 shows examples of the setting and behavior for inheriting attributes.

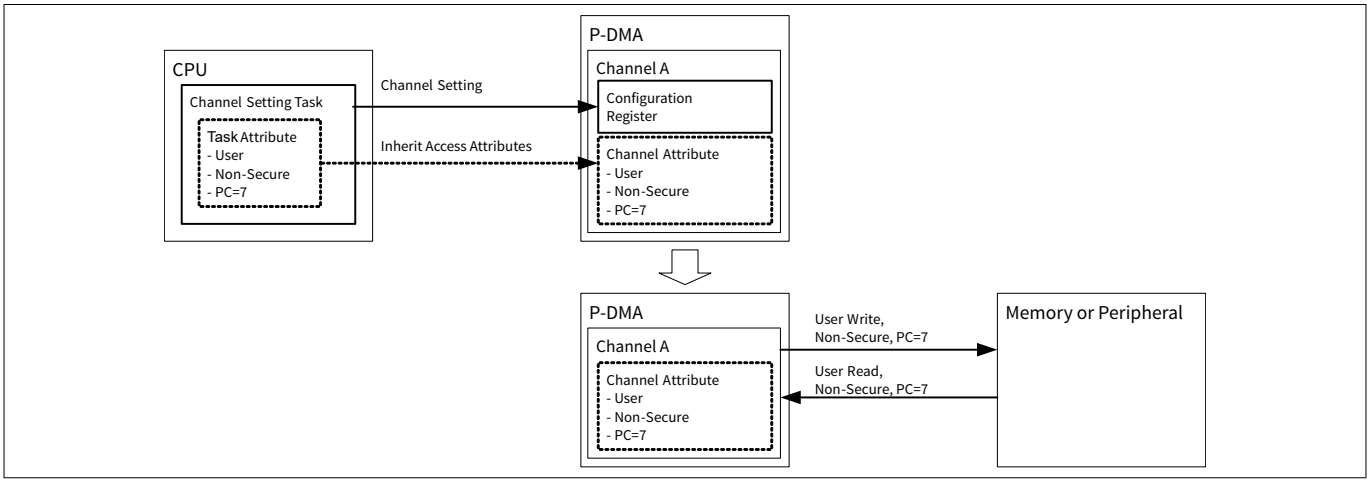

Figure 4 Setting and behavior example for attribute inheritance

3.3 User/privileged attribute switching

This section describes attribute switching of both CPUs supporting user/privileged attributes. CPUs support two operating modes and two privilege levels as follows:

- Operation mode
  - Thread mode: This mode is used to execute application software. This mode can run in privileged level or user level.
  - Handler mode: This mode is used to handle exceptions. This mode only runs in privileged level.
- Privileged levels
  - User level: The software has limited access
  - Privileged level: The software can use all instructions and access all resources

Privileged level is switched by the CONTROL register. It is a CPU-specific register. Switching from privileged level to user level is performed by the CONTROL register. However, the CONTROL register can be rewritten only with the privileged level. Therefore, switching from the user level to the privileged level must always go through the handler mode. The CPU enters the handler mode when an exception or interrupt occurs. Figure 5 shows an

example of user/privileged level switching by the SVC (Supervisor call) instruction exception. The SVC instruction generates an exception and can enter the handler mode.

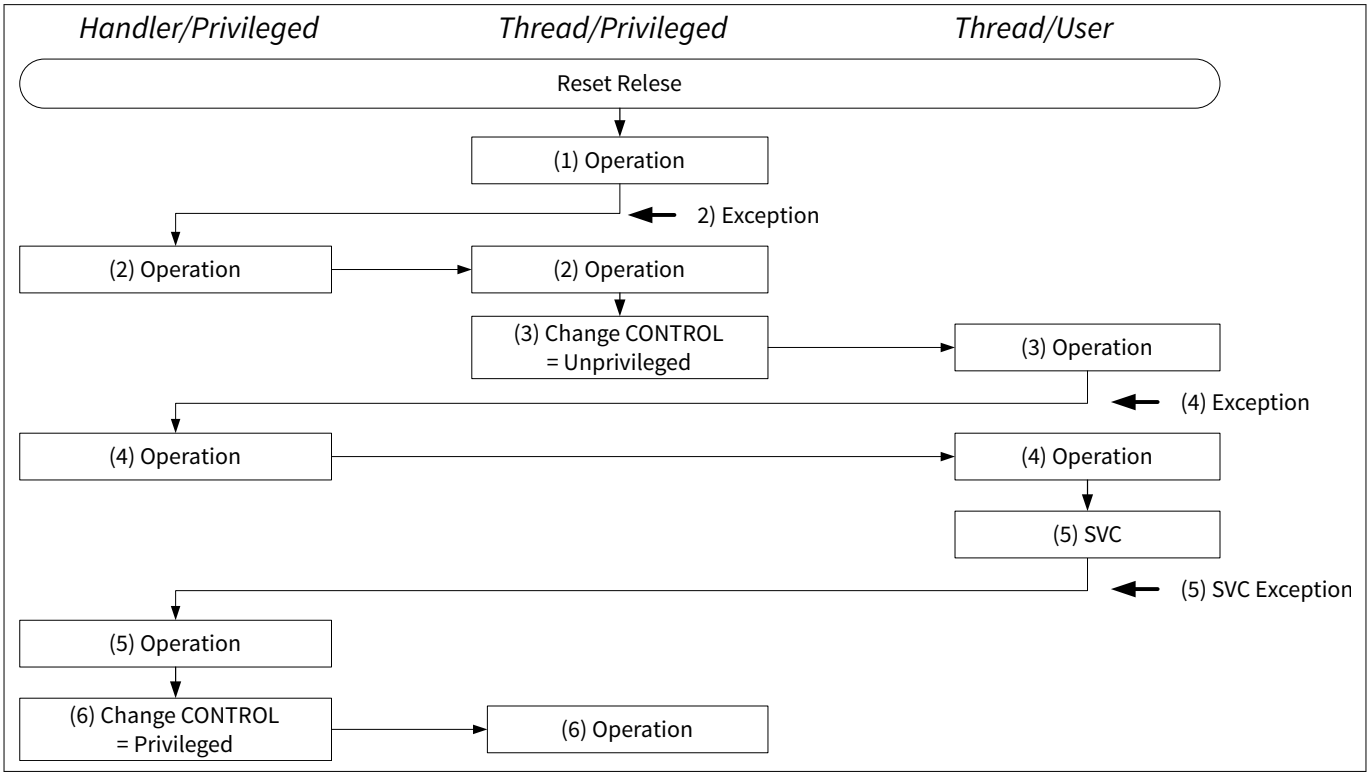

Figure 5 Example user/privileged level switching for both CPUs

1. CPUs are started in thread/privileged mode after reset release.
2. When an exception occurs in thread/privileged mode, the handler/privileged mode is entered, and upon return from handler processing, thread/privileged mode is entered again.
3. In the thread/privileged mode, transition to the thread/user mode is allowed by the CONTROL register.
4. When an exception occurs in the thread/user mode, the handler/privileged mode is entered, and upon return from handler processing, the thread/user mode is entered again.
5. When switching from the thread/user mode to thread/privileged mode, use SVC instruction to enter the handler/privileged mode. The SVC instruction can cause an SVC exception.
6. Set the privileged level with the CONTROL register in the handler/privileged level. The CPU transitions to the thread/privileged mode after returning from handler processing.

See the Arm® documentation sets for CM4, CM7, and CM0+ for more details.

You need to register the SVC handler in advance.

3.3.1 User/privileged attribute switching procedure

This section explains how to switch between privileged and user modes.

3.3.2 Configuration

Table 2 lists the functions in SDL for user/privileged attribute switching using SVC instruction.

Table 2 List of functions

Functions	Description	Remarks
`SetUserMode()`	Change privileged level to user	-
`SetPrivilegedMode()`	Change privileged level to privileged	-
`SVC_SetPrivilegedMode()`	Generates SVC interrupt and change privileged level to privileged.	-
`Cy_SysLib_SvcHandler(pSvcArgs)`	SVC handler pSvcArgs: SVC Index	Change to privileged if index is “2”

The following code shows an example of switching using SVC.

Code Listing 1 Example of user/privileged switching using SVC

```
int main(void)
{
    SystemInit();      /* CPUs are started in Thread/Privileged mode after reset release. */

    __enable_irq();    /* CPUs are started in Thread/Privileged mode after reset release. */


    :
    /* The CPU works in user mode from here */
    SetUserMode();   /* Change Privileged Mode to User Mode. See Code Listing 2. */


    :
    /* The CPU works in privileged mode from here */
    SVC_SetPrivilegedMode();   /* Change from User Mode to Privileged Mode. See Code Listing 3.
*/

    :

    /* The CPU works in user mode again from here */
    SetUserMode();   /* Change from Privileged Mode to User Mode. See Code Listing 2. */

    :

    for(;;);
}
```

Code Listing 2 SetUserMode() function

```
void SetUserMode(void)
{
    __ASM("MRS r0, CONTROL"); // Read CONTROL register into R0   /* Read CONTROL Register */
    __ASM("ORR r0, r0, #1");  // nPRIV -> 1   /* (3) Change to User Mode */
    __ASM("MSR CONTROL, r0"); // Write R0 into CONTROL register   /* Write back to CONTROL
Register */
}
```

Code Listing 3 SVC_SetPrivilegedMode() function

```
void SVC_SetPrivilegedMode(void)
{
    /* Set Index to “2” */
    /* (5) SVC Exception with Index 2. It calls the SVC handler. See Code Listing 4. */
    __ASM("SVC 0x02"); // SVC index = 2: Get privileged mode
}
```

Code Listing 4 SVC handler

```
void Cy_SysLib_SvcHandler(uint32_t* pSvcArgs)
{
    uint8_t svcIdx = ((char*)pSvcArgs[6])[-2];

    switch(svcIdx)
    {
    case 0:        /* SVC Processing for Index 0. */
        :
        break;
    case 1:        /* SVC Processing for Index 1. */
        :
        break;
    case 2:
        SetPrivilegedMode();        /* SVC Processing for Index 2. Change to Privileged Mode.
See Code Listing 5. */
        break;
    default:
        break;
    }
}
```

Code Listing 5 SetPrivilegedMode() function

```
void SetPrivilegedMode(void)
{
    __ASM("MRS r0, CONTROL"); // Read CONTROL register into R0    /* Read CONTROL Register */
    __ASM("BIC r0, r0, #1");  // nPRIV -> 0    /* (6) Change to Privileged Mode */
    __ASM("MSR CONTROL, r0"); // Write R0 into CONTROL register    /* Write back to CONTROL
Register */
}
```

3.4 Protection context attribute setting

Protection contexts (PCs) are used to isolate software execution for security and safety purposes. PCs are used as the PC attribute for all bus transfers that are initiated by the master. SMPUs and PPUs allow or restrict bus transfers based on the PC attribute.

The series supports eight PCs. Protection contexts 0 and 1 out of eight PCs are special; these are controlled by hardware. In addition, PC0 has unrestricted access.

Specific bus masters have associated PC fields (PROT_MPUx_MS_CTL.PC and PROT_SMPU_MSx_CTL.PC_MASK_15_TO_1 and PC_MASK_0).

A bus master protection context is changed by reprogramming the associated PROT_MPUx_MS_CTL.PC field. The PROT_SMPU_MSx_CTL.PC_MASK_15_TO_1 and PC_MASK_0 fields restrict the PCs that can be set for the associated bus master.

For example, if PROT_SMPU_MSx_CTL.PC_MASK_15_TO_1 and PC_MASK_0 = “0x06” (PC1, 2 = "1"), the PCs to which the associated bus master can be set are “PC = 1” and “PC = 2”. A bus master cannot be changed to a PC not allowed (PC = 0,3,4,5,6,7).

Figure 6 shows an example of changing the flow of PCs.

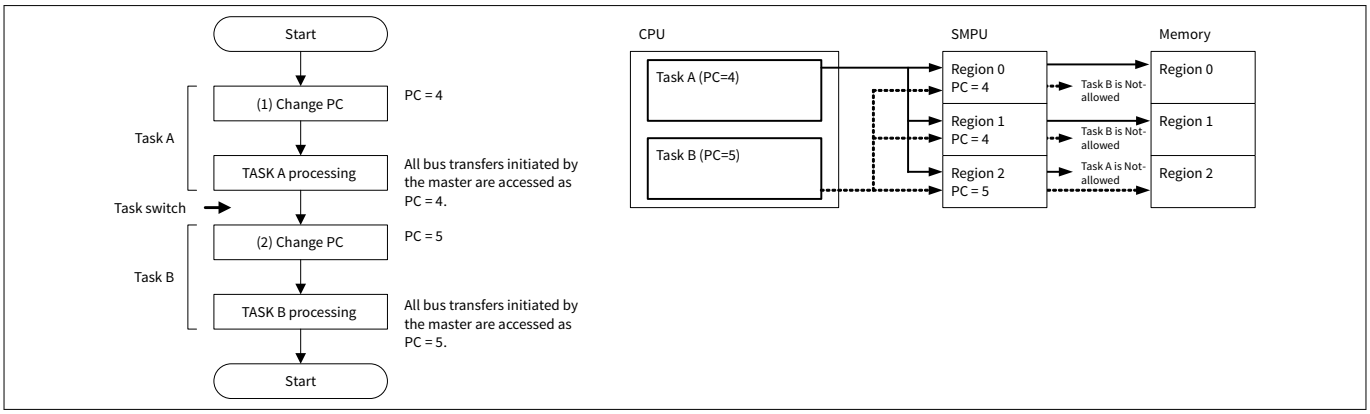

Figure 6 Change flow of PCs and behavior

***Note**: PC values that can be set by each master are restricted by PROT_SMPU_MSx_CTL.PC_MASK_15_TO_1 and PC_MASK_0.*

***Note**: If the access attributes, such as PC or secure, change when the CM7 cache memory is enabled, data that is not allowed access, such as the new PC or non-secure may be stored in the cache memory. In this case, you need to run the cache memory clean and invalidate before switching the attribute of protection context and secure. See AN224432 - Multi core handling guide in TRAVEO™ T2G [5] for cache memory handling.*

This allows a single bus master to take on different protection roles by reprogramming only the protection context field without changing the settings of SMPUs and PPUs.

3.4.1 Protection context attribute switching procedure

This section explains how to switch protection context shown in Figure 6.

- Region 0 and 1: PC = 4 access has permissions
- Region 2: PC = 5 access has permissions

3.4.2 Configuration

Table 3 and Table 4 list the parameters and functions in SDL for protection context switching.

