使用指南

UG_N32G401 系列 MCU BOOT 接口指令使用指南

简介

使用指南主要描述 N32G401 系列 MCU 的 BOOT 接口指令，便于使用国民技术 BOOT Loader 进行下载开发。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

目录

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

1. BOOT简述

芯片的固件程序即 BOOT 主要提供用户程序下载，API 等功能。

本文档详细描述了 N32G401 系列芯片 BOOT 的功能、实现及使用介绍。N32G401 系列芯片的 FLASH 存储区最大为 64KB。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

1.1 BOOT功能定义

◆ 用户程序下载功能

- 支持 USART（USART1，使用 GPIO 为 PA9-TX、PA10-RX，波特率协商）；
- 支持下载数据 CRC32 校验；
- 支持加密下载（AES-128 ECB）；
- 支持 FLASH 分区和分区擦除下载时密钥认证；
- 支持分区密钥更新；
- 支持上电 BOOT 自校验；
- 支持软件复位芯片。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

2. BOOT流程及命令处理

N32G401 系列芯片的固件程序 BOOT，支持通过 USART 接口下载用户程序和数据。下面阐述相关命令处理流程。

2.1. 命令及数据结构

2.1.1. 命令列表

Table2-1 命令定义

命令名称	键值	说明
CMD_SET_BR	0x01	设置串口波特率（仅使用串口时有效）
CMD_GET_INF	0x10	读取芯片型号索引、BOOT 版本号、芯片 ID
CMD_GET_RNG	0x20	获取随机数
CMD_KEY_UPDATE	0x21	更新加密下载密钥或者分区认证密钥
CMD_FLASH_ERASE	0x30	擦除 FLASH
CMD_FLASH_DWNLD	0x31	下载用户程序到 FLASH
CMD_DATA_CRC_CHECK	0x32	CRC 校验下载用户程序
CMD_OPT_RW	0x40	读取/配置选项字节（包含了读保护等级、FLASH 页写保护、Data0/1 配置、USER 配置）
CMD_USERX_OP	0x41	获取分区 USERX 大小，配置分区 USERX 大小
CMD_SYS_RESET	0x50	系统复位

2.1.2. 数据结构

这里介绍下文阐述中的一些约定，其中，“<>”代表必须包含的字段，“()”代表根据参数不同包含的字段。

上下层指令数据结构

1、上层指令结构：

<CMD_H + CMD_L + LEN + Par> + (DAT)。

CMD_H 代表一级命令字段，CMD_L 代表二级命令字段；LEN 代表发送数据长度；Par 代表 4 个字节命令参数；DAT 代表上层指令往下层发送的具体数据；

2、下层应答结构：

< CMD_H + CMD_L + LEN > + (DAT) + <CR1+CR2>。

CMD_H 代表一级命令字段，CMD_L 代表二级命令字段，下层的命令字段和对应上层

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

的命令字段相同；LEN 代表发送数据长度；DAT 代表下层向上层应答的具体数据；CR1+CR2 代表向上层返回的指令执行结果，若上层发送命令一级、二级命令字段不属于任何命令，BOOT 回复 CR1=0xBB，CR2 = 0xCC。

串口支持的命令数据结构：

1、上位机下发上层指令：

STA1 + STA2 + {上层指令结构} + XOR。

STA1 和 STA2 是串口发送命令的起始字节，STA1=0xAA，STA2=0x55。用于芯片识别上位机发送串口数据流。

XOR 代表之前命令字节的异或运算值（STA1 + STA2 + {上层指令结构}）。

2、上位机接收下层应答：

STA1 + STA2 + {下层应答结构} + XOR。

STA1 和 STA2 是串口发送命令的起始字节，STA1=0xAA，STA2=0x55。用于上位机识别芯片发送串口数据流

XOR 代表之前命令字节的异或运算值（STA1 + STA2 + {下层应答结构}）。

2.2. 命令说明

2.2.1. CMD_SET_BR

该命令用于修改串口波特率。

上层指令：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x01 一级命令字段							
1(CMD_L)	0x00 二级命令字段							
2~3(LEN)	发送数据长度：0x00,0x00							
4~7(Par)	Par[0~3]：设置波特率参数							
(DAT)	无							

- Par[0~3]，串口波特率协商设置值可以设定最大，设定范围为 2.4Kbps～4Mbps，默

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

认波特率为 9600bps；

- 保留值：0x00；

底层应答：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x01 一级命令字段							
1(CMD_L)	0x00 二级命令字段							
2~3(LEN)	发送数据长度：0x00,0x00							
(DAT)	无							
4(CR1)	状态字节 1							
5(CR2)	状态字节 2							

