

Application note

Use the MMU to protect FLASH partitions in multi-user scenarios

Introduction

In the process of embedded product development, sometimes there are scenarios in which multiple users are required to develop application software in stages within a single MCU. In this scenario, the codes and data of each user may not be shared with other users due to copyright or security considerations. So how do you solve these problems?

This document is mainly aimed at the above-mentioned application scenarios of the Nations. MCU series products, and guides users how to use the Nations MCU, through the built-in memory management unit (Memory Management Unit, MMU) to achieve the multi-user area division and access permissions of the FLASH main storage area Management, so as to solve the problem of code copyright protection and data security in the multi-user development process. Therefore, it can be widely used in various copyright protection, sensitive data and multi-user code protection scenarios.

This document is only applicable to Nations MCU products with built-in MMU. Currently, the supported product series include N32G05x series.

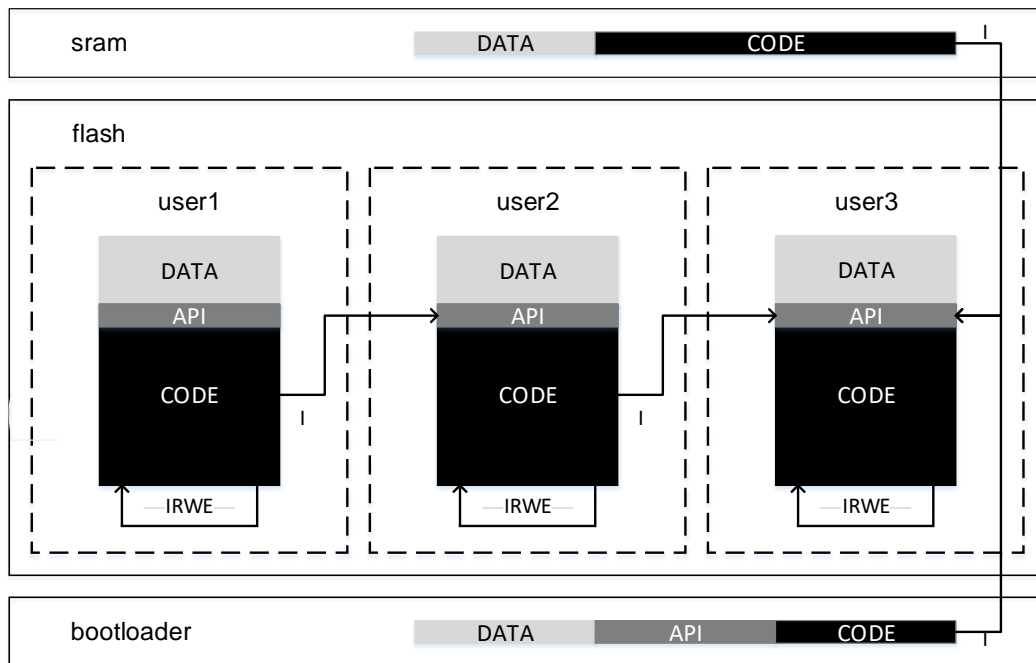
CONTENTS

1 Implementation mechanism of partition protection	1
2 Function description of the MMU	2
2.1 User area division	2
2.2 Access permission management	4
3 Operating Instruction.....	5
3.1 The operating environment.....	5
3.2 Operation steps	5
3.2.1 Device enters the Bootloader	5
3.2.2 Device connection tool	5
3.2.3 Configuration partition.....	6
4 Example project.....	8
4.1 Section address configuration.....	8
4.1.1 Sct distributed load file.....	8
4.2 Generating a bin file	10
4.3 Partition access operation	11
4.3.1 Call API.....	13
4.3.2 Read and write data-MMU abnormal alarm.....	14
4.3.3 Interrupt handling	14
5 Conclusion	16
6 Version history	17
7 Notice	18

1 Implementation mechanism of partition protection

Generally, the FLASH memory (FLASH) in the MCU chip is connected to the memory bus, and the CPU can access any area in the FLASH without limit. Multiple user areas should be divided and protected for FLASH in a single MCU to avoid different users reading or modifying FLASH contents in other user areas directly by CPU instructions. We can use the Nations MCU built-in MMU, set the FLASH the main storage area partition and access, at the same time can protect all the application code and data storage area from illegal access and tampering, and indicates the memory and the protected registers of illegal access errors, all unauthorized operation will trigger the MMU abnormal alarm, To achieve multi-user FLASH partition protection.

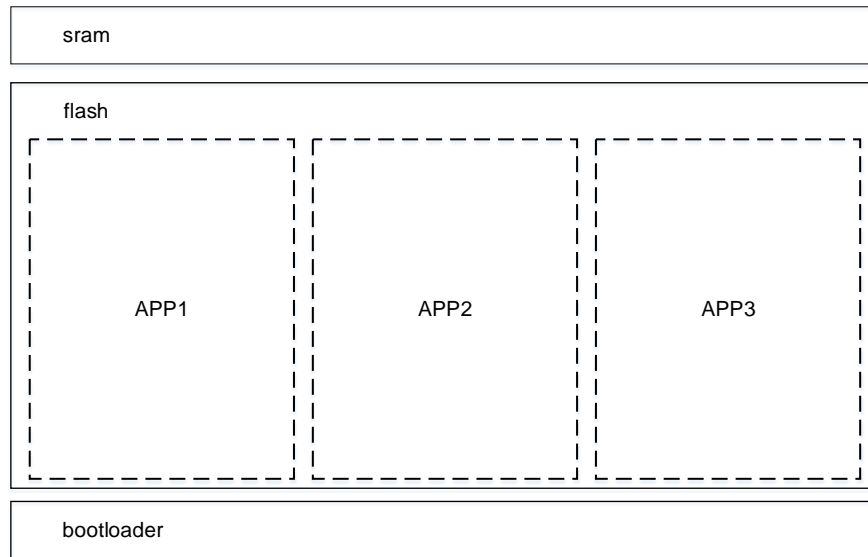
Figure 1-1 MMU partition protection implementation mechanism