Table 3 List of parameters

Parameters	Description	Value
RESERVED_MEMORY_BLOCK_SIZE	Define the memory size of each region	0x400
PROTECTION_CONTEXT_OF_TASK_A	Define protection context number for TASK A	4u
PROTECTION_CONTEXT_OF_TASK_B	Define protection context number for TASK B	5u
PC_MASK_OF_TASK_A	Define PROT_SMPU_MSx_CTL.PC_MASK value for enabling PC = 4.	-
PC_MASK_OF_TASK_B	Define PROT_SMPU_MSx_CTL.PC_MASK value for enabling PC = 5.	-
gReservedRam.taskA_Region0/1/2	Set start address and memory size of region 0/1/2	Memory size = RESERVED_MEMORY_BLOCK_SIZE
gSmpuStructConfigOfTask(A/B).address	Set SMPU region (Base address)	gReservedRam.taskA_Region0/1/2
gSmpuStructConfigOfTask(A/B).regionSize	Set SMPU region (Region size)	CY_PROT_SIZE_1KB (1 KB)
gSmpuStructConfigOfTask(A/B).subregions	Set SMPU region (Subregion setting)	0x00u (Not used)
gSmpuStructConfigOfTask(A/B).userPermission	Set SMPU region (User permission setting)	CY_PROT_PERM_RWX (= 0x07u) Full access for user
gSmpuStructConfigOfTask(A/B).privPermission	Set SMPU region (Privileged permission setting)	CY_PROT_PERM_RWX (= 0x07u) Full access for privileged
gSmpuStructConfigOfTask(A/B).secure	Set SMPU region (Non-secure setting)	False (Non-secure)
gSmpuStructConfigOfTask(A/B).pcMatch	Set SMPU region (PC match setting)	False (PC field participates in "matching")
gSmpuStructConfigOfTask(A/B).pcMask	Set SMPU region (PC_MASK setting)	Region0/1: PC_MASK_OF_TASK_A Region2: PC_MASK_OF_TASK_B
PROT_SMPU_SMPU_STRUCT0/1/2	Define the base address of PROT_SMPU_SMPU_STRUCT0/1/2 It depends on the product. See registers TRM.	-
CPUSS_MS_ID_CM4	Define bus master identifiers. It depends on the product. See Master identifier.	14

Table 4 List of functions

Functions	Description	Value
Cy_Prot_ConfigBusMaster(busMaster, privileged, secure, pcmask)	PROT_PROT_SMPU_MSx_CTL setting busMaster: Bus master identifiers privileged; P field setting secure: NS filed setting pcmask: PC_MASK field setting See registers TRM.	busMaster: CPUSS_MS_ID_CM4 privileged; true (User mode) secure: false (Non-secure) pcmask: PC_MASK field setting
Cy_Prot_ConfigSmpuSlaveStruct(*base, *config)	SMPU region setting *base: Register base address *config: Configuration parameter	*base: PROT_SMPU_SMPU_STRUCT0/1/2 *config: gSmpuStructConfigOfTask(A/B)
Cy_Prot_EnableSmpuSlaveStruct(*base)	SMPU region enable *base: Register base address	*base: PROT_SMPU_SMPU_STRUCT0/1/2
Cy_Prot_SetActivePC(busMaster, PC)	PROT_MPU_MSx_CTL setting busMaster: Bus master identifiers PC: PC value	busMaster: CPUSS_MS_ID_CM4 PC: PROTECTION_CONTEXT_OF_TASK_A or PROTECTION_CONTEXT_OF_TASK_B

The following description will help you understand the register notation of the driver part of SDL:

- addrMpu->un**MS_CTL**.u32Register is the PROT_MPUx_MS_CTL register mentioned in the registers TRM. Other registers are also described in the same manner. "**x**" signifies the bus master identifiers.
- Performance improvement measures
- For register setting performance improvement, the SDL writes complete 32-bit data to the register. Each bit field is generated in advance in a bit writable buffer and written to the register as the final 32-bit data.

```
tempSL_ATT0.u32Register = base->unSL_ATT0.u32Register;
tempSL_ATT0.stcField.u1PC1_UR = (config->userPermission & CY_PROT_PERM_R);
tempSL_ATT0.stcField.u1PC1_UW = (config->userPermission & CY_PROT_PERM_W) >> 1;
tempSL_ATT0.stcField.u1PC1_PR = (config->privPermission & CY_PROT_PERM_R);
tempSL_ATT0.stcField.u1PC1_PW = (config->privPermission & CY_PROT_PERM_W) >> 1;
tempSL_ATT0.stcField.u1PC1_NS = !(config->secure);
base->unSL_ATT0.u32Register = tempSL_ATT0.u32Register;
```

See `cyip_prot_v2.h` and `cyip_peri_ms_v2.h` under `hdr/rev_x/ip` for more information on the union and structure representation of registers.

Code Listing 6 shows an example of switching protection context.

Code Listing 6 Example of switching protection context

```
#define RESERVED_MEMORY_BLOCK_SIZE (0x400) // 1K   /*Define each region size */

#define PROTECTION_CONTEXT_OF_TASK_A (4u)   /* Define Protection context for Task A (PC=4) */
#define PROTECTION_CONTEXT_OF_TASK_B (5u)   /* Define Protection context for Task B (PC=5) */

#define PC_MASK_OF_TASK_A (1u<<(PROTECTION_CONTEXT_OF_TASK_A-1u))   /* Define PC_Mask for each
SMPU region. */
#define PC_MASK_OF_TASK_B (1u<<(PROTECTION_CONTEXT_OF_TASK_B-1u))   /* Define PC_Mask for each
SMPU region. */

struct
   /* Define SRAM region. */
{
    uint8_t taskA_Region0[RESERVED_MEMORY_BLOCK_SIZE];
    uint8_t taskA_Region1[RESERVED_MEMORY_BLOCK_SIZE];
    uint8_t taskB_Region2[RESERVED_MEMORY_BLOCK_SIZE];
} gReservedRam;

cy_stc_smpu_cfg_t gSmpuStructConfigOfTaskA =
   /* Configure SMPU for region 0 and 1. (PC=4 access has permissions) */
{
    .address        = NULL,              // Will be updated in run time
    .regionSize     = CY_PROT_SIZE_1KB,
    .subregions     = 0x00u,
    .userPermission = CY_PROT_PERM_RWX,
    .privPermission = CY_PROT_PERM_RWX,
    .secure         = false,             // Non secure
    .pcMatch        = false,
    .pcMask         = PC_MASK_OF_TASK_A, // only enable for task A
};





cy_stc_smpu_cfg_t gSmpuStructConfigOfTaskB =
   /* Configure SMPU for region 2. (PC=5 access has permissions) */
{
    .address        = NULL,              // Will be updated in run time
    .regionSize     = CY_PROT_SIZE_1KB,
    .subregions     = 0x00u,
    .userPermission = CY_PROT_PERM_RWX,
    .privPermission = CY_PROT_PERM_RWX,
    .secure         = false,             // Non secure
    .pcMatch        = false,
    .pcMask         = PC_MASK_OF_TASK_B, // only enable for task B      /*Enabled PC=5 by
PC_MASK */
};
```

```
int main(void)
{
    SystemInit();

    cy_en_prot_status_t status;

   /*Set PROT_SMPU_MS14_CTL.PC_MASK. See Configuration Example of SMPU for SMPU setting details.
(*) */
    /* Setting for MS14_CTL (for CM4) to allow the PC value to become 4 or 5 */
    status = Cy_Prot_ConfigBusMaster(CPUSS_MS_ID_CM4, true, false, (PC_MASK_OF_TASK_A|
PC_MASK_OF_TASK_B));
    CY_ASSERT(status == CY_PROT_SUCCESS);

    /* Setting for SMPU_STRUCT 0 */
    /* Setting SMPU_STRUCT 0 for task A */
   /*Enable SMPU region 0.  For details on setting SMPU, see Configuration Example of SMPU. */
    gSmpuStructConfigOfTaskA.address = (uint32_t*)gReservedRam.taskA_Region0;
   /*Enable SMPU region 0.  For details on setting SMPU, see Configuration Example of SMPU. */
    status = Cy_Prot_ConfigSmpuSlaveStruct(PROT_SMPU_SMPU_STRUCT0, &gSmpuStructConfigOfTaskA);
   /*Enable SMPU region 0.  For details on setting SMPU, see Configuration Example of SMPU. */
    CY_ASSERT(status == CY_PROT_SUCCESS);

    /* Enable SMPU_STRUCT 0 */
   / *Enable SMPU region 0.  For details on setting SMPU, see Configuration Example of SMPU. */
    status = Cy_Prot_EnableSmpuSlaveStruct(PROT_SMPU_SMPU_STRUCT0);

    CY_ASSERT(status == CY_PROT_SUCCESS);

    /* Setting for SMPU_STRUCT 1 */
    /* Setting SMPU_STRUCT 1 for task A */
   /*Enable SMPU region 1.  For details on setting SMPU, see Configuration Example of SMPU. */
    gSmpuStructConfigOfTaskA.address = (uint32_t*)gReservedRam.taskA_Region1;
   /*Enable SMPU region 1.  For details on setting SMPU, see Configuration Example of SMPU. */
    status = Cy_Prot_ConfigSmpuSlaveStruct(PROT_SMPU_SMPU_STRUCT1, &gSmpuStructConfigOfTaskA);
   /*Enable SMPU region 1.  For details on setting SMPU, see Configuration Example of SMPU. */
    CY_ASSERT(status == CY_PROT_SUCCESS);

    /* Enable SMPU_STRUCT 1 */
    /*Enable SMPU region 1.  For details on setting SMPU, see Configuration Example of SMPU. */
    status = Cy_Prot_EnableSmpuSlaveStruct(PROT_SMPU_SMPU_STRUCT1);
    CY_ASSERT(status == CY_PROT_SUCCESS);

    /* Setting for SMPU_STRUCT 2 */
    /* Setting SMPU_STRUCT 2 for task B */
   /*Set SMPU region 2. For details on setting SMPU, see Configuration Example of SMPU. */
    gSmpuStructConfigOfTaskB.address = (uint32_t*)gReservedRam.taskB_Region2;
   /*Set SMPU region 2. For details on setting SMPU, see Configuration Example of SMPU. */
    status = Cy_Prot_ConfigSmpuSlaveStruct(PROT_SMPU_SMPU_STRUCT2, &gSmpuStructConfigOfTaskB);
   /*Set SMPU region 2. For details on setting SMPU, see Configuration Example of SMPU. */
    CY_ASSERT(status == CY_PROT_SUCCESS);

    /* Enable SMPU_STRUCT 2 */
    /*Enable SMPU region 2. For details on setting SMPU, see Configuration Example of SMPU. */
```

```
    status = Cy_Prot_EnableSmpuSlaveStruct(PROT_SMPU_SMPU_STRUCT2);
    CY_ASSERT(status == CY_PROT_SUCCESS);
   for(;;)
    {
        /* Setting for MPU so that CM4 PC for task A   */
      /*(1) Change protection context to PC=4 for TASK A. See Code Listing 7. */
        status = Cy_Prot_SetActivePC(CPUSS_MS_ID_CM4, PROTECTION_CONTEXT_OF_TASK_A);
        CY_ASSERT(status == CY_PROT_SUCCESS);

        /* Do task A */
       /*Access to RAM region 0 and 1. See Code Listing 8 */
        Routine_TaskA();

        /* Setting for MPU so that CM4 PC for task B   */
    /*(2) Change protection context to PC=5 for TASK B. See Code Listing 7. */
        status = Cy_Prot_SetActivePC(CPUSS_MS_ID_CM4, PROTECTION_CONTEXT_OF_TASK_B);
        CY_ASSERT(status == CY_PROT_SUCCESS);

        /* Do task B */
       /*Access to RAM region 2. See Code Listing 8. */
        Routine_TaskB();
    }
}
```

Note: *(*) This process specifies the value of the protection context that can be set by the corresponding master. In a secure system, it is run by secure master. See* Protection properties of bus transfer *for more details.*

Code Listing 7 Cy_Prot_SetActivePC() function

```
cy_en_prot_status_t Cy_Prot_SetActivePC(en_prot_master_t busMaster, uint32_t pc)
{
    cy_en_prot_status_t status = CY_PROT_SUCCESS;
    un_PROT_MPU_MS_CTL_t tProtMpuMsCtl = {0ul};
    volatile stc_PROT_MPU_t* addrMpu = (stc_PROT_MPU_t*)(&PROT->CYMPU[busMaster]);

    if(pc > (uint32_t)CY_PROT_MS_PC_NR_MAX)   /* Define Protection context for Task A (PC=4) */
    {
        /* Invalid PC value - not supported in device */
        status = CY_PROT_BAD_PARAM;
    }
    else
    {
        tProtMpuMsCtl.stcField.u4PC = pc;    /* Change protection context. */
        addrMpu->unMS_CTL.u32Register = tProtMpuMsCtl.u32Register;
        status = ((addrMpu->unMS_CTL.stcField.u4PC != pc) ? CY_PROT_FAILURE : CY_PROT_SUCCESS);
    }

    return status;
}
```

Code Listing 8 Routine_TaskA() and Routine_TaskB() function

```
void Routine_TaskA(void)
    /* Access to region 0 and 1 with TASK A. If these regions are accessed with TASK B, it will
cause bus fault. */
{
    for(uint32_t i = 0; i < RESERVED_MEMORY_BLOCK_SIZE; i++)
    {
        gReservedRam.taskA_Region0[i] += 1;
    }

    for(uint32_t i = 0; i < RESERVED_MEMORY_BLOCK_SIZE; i++)
    {
        gReservedRam.taskA_Region1[i] += 1;
    }
}

void Routine_TaskB(void)
    /* Access to region 2 with TASK B. If these regions are accessed with TASK A, it will cause
bus fault. */
{
    for(uint32_t i = 0; i < RESERVED_MEMORY_BLOCK_SIZE; i++)
    {
        gReservedRam.taskB_Region2[i] += 1;
    }
}
```

3.5 Bus transfer evaluation

3.5.1 Evaluation process

The evaluation of bus transfer by protection units is divided into two independent processes.

- Matching process: For each protection structure, this process determines whether a transfer address is contained within the address range.
- Access evaluation process: For each protection structure, this process evaluates the bus transfer access attributes against the access control attributes.

The following pseudo code shows the evaluation process of bus transfer.

```
/* Matching Process */
match = 0;
for (i = n-1; i >= 0; i--)   // n: number of protection regions
   if (Match (“transfer address”, “protection context”) {
      match = 1; break;
   }

/* Access Evaluation Process */
if (match)
   AccessEvaluate (“access attributes”, “protection context”);
else
   “access allowed”
```

***Note**:* *If no protection structure provides a match, access is allowed.*

***Note**:* *If multiple protection structures provide a match, the access control attributes for access evaluation are provided by the protection structure with the highest index.*

A protection unit evaluates the protection structures in the decreasing order. In other words, higher-indexed structures take precedence over lower-indexed structures.

When transfer addresses do not match, the protection structure with the next highest index is evaluated. When transfer addresses match, bus transfer access attributes are evaluated by the access evaluation process. If transfer access attributes do not match with the access evaluation process, it is detected as an access violation. Therefore, the protection structure with the next highest index is not evaluated.

3.5.2 PC_MATCH operation

SMPU has a PC_MATCH field. PC_MATCH controls "matching" and "access evaluation" processes.

- Case of PC_MATCH = 0

The following pseudo code shows the evaluation process when PC_MATCH = 0.

```
match = 0;
for (i = n-1; i >= 0; i--)   // n: number of protection regions
   if (Match (“transfer address”) {
      match = 1; break;
   }

if (match)
   AccessEvaluate (“access attributes”, “protection context”);
else
   “access allowed”
```

When PC_MATCH = “0”, protection context is evaluated only in the access evaluation process.