- 状态字节(CR1、CR2)根据命令执行情况分为：
  1. 返回成功：状态标志位(0xA0、0x00)。
  2. 返回失败：状态标志位(0xB0、0x00)。

下面是波特率协商支持的波特率值(√ 表示支持，/ 表示不支持)：

时钟参数 (MHz)		波特率															
		2400	4800	9600	14400	19200	38400	57600	115200	128000	256000	576000	923076	1000000	2000000	3000000	4000000
HSE	4	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	6	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/
	8	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	16	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
	24	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/
	32	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
HSI		√	√	√	√	√	√	√	√	√	√	√	√	/	/	/	/

2.2.2. CMD_GET_INF

该命令提供的功能是读取 BOOT 版本号、芯片型号索引、芯片 ID、芯片系列化信息共 4 种信息。

上层指令：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x10 一级命令字段							

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

1(CMD_L)	0x00 二级命令字段
2~3 (LEN)	发送数据长度
4~7(Par)	保留
(DAT)	无

- 保留值：0x00。
- LEN 发送数据长度：0x00(LEN[0])、0x00(LEN[1])，LEN = LEN[0] +(LEN[1]<<8)。

底层应答：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x10 一级命令字段							
1(CMD_L)	0x00 二级命令字段							
2~3 (LEN)	数据长度							
4~54(DAT)	BOOT 版本号、芯片型号索引、芯片 ID							
55(CR1)	状态字节 1							
56(CR2)	状态字节 2							

- 过程字节(CMD_H)和上层指令中的(CMD_H)对应。
- LEN 是数据长度：0x33(LEN[0])、0x00(LEN[1])，LEN = LEN[0] + (LEN[1]<<8)。
- DAT[0]：0x05，芯片型号索引
- DAT[1]：0xXY，BOOT 版本号(BCD 码)

  0x10：指示 BOOT 使用的命令集版本，表示使用 V1.0 的命令集版本。
- DAT[2]：BOOT 命令集版本
- DAT[3~50] 48Byte
  1. DAT[3~18]：16Byte UCID（UCID 的详细定义见用户手册）；
  2. DAT[19~30]：12Byte Chip ID(UID) （UID 的详细定义见用户手册）；
  3. DAT[31~34]：4Byte DBGMCU_IDCODE（DBGMCU_IDCODE 的详细定义见用户手册）；
  4. DAT[35~50]：16Byte 芯片型号；
- 状态字节(CR1、CR2)根据命令执行情况分为：
  1. 返回成功：状态标志位(0xA0、0x00)。
  2. 返回失败：状态标志位(0xB0、0x00)。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

2.2.3. CMD_KEY_RNG

获取用户需校验所需密钥的随机数。

上层指令：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x20 一级命令字段							
1(CMD_L)	0x00 二级命令字段							
2~3(LEN)	发送数据长度							
4~7(Par)	保留							
(DAT)	无							

- 保留值：0x00；
- LEN 发送数据长度：0x00(LEN[0])、0x00(LEN[1])，LEN＝LEN[0]＋(LEN[1]<<8)。

底层应答：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x20 一级命令字段							
1(CMD_L)	0x00 二级命令字段							
2~3(LEN)	发送数据长度							
4~19(DAT)	16Bytes 的伪随机数							
20(CR1)	状态字节 1							
21(CR2)	状态字节 2							

- LEN 发送数据长度：0x10(LEN[0])、0x00(LEN[1])，LEN＝LEN[0]＋(LEN[1]<<8)。
- 16Byte 的伪随机数由软件算法生成。
- 状态字节(CR1、CR2)根据命令执行情况分为：
  1. 返回成功：状态标志位(0xA0、0x00)。
  2. 返回失败：状态标志位(0xB0、0x00)。

2.2.4. CMD_KEY_UPDATE

用户可以对加密下载密钥和分区认证密钥更新，更新前需要使用 CMD_KEY_RNG 获取随机数，随机数用于上位机生产 16Bytes 的旧密钥认证值，再通过 CMD_KEY_UPDATE

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

等命令发送给 BOOT，BOOT 通过该认证值认证旧密钥是否正确，由此来确认是否更新密钥。新的密钥需要用旧密钥解密。

上层指令：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x21 一级命令字段							
1(CMD_L)	二级命令字段：密钥索引 ID							
2~3(LEN)	发送数据长度							
4~7(Par)	保留值：0x00							
8~55(DAT)	DAT[0~15]：16Bytes 的旧密钥认证值							
	DAT[16~31]：16Bytes 的新密钥加密值							
	DAT[32~47]： CRC32 校验加密值 4Bytes 的(旧密钥+新密钥值)CRC32 校验值 + 12Bytes 填充值 0x00 再将 16Bytes 的数据用旧密钥加密							

