
使用MMU进行多用户场景下的FLASH分区保护

简介

在嵌入式产品研发过程中，有时会存在单个MCU内部需要多个用户分阶段进行应用软件开发场景，在此场景中，各用户的代码及数据可能出于版权或安全考虑，不方便公开给其它几个用户共享。那如何解决这类问题呢？

本文档主要针对国民技术MCU系列产品在上述应用场景，指导用户如何使用国民技术的MCU，通过内置的存储器管理单元（Memory Management Unit，简称MMU）实现FLASH主存储区的多用户区域划分及访问权限管理，从而解决多用户开发过程中的代码版权保护及数据安全问题。因此，可以广泛应用于各种版权保护、敏感数据和多用户代码保护等场景中。

本文档仅适应于内置MMU的国民技术MCU产品，目前支持的产品系列有N32A455系列、N32G452系列、N32G455系列、N32G457系列、N32G4FR系列、N32WB452系列、N32L43x系列、N32G43x系列和N32L40x系列产品。

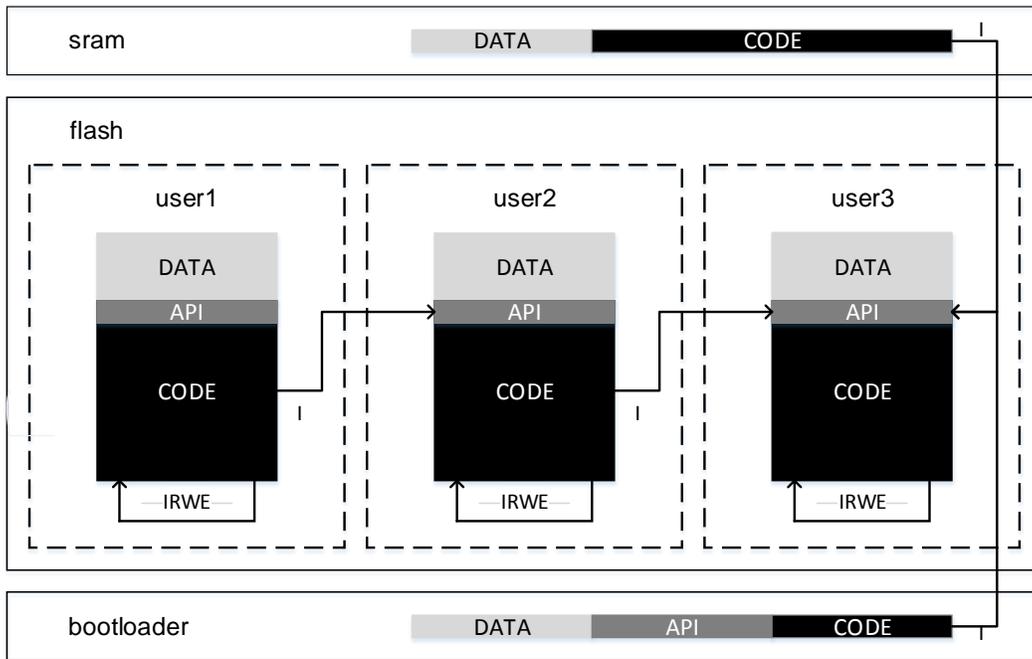
目录

1 分区保护实现机制	1
2 MMU 功能说明	2
2.1 用户区域划分	2
2.2 访问权限管理	3
3 操作说明	4
3.1 操作环境	4
3.2 操作步骤	4
3.2.1 设备进入 <i>Bootloader</i>	4
3.2.2 设备连接工具	4
3.2.3 配置分区	5
3.2.4 程序下载	6
3.2.4.1 通过调试接口下载	6
3.2.4.2 通过内置 <i>Bootloader</i> 下载	7
4 示例工程	11
4.1 SECTION 地址配置	11
4.1.1 <i>Sct</i> 分散加载文件	11
4.2 生成 BIN 文件	13
4.3 分区访问操作	14
4.3.1 调用 <i>API</i>	15
4.3.2 读写数据- <i>MMU</i> 异常报警	17
4.3.3 中断处理	17
5 结论	19
6 历史版本	20
7 声明	21

1 分区保护实现机制

通常MCU片内的闪存（FLASH）挂接在内存总线上，CPU可以无限制的访问FLASH内的任何区域。要实现对单颗MCU片内FLASH进行多个用户区域划分并保护，避免在片内不同用户通过CPU指令直接读取或修改其它用户区的FLASH内容。我们可以使用国民技术MCU内置的MMU，将FLASH主存储区的区域进行划分和设置访问权限，同时可保护各个应用存储区域内的代码与数据不被非法访问及篡改，并指示出存储器及受保护的寄存器的非法访问错误，所有越权操作都将触发MMU异常报警，从而实现多用户下的FLASH分区保护功能。