Figure 7 shows the operation example when PC_MATCH of Region5 is ‘0’ and PC_MATCH of Region4 is ‘0’. Table 5 shows the settings for each region.

Table 5 Region setting1 for PC_MATCH operation

Region	PC_MATCH	Region address	Protection context	User
Region4	0	AA	4	Read/Write
Region5	0	AA	5	Read only

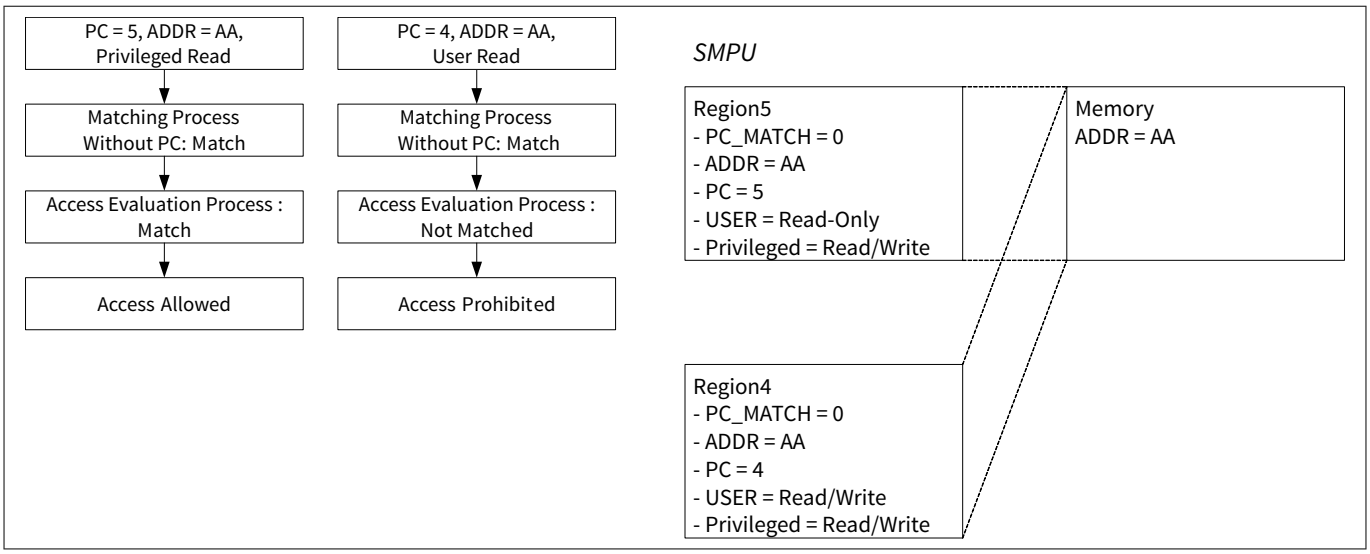

Figure 7 PC_MATCH operation example 1

In this case, the protection context is not evaluated by the matching process. Therefore, both PC = 4 access and PC = 5 access is "match" in the matching process. The protection context is evaluated by the access evaluation process. For PC = 5, access is allowed; for PC = 4, access is not allowed. As a result, PC = 4 access cannot access this address because PC = 4 access is prohibited by Region5 with a higher priority than Region4.

- Case of PC_MATCH = 1

The following pseudo code shows the evaluation process when PC_MATCH = 1.

```
match = 0;
for (i = n-1; i >= 0; i--)   // n: number of protection regions
   if (Match (“transfer address”, “protection context”) {
      match = 1; break;
   }

if (match)
   AccessEvaluate (“access attributes”, “protection context”);
else
   “access allowed”
```

When PC_MATCH = "1", the protection context is evaluated not only by the access evaluation process, but also by the matching process.

Figure 8 shows the operation example when PC_MATCH of Region5 is ’1’ and PC_MATCH of Region4 is ‘0’. Table 6 shows the settings for each region.

Table 6 Region setting2 for PC_MATCH operation

Region	PC_MATCH	Region address	Protection context	User
Region4	0	AA	4	Read/Write
Region5	1	AA	5	Read only

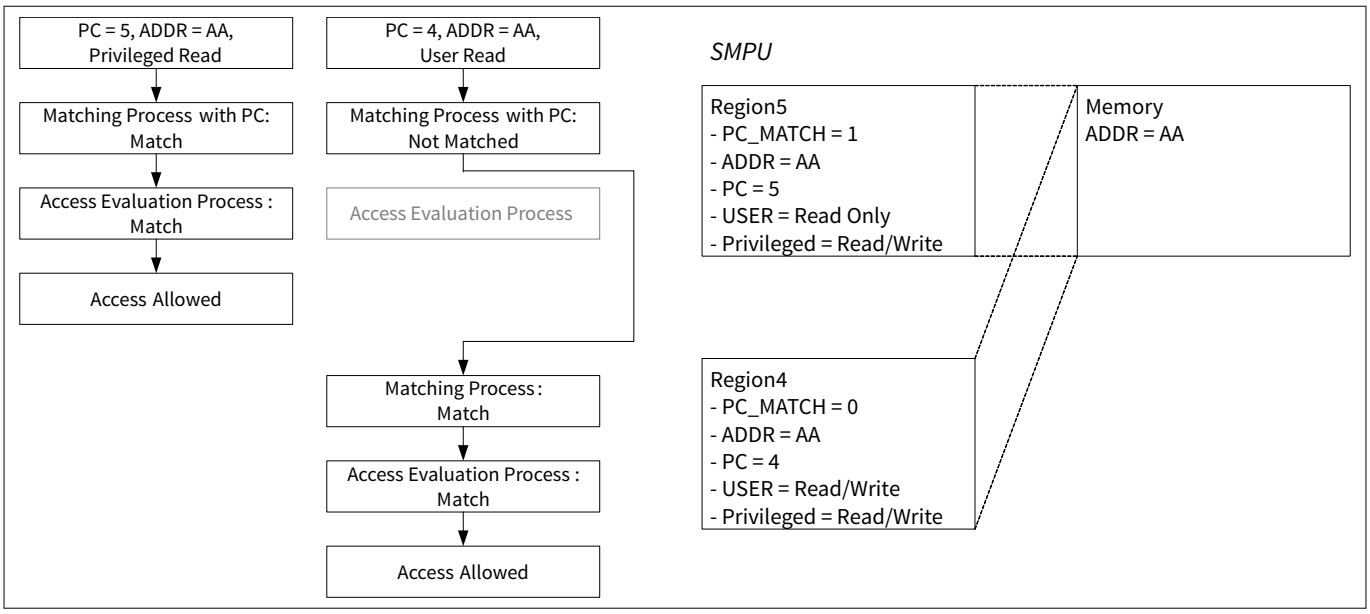

Figure 8 PC_MATCH operation example 2

In this case, the protection context is also evaluated by the matching process. PC = 5 access is "match" in the matching process, and is evaluated by the access evaluation process. However, PC = 4 access is "Not matched", and is evaluated by the matching process with Region4 of the next highest priority. It is evaluated by the access evaluation process after the matching process, and access is allowed.

It is possible to assign different attributes to the same address area depending on the protection context by using PC_MATCH.

***Note**: PC_MATCH is provided only for the SMPU. This functionality is not supported because a PPU structure provides access attributes for all protection contexts.*

***Note**: When the region address has only one attribute, use PC_MATCH with "0".*

3.6 Master identifier

Each bus master has a dedicated master identifier. This identifier is used for correspondence with the register suffix in protection units and identification of access violation master by protection units. Table 7 lists the master identifiers. See the related datasheet for bus master identifier using products.

Table 7 Master identifiers

Master identifier	Bus master		
	CYT2B7 series	**CYT2B7 series**	**CYT4DN series**
0	CM0+ CPU	CM0+ CPU	CM0+ CPU
1	CRYPTO component	CRYPTO component	CRYPTO component

(table continues...)

Table 7 (continued) Master identifiers

Master identifier	Bus master		
	CYT2B7 series	CYT2B7 series	CYT4DN series
2	P-DMA 0	P-DMA 0	P-DMA 0
3	P-DMA 1	P-DMA 1	P-DMA 1
4	M-DMA	M-DMA	M-DMA
5	-	SDHC	-
9	-	Ethernet 0	Ethernet 0
10	-	Ethernet 1	-
12	-	-	Video subsystem
13	-	CM7_1 CPU	CM7_1 CPU
14	CM4 CPU	CM7_0 CPU	CM7_0 CPU
15	Test controller	Test controller	Test controller

3.7 Protection violation

If the MPU that is implemented as part of the CPU detected access violations, invoke the programmable-priority MemManage fault or HardFault handler. If an MPU fault occurs on an access that is not in the TCM, the AXI or AHB transactions for that access are not performed. See the Arm® documentation sets for CM4, CM7, and CM0+ for more MPU details.

If the MPU that is implemented as part of the bus infrastructure and SMPU detects a bus transfer that causes a violation of the protection status, the bus transfer results in a bus error.

In case of write transfers that violate PPU protection, the bus master will not see the bus error when buffering is enabled (CPUSS_BUFF_CTL.WRITE_BUFF = 1). This is because AHB-Lite bridges in the bus infrastructure will buffer the write transfer and send the OK response to masters. In this case, the system must depend on the fault reported by the PPU. Write transfers that violate the PPU cause a bus error if buffering is disabled (CPUSS_BUFF_CTL.WRITE_BUFF = 0). Read transfers that violate PPU protection always result in a bus error.

The bus transfers that violate protection units do not reach their target memory location or peripheral register.

Protection violation detected by the MPU that is implemented as part of the bus infrastructure, SMPU, and PPU is captured in the fault report structure. The fault report structure can generate an interrupt to indicate the occurrence of a fault. In addition, information on the violating bus transfer is communicated to the fault report structure.

The fault reporting structure captures the following information:

- Violating address
- Violating attribute
  - User read/user write/user execute
  - Privileged read/privileged write/privileged execute
  - Non-secure
  - Protection context identifier
- Violating master identifier
- Protection units that detected the violation or fault type[1)]

[1] Depends on the detected fault. See the registers TRM.

4 Protection units structure

4.1 MPU structure

Figure 9 shows the MPU structure that is implemented as part of the bus infrastructure. See the Arm® documentation sets for CM4, CM7, and CM0+ for details of the MPU that is implemented as part of CM4, CM7, and CM0+.

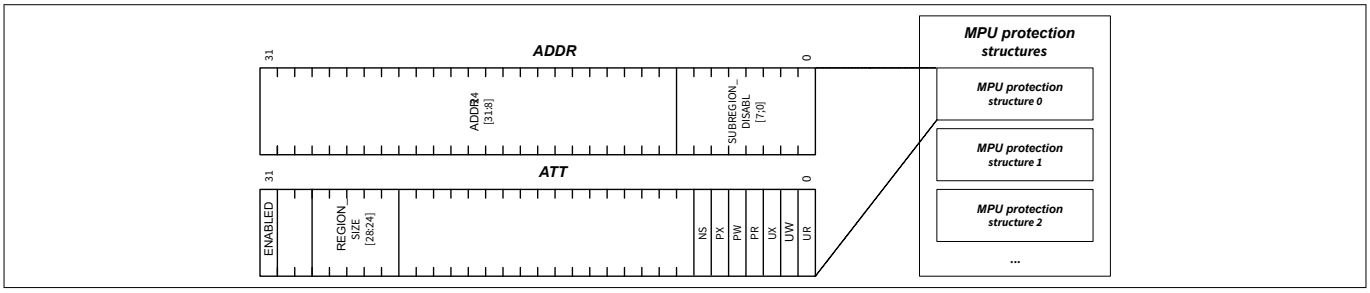

Figure 9 MPU structure

The MPU protection structure sets the property to be allowed and restricted by master access. An MPU protection identifies the following properties:

- Address range
  - ADDR.ADDR24 [31:8]: Specifies the base address of the region
  - ATT.REGION_SIZE [28:24]: Specifies the size of a region. The region size is in the range of [256 B, 4 GB]
  - ADDR.SUBREGION_DISABLE [7:0]: Individual disable settings for eight subregions within the region
- Access attribute
  - ATT.UR: Control for user read access
  - ATT.UW: Control for user write access
  - ATT.UX: Control for user execute access
  - ATT.PR: Control for privileged read access
  - ATT.PW: Control for privileged write access
  - ATT.PX: Control for privileged execute access
  - ATT.NS: Control for secure access
- Region enable
  - ATT.ENABLED: Region enable

The MPU does not provide a protection context. The definition of this MPU type follows the Arm® MPU definition (in terms of memory region and access attribute definition) to ensure a consistent software interface.

A region can be partitioned into eight equally sized subregions; it is possible to specify individual enables for the subregions within a region with the ADDR.SUBREGION_DISABLE field.

For example, when SUBREGION_DISABLE is 0x82 (bit fields 1 and 7 are '1') in the divided subregion [0: 7], subregion1, 7 are disabled, subregion 0, 2, 3, 4, 5, and 6 are enabled. Table 8 shows the areas of the eight subregions and the enable/disable states if the start address is 0x10005400, and the region ranges from 0x10005400 to 0x100055ff (512 bytes).

Table 8 Each subregion area and state

Subregion	Area	State
Subregion 0	0x10005400 to 0x1000543f	Enable

(table continues...)

Table 8 (continued) Each subregion area and state

Subregion	Area	State
Subregion 1	0x10005440 to 0x1000547f	Disable
Subregion 2	0x10005480 to 0x100054bf	Enable
Subregion 3	0x100054c0 to 0x100054ff	Enable
Subregion 4	0x10005500 to 0x1000553f	Enable
Subregion 5	0x10005540 to 0x1000557f	Enable
Subregion 6	0x10005580 to 0x100055bf	Enable
Subregion 7	0x100055c0 to 0x100055ff	Disable

4.2 SMPU structure

Figure 10 shows the SMPU structure.

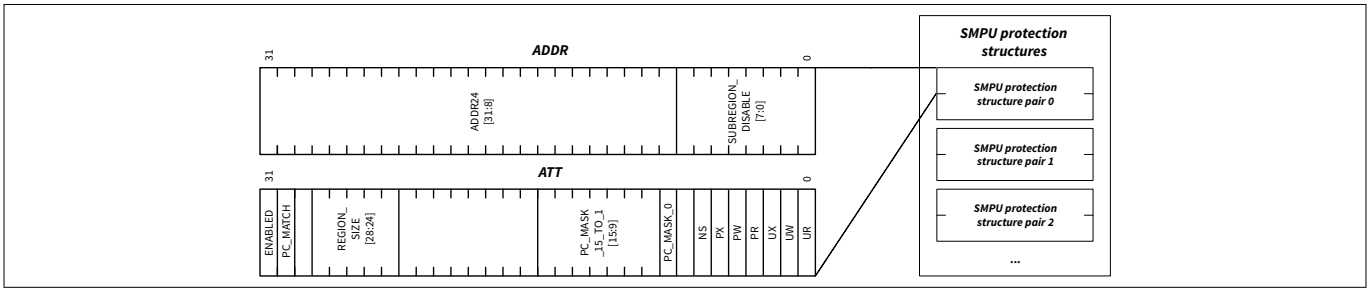

Figure 10 SMPU structure

The SMPU protection structure sets the property to be allowed and restricted by master access. SMPU protection identifies the following properties:

- Address range
  - ADDR.ADDR24 [31:8]: Specifies the base address of a region
  - ATT.REGION_SIZE [28:24]: Specifies the size of a region. The region size is in the range of [256 B, 4 GB].
  - ADDR.SUBREGION_DISABLE [7:0]: Individual disables for eight subregions within the region
- Access attribute
  - ATT.UR: Control for user read access
  - ATT.UW: Control for user write access
  - ATT.UX: Control for user execute access
  - ATT.PR: Control for privileged read access
  - ATT.PW: Control for privileged write access
  - ATT.PX: Control for privileged execute access
  - ATT.NS: Control for secure access
  - ATT.PC_MASK_15_TO_1 and PC_MASK_0: Control for individual protection contexts
  - The PC_MASK_0 field is always ‘1’. In other words, PC=0 is always allowed.
  - ATT.PC_MATCH: Specifies whether the PC field participates in the "matching" process or the "access evaluation" process. See PC_MATCH operation for more details.
- Region enable
  - ATT.ENABLED: Region enable

The SUBREGION function of SMPU is the same as that of MPU.