- CMD_L：代表需要更新的密钥索引 ID

    1. ID(0x00~0x01)：密钥索引 ID，0x00 代表分区 1，0x01 代表分区 3。

- LEN 发送数据长度：0x30(LEN[0])、0x00(LEN[1])，LEN＝LEN[0]＋(LEN[1]<<8)。
- 保留值：0x00。
- DAT[32~47]：CRC32 校验值。
- DAT[0~15]：上位机用 CMD_KEY_RNG 获取的 16 位随机数和旧密钥生成的认证值。
- DAT[16~31]：用旧密钥加密的新密钥，BOOT 用旧密钥解密后再保存新密钥。

底层应答：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x21 一级命令字段							
1(CMD_L)	二级命令字段：密钥 ID							
2~3(LEN)	发送数据长度							
(DAT)	1byte，更新次数最大 12 次							
4(CR1)	状态字节 1							
5(CR2)	状态字节 2							

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

- LEN 发送数据长度：0x01(LEN[0])、0x00(LEN[1])，LEN＝LEN[0]＋(LEN[1]<<8)。
- DAT[0]：1byte，更新次数最大 12 次，两个分区共享次数，返回 0x0D 时不能再更新了，第一次是返回 0x02。
- 状态字节(CR1、CR2)根据命令执行情况分为：
  1. 返回成功：状态标志位(0xA0、0x00)
  2. 返回失败：状态标志位(CR1、CR2)

  (1)、(0xB0、0x00)：返回失败；

  (2)、(0xB0、0x10)：密钥索引 ID 范围错误；

  (3)、(0xB0、0x11)：新密钥 CRC 校验错误；

  (4)、(0xB0、0x20)：旧密钥认证失败；

  (5)、(0xB0、0x3F)：更新管理信息失败；

2.2.5. CMD_FLASH_ERASE

BOOT 提供以页为单位擦除 FLASH 的功能，认证擦除前需要使用 CMD_KEY_RNG 获取随机数，擦除页地址编号和和页数由用户提供，擦除的 FLASH 空间不能超过整个 FLASH 空间，且至少擦除 1 个页(512Byte)。

上层指令：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x30 一级命令字段							
1(CMD_L)	0x00 二级命令字段							
2~3(LEN)	发送数据长度(0)							
4~7(Par)	页地址编号 2 字节：0~255 页数 2 字节:1~256							
8~23(DAT)	DAT[0:15]：16 字节 USER1/3 分区认证的密钥认证值							

- CMD_L：擦除分区号
  1. 0x00=USER1
  2. 0x02=USER3
- LEN 发送数据长度：0x10(LEN[0])、0x00(LEN[1])，LEN＝LEN[0]＋(LEN[1]<<8)。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

- 擦除地址和范围由 Par 字段中的 4 个字节构成

  Par[0~1]：页地址编号 2 字节(0~255)

  页地址编号 = Par [0] + Par [1]<<8；

  Par[2~3]：页数 2 字节(1~256)

  页数 = Par [2] + Par [3]<<8；

  0 号页首地址为 0x0800_0000，以后的页地址编号加 1，首地址累加 0x800。

  比如:

  1 号页首地址为 0x0800_0000 + 1*0x800 = 0x0800_0800

  2 号页首地址为 0x0800_0000 + 2*0x800 = 0x0800_1000

  整个擦除的地址范围

  比如：页地址编号为 0x01，页数为 0x02

  则擦除的地址范围：

  (0x0800_0000 + 1*0x800) ~ (0x0800_0000 + 1*0x800 + 2*0x800)

  即（页地址编号的首地址） ~ （页地址编号的首地址 + 页数*页的大小）

- DAT[0:15]，16 字节分区认证的密钥认证值：

  当没有启用分区认证时，可以输入任意值，BOOT 程序不会用到该认证值；

底层应答：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x30 一级命令字段							
1(CMD_L)	二级命令字段：擦除区域							
2~3(LEN)	发送数据长度							
(DAT)	无							
4(CR1)	状态字节 1							
5(CR2)	状态字节 2							

- LEN 发送数据长度：0x00(LEN[0])、0x00(LEN[1])，LEN = LEN[0] + (LEN[1]<<8)。
- 状态字节(CR1、CR2)根据命令执行情况分为：
  1. 返回成功：状态标志位(0xA0、0x00)。
  2. 返回失败：状态标志位(CR1, CR2)。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