2 Function description of the MMU

MMU can realize region division and access permission management of FLASH main storage area, and can divide independent storage space for different applications of MCU (see Figure 2-1), and manage access permission.

Figure 2-1 Memory area division



2.1 User area division

The FLASH main storage area can be divided into USER1 (default), USER2, and USER3 at most. In practice, the user area can be divided into the following situations. For the Settings of each situation, refer to Table 2-1

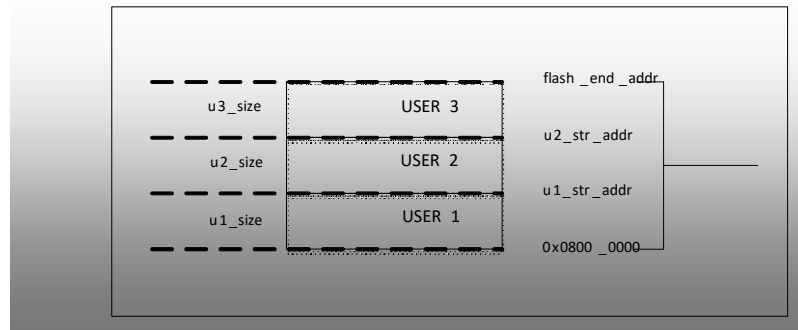
Table 2-1 User Partition Setting Instructions

Description	Partition setup sequence	FLASH space size involving authority management ⁽¹⁾			Instructions
		user1	user2	user3	
No partition, default is that the user1 area is not sealed	-	-	-	-	The user1 area is flash_size and does not have the access permission management function
No partition, the user1 area is sealed	user1	user1_size	-	-	The user1 area is flash_size
Two partitions, USER1 unsealed and USER3 sealed	user3→user2	-	0	user3_size	The space of user1 and user3 is flash_size. User1 does not have the access permission management function
Two partitions, USER1 sealed and USER3 sealed	user3→user2→user1	user1_size	0	user3_size	The space size of user1 and user3 is flash_size

Three partitions, USER1 unsealed and USER2&USER3 sealed	user3→user2	-	user2_size	user3_size	The space of user1, user2, and user3 is flash_size. User1 does not have the access permission management function
Three partitions, all sealed	user3→user2→user1	user1_size	user2_size	user3_size	User1, user2, and user3 are flash_size
Description: (1) " FLASH space size involving authority management" refers to the FLASH main storage space with partition size set.					

When the FLASH primary storage partition is divided into three regions, USER1 (default), USER2, and USER3, as shown in Figure 2-2. The granularity of the partition is 4KB.

Figure 2-2 FLASH main storage area division relationship



For details about how to set user partitions in the FLASH primary storage area, see Table 2-2. You can divide regions by setting the size of each user partition. Partition Settings are static Settings. Once set, the MCU will automatically load the configuration every time it is powered on. In particular, partition Settings can only be operated once, and the operation is irreversible.

Table 2-2 FLASH main storage area partition setting instructions

Partition users	The storage area	Partition size range
USER1	$0x0800_0000 \sim (0x0800_0000 + u1_size - 1)$	$4KB^1 \sim (flash_size) KB$
USER2	$(0x0800_0000 + u1_size) \sim (flash_end_addr - u3_size)$	$0 KB \sim (flash_size - 8)KB$
USER3	$(flash_end_addr - u3_size + 1) \sim (flash_end_addr)^2$	$0 KB \sim (flash_size - 4)KB$
Description: (1) The granularity of the partition is 4KB; (2) Flash_end_addr varies according to model, and the corresponding flash_size is also different. Flash_size should be the sum of the size of the flash_area USER1, USER2, and USER3. The size is $(flash_end_addr - 0x0800_0000 + 1)$. Note: User partition Settings cannot be reset		

2. 2 Access permission management

The operation permissions of each area of FLASH main storage area are managed through user area division to realize memory access control. Table 2-3 provides the access permissions of each user area before and after FLASH main storage area division.

Table 2-3 User permission table

	Visited area					
	user1		user2		user3	
Program ownership /	Whether the partitions		Whether the partitions		Whether the partitions	
Access method	N ¹	Y	N	Y	N	Y
user1 code	IRWE ^{2, 3}	IRWE	IRWE	I	IRWE	I
user2 code	IRWE	I	IRWE	IRWE	IRWE	I
user3 code	IRWE	I	IRWE	I	IRWE	IRWE
SRAM code	IRWE	I	IRWE	I	IRWE	I
DMA1/DMA2	RW	-	RW	-	RW	-
JTAG/SWD	IRWE	I	IRWE	I	IRWE	I
Description: (1) Before the partition, USER1, USER2, and USER3 are regarded as the same area, and all FLASH space is USER1 by default; (2) I represents addressing, R represents reading, W represents writing, and E represents erasing; (3) "Write Protection (WRP) Enable" is at the same level as "Access Rights Management for MMU Partitions". Note: If the USER1 area size is not set (see section 3.2.1 to section 3.2.3 for "Operation step"), the USER1 area does not have access permission management.						