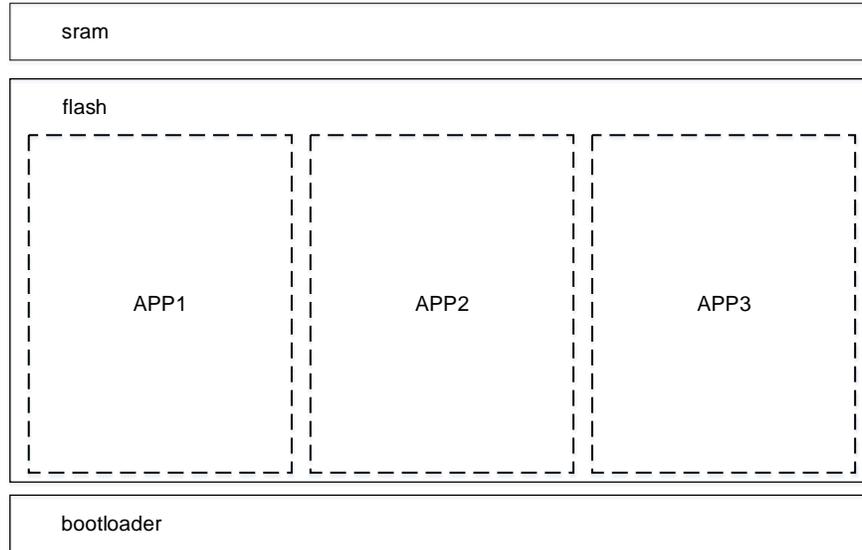
图1-1 MMU分区保护实现机制



2 MMU功能说明

MMU可实现FLASH主存储区的区域划分和访问权限管理，可为MCU的不同应用划分独立的存储空间（见图 2-1），并对访问权限进行管理。

图 2-1 存储器区域划分



2.1 用户区域划分

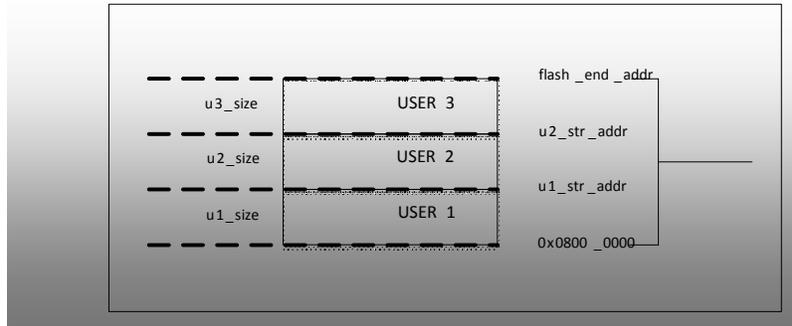
FLASH主存储区至多可划分为USER1（默认）、USER2和USER3三个区域。在实际使用中，用户区域划分有以下几种情况，各种情况的设置说明可参考表 2-1。

表 2-1 用户分区设置说明

情况描述	分区设置顺序	涉及权限管理的 FLASH 空间大小 ³			说明
		user1	user2	user3	
没有分区，默认为 user1 区域	-	-	-	-	user1 区域大小为 flash_size，没有访问权限管理功能
设置 1 个分区，不保留默认用户区域 ¹	user1	flash_size	-	-	
设置 1 个分区，保留默认用户区域(user1) ²	user3	-	-	user3_size	user1、user3 空间大小和为 flash_size，user1 没有访问权限管理功能
设置 2 个分区，不保留默认用户区域	user3→user1	user1_size	-	user3_size	user1、user3 空间大小和为 flash_size
设置 2 个分区，保留默认用户区域(user1)	user3→user2	-	user2_size	user3_size	user1、user2 和 user3 空间大小和为 flash_size，user1 没有访问权限管理功能
设置 3 个分区	user3→user2→user1	user1_size	user2_size	user3_size	user1、user2 和 user3 空间大小和为 flash_size
说明：					
(1) “不保留默认用户区域”指 FLASH 主存储区所有空间通过分区设置划分用户区域，各分区均涉及访问权限管理功能；					
(2) “保留默认用户区域”指不对 user1 进行分区设置，即保留 user1 区域开放、不涉及访问权限管理；					
(3) “涉及权限管理的 FLASH 空间”指的是已设置分区大小的 FLASH 主存储区空间。					

当FLASH主存储区划分为3个区域时，如图 2-2所示，分别为USER1（默认）、USER2和USER3，分区的颗粒度为16KB。

图 2-2 FLASH 主存储区域划分关系



FLASH主存储区的用户分区设置说明详见表 2-2。通过设置各用户分区的大小实现区域划分。分区设置属于静态设置，一旦设置，MCU每次上电会自动加载配置。特别指出，分区设置只能操作一次，且操作不可逆。

表 2-2 FLASH 主存储区分区设置说明

分区用户	存储区域	分区大小范围
USER1	0x0800_0000 ~ (0x0800_0000 + u1_size - 1)	16KB ¹ ~ (flash_size) KB
USER2	(0x0800_0000 + u1_size) ~ (flash_end_addr - u3_size)	0 KB ~ (flash_size - 32)KB
USER3	(flash_end_addr - u3_size + 1) ~ (flash_end_addr) ²	0 KB ~ (flash_size - 16)KB

说明：
 (1) 分区的颗粒度为 16KB；
 (2) 不同型号的 flash_end_addr 会有差异，对应 flash_size 也不同，flash_size 应为 USER1、USER2 和 USER3 区域大小之和，其大小为 (flash_end_addr - 0x0800_0000 + 1) KB。
注意：用户分区设置无法重置

2.2 访问权限管理

通过用户区域划分来管理FLASH主存储区各区域的操作权限，实现存储器访问控制，表 2-3提供了FLASH主存储区分区前后各用户区域的访问权限。

表 2-3 用户权限表

程序归属/ 访问方式	被访问区域					
	user1		user2		user3	
	是否分区		是否分区		是否分区	
	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

说明：
 (1) 分区前，USER1、USER2 和 USER3 视为同一个区域，所有 FLASH 空间默认为 USER1；
 (2) I 表示取址，R 表示读，W 表示写，E 表示擦除；
 (3) 写保护(WRP)使能与 MMU 分区的访问权限管理同级。
注意：如果不设置 USER1 区域大小（设置“操作步骤”见 3.2.1~3.2.3 小节），则 USER1 区域不具备访问权限管理功能。

3 操作说明

对MCU内置的FLASH主存储区进行分区操作，可通过国民技术提供的PC端的Nations MCU Download Tool工具实现，关于工具的使用方法可参考《Nations MCU 下载工具使用手册》。

3.1 操作环境

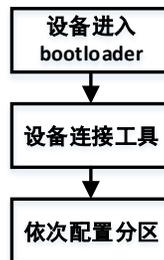
- 硬件环境：PC（系统Windows XP/7/10）、开发板N32A455全功能开发板 V1.0（含N32A455VEL7芯片）
- 目标设备：N32A455VEL7芯片
- 软件环境：下载工具(Nations MCU Download Tool.exe)、USB转串口驱动

注意：Bootloader支持USB接口或USART接口下载，使用前请确认已安装USB DFU驱动或USB转串口驱动。同时，确认目标设备已进入Bootloader状态，以便设备与下载工具正常连接。关于如何让目标设备进入Bootloader状态，可详细参考目标设备芯片的用户手册。本文档以N32A455VEL7芯片使用USART接口下载为例进行举例说明。