(1)、(0xB0、0x00)：返回失败；

(2)、(0xB0、0x20)：密钥认证失败；

(3)、(0xB0、0x30)：擦除 FLASH 页被 RDP 保护；

(4)、(0xB0、0x31)：擦除 FLASH 页被 WRP 保护；

(5)、(0xB0、0x32)：擦除 FLASH 页被分区保护；

(6)、(0xB0、0x33)：擦除 FLASH 页范围跨分区；

(7)、(0xB0、0x34)：擦除 FLASH 地址范围越界（指超出整个 FLASH 大小）；

(8)、(0xB0、0x37)：擦除 FLASH 失败。

(9)、(0xB0、0x3F)：更新管理信息失败；

2.2.6. CMD_FLASH_DWNLD

该命令提供用户下载代码到指定 FLASH 中，认证下载、加密下载或者认证加密下载前需要使用 CMD_KEY_RNG 获取随机数。数据长度必须 16 字节对齐（不足上位机自动补 0x00），都由上层命令提供。对于分区认证加密下载时，需要提供分区号。加密下载的数据需要通过加密下载密钥（即对应分区认证的密钥）对传输的数据解密成明文再写入 FLASH。

上层指令：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x31 一级命令字段							
1(CMD_L)	二级命令字段：下载分区号							
2~3(LEN)	发送数据长度							
4~7(Par)	下载 FLASH 的起始地址							
8~23(DAT)	DAT[0:15]：16 字节 USER1/3 分区认证的密钥认证值							
24~(24+N)(DAT)	DAT[16~16+N]：下载的具体数据							
(24+N+1)~(24+N+4)(DAT)	DAT[16+N+1~16+N+4]：数据的 4Byte CRC32 校验值							

- CMD_L：下载分区号
  1. 0x00=USER1；
  2. 0x02=USER3;
- LEN 发送数据长度：0xXX(LEN[0])、0xXX(LEN[1])，LEN = LEN[0] + (LEN[1]<<8)
- Par[0~3]：下载 FLASH 的起始地址，合成规则为 Address = Par[0] | Par[1]<<8 |

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

Par[2]<<16 | Par[3]<<24。

- DAT[0~15]：16 字节分区认证的密钥认证值，**加密下载的密钥和分区认证的密钥是同一个!!!**：

  1. 如果没有使能分区认证时，可以输入为全 0x00。

- DAT[16~16+N]：下载的具体数据，数据总个数为 N+1

  USART：最大 128 个字节，16<=N+1<=144，N+1 必须为 16 的倍数。

- DAT[16+N+1~16+N+4]：非加密数据的 4Byte CRC32 校验值

底层应答：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x31 一级命令字段							
1(CMD_L)	二级命令字段：下载分区号							
2(LEN)	发送数据长度							
(DAT)	无							
3(CR1)	状态字节 1							
4(CR2)	状态字节 2							
5(XOR)	异或运算结果							

- LEN 发送数据长度：0x00(LEN[0])、0x00(LEN[1])，LEN＝LEN[0]＋(LEN[1]<<8)。
- 状态字节(CR1、CR2)根据命令执行情况分为：

  1. 下载成功：状态标志位(0xA0、0x00)。
  2. 下载失败：状态标志位(CR1, CR2)。

  (1)、(0xB0、0x00)：返回失败；

  (2)、(0xB0、0x20)：密钥认证失败；

  (3)、(0xB0、0x21)：密钥认证失败次数超过限制；

  (4)、(0xB0、0x30)：下载 FLASH 地址被 RDP 保护；

  (5)、(0xB0、0x31)：下载 FLASH 地址被 WRP 保护；

  (6)、(0xB0、0x32)：下载 FLASH 地址被分区保护；

  (7)、(0xB0、0x33)：下载 FLASH 地址范围跨分区；

  (8)、(0xB0、0x34)：下载 FLASH 地址范围越界（指超出整个 FLASH 大小）；

  (9)、(0xB0、0x35)：下载 FLASH 起始地址不是 16 字节对齐；

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

(10)、(0xB0、0x36)：下载 FLASH 数据长度不是 16 的倍数；

(11)、(0xB0、0x37)：编程 FLASH 失败；

(12)、(0xB0、0x3F)：更新管理信息失败；

2.2.7. CMD_DATA_CRC_CHECK

该命令用于校验下载数据是否正确，考虑到下载速度的因素和下载失败概率比较小，所以采用数据下载完成后统一进行 CRC 校验，上层指令需提供下载数据的 CRC 值和校验起始地址以及校验长度。CRC 校验前需要使用 CMD_KEY_RNG 获取随机数。