4.3 PPU structure

Figure 11 shows the PPU structure.

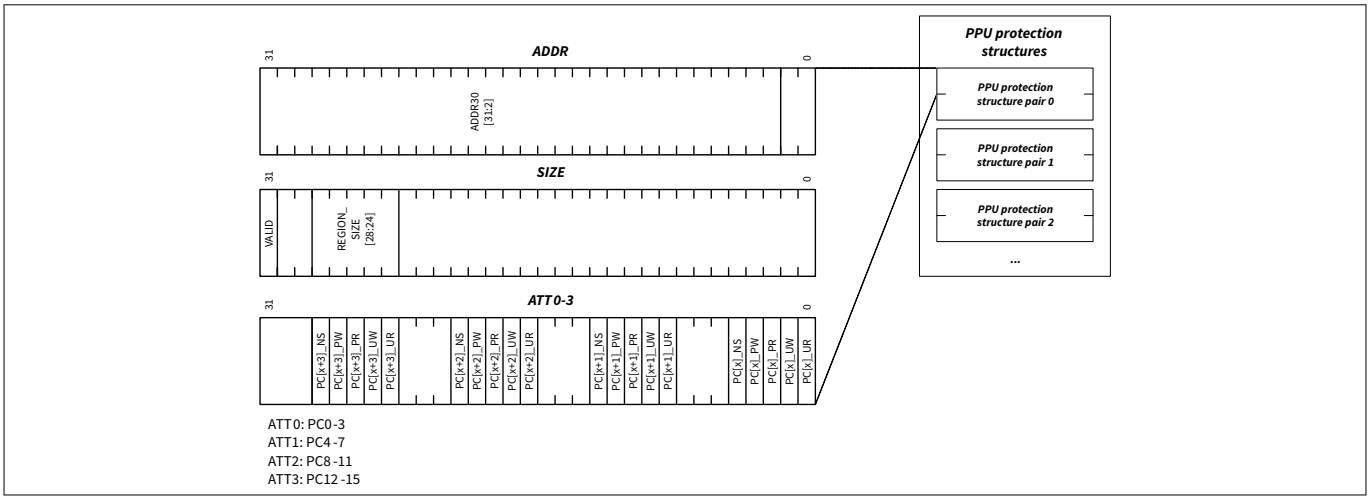

Figure 11 PPU structure

The PPU protection structure sets the property to be allowed and restricted by master access. The PPU can have independent attribute settings for all protection context attributes. PPU protection identifies the following properties:

- Address range
  - ADDR.ADDR30 [31:2]: Specifies the base address of a region
  - SIZE.REGION_SIZE [28:24]: Specifies the size of a region. The region size is in the range of [4 B, 2 GB].

In the fixed PPU structure, it has a fixed, constant address region.

- Access attribute
  - ATT.PCx_UR: Control for PCx user read access
  - ATT.PCx_UW: Control for PCx user write access
  - ATT.PCx_PR: Control for PCx privileged read access
  - ATT.PCx_PW: Control for PCx privileged write access
  - ATT.PCx_NS: Control for PCx secure access
- Region enable
  - SIZE.VALID: Region enable

***Note**: In the series, the protection context is supported from 0 to 7. Therefore, only ATT0,1 are present.*

4.4 Protection pair structure

Registers of protection units are the same registers as other peripherals. Furthermore, registers of protection structure can be included in the address range of another protection structure as with peripherals. Therefore, protection structure can be protected by the protection structure.

The protection structure that protects the protection structure is called the master structure, and the protection structure to be protected by master is called the slave structure. The slave structure protects peripherals.

The protection structure of a slave and master is referred to as a protection pair. SMPUs and PPUs have protection pairs. Figure 12 shows the protection pair structure.

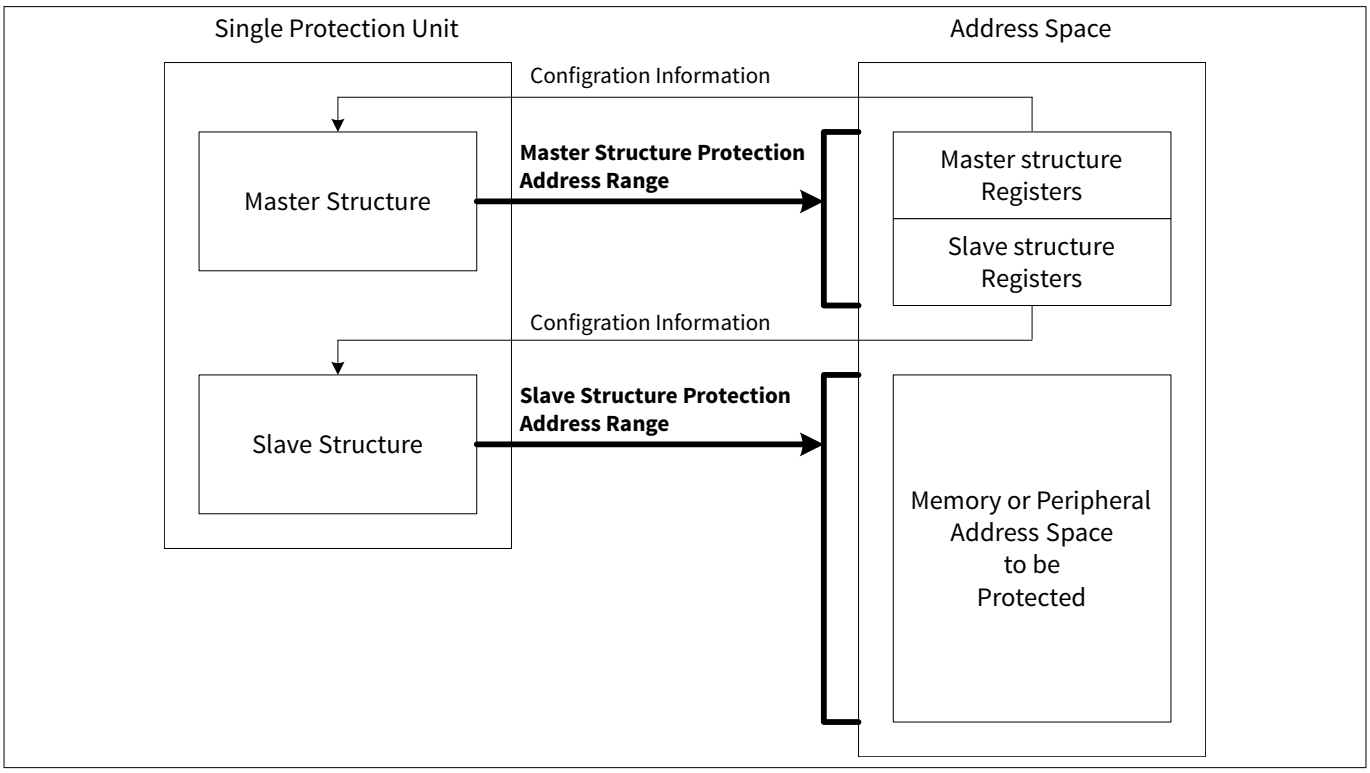

Figure 12 Protection pair structure

The master structure that protects the slave protection structure has the following features:

- Address range
  - ADDR.ADDR: Read-only; it has a fixed, constant address region.
  - ATT.REGION_SIZE: Read-only; it has a fixed, constant address region.
  - ADDR.SUBREGION_DISABLE: Read-only; it has a fixed, constant address region.
- Access attribute
  - ATT.UR: Fixed to ‘1’; User read accesses are always allowed
  - ATT.UW: Control for user write access
  - ATT.UX: Fixed to ‘0’; User execute accesses are never allowed
  - ATT.PR: Fixed to ‘1’; Privileged read accesses are always allowed
  - ATT.PW: Control for privileged write access
  - ATT.PX: Fixed to ‘0’; Privileged execute accesses are never allowed.
  - ATT.NS: Control for secure access

The above is an example of the SMPU master structure.

In master structure, protected region is fixed; read access is always allowed, and execution access is not allowed. SMPUs can be enabled or disabled, but PPUs cannot disabled.

5 Configuration example of protection units

An example of using the protection units is explained according to the following usage assumptions.

***Note**: The addresses and peripheral channel numbers shown in this section are those of the CYT2B series. See the technical reference manual for the actual addresses and peripheral channel numbers.*

5.1 Configuration example of MPU implemented as part of CPU

This section explains how to protect the area used by the operating system (OS) from tasks accesses, and shows an example of the configuration of the MPU.

5.1.1 Use case

This section provides configuration examples for MPU. An MPU distinguishes between user/privileged, read/write, and execute accesses. Table 9 shows the access restriction for the MPU.

Table 9 Example access restriction for MPU implemented as part of the CPU

Region	Attribute
Region 0 (Background address) Base address: 0x00000000 Size: 4 GB	Privileged: Read/write User: Read/write Execution is permitted
Region 1 (Code Flash) Base address: 0x10000000 Size: 8 MB	Privileged: Read only User: Read only Execution is permitted
Region 2 (Work Flash) Base address: 0x14000000 Size: 256 KB	Privileged: Read only User: No access Execution is not permitted
Region 3 (SRAM) Base address: 0x08000000 Size: 1 MB	Privileged: Read/write User: Read/write Execution is permitted
Region 4 (Peripheral registers) Base address: 0x40000000 Size: 64 MB	Privileged: Read/write User: Read/write Execution is not permitted
Region 5 (System registers for ARM) Base address: 0xE0000000 Size: 512 MB	Privileged: Read/write User: Read/write Execution is not permitted
Other regions (Unused)	-

Region 0 is used as the background region. If no attributes are specified by another region, the background region will be applied.

Note that when the MPU implemented as part of the CPU is enabled, access to unconfigured areas will cause access violations. To prevent unintended access violations, this type of MPU supports overlapping. Therefore, higher region number has the highest priority, while the lowest region number (Region 0) has the lowest priority. Attributes of a region that overlaps Region0 have higher priority than attributes of Region0. That is, Region0 can be used as a background region (determination of the attributes of all area).

See the Arm® documentation sets for CM4, CM7, and CM0+ for more MPU details.

Region 1 is read-only for both privileged and user access. Execution is allowed, but data cannot be written. Region 2 is read-only for privileged only. You cannot access it. Data cannot be written by both privileged and user access, and execution is not allowed. Region 3 can be accessed from either privileged or user, and execution is allowed. Region 4 and 5 can be accessed from either privileged or user, and execution is not allowed.

5.1.2 Setting procedure

This type of MPU is set by CPU-specific registers. The MPU must be disabled when it is set, and it is necessary to set the MPU in the privileged level. Figure 13 shows an example of how to set an MPU.

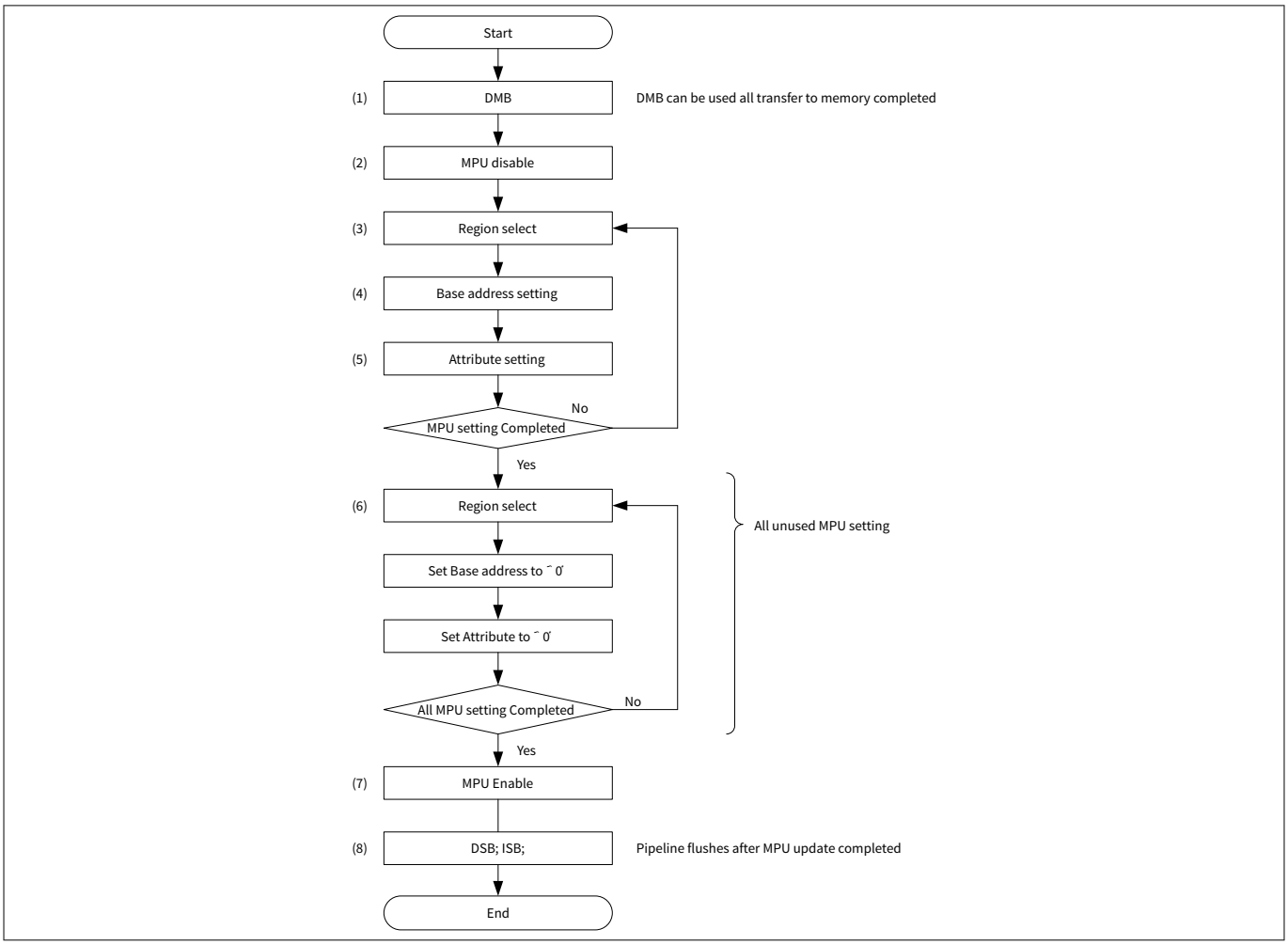

Figure 13 Setting procedure example of MPU implemented as part of the CPU

The MPU must be disabled when setting it. First, specify the region to be set with the MPU_RNR register. After setting MPU_RNR, set the base address, region size, and access attribute with the MPU_RBAR and MPU_RASR registers. Repeat this for each region. Also, MPU_RBAR and MPU_RASR registers of unused regions are set to '0'. Finally, the MPU is enabled.