3 Operating Instruction

Partitioning the MCU built-in FLASH main memory area by using the Nations MCU Download Tool on the PC provided by Nations. For details about how to use the Tool, see “*Nations MCU Download Tool User Manual*”.

3.1 The operating environment

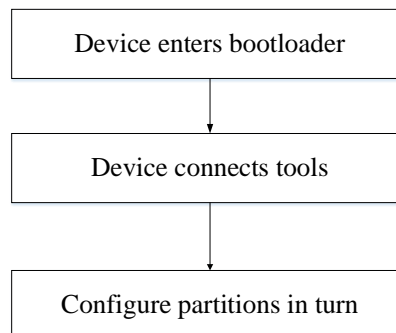
- Hardware environment: PC (Windows XP/7/10), development board N32G05XRBQ7-STB V1.0 (including N32G05XRBQ7 chip)
- Target device: N32G05XRBQ7 chip
- Software environment: Download tool (Nations MCU Download tool. Exe), USB DFU driver or USB-to-serial driver (optional)

Note: Bootloader supports USB interface or UART interface download, please confirm that the USB DFU driver or USB to serial port driver has been installed before use. At the same time, confirm that the target device has entered the Bootloader state, so that the device can be connected to the download tool normally. For details on how to make the target device enter the Bootloader state, please refer to the user manual of the target device chip. This document uses the N32G05XRBQ7 chip to download using the UART interface as an example for illustration.

3.2 Operation steps

Figure 3-1 shows the process for dividing user areas in the FLASH primary storage area. The following describes how to set partitions.

Figure 3-1 Partition setup steps



3.2.1 Device enters the Bootloader

N32G05XRBQ7 BOOT0 pin is connected to VDD, PB2 pin is connected to GND, the chip is powered on and enters the Bootloader.

Note: For the development board N32G05XRBQ7-STB V1.0, use the UART interface, then connect the USB Debug Port interface for power supply, otherwise use the USB COMM interface for power supply.