上层指令：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x32 一级命令字段							
1(CMD_L)	二级命令字段：校验分区号							
2~3(LEN)	发送数据长度							
4~7(Par)	32bit CRC 校验值							
8~23(DAT)	DAT[0~15]：16 字节 USER1/3 分区认证的密钥认证值							
24~27(DAT)	DAT[16~19]：校验起始地址							
28~31(DAT)	DAT[20~23]：校验长度(单位：字节，长度最小 2KB)							

- CMD_L：校验分区号

  1: 0x00=USER1；

  2: 0x02=USER3;

- LEN 发送数据长度：0x18(LEN[0])、0x00(LEN[1])，LEN = LEN[0] + (LEN[1]<<8)；

- Par[0~3]：32bit CRC 校验值，其合成规则为 CRC32 = Par[0] | Par[1]<<8 | Par[2]<<16 | Par[3]<<24；

- DAT[0:15]：分区认证的密钥认证值；

- DAT [16~19]：校验起始地址，其合成规则为 Address = DAT[16] | DAT[17]<<8 | DAT[18]<<16 | DAT[19]<<24，Address 只能是在 FLASH 范围内；

- DAT [20~23]：校验长度，其合成规则为 CRC_LEN = DAT[20] | DAT[21]<<8 | DAT[22]<<16 | DAT[23]<<24，CRC_LEN 只能是在有效范围内，长度大于 2KB，且是 16 的

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

倍数；

底层应答：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x32 一级命令字段							
1(CMD_L)	二级命令字段：校验分区号							
2~3(LEN)	发送数据长度							
(DAT)	无							
4(CR1)	状态字节 1							
5(CR2)	状态字节 2							

- LEN 发送数据长度：0x00(LEN[0])、0x00(LEN[1])，LEN＝LEN[0]＋(LEN[1]<<8)。
- 状态字节(CR1、CR2)根据命令执行情况分为：

1. 校验成功：状态标志位(0xA0、0x00)。
2. 校验失败：状态标志位(CR1, CR2)

(1)、(0xB0、0x00)：返回失败；

(2)、(0xB0、0x20)：CRC 校验密钥认证失败；

(3)、(0xB0、0x21)：CRC 校验密钥认证失败次数超过限制；

(4)、(0xB0、0x32)：CRC 校验地址被分区保护；

(5)、(0xB0、0x33)：CRC 校验地址范围跨分区；

(6)、(0xB0、0x34)：CRC 校验地址范围越界（指超出整个 FLASH 大小）；

(7)、(0xB0、0x35)：CRC 校验地址不是 16 字节对齐；

(8)、(0xB0、0x36)：CRC 校验长度不是 16 的倍数，或者长度小于 2KB；

(9)、(0xB0、0x38)：CRC 校验失败；

(10)、(0xB0、0x3F)：更新管理信息失败；

2.2.8. CMD_OPT_RW

该命令用于选项字节读写（包含了读保护等级、FLASH 页写保护、Data0/1 配置、USER 配置）。当配置了分区，BOOT 不允许将读保护级别由 L1 降为 L0，因为会导致用户区 mass erase。

上层指令：

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x40 一级命令字段							
1(CMD_L)	二级命令字段							
2~3(LEN)	发送数据长度							
4~7(Par)								
8~23(DAT)	选项字节配置 16 个字节							

- CMD_L 二级命令字段：
  1. 0x00：获取选项字节。
  2. 0x01：配置选项字节。
  3. 0x02：配置选项字节，再复位。
- LEN 发送数据长度：0x10(LEN[0])、0x00(LEN[1])，LEN＝LEN[0]＋(LEN[1]<<8)。
- DAT[0~15]：选项字节配置 16 个字节

RDP、nRDP、USER、nUSER、Data0、nData0、Data1、nData1、WRP0、nWRP0、WRP1、nWRP1、RDP2、nRDP2、USER2 、nUSER2；

1. CMD_L＝0x00：全部为 0x00。
2. CMD_L＝0x01/0x02：配置选项字节为要写入的值。

底层应答：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x40 一级命令字段							
1(CMD_L)	二级命令字段							
2~3(LEN)	发送数据长度							
4~19(DAT)	选项字节配置 16 个字节							
20(CR1)	状态字节 1							
21(CR2)	状态字节 2							

- LEN 发送数据长度：0x10(LEN[0])、0x00(LEN[1])，LEN＝LEN[0]＋(LEN[1]<<8)。
- DAT[0~15]：当前选项字节配置 16 个字节