3.2 操作步骤

FLASH主存储区用户区域划分流程如图 3-1，以下详细介绍分区设置操作步骤。

图 3-1 分区设置步骤



3.2.1 设备进入Bootloader

N32G457VEL7 BOOT0引脚接VDD，PB2引脚接GND，芯片上电进入Bootloader。

注意：对于开发板N32G45XVL-STB V1.1，使用USART接口，则连接USB Debug Port接口供电。

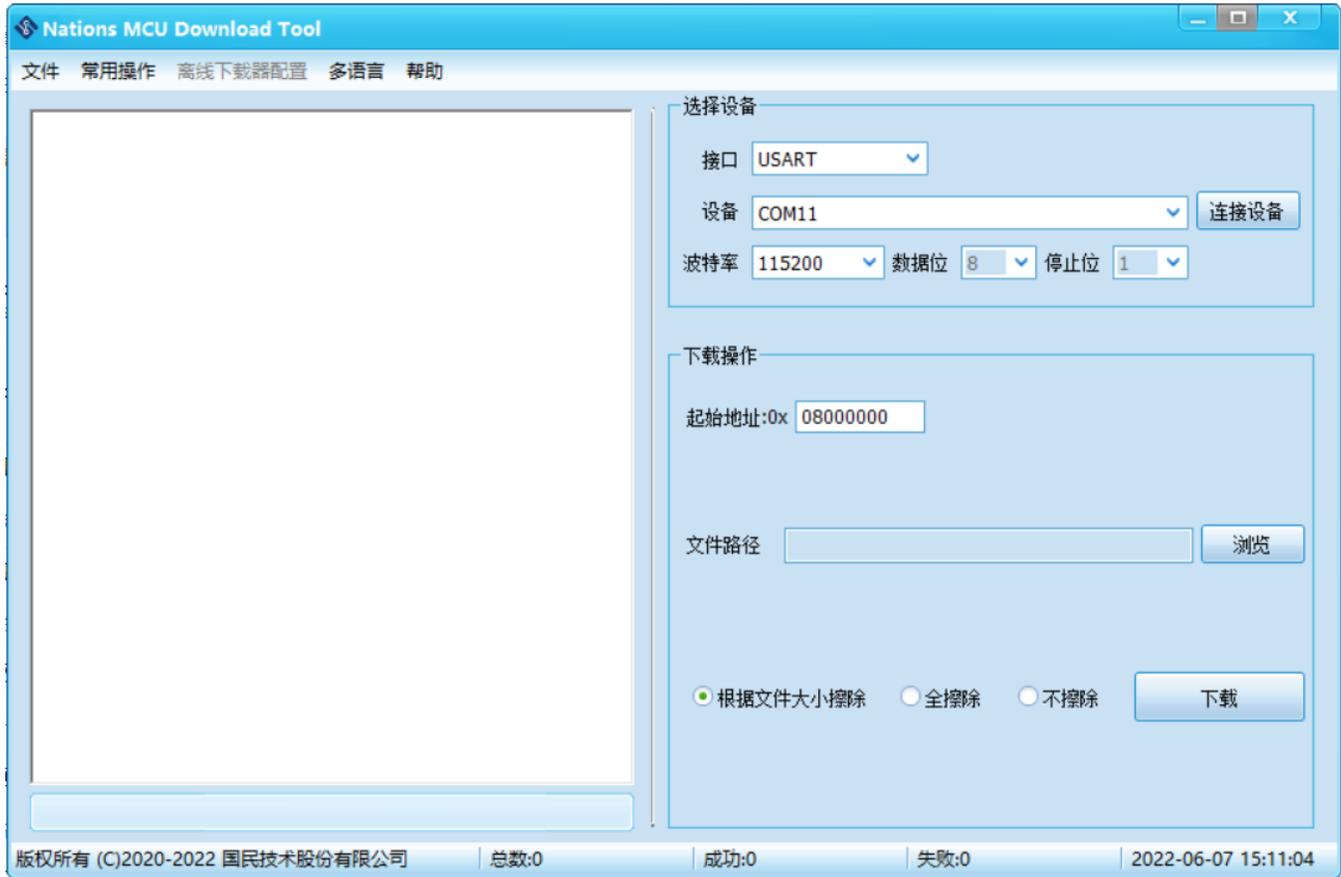
3.2.2 设备连接工具

双击NZDownloadTool.exe，打开下载工具，界面如图 3-2所示。此处，将重点关注“选择设备”区域。接口选择“USART”。选择匹配的端口号，作为设备。“COM端口号”可通过PC的“设备管理器”查看，图 3-2中连接MCU的串口被识别为“COM11”。同时，设置USART的波特率（可使用默认配置“115200”），单击“连接设备”按键，左边显示界面会提示“设备已连接”，此时，设备与工具已正常连接。

注意：N32A455VEL7中 Bootloader中USART1使用PA9与PA10分别作为TX与RX，请确保PA9与PA10与串口的

TX与RX已正确连接。

图 3-2 下载工具界面



3.2.3 配置分区

单击“常用操作”下拉菜单中的“配置分区”按键，弹出配置分区对话框，依次选择分区用户ID（USER1、USER2或USER3），并输入分区的FLASH大小（数值以分区颗粒度16KBs为单位设置）。如图 3-3所示，假设需为USER3划分128KB区域，则分区选择“USER3”，大小输入0x08。点击“配置分区”，确认配置分区，完成当前用户ID的区域划分。