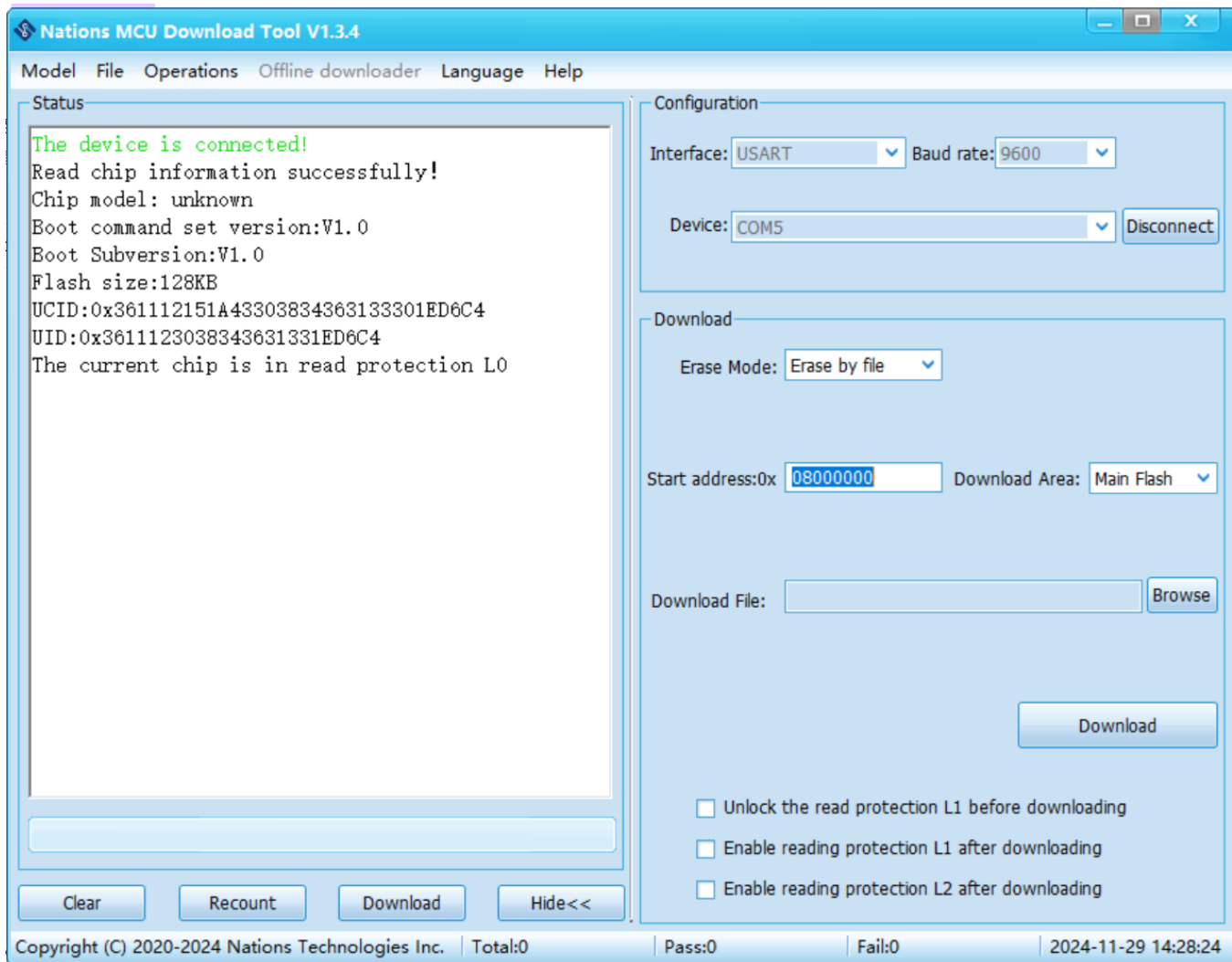
3.2.2 Device connection tool

Double-click Nations MCU Download Tool.exe to open the download tool. The interface is shown in Figure 3-2. Here, the focus will be on the "Select Device" area. The interface defaults to "UART". Select the matching port number as the device. The "COM port number" can be viewed through the "Device Manager" of the PC. The serial port connected to the MCU in Figure 3-2 is identified as "COM3". At the same time, set the baud rate of UART (the default

configuration "9600" can be used), click the "connect" button, the left display interface will prompt "The device is connected!". At this time, the device and the tool have been connected normally.

Note: UART1 in the Bootloader of N32G05XRBQ7 uses PA9 and PA10 as TX and RX respectively. Please ensure that PA9 and PA10 are properly connected to TX and RX of the serial port.

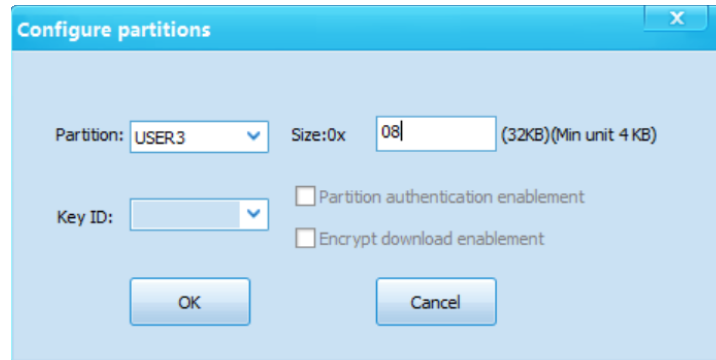
Figure 3-2 Download tool interface



3.2.3 Configuration partition

Click the "Configure partition" button in the "Common operations" area to pop up the Configure Partition dialog box, select the partition user ID (USER1, USER2 or USER3) in turn, and enter the FLASH size of the partition (the value is set in the unit of partition granularity 4KB). As shown in Figure 3-3, suppose you need to partition a 32KB area for USER3, select "USER3" for the partition and enter 0x08 for the size. Click "Configure Partition" to confirm the configuration partition and complete the area division of the current user ID.

Figure 3-3 Interface for configuring partitions



Note:

- (1) The partition configuration operation is irreversible, please operate with caution
- (2) If multiple partitions need to be configured, each user can enter the Bootloader configuration respectively. For details about the configuration size and sequence, see Table 2-1 and “*Nations MCU Download Tool User Manual*”. Improper operations may lead to configuration failure.

4 Example project

In order to demonstrate the execution mode of programs after partitioning the FLASH main storage area, such as function calling methods between different partition areas, different effects of normal or abnormal data reading, and interrupt handling methods, three example projects will be provided as projects for three partition user IDs: USER1, USER2, and USER3.

The following sections will focus on section address configuration, generation of bin files, and access operations between user partitions.

4.1 Section address configuration

Take the N32G05XRBQ7 chip as an example. Assume that the USER1, USER2, and USER3 user areas are 64KB, 32KB, and 32KB respectively. In this case, the partition relationship of the FLASH main storage area is shown in Figure 4-1. Each user can negotiate and divide the FLASH main storage area according to the actual code amount of the application in each partition.

Figure 4-1 Flash main storage area partition relationship



In addition to partition the FLASH main storage area, to avoid global variable storage space conflicts among different partitioning programs, you can also partition the 16KB SRAM space of N32G05XRBQ7. The SRAM of each user can store global variables in the corresponding program. Since chip program execution starts at address 0x08000000, USER1 acts as the end user and handles both stack and interrupt responses. So USER1's SRAM can also be used as stack space. The address specified by the global variable needs to escape the stack (See the project's .map file for the stack top address)

SRAM partition is optional because the MMU of the N32G05XRBQ7 only manages partition access to the main FLASH storage area. SRAM is actually shared by USER1, USER2, and USER3. Dividing the SRAM into multiple regions is only for the stability of program execution (preventing overlapping of global variable spaces in different partitions) and does not provide the function of "protecting data security in user SRAM". According to the actual application, the space of global variables can be allocated by users through mutual negotiation without dividing SRAM. In this example, USER1, USER2, and USER3 share 16KB SRAM.

After the user area is divided, the application programs of each user need to be downloaded to different address spaces. Therefore, the corresponding projects need to configure their respective section addresses to avoid program download failure or abnormal operation because the address space allocated by the program is inconsistent with the download address.