RDP、nRDP、USER、nUSER、Data0、nData0、Data1、nData1、WRP0、nWRP0、WRP1、nWRP1、RDP2、nRDP2、USER2、nUSER2；

- 状态字节(CR1、CR2)根据命令执行情况分为：

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

1. 返回成功：状态标志位(0xA0、0x00)。
2. 校验失败：状态标志位(CR1, CR2)

(1)、(0xB0、0x00)：返回失败；

(2)、(0xB0、0x39)：已配分区，不允许读保护级别由 L1 降为 L0；

2.2.9. CMD_ USERX_OP

该命令用于读取或者配置分区 USER1/3 大小，分区配置完成后对应的分区自动使能封口，分区 USER1/3 大小只能配置一次。

建议用户的配置流程：

1.如果需要分两个区，只配置 USER3（配置完自动封口）即可。如果需要对 USER1 也封口，再配置一下 USER1。USER1 + USER3 的大小必须为整个 FLASH 的大小；

上层指令：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x41 一级命令字段							
1(CMD_L)	二级命令字段							
2~3(LEN)	发送数据长度							
4~7(Par)	Par[0]：分区 USER1/3							
	Par [1]：分区 USER1/3 大小							
	Par [2]：分区认证密钥索引 ID							
	Par [3]：分区认证和加密下载使能配置							
DAT	无							

- CMD_L 二级命令字段：
  1. 0x00：读取分区 USER1/3 大小配置。
  2. 0x01：配置分区 USER1/3 大小、密钥 ID、分区认证/加密下载使能。
- LEN 发送数据长度：0x00(LEN[0])、0x00(LEN[1])，LEN＝LEN[0]＋(LEN[1]<<8)。
- Par[0]：分区号
  1. 0x00：分区 USER1。
  2. 0x02：分区 USER3。
- Par [1]：

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

1. CMD_L = 0x00：0x00。
2. CMD_L = 0x01：分区 USER1/3 大小配置

分区大小的输入范围：0x1(2KB) … 0x07(14KB)、0x20(64KB)，USER1+ USER3 = 64KB；用户区 USER1/3 大小配置后自动封口。

分区大小和地址确定

分区的起始地址确定为 0x0800_0000，分区的末地址为起始地址加整个 FLASH 的容量（比如 FLASH 的容量为 64K，则末地址为 0x0800_0000 + 64/2*0x800 = 0x0800_FFFF）。

如果 USER1 分区了，则 USER1 的分区地址范围为 0x0800_0000 ~ (0x0800_0000 + USER1_Size*0x800)。

如果 USER3 分区了，则 USER3 的分区地址范围为 (0x0801_0000 – USER3_Size*0x800) ~ 0x0800_FFFF（例如 FLASH 末地址为 0x0800_FFFF）。

- Par [2]：

1. CMD_L = 0x00：0xFF。
2. CMD_L = 0x01：0x00~0x01 加密下载/分区认证密钥索引 ID，

0xFF 表示不配置索引 ID，如果对应的 USERX 未配置 ID 则不判断 Par[3]的值；

- Par [3]：

分区认证和加密下载使能配置，0xXY

X = 0 – 不使能分区认证，可以配置为 1；

X = 1 – 使能分区认证，不能配置为 0；

Y = 0 – 不使能加密下载，可以配置为 1；

Y = 1 – 使能加密下载，不能配置为 0；

1. CMD_L = 0x00：读取状态，保留值 0x00；
2. CMD_L = 0x01：配置状态，配置值 0xXY；

底层应答：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x41 一级命令字段							

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

1(CMD_L)	二级命令字段
2~3(LEN)	发送数据长度
4~7(DAT)	DAT[0]：分区 USER1/3
	DAT[1]：分区 USER1/3 大小
	DAT [2]：分区认证密钥索引 ID 配置状态
	DAT [3]：读取的分区认证和加密下载使能配置
8(CR1)	状态字节 1
9(CR2)	状态字节 2

- LEN 发送数据长度：0x02(LEN[0])、0x00(LEN[1])，LEN = LEN[0] + (LEN[1]<<8)。
- DAT[0]：分区号
  1. 0x00：分区 USER1。
  2. 0x02：分区 USER3。
- DAT[1]：读取的当前分区 USER1/3 大小

  分区大小的输出范围：0x0(0KB)、0x1(2KB) … 0x07(14KB)、0x20(64KB)，

  0x0 表示未配置分区大小，USER1 + USER3 = 64KB；
- DAT [2]：
  1. 0x00，已经配置 ID；
  2. 0xFF，未配置 ID
- DAT [3]：