It is also possible to specify the region number to set the MPU directly with the MPU_RBAR register. MPU_RASR also be used to set the subregion and memory attributes such as normal memory, strongly-ordered, and device.

See the Arm® documentation sets for CM4, CM7, and CM0+ for more details.

5.1.3 Configuration

Table 10 and Table 11 list the parameters and functions of the configuration part in SDL for MPU configuration.

Table 10 List of parameters

Parameters	Description	Value
CY_MPU_MAX_NUM	Defines the number of supported MPU data regions. Value of MPU_TYPE.DREGION	-
MPU_RBAR_ADDR_Msk	Define base address mask	(0x7FFFFFFUL << MPU_RBAR_ADDR_Pos) MPU_RASR_SRD_Pos = 5u
MPU_RASR_SRD_Pos	Defines subregion disable (SRD) field position in MPU_RASR	8ul
MPU_CTRL_ENABLE_Msk	Defines MPU enable bit mask	1ul
CY_MPU_DISABLE_USE_DEFAULT_MAP	Enables privileged software access to the default memory map in MPU_CTRL	0ul
CY_MPU_DISABLED_DURING_FAULT_NMI	Enables the operation of MPU during hard fault, NMI, and FAULTMASK handlers in MPU_CTRL	0ul
BACKGROUND_REGION_ADDR	Defines background base address	0x00000000ul
CODE_FLASH_REGION_ADDR	Defines code flash base address	0x10000000ul
WORK_FLASH_REGION_ADDR	Defines work flash base address	0x14000000ul
SRAM_REGION_ADDR	Defines SRAM base address	0x08000000ul
PERI_REGISTER_REGION_ADDR	Defines peripheral registers base address	0x40000000ul
ARM_SYS_REGISTER_REGION_ADDR	Defines ARM system registers base address	0xE0000000ul
BACKGROUND_MPU_NO	Defines region number of background	0ul
CODE_FLASH_MPU_NO	Defines region number of code flash	1ul
WORK_FLASH_MPU_NO	Defines region number of Work flash	2ul
SRAM_MPU_NO	Defines region number of SRAM	3ul
PERI_REGISTER_MPU_NO	Defines region number of peripheral registers	4ul
ARM_SYS_REGISTER_MPU_NO	Defines region number of ARM system registers	5ul
g_mpuCfg.addr	Sets base address	-
g_mpuCfg.size	Sets region size	-

(table continues...)

Table 10 (continued) List of parameters

Parameters	Description	Value
g_mpuCfg.permission	Sets region access permission CY_MPU_ACCESS_P_FULL_ACCESS: Privileged: Read/write, User: Read/write CY_MPU_ACCESS_P_PRIV_RO: Privileged: Read only, User: No access CY_MPU_ACCESS_P_RO: Privileged: Read only, User: Read only	-
g_mpuCfg.attribute	Sets region memory access attributes. CY_MPU_ATTR_NORM_MEM_WT: Normal, not shareable, outer and inner write-through. no write allocate. CY_MPU_ATTR_SHR_DEV: Device, shareable. CY_MPU_ATTR_STR_ORD_DEV: Strongly-ordered, shareable.	-
g_mpuCfg.execute	Sets region instruction access disable CY_MPU_INST_ACCESS_EN: Instruction fetches enabled CY_MPU_INST_ACCESS_DIS: Instruction fetches disabled	-
g_mpuCfg.srd	Sets subregion disable	-
g_mpuCfg.enable	Sets region enable CY_MPU_ENABLE: Region enable. CY_MPU_DISABLE: Region disable	-

Table 11 List of functions

Functions	Description	Remarks
`Cy_MPU_Setup (cfg[], cfgSize, privDefMapEn, faultNmiEn)`	Configures MPU cfg[]: MPU config parameters address cfgSize: cpnfiguration parameter size privDefMapEn: Enables privileged software access to the default memory map faultNmiEn: Enables the operation of MPU during hard fault, NMI, and FAULTMASK handlers.	-

The following code shows an example of MPU configuration.

Code Listing 9 Example of MPU configuration

```
#define MPU_TYPE_DREGION_Pos  8UL                              /*!< MPU TYPE: DREGION Position
*/
#define MPU_TYPE_DREGION_Msk  (0xFFUL << MPU_TYPE_DREGION_Pos)  /*!< MPU TYPE: DREGION Mask */
#define CY_MPU_MAX_NUM        ((MPU->TYPE & MPU_TYPE_DREGION_Msk) >> MPU_TYPE_DREGION_Pos)

#define MPU_RBAR_ADDR_Pos     5UL                              /*!< MPU RBAR: ADDR Position */
#define MPU_RBAR_ADDR_Msk     (0x7FFFFFFUL << MPU_RBAR_ADDR_Pos)/*!< MPU RBAR: ADDR Mask */

#define MPU_RASR_SRD_Pos      8UL   /*!< MPU RASR: Sub-Region Disable Position */
#define MPU_CTRL_ENABLE_Msk   (1UL  /*<< MPU_CTRL_ENABLE_Pos*/)  /*!< MPU CTRL: ENABLE Mask */

#define MPU_CFG_ARRAY_SIZE(array) (sizeof(array)/sizeof(cy_stc_mpu_region_cfg_t))

/** Specifies enable/disable privileged software access to the default memory map */
typedef enum
{
    CY_MPU_DISABLE_USE_DEFAULT_MAP = (0ul), /**< If the MPU is enabled, disables use of the
default memory map. Any memory access to a location not covered by any enabled region causes a
fault.  */
:
} cy_en_mpu_privdefena_t;

/** Specifies enable/disable the operation of MPU during hard fault, NMI, and FAULTMASK
handlers. */
typedef enum
{
    CY_MPU_DISABLED_DURING_FAULT_NMI = (0ul),  /**< MPU is disabled during hard fault, NMI, and
FAULTMASK handlers, regardless of the value of the ENABLE bit.  */
:
} cy_en_mpu_hfnmiena_t;

/*  Define each region base address  */
#define BACKGROUND_REGION_ADDR       (0x00000000ul) // Back Ground Region Start Address
#define CODE_FLASH_REGION_ADDR       (0x10000000ul) // Code Flash Region Start Address
#define WORK_FLASH_REGION_ADDR       (0x14000000ul) // Work Flash Region Start Address
#define SRAM_REGION_ADDR             (0x08000000ul) // System RAM Region Start Address
#define PERI_REGISTER_REGION_ADDR    (0x40000000ul) // Peripheral Register Region Start Address
#define ARM_SYS_REGISTER_REGION_ADDR (0xE0000000ul) // ARM System Registers Region Start Address

/*  Define each region number  */
#define BACKGROUND_MPU_NO       (0)
#define CODE_FLASH_MPU_NO       (1)
#define WORK_FLASH_MPU_NO       (2)
#define SRAM_MPU_NO             (3)
#define PERI_REGISTER_MPU_NO    (4)
#define ARM_SYS_REGISTER_MPU_NO (5)

cy_stc_mpu_region_cfg_t g_mpuCfg[] =
{
    /*  Region 0 configuration */
    /*** Back Ground Region ***/
```

```
    {
        .addr       = BACKGROUND_REGION_ADDR,
        .size       = CY_MPU_SIZE_4GB,
        .permission = CY_MPU_ACCESS_P_FULL_ACCESS,
        .attribute  = CY_MPU_ATTR_NORM_MEM_WT,
        .execute    = CY_MPU_INST_ACCESS_EN,
        .srd        = 0x00u,
        .enable     = CY_MPU_ENABLE
    },

    /*  Region 1 configuration  */
    /*** Code Flash Region ***/
    {
        .addr       = CODE_FLASH_REGION_ADDR,
        .size       = CY_MPU_SIZE_8MB,
        .permission = CY_MPU_ACCESS_P_RO,
        .attribute  = CY_MPU_ATTR_NORM_MEM_WT,
        .execute    = CY_MPU_INST_ACCESS_EN,
        .srd        = 0x00u,
        .enable     = CY_MPU_ENABLE
    },

    /*  Region 2 configuration  */
    /*** Work Flash Region ***/
    {
        .addr       = WORK_FLASH_REGION_ADDR,
        .size       = CY_MPU_SIZE_256KB,
        .permission = CY_MPU_ACCESS_P_PRIV_RO,
        .attribute  = CY_MPU_ATTR_NORM_MEM_WT,
        .execute    = CY_MPU_INST_ACCESS_DIS,
        .srd        = 0x00u,
        .enable     = CY_MPU_ENABLE
    },

    /*  Region 3 configuration  */
    /*** System RAM Region ***/
    {
        .addr       = SRAM_REGION_ADDR,
        .size       = CY_MPU_SIZE_1MB,
        .permission = CY_MPU_ACCESS_P_FULL_ACCESS,
        .attribute  = CY_MPU_ATTR_NORM_MEM_WT,
        .execute    = CY_MPU_INST_ACCESS_EN,
        .srd        = 0x00u,
        .enable     = CY_MPU_ENABLE
    },

    /*  Region 4 configuration  */
    /*** Peripheral Register Region ***/
    {
        .addr       = PERI_REGISTER_REGION_ADDR,
        .size       = CY_MPU_SIZE_64MB,
        .permission = CY_MPU_ACCESS_P_FULL_ACCESS,
        .attribute  = CY_MPU_ATTR_SHR_DEV,
```

```
        .execute    = CY_MPU_INST_ACCESS_DIS,
        .srd        = 0x00u,
        .enable     = CY_MPU_ENABLE
    },

    /*  Region 5 configuration  */
    /*** ARM System Registers Region ***/
    {
        .addr       = ARM_SYS_REGISTER_REGION_ADDR,
        .size       = CY_MPU_SIZE_512MB,
        .permission = CY_MPU_ACCESS_P_FULL_ACCESS,
        .attribute  = CY_MPU_ATTR_STR_ORD_DEV,
        .execute    = CY_MPU_INST_ACCESS_DIS,
        .srd        = 0x00u,
        .enable     = CY_MPU_ENABLE
    },
};

int main(void)
{
    SystemInit();

    __enable_irq();

    /********* Core MPU setting **************/
    /*  Configure MPU See Code Listing 10  */
    CY_ASSERT(Cy_MPU_Setup(g_mpuCfg, MPU_CFG_ARRAY_SIZE(g_mpuCfg),
CY_MPU_DISABLE_USE_DEFAULT_MAP, CY_MPU_DISABLED_DURING_FAULT_NMI) == CY_MPU_SUCCESS);
:
    for(;;);
}
```

Code Listing 10 Cy_MPU_Setup () function

```
cy_en_mpu_status_t Cy_MPU_Setup(const cy_stc_mpu_region_cfg_t cfg[], uint8_t cfgSize,
cy_en_mpu_privdefena_t privDefMapEn, cy_en_mpu_hfnmiena_t faultNmiEn)
{
:
    // Ensure all memory accesses are completed before new memory access is committed
    __DMB();   /*  (1) Run Data memory barrier instruction  */

    // Disable the MPU
    MPU->CTRL = 0ul;   /*  (2) Disable MPU  */

    uint32_t i_mpuRegionNo;
    for(i_mpuRegionNo = 0ul; i_mpuRegionNo < CY_MPU_MAX_NUM; i_mpuRegionNo++)
    {
        // Select which MPU region to configure
        MPU->RNR = i_mpuRegionNo;   /*  (3) Select Region by MPU_RNR register  */

        if(i_mpuRegionNo < cfgSize)
        {
            // Configure  region  base  address register
            // VALID and REGION field of RBAR register will be 0 since this function sets RNR
register manually.
            MPU->RBAR = (cfg[i_mpuRegionNo].addr & MPU_RBAR_ADDR_Msk);   /*  (4) Set base
address of this region  */

            uint32_t srd;
            if(cfg[i_mpuRegionNo].size < CY_MPU_SIZE_256B)
            {
                srd = 0ul;
            }
            else
            {
                srd = (cfg[i_mpuRegionNo].srd << MPU_RASR_SRD_Pos);
            }

            // Configure region attribute and size register
                     /*  (5) Set access attribute of this region  */
            MPU->RASR = ((uint32_t)cfg[i_mpuRegionNo].size       |
                         (uint32_t)cfg[i_mpuRegionNo].permission |
                         (uint32_t)cfg[i_mpuRegionNo].attribute  |
                         srd                                     |
                         (uint32_t)cfg[i_mpuRegionNo].enable);
        }
   /*  (6) Unused MPU setting  */
        else // Disables unused regions
        {
            // Configure region base address register
            MPU->RBAR = 0ul;

            // Configure region attribute and size register
            MPU->RASR = 0ul;
        }
```

```
    }

    // Enable the MPU
      /*  (7) Enabling MPU  */
    MPU->CTRL = ((uint32_t)privDefMapEn | (uint32_t)faultNmiEn | MPU_CTRL_ENABLE_Msk);

    // Ensure all memory accesses are completed before next instruction is executed
    __DSB();   /*  (8) Run Data memory barrier and Instruction Synchronization Barrier
instruction  */

    // Flush the pipeline and ensure all previous instructions are completed before executing
new instructions
    __ISB();   /*  (8) Run Data memory barrier and Instruction Synchronization Barrier
instruction  */

    return CY_MPU_SUCCESS;
}
```

5.2 Configuration of MPU implemented as part of bus infrastructure

This type of MPU is set by the MPU.ADDR and MPU.ATT registers, and is used by a test controller. However, normally, this MPU is set with CM0+ as a secure CPU depending on security requirements.

5.3 Configuration example of SMPU

The SMPU provides the memory protection function, and is shared by all bus masters. All bus masters have the same restriction for each region.

The SMPU has a protection pair structure with master/slave. Therefore, the setting the slave structure attribute is restricted by the master structure setting.

5.3.1 Usage assumptions

The SMPU distinguishes user/privileged, secure/non-secure, and protection contexts.

Table 12 shows an example of access restriction for an SMPU.

Table 12 Example access restriction for SMPU

Region	Privileged	User	Secure	Allowed protection context	PC_MATCH	Resources
Region 2 Base address: 0x08019000 Size: 4 KB	Read/write Execution is permitted	Read/write Execution is not permitted	Non-secure	PC = 6	Access evaluation	SRAM
Region 3 Base address: 0x08018000 Size: 4 KB	Read/write Execution is permitted	Read/write Execution is not permitted	Non-secure	PC = 5	Access evaluation	SRAM

Regions 2 and 3 have access restricted by the protection context.

Region 2 can access with protection context = 6, and Region3 can access with protection context = 5.

5.3.2 Setting procedure for SMPU

Figure 14 shows an example of the setting procedure.