图 3-3 配置分区界面



注意：

(1) 分区配置操作不可逆，请慎重操作；

(2) 如需设置多个分区，各用户可分别进入Bootloader配置，配置的大小、顺序等注意事项请参考表 2-1，操作不当可能导致配置失败。

3.2.4 程序下载

分区设置生效后，无法使用调试接口访问用户区域。因此，下载用户应用程序有以下两种方式：

- (1) 分区设置前，通过调试接口或Bootloader下载程序。
- (2) 分区设置后，通过内置的Bootloader下载程序（推荐）；

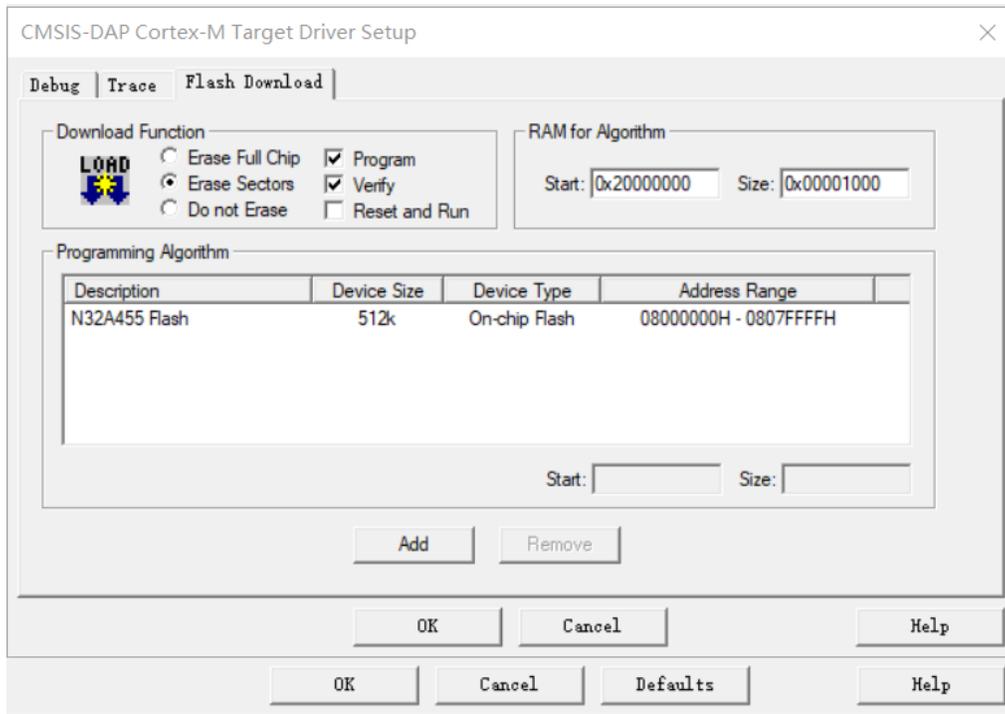
3.2.4.1 通过调试接口下载

如果未设置分区，N32A455VEL7还可以利用调试接口（JTAG或SWD）分别下载各用户的程序。具体的操作步骤与常规情况相同，不再赘述。

以下重点介绍调试接口下载各分区程序的注意事项：

- (1) 确保程序的FLASH和SRAM起始位置及大小设置的正确性，务必与分区配置情况相匹配（其中，FLASH和SRAM起始位置及大小设置请参考4.1.1小节“sct分散加载文件”）；
- (2) 为保证调试接口可分次下载多个程序，在MDK的“Options for Target->Debug ->Use: xx Debugger->Settings->Flash Download”页面中“Download Function”务必不能勾选“Erase Full Chip”（如图 3-4）。

图 3-4 Flash Download 界面



3.2.4.2 通过内置 Bootloader 下载

图 3-5 Bootloader 下载操作步骤



为了保证程序更新的安全，MCU内置的Bootloader还提供了分区认证和加密下载等功能（对应的使能和下载流程请参考《Nations MCU 下载工具使用手册》）。这里以最基本的程序下载流程进行介绍描述。如图 3-5，Bootloader下载操作大致分为4个步骤：设备进入Bootloader、设备连接工具、擦除FLASH和下载程序。

■ 程序下载具体流程如下：

1. 设备进入Bootloader及连接工具

如果设备已连接工具，可跳过该步骤，直接执行步骤3“擦除FLASH”；否则，可参考“操作步骤”3.2.1及3.2.2小节，依次执行步骤1和步骤2，确保MCU与下载工具正常连接。

2. 擦除FLASH

下载的FLASH区域如果是已擦除状态，则跳至步骤4执行；否则，在下载工具主界面单击“常用操作”区域中的“页擦除”按键，在弹出的会话框中，依次选择分区、输入擦除区域的页地址编号（起始页）和页数。如图3-6，如果擦除128KB的USER3区域，则分区选择“USER3”，N32G457VEL7的FLASH页大小为2KB，则USER3分区起始地址0x08060000对应的页编号为0x00C0，页数为0x0040，擦除地址范围为“0x08060000-0x0807FFFF”。确认擦除地址区间正确后，点击“擦除”按键，确认擦除FLASH操作及FLASH擦除成功，则擦除操作完成，关闭“擦除FLASH”会话框返回下载工具主界面。

图 3-6 擦除 FLASH 界面



3. 下载程序

单击“常用操作”下拉菜单中的“分区下载”选项，为USER1、USER2、USER3，依次勾选分区下载使能、选择文件路径（程序BIN所在路径）、输入起始地址（默认为各分区起始地址），核对正确后，点击“确认”，自动下载并返回下载工具主界面。（见图3-8）。

图 3-7 分区下载选择界面

Partition download

USER 1

Starting address: 08000000 Partition download enable

Download file: roject\LedBlink - user 1\MDK-ARM\Objects\LedBlink.bin

Partition authentication enablement

Encrypt download enablement Download file is ciphertext

USER 2

Starting address: 08040000 Partition download enable

Download file: roject\LedBlink - user 2\MDK-ARM\Objects\LedBlink.bin

Partition authentication enablement

Encrypt download enablement Download file is ciphertext

USER 3

Starting address: 08060000 Partition download enable

Download file: roject\LedBlink - user 3\MDK-ARM\Objects\LedBlink.bin

Partition authentication enablement

Encrypt download enablement Download file is ciphertext

图 3-8 下载界面



注意:

- (1) “分区设置”操作与“Bootloader下载程序”操作的先后顺序并没有强制要求。为保证程序的安全性，建议先设置分区，再更新程序；
- (2) 未设置分区且利用Bootloader下载程序，此时，擦除与下载时的所有分区都是默认区域USER1；设置分区后，请根据实际情况，配置选择分区USER1、USER2或USER3；
- (3) 下载起始地址需与程序设置的FLASH起始位置相匹配（可参考4.1.1小节“Sct分散加载文件”），否则程序可能会执行异常。

4 示例工程

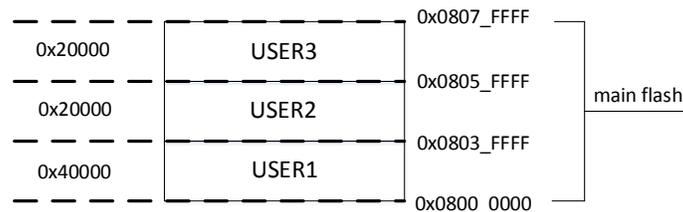
为了展示FLASH主存储区分区后程序的执行方式，将提供三个示例工程，分别作为USER1、USER2和USER3三个分区用户ID的工程。示例工程均是基于N32A455 SDK中GPIO模块的 LedBlink Demo扩展实现（路径：Nationstech.N32A455_Library\projects\n32a455_EVAL\examples\GPIO），主要是为了展示不同分区区域间的函数调用方法、正常或异常读取数据的不同效果以及中断处理方式。

以下小节将重点介绍工程的section地址配置、生成bin文件、用户分区间的访问操作等内容。

4.1 Section地址配置

以N32A455VEL7芯片的 512KB的FLASH主存储区大小为例，假设USER1、USER2、USER3三个用户区域大小分别为256KB、128KB和128KB。此时，FLASH主存储区的区域划分关系如图 4-1所示。各用户可根据各分区应用的实际代码量协商、划分FLASH主存储区。