  读取分区认证和加密下载使能配置，0xXY

  X = 0 – 不使能分区认证，可以配置为 1；

  X = 1 – 使能分区认证，不能配置为 0；

  Y = 0 – 不使能加密下载，可以配置为 1；

  Y = 1 – 使能加密下载，不能配置为 0；
- 状态字节(CR1、CR2)根据命令执行情况分为：
  1. 返回成功：状态标志位(0xA0、0x00)。
  2. 返回失败：状态标志位(0x70、0x00)

  (1)、(0xB0、0x00)：返回失败；

  (2)、(0xB0、0x10)：密钥索引 ID 范围错误；

  (3)、(0xB0、0x3A)：分区大小已经配置，无法再次配置；

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

(4)、(0xB0、0x3B)：分区大小配置错误，必须满足 USER1 + USER3 = FLASH 容量，USER1/3 配置最少为 0x01(2KB)；

(5)、(0xB0、0x3D)：分区密钥索引 ID 配置失败或者已经配置；

(6)、(0xB0、0x3E)：分区认证和加密下载使能配置失败或者已经配置；

(7)、(0xB0、0x3F)：更新管理信息失败；

2.2.10. CMD_SYS_RESET

该命令用于软件复位 BOOT 程序。

上层指令：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x50 一级命令字段							
1(CMD_L)	0x00 二级命令字段							
2~3(LEN)	发送数据长度							
4~7(Par)	保留							
(DAT)	无							

- 保留值：0x00；

底层应答：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x50 一级命令字段							
1(CMD_L)	0x00 二级命令字段							
2~3(LEN)	发送数据长度							
(DAT)	无							
4(CR1)	状态字节 1							
5(CR2)	状态字节 2							

- 状态字节(CR1、CR2)根据命令执行情况分为：
  1. 返回成功：状态标志位(0xA0、0x00)。
  2. 返回失败：状态标志位(0xB0、0x00)。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

2.3. 返回状态字说明

2.3.1. 返回成功状态字

返回成功：状态标志位(0xA0、0x00)。表示上层下发的命令执行成功，返回成功状态字。包含了读取、更新、配置等命令的成功返回值。

2.3.2. 返回失败状态字

返回失败：状态标志位(0xB0、0x00)。表示上层下发的命令由于其他原因（命令接受格式错误或者超时等）执行失败，返回失败状态字。

2.3.3. 返回其他状态字

下列的返回状态字也是返回失败，第二字节的状态字表示不同的错误类型。

(1)、(0xB0、0x10)：密钥索引 ID 范围错误；

(2)、(0xB0、0x11)：新密钥 CRC 校验错误；

(3)、(0xB0、0x20)：密钥认证失败；

(4)、(0xB0、0x21)：密钥认证失败次数超出限制（最多秘钥认证失败 16 次，两个分区共享次数）；

(5)、(0xB0、0x30)：擦除/下载 FLASH 页被 RDP 保护；

(6)、(0xB0、0x31)：擦除/下载 FLASH 页被 WRP 保护；

(7)、(0xB0、0x32)：擦除/下载/CRC 校验地址被分区保护；

(8)、(0xB0、0x33)：擦除/下载/CRC 校验地址范围跨分区；

(9)、(0xB0、0x34)：擦除/下载/CRC 校验地址范围越界（指超出整个 FLASH 大小）；

(10)、(0xB0、0x35)：擦除/下载/CRC 校验起始地址不是 16 字节对齐；

(11)、(0xB0、0x36)：下载/CRC 校验数据长度不是 16 的倍数；数据长度表示擦除 FLASH 的长度，或者是下载代码到 FLASH 的长度，或者是校验 FLASH CRC 值的长度；

(12)、(0xB0、0x37)：擦除/下载 FLASH 编程失败；

(13)、(0xB0、0x38)：CRC 校验失败；

(14)、(0xB0、0x39)：已配分区，不允许读保护级别由 L1 降为 L0；

(15)、(0xB0、0x3A)：分区已经配置，无法再次配置；

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

(16)、 (0xB0、0x3B)：分区大小配置错误，必须满足 USER1 + USER3 = FLASH 容量；

(17)、(0xB0、0x3E)：分区认证和加密下载使能配置失败或者已经配置；

(18)、(0xB0、0x3F)：更新管理信息失败；

(19)、(0xBB、0xCC)：上层发送命令一级、二级命令字段不属于任何命令。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