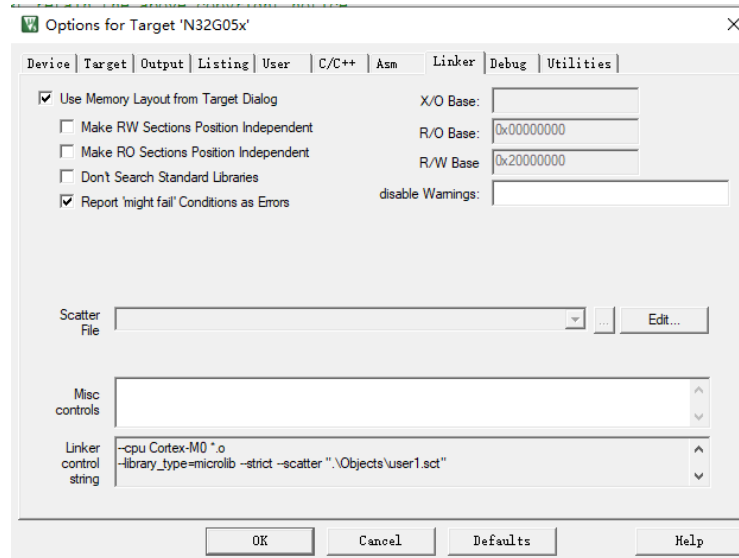
4.1.1 Sct distributed load file

The KEIL linker allocates each section address according to the configuration of the SCT distributed load file and generates the distributed load code, so the location of a section can be customized by modifying the SCT distributed load file.

- Select the SCT file generation method

SCT files can be automatically generated using MDK, or you can use user-defined SCT files. This selection can be configured through the MDK "Options for Target -> Linker->Use Memory Layout from Target Dialog" option, as shown in Figure 4-2

Figure 4-2 Choose how the SCT file is generated42



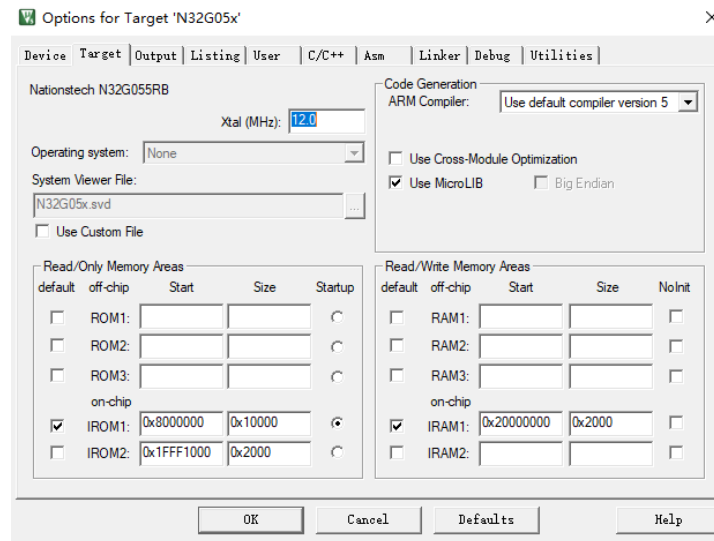
Select the "Use Memory Layout from Target Dialog" option (default for SDK) to generate the SCT file using the memory distribution configuration options of the "Options for Target -> Target" page. In this case, "Options for Target -> Linker-> Scatter File" is invalid. You cannot manually open the generated SCT File for editing. When the project construction is completed, MDK will generate a new SCT file to overwrite the old one.

If you need to manually edit the SCT file, uncheck the "Use Memory Layout from Target Dialog", specify the SCT file path in the options for "Options for Target -> Linker-> Scatter File" box. After that, clicking "Edit" will open the SCT file automatically, and users can edit the file manually.

■ Configure storage distribution through Target control

Select "Options for Target -> Linker->Use Memory Layout from Target Dialog" in MDK. On the "Options for Target -> Target" page, the memory distribution configuration takes effect automatically. The default configuration in the SDK is automatically loaded after selecting the chip model on the "Options for Target -> Device" page. After setting the FLASH partition, reset the memory configuration.

Figure 4-3 Target storage distribution configuration43



In this example, USER1 is used as an example. Figure 4-4 shows the storage distribution configuration on the Options for Target -> Target page. In the on-chip part, IROM1 starts at 0x08000000 and its size is 0x10000, which is exactly the start address and size of USER1's FLASH. If IRAM1 has a start address of 0x20000000 and a size of 0x2000, they are the start address and size of USER1's SRAM region respectively. In the figure, IROM1 and IRAM1 are checked by default, indicating that the current configuration information will be used. If this parameter is unchecked, the storage configuration information will not be used.

The projects of USER2 and USER3 can reset the memory configuration in a similar way. For details, refer to the configuration of the corresponding example projects.

The path of the SCT file generated by MDK through the Target memory distribution configuration in Figure 4-3 is ".Objects \ user1.sct "(default setting of SDK), and the content of the SCT file is shown in Figure 4-4. You can manually edit the Sct file by referring to the file format.