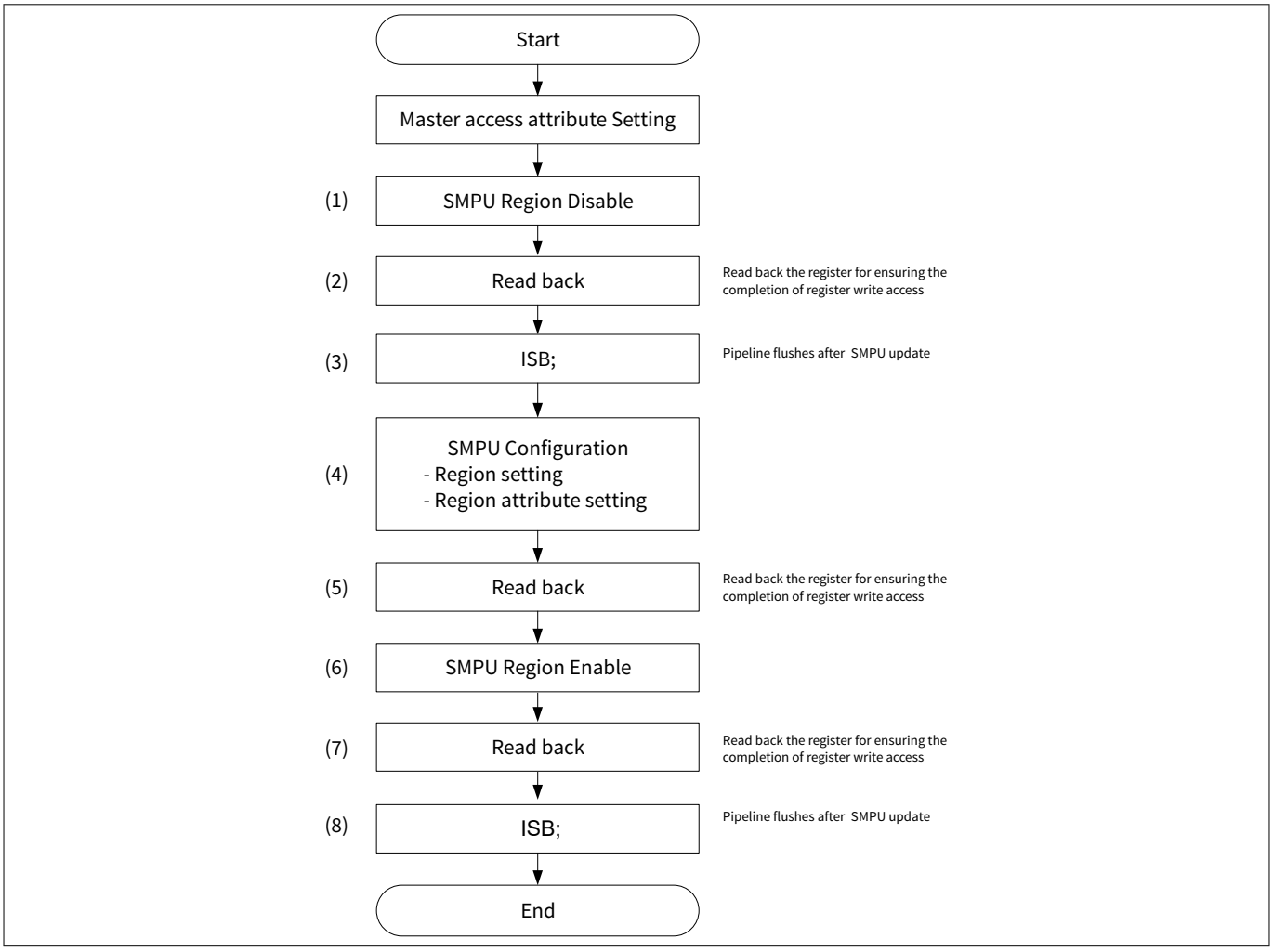

Figure 14 Setting procedure example of SMPU

The access attribute for setting the Slave structure (PROT_SMPU_STRUCTx_ADDR0 and PROT_SMPU_STRUCTx_ATT0) is allowed by the master structure (PROT_SMPU_STRUCTx_ADDR1 and PROT_SMPU_STRUCTx_ATT1).

It is necessary to read back the register for ensuring the completion of register write access when SMPU setting is completed.

5.3.3 Configuration

Table 13 and Table 14 list the parameters and functions of the configuration part in SDL for SMPU configuration.

Table 13 List of parameters

Parameters	Description	Value
MASTER_ID_OF_THIS_CPU	Define the master for which PROT_SMPU_MSx_CTL is set.	CPUSS_MS_ID_CM0 (CM0+)
TP_PRIVILEGED	Define PROT_SMPU_MSx_CTL.P value	1ul (Privileged mode)
TP_SECURE	Define PROT_SMPU_MSx_CTL.NS value	0ul (Non-Secure)
TP_PROT_CONTEXT	Define PROT_SMPU_MSx_CTL.PC value	6ul
TP_PERMITTED_ADDR	Define base address of SMPU Region2	0x08019000UL
TP_PERMITTED_CONTEXT	Define PC value that can access Region2	6ul
TP_PROHIBITED_ADDR	Define base address of SMPU Region3	0x08018000UL
TP_PROHIBITED_CONTEXT	Define PC value that can access Region3	5ul
smpuStruct(2 or 3)Config.address	Set region 2 or 3 base address	Region 2: TP_PERMITTED_ADD Region 3: TP_PROHIBITED_ADDR
smpuStruct(2 or 3)Config.regionSize	Set region 2 or 3 size	CY_PROT_SIZE_4KB (4 KB)
smpuStruct(2 or 3)Config.subregions	Set region 2 or 3 sub-region setting	0x00ul (Unused)
smpuStruct(2 or 3)Config.userPermission	Set region 2 or 3 access attribute for user	CY_PROT_PERM_RWX (Full access)
smpuStruct(2 or 3)Config.privPermission	Set region 2 or 3 access attribute for privileged	CY_PROT_PERM_RWX (Full access)
smpuStruct(2 or 3)Config.secure	Set region 2 or 3 access attribute for non-secure	0ul (Non-secure)
smpuStruct(2 or 3)Config.pcMatc	Set region 2 or 3 PC_MATCH setting	0ul (Access evaluation)

(table continues...)

Table 13 (continued) List of parameters

Parameters	Description	Value
smpuStruct(2 or 3)Config.pcMask	Set region 2 or 3 PC_MASK setting	Region 2: 1ul << (TP_PERMITTED_CONTEXT - 1) (Protection context = 6 is permitted) Region 3: 1ul << (TP_PROHIBITED_CONTEXT - 1) (Protection context = 5 is permitted)
PROT_SMPU_SMPU_STRUCT2	Define base address SMPU structure registers (region 2)	0x40232080ul
PROT_SMPU_SMPU_STRUCT3	Define base address SMPU structure registers (region 3)	0x402320C0ul

Table 14 List of functions

Functions	Description	Value
`Cy_Prot_ConfigBusMaster(busMaster, privileged, secure, pcMask)`	Configure PROT_SMPU_MS0_CTL register busMaster; indicate setting register number privileged: P field setting value secure: NS field setting value pcMask: Specifies a protection context value that can be set by the associated master.	busMaster; MASTER_ID_OF_THIS_CPU privileged: TP_PRIVILEGED secure: TP_SECURE pcMask: 1 << (TP_PROT_CONTEXT-1) (Protection context = 6)
`Cy_Prot_DisableSmpuSlaveStruct(*base)`	SMPU region disable *base: Base address of SMPU structure	*base: PROT_SMPU_SMPU_STRUCT2 or PROT_SMPU_SMPU_STRUCT3
`Cy_Prot_EnableSmpuSlaveStruct(*base)`	SMPU region enable *base: Base address of SMPU structure	*base: PROT_SMPU_SMPU_STRUCT2 or PROT_SMPU_SMPU_STRUCT3

(table continues...)

Table 14 (continued) List of functions

Functions	Description	Value
`Cy_Prot_ConfigSmpuSlaveStruct(*base, config)`	Configure SMPU structure *base: Base address of SMPU structure Config: Configuration data	*base: PROT_SMPU_SMPU_STRUCT2 or PROT_SMPU_SMPU_STRUCT3 Config: smpuStruct(2 or 3)Config

Code Listing 11 shows an example of SMPU configuration.

Code Listing 11 Example of SMPU configuration

```
typedef enum
    /*  Selection of Master CPU ID  */
{
    CPUSS_MS_ID_CM0                 =  0ul,
    CPUSS_MS_ID_CRYPTO              =  1ul,
    CPUSS_MS_ID_DW0                 =  2ul,
    CPUSS_MS_ID_DW1                 =  3ul,
    CPUSS_MS_ID_DMAC                =  4ul,
    CPUSS_MS_ID_SLOW0               =  5ul,
    CPUSS_MS_ID_SLOW1               =  6ul,
    CPUSS_MS_ID_CM4                 = 14ul,
    CPUSS_MS_ID_TC                  = 15ul
} en_prot_master_t;

    /*  Define Master CPU ID to CM0+  */
#define MASTER_ID_OF_THIS_CPU CPUSS_MS_ID_CM0

    /*  Selection of SMPU structure attribute  */
typedef enum
{
    CY_PROT_PERM_DISABLED = 0x00ul, /**< Read, Write and Execute disabled */
    CY_PROT_PERM_R        = 0x01ul, /**< Read enabled */
    CY_PROT_PERM_W        = 0x02ul, /**< Write enabled */
    CY_PROT_PERM_RW       = 0x03ul, /**< Read and Write enabled */
    CY_PROT_PERM_X        = 0x04ul, /**< Execute enabled */
    CY_PROT_PERM_RX       = 0x05ul, /**< Read and Execute enabled */
    CY_PROT_PERM_WX       = 0x06ul, /**< Write and Execute enabled */
    CY_PROT_PERM_RWX      = 0x07ul  /**< Read, Write and Execute enabled */
}cy_en_prot_perm_t;

#define TP_PRIVILEGED         (1ul)              /* privileged */
#define TP_SECURE             (0ul)              /* non secure */
#define TP_PROT_CONTEXT       (6ul)              /* enable context 6 */

/* This area is going to be prohibited accessing from a master who has TP_PROHIBITED_CONTEXT as
context */
#define TP_PROHIBITED_ADDR    (0x08018000UL)
#define TP_PROHIBITED_CONTEXT (5ul)

/* This area is going to be permitted accessing from a master who has TP_PERMITTED_CONTEXT as
context */
#define TP_PERMITTED_ADDR     (0x08019000UL)
#define TP_PERMITTED_CONTEXT  (TP_PROT_CONTEXT)

const cy_stc_smpu_cfg_t smpuStruct2Config =
    /*  Configure SMPU for Region 2.  */
{
    .address        = (uint32_t*)(TP_PERMITTED_ADDR),
    .regionSize     = CY_PROT_SIZE_4KB,                 // 4KB: 0x1000 Byte
    .subregions     = 0x00ul,
```

```
    .userPermission = CY_PROT_PERM_RWX,
    .privPermission = CY_PROT_PERM_RWX,
    .secure         = 0ul,                              // Non secure
    .pcMatch        = 0ul,
    .pcMask         = 1ul << (TP_PERMITTED_CONTEXT - 1),  // enable context
"TP_PERMITTED_CONTEXT"
};

const cy_stc_smpu_cfg_t smpuStruct3Config =
    /*  Configure SMPU for Region 3.  */
{
    .address        = (uint32_t*)(TP_PROHIBITED_ADDR),
    .regionSize     = CY_PROT_SIZE_4KB,                 // 4KB: 0x1000 Byte
    .subregions     = 0x00ul,
    .userPermission = CY_PROT_PERM_RWX,
    .privPermission = CY_PROT_PERM_RWX,
    .secure         = 0ul,                              // Non secure
    .pcMatch        = 0ul,
    .pcMask         = 1ul << (TP_PROHIBITED_CONTEXT - 1), // enable context
"TP_PERMITTED_CONTEXT"
};

int main(void)
{
    SystemInit();

    cy_en_prot_status_t status;
:
    /**************************/
    /* 1. Setting for MSx_CTL */
    /**************************/
    /* 1.1 Setting for MSx_CTL (for this CPU) to allow the PC value to become "TP_PROT_CONTEXT"
*/
    /*  Set PROT_SMPU_MS0_CTL.PC_MASK. See Code Listing 12.  */
    status = Cy_Prot_ConfigBusMaster(MASTER_ID_OF_THIS_CPU, TP_PRIVILEGED, TP_SECURE, 1 <<
(TP_PROT_CONTEXT-1));
    CY_ASSERT(status == CY_PROT_SUCCESS);

    /**************************/
    /* 2. Setting for MPU PC  */
    /**************************/
    /*  Change protection context to TP_PROT_CONTET (PC=6). See Code Listing 7.  */
    /* 2.1 Setting for MPU so that this CPU's PC value becomes "TP_PROT_CONTEXT" */
    status = Cy_Prot_SetActivePC(MASTER_ID_OF_THIS_CPU, TP_PROT_CONTEXT);
    CY_ASSERT(status == CY_PROT_SUCCESS);

    /*********************************/
    /* 3. Setting for SMPU_STRUCT 2 */
    /*********************************/
    /* 3.1 Disable SMPU_STRUCT 2 */
    /*  SMPU Region 2 disabled. See Code Listing 13.  */
    status = Cy_Prot_DisableSmpuSlaveStruct(PROT_SMPU_SMPU_STRUCT2);
    CY_ASSERT(status == CY_PROT_SUCCESS);
```

```
    /* 3.2 Setting SMPU_STRUCT 2 for PERMITTED area */
    /*  Configure SMPU Region 2. See Code Listing 14.  */
    status = Cy_Prot_ConfigSmpuSlaveStruct(PROT_SMPU_SMPU_STRUCT2, &smpuStruct2Config);
    CY_ASSERT(status == CY_PROT_SUCCESS);



    /* 3.3 Enable SMPU_STRUCT 2 */
    /*  SMPU Region 2 enabled. See Code Listing 15.  */
    status = Cy_Prot_EnableSmpuSlaveStruct(PROT_SMPU_SMPU_STRUCT2);
    CY_ASSERT(status == CY_PROT_SUCCESS);

    /********************************/
    /* 4. Setting for SMPU_STRUCT 3 */
    /********************************/
    /* 4.1 Disable SMPU_STRUCT 3 */
    /*  SMPU Region 3 disabled. See Code Listing 13.  */
    status = Cy_Prot_DisableSmpuSlaveStruct(PROT_SMPU_SMPU_STRUCT3);
    CY_ASSERT(status == CY_PROT_SUCCESS);

    /* 4.2 Setting SMPU_STRUCT 3 for PROHIBITED area */
    /*  Configure SMPU Region 3. See Code Listing 14.  */
    status = Cy_Prot_ConfigSmpuSlaveStruct(PROT_SMPU_SMPU_STRUCT3, &smpuStruct3Config);
    CY_ASSERT(status == CY_PROT_SUCCESS);

    /* 4.3 Enable SMPU_STRUCT 3 */
    /*  SMPU Region 3 enabled. See Code Listing 15  */
    status = Cy_Prot_EnableSmpuSlaveStruct(PROT_SMPU_SMPU_STRUCT3);
    CY_ASSERT(status == CY_PROT_SUCCESS);
:
    for(;;);
}
```