图 4-1 Flash 主存储区区域划分关系示例



除了划分FLASH主存储区，为避免不同分区程序的全局变量存储空间冲突，同时也可以划分N32A455VEL7的 144KB SRAM空间，假设USER1、USER2、USER3三个用户SRAM大小分别为72KB、36KB和36KB。各用户的SRAM可存储对应程序中的全局变量。由于芯片程序执行的起始地址为0x08000000，USER1作为终端用户，同时负责处理堆栈与中断响应。所以USER1的SRAM还可用作堆栈空间。

SRAM区域划分是可选操作，原因是N32G457VEL7的MMU只管理FLASH主存储区的分区访问权限。SRAM实际由USER1、USER2、USER3三个用户共享使用。将SRAM划分为多块区域，只是出于程序执行的稳定性考虑（防止不同分区的全局变量空间重叠），并不提供“保护用户SRAM中数据安全”的功能。根据实际应用，也可以不划分SRAM，由用户相互协商分配全局变量的空间。

用户区域划分后，各用户的应用程序需要下载到不同的地址空间，因此对应的工程需要分别配置各自的section地址，以免因为程序分配的地址空间与下载地址不一致造成程序下载失败或者运行异常。

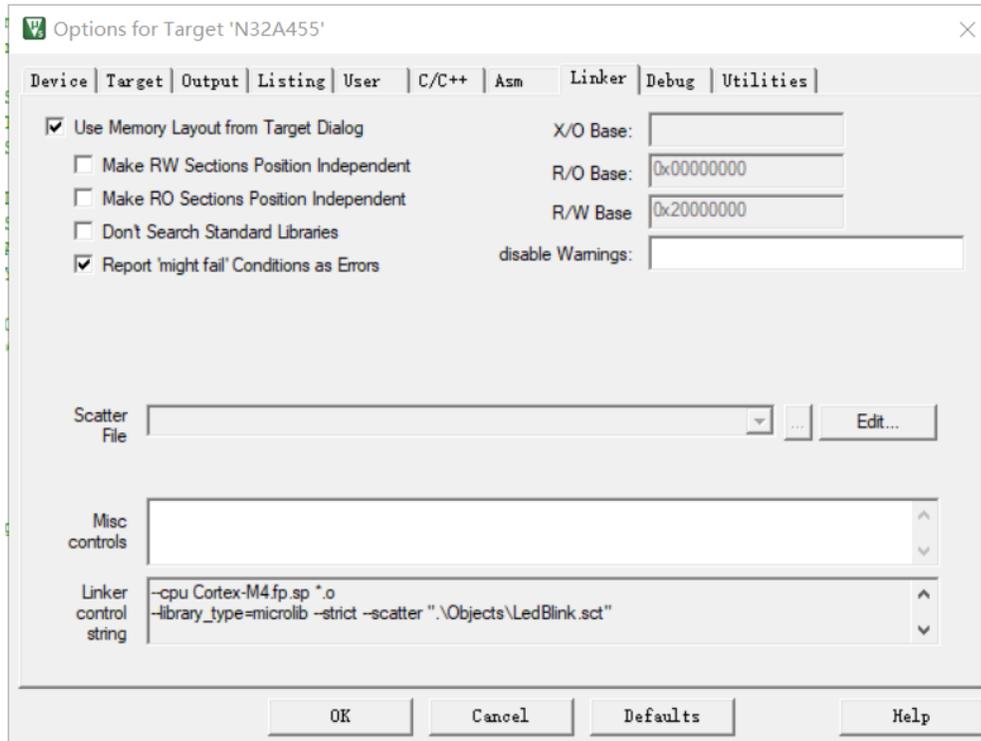
4.1.1 Sct分散加载文件

KEIL链接器根据sct分散加载文件的配置，分配各个section地址，生成分散加载代码，因此通过修改sct分散加载文件可以定制某section的存储位置。

■ 选择sct文件的生成方式

Sct文件可以使用MDK自动生成，也可以使用用户自定义的sct文件。通过MDK的“Options for Target -> Linker->Use Memory Layout from Target Dialog”选项，即可配置该选择，见图 4-2。

图 4-2 选择 sct 文件的产生方式



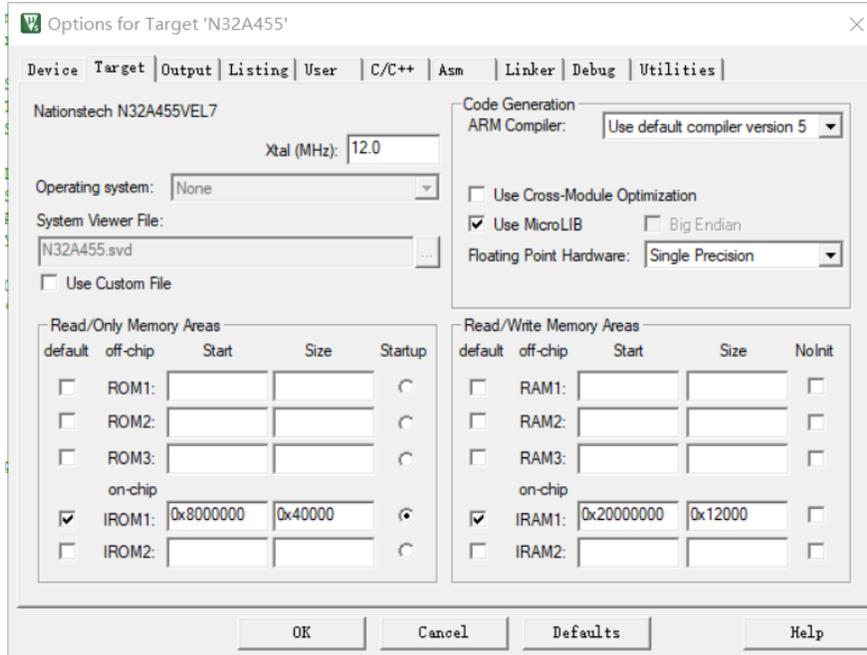
勾选“Use Memory Layout from Target Dialog”选项（SDK默认勾选），则使用“Options for Target -> Target”页面的存储器分布配置选项生成sct文件，此时“Options for Target -> Linker-> Scatter File”是失效的，无法手动打开生成的sct文件进行编辑。工程构建完成，MDK会生成新的sct文件覆盖旧文件。

如果需要手动编辑sct文件，则取消勾选“Use Memory Layout from Target Dialog”选项，同时在“Options for Target -> Linker-> Scatter File”框中指定sct文件的路径。之后，点击“Edit”则自动打开sct文件，用户可手动编辑该文件。