Figure 4-4 SCT file content4

```

; *****
; *** Scatter-Loading Description File generated by uVision ***
; *****

LR_IROM1 0x08000000 0x00010000 { ; load region size_region
ER_IROM1 0x08000000 0x00010000 { ; load address = execution address
    *.o (RESET, +First)
    * (InRoot$$Sections)
    .ANY (+RO)
    .ANY (+XO)
}
RW_IRAM1 0x20000000 0x00002000 { ; RW data
    .ANY (+RW +ZI)
}
}

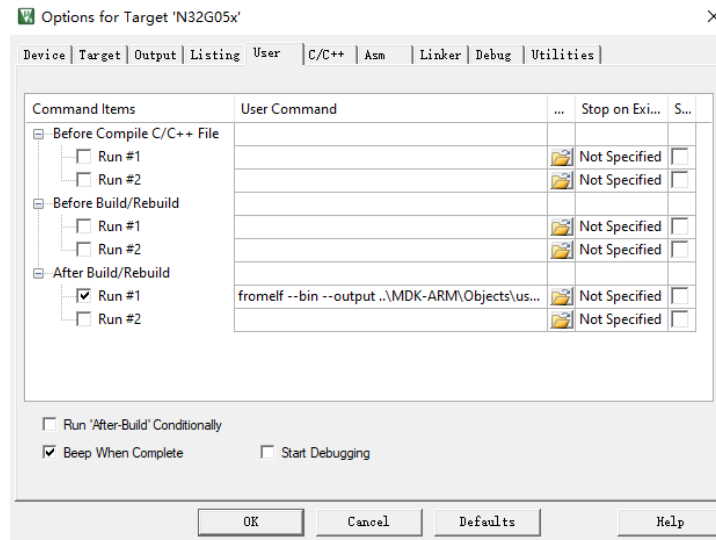
```

4. 2 Generating a bin file

To download the program through *Nations MCU Download Tool*, you need to download the bin file of the program. Here, the fromelf instruction is used to generate a bin file. Users can also write their own Python scripts and enter user instructions to execute the scripts.

On the configuration page of "Options for Target->User" of MDK, the "After Build/Rebuild" column is added to call fromelf tool to form the instruction to generate bin file (generate bin according to axf file), as shown in Figure 4-5

Figure 4-5 Interface for user configuration



The instruction to generate the bin file first calls the fromelf tool, followed by the tool's options, output file name, and input file name. If bin files and axf files are generated in the same folder "..\MDK-ARM\Objects", the user instruction of the sample project can be written as "fromelf --bin --output..\MDK-ARM\Objects\user1.bin ..\ MDK - ARM \ Objects \ user1.axf".