Code Listing 12 Cy_Prot_ConfigBusMaster() function

```
cy_en_prot_status_t Cy_Prot_ConfigBusMaster(en_prot_master_t busMaster, bool privileged, bool
secure, uint32_t pcMask)
{
    cy_en_prot_status_t status = CY_PROT_SUCCESS;
    un_PROT_SMPU_MS0_CTL_t tProtSmpuMs0Ctl = {0};
    uint32_t * addrMsCtl = (uint32_t *)(PROT_BASE + (uint32_t)((uint32_t)busMaster <<
CY_PROT_MSX_CTL_SHIFT));
:
        tProtSmpuMs0Ctl.stcField.u1NS = !secure;
        tProtSmpuMs0Ctl.stcField.u1P = privileged;
       /*  Set available PC values to PROT_SMPU_MS0_CTL.PC_MASK. (*) */
        tProtSmpuMs0Ctl.stcField.u15PC_MASK_15_TO_1 = pcMask;

        *addrMsCtl = tProtSmpuMs0Ctl.u32Register; // regVal;
             /*   Read back  */
        status = ((*addrMsCtl != tProtSmpuMs0Ctl.u32Register) ? CY_PROT_FAILURE :
CY_PROT_SUCCESS);
:
    return status;
}
```

Note: *(*) This process specifies the value of the protection context that can be set by the corresponding master. In secure system, it is run by secure master. See* Protection properties of bus transfer *for more details.*

Code Listing 13 Cy_Prot_DisableSmpuSlaveStruct() function

```
cy_en_prot_status_t Cy_Prot_DisableSmpuSlaveStruct(volatile stc_PROT_SMPU_SMPU_STRUCT_t* base)
{
    cy_en_prot_status_t status = CY_PROT_SUCCESS;

    base->unATT0.stcField.u1ENABLED &= ~CY_PROT_STRUCT_ENABLE; /* (1) Disable SMPU structure  */

    // Check if the SMPU structure really was enabled.
    // Note this also ensures previous write access to complete before execution of below ISB.
    status = (base->unATT0.stcField.u1ENABLED == CY_PROT_STRUCT_ENABLE) ?   /* (2) Read back  */
                CY_PROT_FAILURE : CY_PROT_SUCCESS;

    // Flush the pipeline and ensure all previous instructions are completed before executing
new instructions
    __ISB();   /* (3) Run Instruction Synchronization Barrier instruction  */

    return status;
}
```

Code Listing 14 Cy_Prot_ConfigSmpuSlaveStruct() function

```
cy_en_prot_status_t Cy_Prot_ConfigSmpuSlaveStruct(volatile stc_PROT_SMPU_SMPU_STRUCT_t* base,
const cy_stc_smpu_cfg_t* config)
{
    cy_en_prot_status_t status = CY_PROT_SUCCESS;
    un_PROT_SMPU_SMPU_STRUCT_ADDR0_t tprotSmpuSmpuStruct_ADDR0 = { 0 };
    un_PROT_SMPU_SMPU_STRUCT_ATT0_t  tprotSmpuSmpuStruct_ATT0 = { 0 };

    if(((uint32_t)config->pcMask & CY_PROT_SMPU_PC_LIMIT_MASK) != 0UL)
    {
        /* PC mask out of range - not supported in device */
        status = CY_PROT_BAD_PARAM;
    }
    else
    {

        /*  (4)-1 Set SMPU region  */
        tprotSmpuSmpuStruct_ADDR0.stcField.u8SUBREGION_DISABLE = config->subregions;
        tprotSmpuSmpuStruct_ADDR0.stcField.u24ADDR24 = (uint32_t)((uint32_t)config->address >>
CY_PROT_ADDR_SHIFT);




        /*  (4)-2 Set SMPU region attribute */
        tprotSmpuSmpuStruct_ATT0.stcField.u1PC_MASK_0 = 1; // This value is read only. The
default value is "1".
        tprotSmpuSmpuStruct_ATT0.stcField.u1NS = !(config->secure);
        tprotSmpuSmpuStruct_ATT0.stcField.u15PC_MASK_15_TO_1 = config->pcMask;
        tprotSmpuSmpuStruct_ATT0.stcField.u5REGION_SIZE = config->regionSize;
        tprotSmpuSmpuStruct_ATT0.stcField.u1PC_MATCH = config->pcMatch;
        tprotSmpuSmpuStruct_ATT0.stcField.u1UR = (config->userPermission & CY_PROT_PERM_R);
        tprotSmpuSmpuStruct_ATT0.stcField.u1UW = (config->userPermission & CY_PROT_PERM_W) >> 1;
        tprotSmpuSmpuStruct_ATT0.stcField.u1UX = (config->userPermission & CY_PROT_PERM_X) >> 2;
        tprotSmpuSmpuStruct_ATT0.stcField.u1PR = (config->privPermission & CY_PROT_PERM_R);
        tprotSmpuSmpuStruct_ATT0.stcField.u1PW = (config->privPermission & CY_PROT_PERM_W) >> 1;
        tprotSmpuSmpuStruct_ATT0.stcField.u1PX = (config->privPermission & CY_PROT_PERM_X) >> 2;

        base->unATT0.u32Register = tprotSmpuSmpuStruct_ATT0.u32Register;   // attReg;
        base->unADDR0.u32Register = tprotSmpuSmpuStruct_ADDR0.u32Register; // addrReg;

        status = ((base->unADDR0.u32Register != tprotSmpuSmpuStruct_ADDR0.u32Register) ||
                  (base->unATT0.u32Register != tprotSmpuSmpuStruct_ATT0.u32Register))   //* (5)
Read back */
                    ? CY_PROT_FAILURE : CY_PROT_SUCCESS;
    }

    return status;
}
```

Code Listing 15 Cy_Prot_EnableSmpuSlaveStruct() function

```
cy_en_prot_status_t Cy_Prot_EnableSmpuSlaveStruct(volatile stc_PROT_SMPU_SMPU_STRUCT_t* base)
{
    cy_en_prot_status_t status = CY_PROT_SUCCESS;

    base->unATT0.stcField.u1ENABLED = CY_PROT_STRUCT_ENABLE;   /* (6) Enable SMPU structure */

    // Check if the SMPU structure really was enabled.
    // Note this also ensures previous write access to complete before execution of below ISB.
    status = (base->unATT0.stcField.u1ENABLED != CY_PROT_STRUCT_ENABLE) ?   /* (7) Read back */
                CY_PROT_FAILURE : CY_PROT_SUCCESS;

    // Flush the pipeline and ensure all previous instructions are completed before executing
new instructions
    __ISB();   /* (8) Run Instruction Synchronization Barrier instruction */

    return status;
}
```

5.4 Configuration example of PPU

The PPU provides the peripheral protection function, and is shared by all bus masters.

Generally, the peripheral register address is fixed. Therefore, there are two types of PPUs:

- Fixed PPU with fixed protected address range
- Programmable PPU with programmable protected address range

Typically, the protection base address and size of the programmable PPU are set by CM0+ with the protection context 0 in the boot process.

This section explains how to configure a fixed PPU. A fixed PPU is the same as a programmable PPU except that the protected address area is fixed.

A PPU has also protection pair structure with master/slave settings. Therefore, the setting attribute of slave structure is restricted by the master structure setting.

5.4.1 Usage assumptions

The PPU distinguishes user/privileged, secure/non-secure, and protection context. Fixed PPU configuration is described according to the following use cases.

- Used fixed PPU 228 (GPIO_ENH Port#0)
- Protection context = 5: Privileged and user are not allowed to access to GPIO Port#0
- Protection context = 6: Privileged and user are allowed to access to GPIO Port#0

Table 15 shows an example of access restriction for this fixed PPU.

Table 15 Example access restriction for PPU

Setting PPU	Protection context	Privileged	User	Secure
PPU_FX228	PC = 5	No access	No access	Non-secure
	PC = 6	Read/write	Read/write	

***Note**: See the datasheet for actual addresses and peripheral channel numbers of target product.*

5.4.2 Setting procedure for PPU

Figure 15 shows an example of the setting procedure.

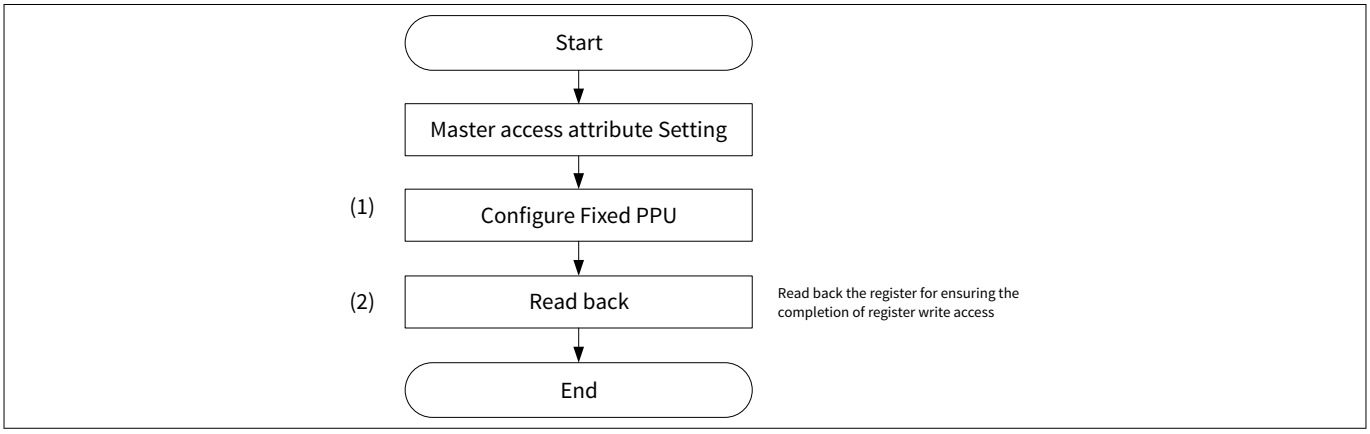

Figure 15 Setting procedure example of PPU

The access attribute for the slave structure (PROT_PPU_FXx_SL_ATT0) setting is allowed by the master structure (PROT_PPU_FXx_MS_ATT0).

It is necessary to read back the register for ensuring the completion of register write access when PPU setting is completed.

5.4.3 Configuration

Table 16 and Table 17 list the parameters and functions of the configuration part in SDL for fixed PPU configuration.

Table 16 List of parameters

Parameters	Description	Value
MASTER_ID_OF_THIS_CPU	Define the master for which PROT_SMPU_MSx_CTL is set.	CPUSS_MS_ID_CM0 (CM0+)
PERI_MS_PPU_FX_GPIO_PRT0_PRT	Define configure fixed PPU register address of target	(volatile stc_PERI_MS_PPU_FX_t*) &PERI_MS->PPU_FX[228] (Shows the base address of fixed PPU 228)
TP_PRIVILEGED	Define PROT_SMPU_MSx_CTL.P value	1ul (Privileged mode)
TP_SECURE	Define PROT_SMPU_MSx_CTL.NS value	0ul (Non-Secure)
TP_PERMITTED_PC	Define protection context for permitted access.	CY_PROT_PC6 (6ul)
TP_PROHIBITED_PC	Define protection context for not permitted access.	CY_PROT_PC5 (5ul)

(table continues...)

Table 16 (continued) List of parameters

Parameters	Description	Value
TP_PERMITTED_PC_MASK	Define PROT_SMPU_MSx_CTL.PC_MASK value for bus master	1ul << (TP_PERMITTED_PC-1ul)
TP_PROHIBITED_PC_MASK	Define PROT_SMPU_MSx_CTL.PC_MASK value for bus master	1ul << (TP_PROHIBITED_PC-1ul)
ppuFixedAttr_AllEnable.userPermission	Set user access attribute for target PC of fixed PPU	CY_PROT_PERM_RWX (Full access)
ppuFixedAttr_AllEnable.privPermission	Set privileged access attribute for target PC of fixed PPU	CY_PROT_PERM_RWX (Full access)
ppuFixedAttr_AllEnable.secure	Set non-secure access attribute for target PC of fixed PPU	TP_SECURE (Non-secure)
ppuFixedAttr_AllDisable.userPermission	Set user access attribute for target PC of fixed PPU	CY_PROT_PERM_DISABLED (No access)
ppuFixedAttr_AllDisable.privPermission	Set privileged access attribute for target PC of fixed PPU	CY_PROT_PERM_DISABLED (No access)
ppuFixedAttr_AllDisable.secure	Set non-secure access attribute for target PC of fixed PPU	TP_SECURE (Non-secure)

Table 17 List of functions

Functions	Description	Value
`Cy_Prot_ConfigPpuFixedSlaveStruct(*base, setPC, config)`	Configure fixed PPU register *base; Base address of fixed PPU structure setPC: Indicate setting PC config: Access attribute	*base: PERI_MS_PPU_FX_GPIO_PRT0_PRT setPC: TP_PERMITTED_PC or TP_PROHIBITED_PC config: &ppuFixedAttr_AllEnable or &ppuFixedAttr_AllDisable

Code Listing 16 shows an example of fixed PPU configuration.