■ 通过Target控制配置存储器分布

勾选MDK的“Options for Target -> Linker->Use Memory Layout from Target Dialog”选项后，“Options for Target -> Target”页面存储器分布配置则自动生效。SDK中默认的配置是在“Options for Target -> Device”页面选择芯片型号后自动加载的，FLASH设置分区后，需重置存储器配置。

图 4-3 Target 存储器分布配置



以本例中USER1为例，工程的“Options for Target -> Target”页面的存储器分布配置如图4-4所示。其中，“on-chip”（片内存储器）部分IROM1 起始地址为 0x08000000，大小为 0x40000，正好是USER1的FLASH起始地址和大小；而IRAM1 起始地址为 0x20000000，大小为 0x12000，则分别是USER1的SRAM区域的起始地址与大小。图中默认已勾选IROM1 及 IRAM1，表示当前配置信息且会被使用；如果取消勾选，则该存储配置信息不会被采用。

而USER2与USER3的工程可以类似方式重置存储器配置，具体可参考对应示例工程的配置情况。

MDK 通过图4-3的Target存储器分布配置生成的sct文件的路径为“.\Objects\LedBlink.sct”（SDK默认设置），Sct文件内容如图 4-4。用户可参考该文件格式，手动编辑sct文件。

图 4-4 Sct 文件内容

```

1 ; *****
2 ; *** Scatter-Loading Description File generated by uVision ***
3 ; *****
4
5 LR_IROM1 0x08000000 0x00040000 { ; load region size_region
6 ER_IROM1 0x08000000 0x00040000 { ; load address = execution address
7 *.o (RESET, +First)
8 *(InRoot$$Sections)
9 .ANY (+RO)
10 .ANY (+XO)
11 }
12 RW_IRAM1 0x20000000 0x00012000 { ; RW data
13 .ANY (+RW +ZI)
14 }
15 }

```

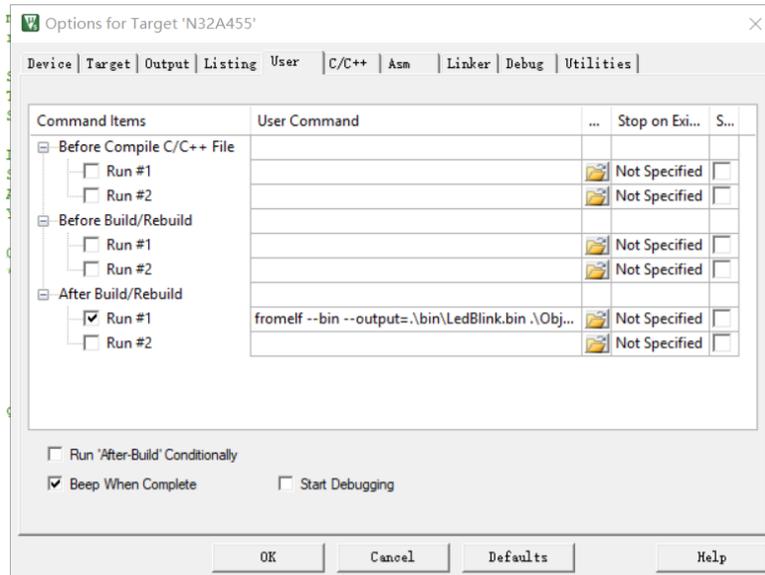
4.2 生成bin文件

通过Nations MCU Download Tool工具下载程序，需要下载程序的bin文件。因此，示例工程还需要设置生成bin文件。这里，介绍利用fromelf指令生成bin文件的方法。用户也可以自行编写 python 脚本，并输入用户指令执行该脚本。

在 MDK的“Options for Target->User”配置页面中，“After Build/Rebuild”一栏添加调用 fromelf工具形成生

成 bin 文件指令（根据 axf 文件生成 bin），见图 4-5。

图 4-5 User配置页面



生成 bin 文件指令首先调用fromelf 工具，随后是工具的选项及输出文件名、输入文件名。假如将bin文件和axf 文件生成在相同文件夹“..\MDK-ARM\Objects”内，则示例工程的用户指令可写为“fromelf --bin --output ..\MDK-ARM\Objects\LedBlink.bin ..\MDK-ARM\Objects\LedBlink.axf”。所以，在第3.2.4.2小节“通过内置Bootloader下载”的步骤4“下载程序”中，文件路径选项选中该路径下的bin文件即可。