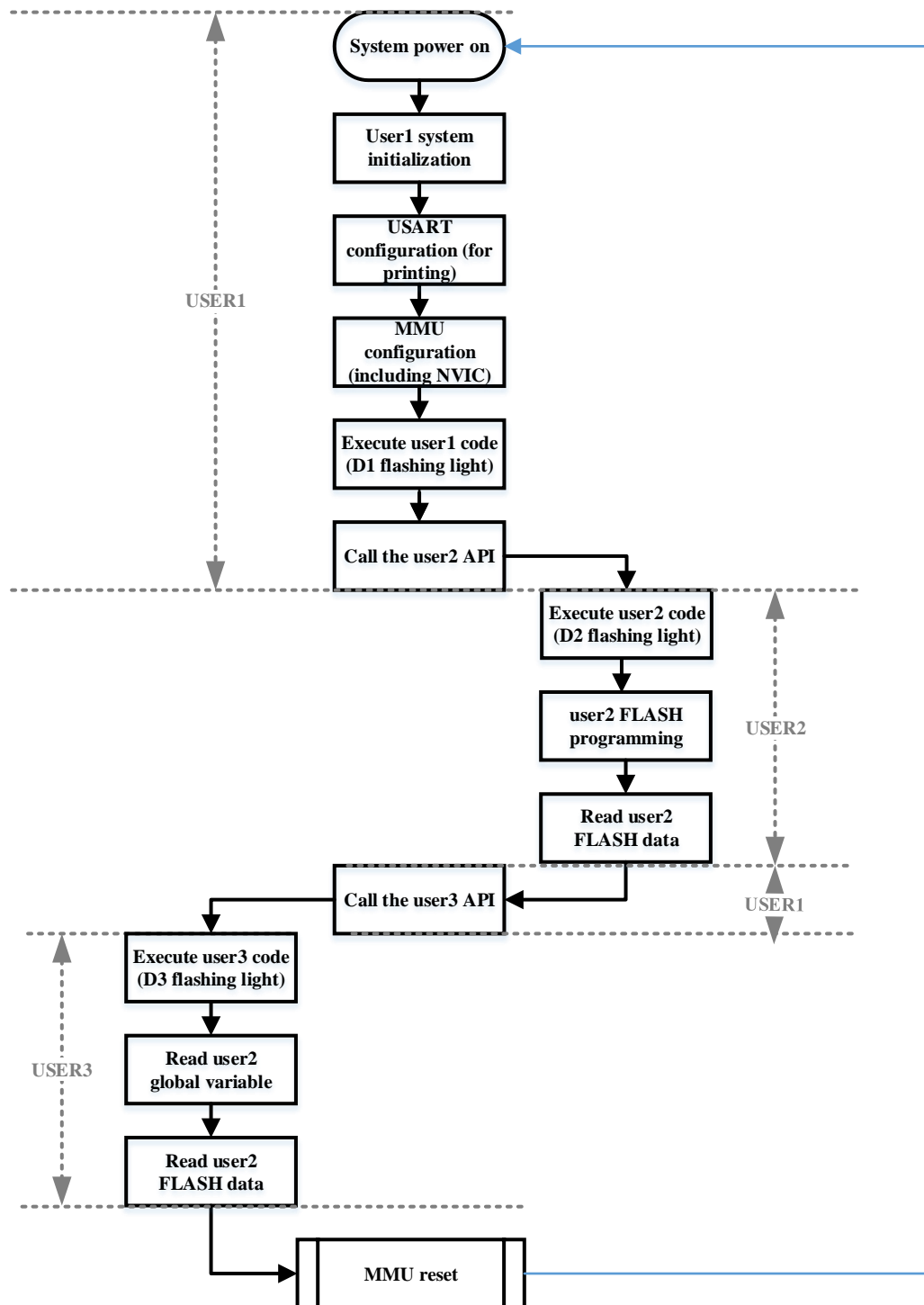
4. 3 Partition access operation

The sample projects for USER1, USER2, and USER3 work together to demonstrate mutual access between different partitions. Download the sample projects of USER1, USER2, and USER3 to the N32G05XRBQ7 chip respectively. After being powered on again, the chip with three partitions will execute the code according to the flow shown in Figure 4-6 (refer to the partition size configuration in section 4.1 "Section address configuration" for sample project). 4.1Chip program execution start address is 0x08000000, so USER1 as the end user is responsible for the control of the entire application process, including system initialization, stack processing, interrupt processing and other operations.

The MMU limits the read and write operations between FLASH partitions. The access between partitions is realized by invoking API. For example, USER2 and USER3 implement applications with certain functions (encapsulated in API form) respectively, and USER1 accesses the application functions of USER2 or USER3 by invoking the API. All unauthorized operations involving MMU (such as debugging interface/program reading or writing unauthorized, of reading or writing unauthorized interrupt vector table address , etc.) will trigger the MMU abnormal alarm and inform the user in time in the way of reset or interruption.

The following highlights three partition access operations: calling API across partitions, reading and writing data across partitions, and interrupt handling.

Figure 4-6 Example project execution



4.3.1 Call API

The cross-partition call API is essentially the execution of a program by jumping to a function at a specified location. Functions can be assigned addresses automatically by the compiler (see the project's .map file), or they can be assigned addresses by users of each partition (recommended). In API scenarios that provide multiple cross-partition access, specifying fixed addresses for functions is clearly advantageous. The "__attribute__" keyword in MDK can specify the address.

In this case, USER1 calls the API of USER2 and USER3, respectively. This section describes how USER1 invokes USER2 API for reference.

The FLASH of USER2 ranges from 0x0801_0000 to 0x0801_7FFF, and the SRAM ranges from 0x2000_2000 to 0x2000_2FFF. In the user2_demo.c of sample project user2, place function "void Test_User2(void)" at address 0x08016000 (see Figure 4-7).

Figure 4-7 Specifies the function address4

```
uint32_t test_data __attribute__((at(0x20002A00)));
void Test_User2(void) __attribute__((section(".ARM.__at_0x08016000")));

void Test_ProgramFlashWord(uint32_t Address, uint32_t Data)
{
}

void Test_InitData(void)
{
}

void Test_User2(void)
{
    uint32_t flash_write_data = 0x76543210;
    Test_InitData();
    /* USART Configuration */
    // log_init();
    /* Output a message on Hyperterminal using printf function */
    printf("\n\rHello! Here is USER2 Example!\n\r");

    /* LED2 Blinks */
    Test_LedBlink(LED2_PORT, LED2_PIN);

    /* Program USER2 FLASH */
    Test_ProgramFlashWord(0x08017800, flash_write_data);

    /* Read USER2 FLASH */
    printf("USER2 Get USER2 FLASH *0x08017800 = 0x%X\r\n", *((__IO uint32_t*)(0x08017800)));

    /* Read USER2 FLASH */
    printf("USER2 Get USER2 SRAM *0x20002A00 = 0x%X\r\n", *((__IO uint32_t*)(0x20002A00)));
}
```

USER2 provides the jump address of the function to other partition users so that they can jump to this address and call API functions. To facilitate co-development by multiple users, USER2 can use macros in the user2_demo.h file to define jump addresses and jump operations for functions (see Figure 4-8). After that, different users can get information about the jump to the application through the header file. The example project demonstrates the jump of a function without parameters, and users can further extend the API function definition (such as returning a function of a specified type with parameters, etc.).

Figure 4-8 Jump address and function pointer

```
44 typedef void (*pFunction)(void);
45
46 #define USER2_FUNC_ADDR (0x08016001)
47 #define API_FuncEntry2 ((pFunction)(USER2_FUNC_ADDR))
```

For USER1, you can choose to add user_2 demo. h to the example project user1 (renamed user_2 demo. api. h). Afterwards, the USER1 program can jump to USER2 to execute functions, such as flashing D2 lights, by calling the API "API_SuncExit2()".

4.3.2 Read and write data-MMU abnormal alarm

After the FLASH partition configuration takes effect, cross-partition data reading, FLASH programming, SRAM code accessing the user partition, DMA or debugging interface accessing the user partition will trigger the MMU exception alarm (The default alarm method is MMU reset, see section 4.3.3 "MMU Reset" for details). 4.3.3 The example projects for USER2 and USER3 demonstrate normal and abnormal data reading and writing, respectively.