Code Listing 16 Example of fixed PPU configuration

```
#define PERI_MS_PPU_FX_GPIO_PRT0_PRT            ((volatile stc_PERI_MS_PPU_FX_t*) &PERI_MS-
>PPU_FX[228])

typedef enum
    /*  Selection of Master CPU ID  */
{
    CPUSS_MS_ID_CM0                 =  0ul,
    CPUSS_MS_ID_CRYPTO              =  1ul,
    CPUSS_MS_ID_DW0                 =  2ul,
    CPUSS_MS_ID_DW1                 =  3ul,
    CPUSS_MS_ID_DMAC                =  4ul,
    CPUSS_MS_ID_SLOW0               =  5ul,
    CPUSS_MS_ID_SLOW1               =  6ul,
    CPUSS_MS_ID_CM4                 = 14ul,
    CPUSS_MS_ID_TC                  = 15ul
} en_prot_master_t;

    /*  Define Master CPU ID to CM0+  */
#define MASTER_ID_OF_THIS_CPU CPUSS_MS_ID_CM0


typedef enum
    /*  Define protection context number  */
{
    CY_PROT_PC0  = 0ul,  /**< PC = 0 */
    CY_PROT_PC1  = 1ul,  /**< PC = 1 */
    CY_PROT_PC2  = 2ul,  /**< PC = 2 */
    CY_PROT_PC3  = 3ul,  /**< PC = 3 */
    CY_PROT_PC4  = 4ul,  /**< PC = 4 */
    CY_PROT_PC5  = 5ul,  /**< PC = 5 */
    CY_PROT_PC6  = 6ul,  /**< PC = 6 */
    CY_PROT_PC7  = 7ul,  /**< PC = 7 */
    CY_PROT_PC_NUM
} cy_en_prot_pc_t;

#define TP_PRIVILEGED         (1ul)              /* privileged */
#define TP_SECURE             (0ul)              /* non secure */
#define TP_PERMITTED_PC       (CY_PROT_PC6)      /* context 6 */
#define TP_PROHIBITED_PC      (CY_PROT_PC5)      /* context 5 */
#define TP_PERMITTED_PC_MASK  (1ul << (TP_PERMITTED_PC-1ul))
#define TP_PROHIBITED_PC_MASK (1ul << (TP_PROHIBITED_PC-1ul))

typedef enum
    /*  Selection of Fixed PPU structure attribute  */
{
    CY_PROT_PERM_DISABLED = 0x00ul, /**< Read, Write and Execute disabled */
    CY_PROT_PERM_R        = 0x01ul, /**< Read enabled */
    CY_PROT_PERM_W        = 0x02ul, /**< Write enabled */
    CY_PROT_PERM_RW       = 0x03ul, /**< Read and Write enabled */
    CY_PROT_PERM_X        = 0x04ul, /**< Execute enabled */
    CY_PROT_PERM_RX       = 0x05ul, /**< Read and Execute enabled */
```

```
    CY_PROT_PERM_WX       = 0x06ul, /**< Write and Execute enabled */
    CY_PROT_PERM_RWX      = 0x07ul  /**< Read, Write and Execute enabled */
}cy_en_prot_perm_t;

    /*  Configure Fixed PPU for full access  */
const cy_stc_ppu_gr_cfg_t  ppuFixedAttr_AllEnable =
{
    .userPermission = CY_PROT_PERM_RWX,
    .privPermission = CY_PROT_PERM_RWX,
    .secure         = TP_SECURE,
};

    /*  Configure Fixed PPU for no access  */
const cy_stc_ppu_gr_cfg_t  ppuFixedAttr_AllDisable =
{
    .userPermission = CY_PROT_PERM_DISABLED,
    .privPermission = CY_PROT_PERM_DISABLED,
    .secure         = TP_SECURE,
};

int main(void)
{
    SystemInit();

    cy_en_prot_status_t status;

    __enable_irq();

    Cy_SysEnableApplCore(CY_CORTEX_M4_APPL_ADDR);

    /*********************************************/
    /* 1. Setting for GPIO 0 Register attribute */
    /*********************************************/
    /*  Configure Fixed PPU for protection context = 5. See See Code Listing 17.  */
    /* 1_1. Set permissions so that master whose PC is 5 can not access GPIO 0 */
    status = Cy_Prot_ConfigPpuFixedSlaveStruct(PERI_MS_PPU_FX_GPIO_PRT0_PRT, TP_PROHIBITED_PC,
&ppuFixedAttr_AllDisable);
    CY_ASSERT(status == CY_PROT_SUCCESS);

    /*  Configure Fixed PPU for protection context = 6. See Code Listing 17.  */
    /* 1_2. Set permissions so that master whose PC is 6 can access GPIO 0 */
    status = Cy_Prot_ConfigPpuFixedSlaveStruct(PERI_MS_PPU_FX_GPIO_PRT0_PRT, TP_PERMITTED_PC,
&ppuFixedAttr_AllEnable);
    CY_ASSERT(status == CY_PROT_SUCCESS);

    /*********************************************/
    /* 2. Setting for MPUx (MPU for this Master) */
    /*********************************************/
    /* 2_1. Setting for MSx_CTL to allow the PC value to become "TP_PERMITTED_PC" or
"TP_PROHIBITED_PC" */
    /*  Set PROT_SMPU_MS0_CTL.PC_MASK for protection context = 5 and 6. For setting SMPU
details, see Configuration Example of SMPU.  */
    status = Cy_Prot_ConfigBusMaster(MASTER_ID_TO_BE_CHECKED, TP_PRIVILEGED, TP_SECURE,
```

```
TP_PERMITTED_PC_MASK|TP_PROHIBITED_PC_MASK);
    CY_ASSERT(status == CY_PROT_SUCCESS);

    for(;;);
}
```

Code Listing 17 Cy_Prot_ConfigPpuFixedSlaveStruct() function

```
cy_en_prot_status_t Cy_Prot_ConfigPpuFixedSlaveStruct(volatile stc_PERI_MS_PPU_FX_t* base,
cy_en_prot_pc_t setPC, const cy_stc_ppu_gr_cfg_t* config)
{
    cy_en_prot_status_t status = CY_PROT_SUCCESS;
    un_PERI_MS_PPU_PR_SL_ATT0_t tempSL_ATT0 = { 0 };
    un_PERI_MS_PPU_PR_SL_ATT1_t tempSL_ATT1 = { 0 };
    un_PERI_MS_PPU_PR_SL_ATT2_t tempSL_ATT2 = { 0 };
    un_PERI_MS_PPU_PR_SL_ATT3_t tempSL_ATT3 = { 0 };

:

    switch(setPC)
    {
    :
    /* Set Fixed PPU region attribute for protection context = 1 */
    case CY_PROT_PC1:
        /* (1) Set Fixed PPU region attribute for protection context = 1 */
        tempSL_ATT0.u32Register = base->unSL_ATT0.u32Register;
        tempSL_ATT0.stcField.u1PC1_UR = (config->userPermission & CY_PROT_PERM_R);
        tempSL_ATT0.stcField.u1PC1_UW = (config->userPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT0.stcField.u1PC1_PR = (config->privPermission & CY_PROT_PERM_R);
        tempSL_ATT0.stcField.u1PC1_PW = (config->privPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT0.stcField.u1PC1_NS = !(config->secure);
        base->unSL_ATT0.u32Register = tempSL_ATT0.u32Register;
        status = (base->unSL_ATT0.u32Register != tempSL_ATT0.u32Register) ? CY_PROT_FAILURE :
CY_PROT_SUCCESS;    /* (2) Read back */
        break;

    /* Set Fixed PPU region attribute for protection context = 2 */
    case CY_PROT_PC2:
        tempSL_ATT0.u32Register = base->unSL_ATT0.u32Register;
        tempSL_ATT0.stcField.u1PC2_UR = (config->userPermission & CY_PROT_PERM_R);
        tempSL_ATT0.stcField.u1PC2_UW = (config->userPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT0.stcField.u1PC2_PR = (config->privPermission & CY_PROT_PERM_R);
        tempSL_ATT0.stcField.u1PC2_PW = (config->privPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT0.stcField.u1PC2_NS = !(config->secure);
        base->unSL_ATT0.u32Register = tempSL_ATT0.u32Register;
        status = (base->unSL_ATT0.u32Register != tempSL_ATT0.u32Register) ? CY_PROT_FAILURE :
CY_PROT_SUCCESS;    /* Read back */
        break;

    /* Set Fixed PPU region attribute for protection context = 3 */
    case CY_PROT_PC3:
        tempSL_ATT0.u32Register = base->unSL_ATT0.u32Register;
        tempSL_ATT0.stcField.u1PC3_UR = (config->userPermission & CY_PROT_PERM_R);
        tempSL_ATT0.stcField.u1PC3_UW = (config->userPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT0.stcField.u1PC3_PR = (config->privPermission & CY_PROT_PERM_R);
        tempSL_ATT0.stcField.u1PC3_PW = (config->privPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT0.stcField.u1PC3_NS = !(config->secure);
        base->unSL_ATT0.u32Register = tempSL_ATT0.u32Register;
        status = (base->unSL_ATT0.u32Register != tempSL_ATT0.u32Register) ? CY_PROT_FAILURE :
```

```
CY_PROT_SUCCESS;    /* Read back */
        break;

    /* Set Fixed PPU region attribute for protection context = 4 */
    case CY_PROT_PC4:
        tempSL_ATT1.u32Register = base->unSL_ATT1.u32Register;
        tempSL_ATT1.stcField.u1PC4_UR = (config->userPermission & CY_PROT_PERM_R);
        tempSL_ATT1.stcField.u1PC4_UW = (config->userPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT1.stcField.u1PC4_PR = (config->privPermission & CY_PROT_PERM_R);
        tempSL_ATT1.stcField.u1PC4_PW = (config->privPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT1.stcField.u1PC4_NS = !(config->secure);
        base->unSL_ATT1.u32Register = tempSL_ATT1.u32Register;
        status = (base->unSL_ATT1.u32Register != tempSL_ATT1.u32Register) ? CY_PROT_FAILURE :
CY_PROT_SUCCESS;    /* Read back */
        break;

    /* Set Fixed PPU region attribute for protection context = 5 */
    case CY_PROT_PC5:
        tempSL_ATT1.u32Register = base->unSL_ATT1.u32Register;
        tempSL_ATT1.stcField.u1PC5_UR = (config->userPermission & CY_PROT_PERM_R);
        tempSL_ATT1.stcField.u1PC5_UW = (config->userPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT1.stcField.u1PC5_PR = (config->privPermission & CY_PROT_PERM_R);
        tempSL_ATT1.stcField.u1PC5_PW = (config->privPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT1.stcField.u1PC5_NS = !(config->secure);
        base->unSL_ATT1.u32Register = tempSL_ATT1.u32Register;
        status = (base->unSL_ATT1.u32Register != tempSL_ATT1.u32Register) ? CY_PROT_FAILURE :
CY_PROT_SUCCESS;    /* Read back */
        break;

    /* Set Fixed PPU region attribute for protection context = 6 */
    case CY_PROT_PC6:
        tempSL_ATT1.u32Register = base->unSL_ATT1.u32Register;
        tempSL_ATT1.stcField.u1PC6_UR = (config->userPermission & CY_PROT_PERM_R);
        tempSL_ATT1.stcField.u1PC6_UW = (config->userPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT1.stcField.u1PC6_PR = (config->privPermission & CY_PROT_PERM_R);
        tempSL_ATT1.stcField.u1PC6_PW = (config->privPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT1.stcField.u1PC6_NS = !(config->secure);
        base->unSL_ATT1.u32Register = tempSL_ATT1.u32Register;
        status = (base->unSL_ATT1.u32Register != tempSL_ATT1.u32Register) ? CY_PROT_FAILURE :
CY_PROT_SUCCESS;    /* Read back */
        break;

    /* Set Fixed PPU region attribute for protection context = 7 */
    case CY_PROT_PC7:
        tempSL_ATT1.u32Register = base->unSL_ATT1.u32Register;
        tempSL_ATT1.stcField.u1PC7_UR = (config->userPermission & CY_PROT_PERM_R);
        tempSL_ATT1.stcField.u1PC7_UW = (config->userPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT1.stcField.u1PC7_PR = (config->privPermission & CY_PROT_PERM_R);
        tempSL_ATT1.stcField.u1PC7_PW = (config->privPermission & CY_PROT_PERM_W) >> 1;
        tempSL_ATT1.stcField.u1PC7_NS = !(config->secure);
        base->unSL_ATT1.u32Register = tempSL_ATT1.u32Register;
        status = (base->unSL_ATT1.u32Register != tempSL_ATT1.u32Register) ? CY_PROT_FAILURE :
CY_PROT_SUCCESS;    /* Read back */
```

```
            break;

        default:
            return CY_PROT_BAD_PARAM;
        }

        return status;
    }
```

6 Glossary

Terms	Description
CRYPTO	Cryptography component. See the Cryptography block chapter of the architecture TRM for details.
DMB	Data memory barrier. It is instruction in the thumb instruction set.
DSB	Data synchronization barrier. It is instruction in the thumb instruction set.
ISB	Instruction synchronization barrier. It is instruction in the thumb instruction set.
M-DMA	Memory DMA. See the Direct memory access chapter of the architecture TRM for details.
MPU	Memory protection unit
PCs	Protection contexts. See the Protection context” section in the Protection unit chapter of the architecture TRM for details.
P-DMA	Peripheral DMA. See the Direct memory access chapter of the architecture TRM for details.
PPU	Peripheral protection unit
SMPU	Shared memory protection unit

7 Related documents

The following are the TRAVEO™ T2G family series datasheets and technical reference manuals. Contact Technical support to obtain these documents.

[1] Device datasheet

- CYT2B7 datasheet 32-bit Arm® Cortex®-M4F microcontroller TRAVEO™ T2G family
- CYT2B9 datasheet 32-bit Arm® Cortex®-M4F microcontroller TRAVEO™ T2G family
- CYT4BF datasheet 32-bit Arm® Cortex®-M7 microcontroller TRAVEO™ T2G family
- CYT4DN datasheet 32-bit Arm® Cortex®-M7 microcontroller TRAVEO™ T2G family (Doc No. 002-24601)
- CYT3BB/4BB datasheet 32-bit Arm® Cortex®-M7 microcontroller TRAVEO™ T2G family
- CYT3DL datasheet 32-bit Arm® Cortex®-M7 microcontroller TRAVEO™ T2G family (Doc No. 002-27763)

[2] Body controller entry family

- TRAVEO™ T2G automotive body controller entry family architecture technical reference manual (TRM)
- TRAVEO™ T2G automotive body controller entry registers technical reference manual (TRM) for CYT2B7
- TRAVEO™ T2G automotive body controller entry registers technical reference manual (TRM) for CYT2B9

[3] Body controller high family

- TRAVEO™ T2G automotive body controller high family architecture technical reference manual (TRM)
- TRAVEO™ T2G automotive body controller high registers technical reference manual (TRM) for CYT4BF
- TRAVEO™ T2G automotive body controller high registers technical reference manual (TRM) for CYT3BB/4BB

[4] Cluster 2D family

- TRAVEO™ T2G automotive cluster 2D family architecture technical reference manual (TRM) (Doc No. 002-25800)
- TRAVEO™ T2G automotive cluster 2D registers technical reference manual (TRM) for CYT4DN (Doc No. 002-25923)
- TRAVEO™ T2G automotive cluster 2D registers technical reference manual (TRM) for CYT3DL (Doc No. 002-29854)

[5] Application note

- AN 224432 - Multi core handling guide in TRAVEO™ T2G

8 Other references

A sample driver library (SDL) including startup as sample software to access various peripherals is provided. SDL also serves as a reference, to customers, for drivers that are not covered by the official AUTOSAR products. The SDL cannot be used for production purposes as it does not qualify to any automotive standards. The code snippets in this application note are part of the SDL. Contact Technical support to obtain the SDL.

Revision history

Document version	Date of release	Description of changes
**	2018-03-09	New Application Note.
*A	2018-11-06	Changed target parts number (CYT2B series).
*B	2019-02-20	Added target parts number (CYT4B series).
*C	2019-07-25	Added target parts number (CYT4D series).
*D	2020-02-14	Changed target parts number (CYT2/ CYT4 series). Added target parts number (CYT3 series).
*E	2021-02-01	Moved to Infineon Template Updated code examples using SDL
*F	2021-04-23	Added note for 3.1 Protection Properties of Bus Transfer Added note for 3.4 Protection Context Attribute Setting. Added target parts number (CYT3DL series)
*G	2021-11-22	Fixed of errors description. Change function name from GetUserMode/GetPrivilegedMode/ SVC_GetPrivilegedMode to SetUserMode/SetPrivilegedMode/ SVC_SetPrivilegedMode in Table 2 and Code Listing 1 to Code Listing 5.
*H	2022-09-13	Changed description in Introduction. Added description in Protection properties of bus transfer. Added Note in PC_MATCH operation.
*I	2023-11-27	Template update; no content update.

Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

Edition 2023-11-27

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about any aspect of this document?

Email: erratum@infineon.com

Document reference
IFX-mpm1681719678863

Important notice

The information contained in this application note is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this application note.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

Warnings

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.