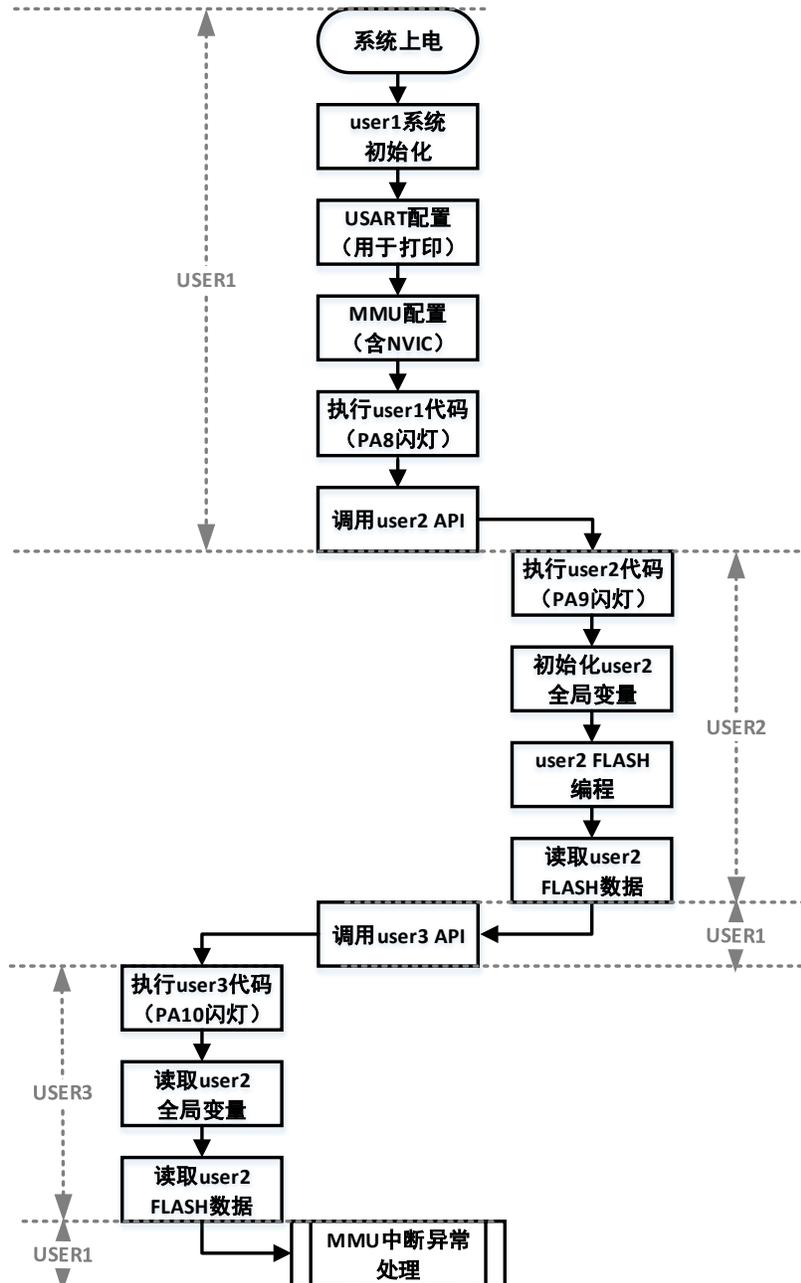
4.3 分区访问操作

USER1、USER2和USER3的示例工程配合演示了不同分区间的相互访问操作。将USER1、USER2和USER3的示例工程分别下载到N32A455VEL7芯片上，重新上电后，已设置3个分区的芯片将会按图 4-6展示的流程执行代码（示例工程参考4.1小节“Section地址配置”的分区大小配置）。芯片程序执行起始地址为0x08000000，因此USER1作为终端用户负责控制整个应用流程，包括系统初始化、堆栈处理、中断处理等操作。

MMU限制了FLASH不同分区间的读、写操作，分区间的相互访问通过调用API实现。例如，USER2与USER3各自实现具有一定功能的应用（以API形式封装），USER1则通过调用API访问USER2或USER3的应用功能。MMU同时也限制了分区用户重定位中断向量表操作(SCB->VTOR)，只有终端用户USER1具有设置SCB->VTOR的权限，且中断向量表的地址必须在USER1的FLASH空间内。所有涉及MMU的越权操作（调试接口/程序读或写越权、中断向量表地址读或写越权等），都将触发MMU异常报警，并以复位或者中断的方式及时告知用户。

以下将重点介绍三个分区访问操作：跨分区调用API、跨分区读写数据以及中断处理。

图 4-6 示例工程执行流程



4.3.1 调用API

跨分区调用API本质是通过跳转至指定位置的函数，执行程序。函数可以由编译器自动为其分配地址（详见工程的.map文件），也可以由各分区用户指定地址（推荐）。在提供多个跨分区访问功能的API场景中，为函数指定固定地址，显然更有优势。而MDK中“__attribute__”关键字可实现指定地址的功能。

本例中，USER1分别调用USER2和USER3的API。这里主要介绍“USER1调用USER2 API”的操作，以供参

考。

USER2的FLASH范围为0x0804_0000~0x0805_FFFF，SRAM范围为0x2001_2000~0x2001_AFFF。在示例工程LedBlink – user2中，将user2_demo.c文件中的示例demo（函数“void Test_User2(void)”）定义在0x08041000地址（见图 4-7）。

图 4-7 指定函数地址

```

87 void Test_User2(void) __attribute__((section(".ARM.__at_0x08041000")));
88
89 /**
90  * @brief USER2_Demo
91  *
92  */
93 void Test_User2(void)
94 {
95     /* USART Configuration */
96     // USART_Configuration();
97     /* Output a message on Hyperterminal using printf function */
98     printf("\n\rHello! Here is USER2 Example!\n\r");
99
100    /* LED(PA9) Blinks */
101    Test_LedBlink(GPIOA, GPIO_PIN_9);
102
103    /* Initialize the global variable of USER2 */
104    Test_InitData();
105
106    /* Program USER2 FLASH */
107    Test_ProgramFlashWord(0x08042000, ~test_data);
108
109    /* Read USER2 FLASH */
110    printf("Get USER2 FLASH Data = 0x%X\r\n", *((_IO uint32_t*) (0x08042000));
111 }

```

USER2将函数的跳转地址提供给其它分区用户，以便其通过跳转至该地址，实现API功能调用。为了方便多个用户共同开发，USER2可在user2_demo.h文件中利用宏定义函数的跳转地址以及跳转操作（如图 4-8所示）。之后，不同用户可通过头文件获知应用程序的跳转信息。

图 4-8 跳转地址和函数指针

```

50
51 typedef void (*pFunction)(void);
52
53 #define USER2_FUNC_ADDR (0x08041001)
54 #define API_FuncEntry2 ((pFunction)(USER2_FUNC_ADDR))
55

```

对于USER1，可以选择将user2_demo.h添加进示例工程LedBlink – user1中，或者移植USER2跳转相关的定义（如图 4-8所示，详见user1_demo.h）。之后，USER1的程序通过调用API“API_FuncEntry2();”即可跳转至USER2执行函数，实现PA9闪灯等操作。

示例工程演示的是无参数函数的跳转，用户可进一步扩展API函数定义（如有参数函数，返回指定类型函数等）。

注意：跨分区调用API本质并不限制跳转的函数。但有一特例需特别指出，无法跳转至复位函数。原因是startup_n32a455.s中Reset_Handler函数处理（如图 4-9）涉及有跨分区操作，会触发MMU异常报警。

图 4-9 Reset_Handler 函数定义

```

170
171 ; Reset handler
172 Reset_Handler PROC
173     EXPORT Reset_Handler           [WEAK]
174     IMPORT __main
175     IMPORT SystemInit
176     LDR R0, =SystemInit
177     BLX R0
178     LDR R0, =__main
179     BX R0
180 ENDF
181

```

4.3.2 读写数据-MMU异常报警

FLASH分区配置生效后，跨分区的数据读取和FLASH编程、SRAM代码访问用户分区、DMA1/DMA2或调试接口访问用户分区等操作均会触发MMU异常报警（中断报警方式及处理方法详见4.3.3小节“中断处理”）。USER2与USER3的示例工程分别演示了正常及异常读写数据两种情况。

在示例工程LedBlink - user2的user2_demo.c文件中，示例demo演示了USER2读写所属分区区域（SRAM或FLASH）内的数据，代码详见图 4-7，将USER2 SRAM中全局变量test_data的取反值写入USER2 FLASH指定位置0x0804_2000，并确认写入地址0x0804_2000的数据是否正确。以上操作均为常规操作，不再赘述具体操作方法。需特别指出，由于USER2的示例工程没有执行启动流程，因此USER2的全局变量初值不一定是0，用户使用全局变量前请注意初始化变量。