In the user2_demo.c file of the example project LedBlink - user2, the example demo demonstrates that User2 reads and writes data in the owning partition area (SRAM or FLASH), as shown in Figure 4-7. Write the reversed value of the global variable test_data in USER2 SRAM to the position 0x0801_7800 specified by USER2 FLASH, and verify that the data written to address is correct. The above operations are routine operations, and the specific operation methods will not be described. It is important to note that the initial value of the global variable of USER2 may not be 0 because the example project of USER2 did not execute the startup process. Please initialize the global variable before using it.

USER3 can read and write USER2 SRAM. However, USER3 cannot write to USER2 FLASH or read data from USER2 FLASH due to the partition permission management function of the MMU. In USER3's example project USER3, the file user3_demo.c contains the sample demo code that lines 66 in Figure 4-9 will trigger an MMU abnormal reset alarm (the default).

Figure 4-9 USER3 reading data

45

```
void Test_User3(void) __attribute__((section(".ARM.__at_0x08019000")));

void Test_User3(void)
{
    /* Output a message on Hyperterminal using printf function */
    printf("\n\rHello! Here is USER3 Example\n\r");

    /* LED3 Blinks */
    Test_LedBlink(LED3_PORT, LED3_PIN);

    /* Read USER2 SRAM */
    printf("USER3 Get USER2 SRAM *0x20002A00 = 0x%X\r\n", *(__IO uint32_t*)(0x20002A00));

    /* Read USER2 FLASH */
    printf("USER3 Get USER2 FLASH *0x08017800 = 0x%X\r\n", *(__IO uint32_t*)(0x08017800));
}
```

4.3.3 Interrupt handling

There are two ways to trigger MMU abnormal alarms: reset (default) or interrupt. In this example, we will demonstrate MMU reset.

View the reset flag by printing the RCC ->CTRLSTS register.


```
void Test_User1(void)
{
    /* Output a message on Hyperterminal using printf function */
    printf("\n\rHello! Here is USER1 Example\n\r");

    printf("\n\rRCC_CTRLSTS Value: 0x%x\n\r", RCC->CTRLSTS);

    /* LED(PB0) Blinks */
    Test_LedBlink(LED1_PORT, LED1_PIN);

    /* Jump to API of USER2 */
    API_FuncEntry2();

    /* Jump to API of USER3 */
    API_FuncEntry3();

    printf("USER1 Example End\n\r");
}
```

Through testing, it will be found that USER3 has reset and the MMURSTF flag is set when reading USER2 data.

```
Hello! Here is USER1 Example

RCC_CTRLSTS Value: 0x18

Hello! Here is USER2 Example!

USER2 Get USER2 FLASH *0x08017800 = 0x76543210
USER2 Get USER2 SRAM *0x20002A00 = 0x1234567

Hello! Here is USER3 Example

USER3 Get USER2 SRAM *0x20002A00 = 0x1234567
U□

Hello! Here is USER1 Example

RCC_CTRLSTS Value: 0x1c
```

5 Conclusion

The FLASH can be divided into three regions (USER1, USER2 or USER3) by using the MMU embedded in the MCU chip of Nations, and the access control function is provided for each user region. It can not only protect internal memory attacks (such as mutual access between different user areas, SRAM access, etc.), but also resist some external attacks (such as debugging interface access, DMA access, etc.).

Users can set partitions and download programs through the Bootloader. Once the partition is successfully set, the user area division and permission management functions take effect immediately. In addition, the partition configuration can only be set once and cannot be reset. The operation is irreversible. These features enable the MMU to prevent unauthorized access to the FLASH and effectively protect data and code stored in the FLASH. Thus, it plays a security role in application scenarios such as copyright protection and sensitive data protection.

6 Version history

Version	Date	Modify
V1.0	2024.5.22	New document

7 Notice

This document is the exclusive property of Nations Technologies Inc. (Hereinafter referred to as NATIONS). This document, and the product of NATIONS described herein (Hereinafter referred to as the Product) are owned by NATIONS under the laws and treaties of the People's Republic of China and other applicable jurisdictions worldwide.

NATIONS does not grant any license under its patents, copyrights, trademarks, or other intellectual property rights. Names and brands of third party may be mentioned or referred thereto (if any) for identification purposes only.

NATIONS reserves the right to make changes, corrections, enhancements, modifications, and improvements to this document at any time without notice. Please contact NATIONS and obtain the latest version of this document before placing orders.

Although NATIONS has attempted to provide accurate and reliable information, NATIONS assumes no responsibility for the accuracy and reliability of this document.

It is the responsibility of the user of this document to properly design, program, and test the functionality and safety of any application made of this information and any resulting product. In no event shall NATIONS be liable for any direct, indirect, incidental, special, exemplary, or consequential damages arising in any way out of the use of this document or the Product.

NATIONS Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, "Insecure Usage".

Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, all types of safety devices, and other applications intended to support or sustain life.

All Insecure Usage shall be made at user's risk. User shall indemnify NATIONS and hold NATIONS harmless from and against all claims, costs, damages, and other liabilities, arising from or related to any customer's Insecure Usage.

Any express or implied warranty with regard to this document or the Product, including, but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement are disclaimed to the fullest extent permitted by law.

Unless otherwise explicitly permitted by NATIONS, anyone may not use, duplicate, modify, transcribe or otherwise distribute this document for any purposes, in whole or in part.