USER3可以读写USER2 SRAM。但由于MMU的分区权限管理功能，USER3却无法写USER2 FLASH或读取USER2 FLASH的数据。在USER3的示例工程LedBlink - user3中，文件user3_demo.c包含示例demo代码，如图 4-10中70行的操作将触发MMU异常复位报警（默认）。

图 4-10 USER3 读取数据

```

48  /**
49   * @brief USER3_Demo
50   *
51   */
52  void Test_User3(void)
53  {
54      uint32_t i;
55
56      /* USART Configuration */
57      // USART_Configuration();
58      /* Output a message on Hyperterminal using printf function */
59      printf("\n\rHello! Here is USER3 Example\n\r");
60
61      /* LED(PA10) Blinks */
62      Test_LedBlink(GPIOA, GPIO_PIN_10);
63
64      /* Read USER2 SRAM */
65      printf("Get USER2 SRAM Data = 0x%x\r\n", *(__IO uint32_t*)(0x20012100));
66
67      /* Read USER2 FLASH (at address 0x08042000) */
68      for(i = 0; i < 20; i++)
69      {
70          data[i] = *(__IO uint32_t*)(0x08042000 + i);
71      }
72  }

```

4.3.3 中断处理

由于USER2与USER3无法重定位中断向量表(SCB->VTOR)，USER2与USER3用户涉及的所有中断操作均由终端用户USER1处理。所以三个用户需要协作完成中断处理。USER2与USER3需将各自的中断处理告知USER1，并添加至USER1的程序中进行处理。如果USER2与USER3的中断服务函数涉及的操作需要保密，建议以4.3.1小节“调用API”介绍的方式，将中断处理内容封装为指定到固定位置的API，由USER1调用API处理相应的中断。

MMU异常报警的方式有两种：复位（默认）或中断。本例中，我们将演示MMU中断处理。在n32a455_mmu.c文件中，提供函数“void MMU_Init(MMU_ALARM_MODE mode)”，用于配置MMU异常报警方式。

示例工程LedBlink - user1中演示了如何使用MMU中断异常报警。User1_mmu_demo.c文件提供了MMU中断异

常报警的配置方法（示例代码如图 4-11），同时在user1_mmu_it.c文件中补充定义了MMU中断处理函数（见图 4-12）。USER1、USER2或USER3的任何越权操作均会触发调用该MMU中断处理函数。

图 4-11 MMU 中断异常报警配置

```

45 void NVIC_Configuration(void)
46 {
47     NVIC_InitType NVIC_InitStructure;
48
49     /* Enable MMU IRQChannel */
50     NVIC_InitStructure.NVIC_IRQChannel          = MMU_IRQn;
51     NVIC_InitStructure.NVIC_IRQChannelPreemptionPriority = 0;
52     NVIC_InitStructure.NVIC_IRQChannelSubPriority   = 0;
53     NVIC_InitStructure.NVIC_IRQChannelCmd         = ENABLE;
54     NVIC_Init(&NVIC_InitStructure);
55 }
56
57 /**
58  * @brief MMU_Config.
59  */
60 void MMU_Configuration(void)
61 {
62     /* NVIC Configuration */
63     NVIC_Configuration();
64
65     /* Configure mode of MMU alarm */
66     MMU_Init(MMU_INT_EN);
67 }

```

图 4-12 MMU 中断处理示例

```

136 /**
137  * @brief This function handles MMU interrupt request.
138  */
139 void MMU_IRQHandler(void)
140 {
141     NVIC->ICPR[2] |= (uint32_t)(1UL << ((uint32_t)16));
142     *((volatile unsigned long *) (MMU_BASE + 0x04)) = 0;
143     while(*((volatile unsigned long *) (MMU_BASE + 0x04)))
144     {
145     }
146 }
147
148 printf("MMU Alarms~~~\r\n");
149 }
150

```

5 结论

利用国民技术MCU芯片内置的MMU，可将其FLASH至多划分为3个区域（USER1、USER2或USER3），并为各个用户区域提供访问权限控制功能。它既能防护存储器内部的攻击（如不同用户区域间相互访问、SRAM访问等），也能抵御部分外部攻击（如调试接口访问、DMA访问等）。

用户通过Bootloader可以设置分区，也可以下载程序。一旦分区设置成功，用户区域划分及权限管理功能将及时生效。同时，分区配置只能设置一次、无法重置且操作不可逆。这些特点使得MMU可以防止对FLASH的非法访问，有效保护存储在FLASH中的数据和代码。从而，在版权保护、敏感数据保护等应用场景中发挥安全作用。

6 历史版本

版本	日期	备注
V1.0	2022.10.20	新建文档

7 声明

国民技术股份有限公司（下称“国民技术”）对此文档拥有专属产权。依据中华人民共和国的法律、条约以及世界其他法域相适用的管辖，此文档及其中描述的国民技术产品（下称“产品”）为公司所有。

国民技术在此并未授予专利权、著作权、商标权或其他任何知识产权许可。所提到或引用的第三方名称或品牌（如有）仅用作区别之目的。

国民技术保留随时变更、订正、增强、修改和改良此文档的权利，恕不另行通知。请使用者在下单购买前联系国民技术获取此文档的最新版本。

国民技术竭力提供准确可信的资讯，但即便如此，并不推定国民技术对此文档准确性和可靠性承担责任。

使用此文档信息以及生成产品时，使用者应当进行合理的设计、编程并测试其功能性和安全性，国民技术不对任何因使用此文档或本产品而产生的任何直接、间接、意外、特殊、惩罚性或衍生性损害结果承担责任。

国民技术对于产品在系统或设备中的应用效果没有任何故意或保证，如有任何应用在其发生操作不当或故障情况下，有可能致使人员伤亡、人身伤害或严重财产损失，则此类应用被视为“不安全使用”。

不安全使用包括但不限于：外科手术设备、原子能控制仪器、飞机或宇宙飞船仪器、所有类型的安全装置以及其他旨在支持或维持生命的应用。

所有不安全使用的风险应由使用人承担，同时使用人应使国民技术免于因为这类不安全使用而导致被诉、支付费用、发生损害或承担责任时的赔偿。

对于此文档和产品的任何明示、默示之保证，包括但不限于适销性、特定用途适用性和不侵权的保证，国民技术可在法律允许范围内进行免责。

未经明确许可，任何人不得以任何理由对此文档的全部或部分进行使用、复制、修改、抄录和传播。