3. BOOT使用说明

3.1. 上位机控制流程

上位机支持用户擦除 FLASH 区，用户代码下载，下载代码完整性校验。上位机通过读取分区信息，自动识别用户输入的擦除、下载、校验地址范围需要认证。

上位机支持用户选择是否使能加密下载来保护用户代码。

上位机支持用户读取和配置分区 USER1/3 大小。当用户配置分区大小后不能再修改。

上位机支持用户更新安全密钥（用于分区认证和加密下载）。

上位机支持用户更新选项字节读取和修改。

进 BOOT：进入 BOOT，此时可以与 PC TOOL 通过 USART1 接口交互；

芯片固件完整性校验：选择从系统存储区启动，BOOT 自动进行完整性自校验，校验失败时会进入死循环，后续的功能无法使用；

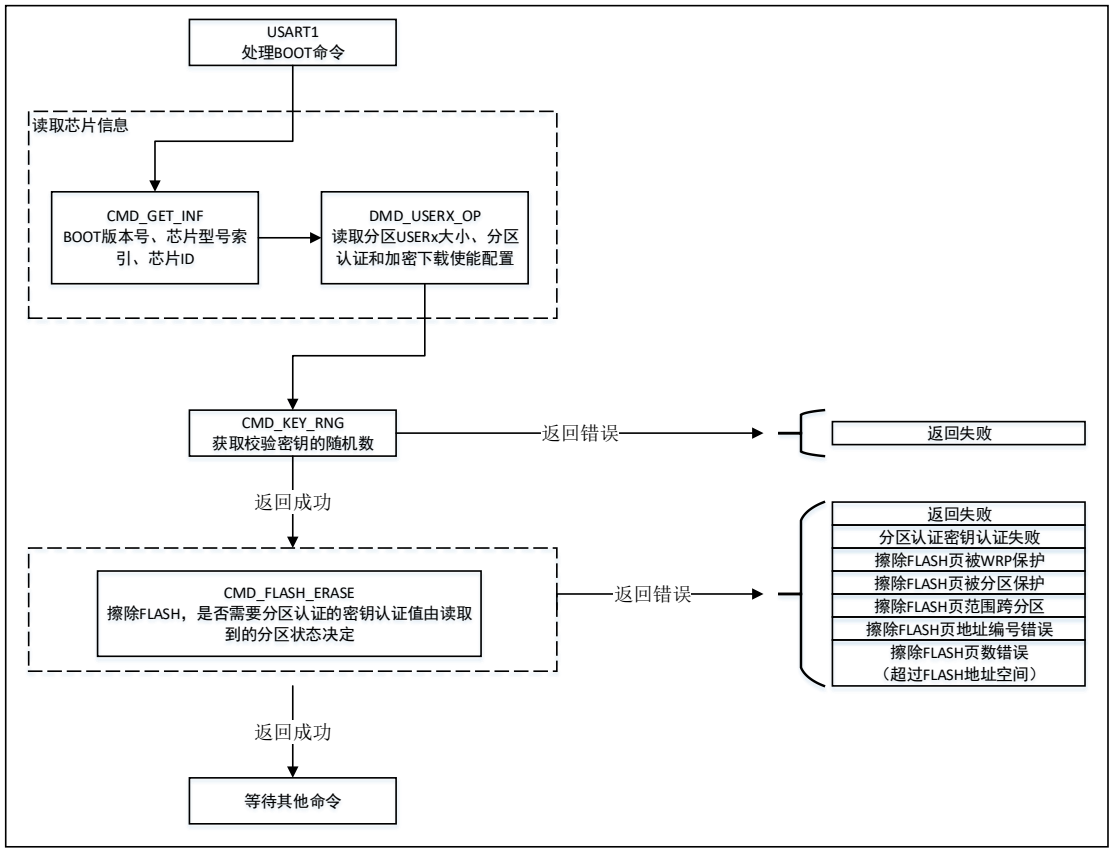
命令集交互：PC TOOL 依据 BOOT 支持的命令集发送不同的命令来使用相应的功能；

1. 读取 BOOT 版本号、芯片型号索引、芯片 ID；
2. 获取 16byte 随机数；
3. 更新安全密钥（用于分区认证和加密下载）；
4. 擦除 FLASH；
5. 下载用户程序到 FLASH；
6. CRC 校验下载的用户程序；
7. 读取/配置选项字节（包含了读保护等级、FLASH 页写保护、Data0/1 配置、USER 配置）；
8. 获取分区 USERX 大小，配置分区 USERX 大小；
9. 系统复位，可以复位 BOOT 程序重新运行；

3.1.1. 擦除命令控制流程图

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

Figure3-1 擦除命令控制流程图

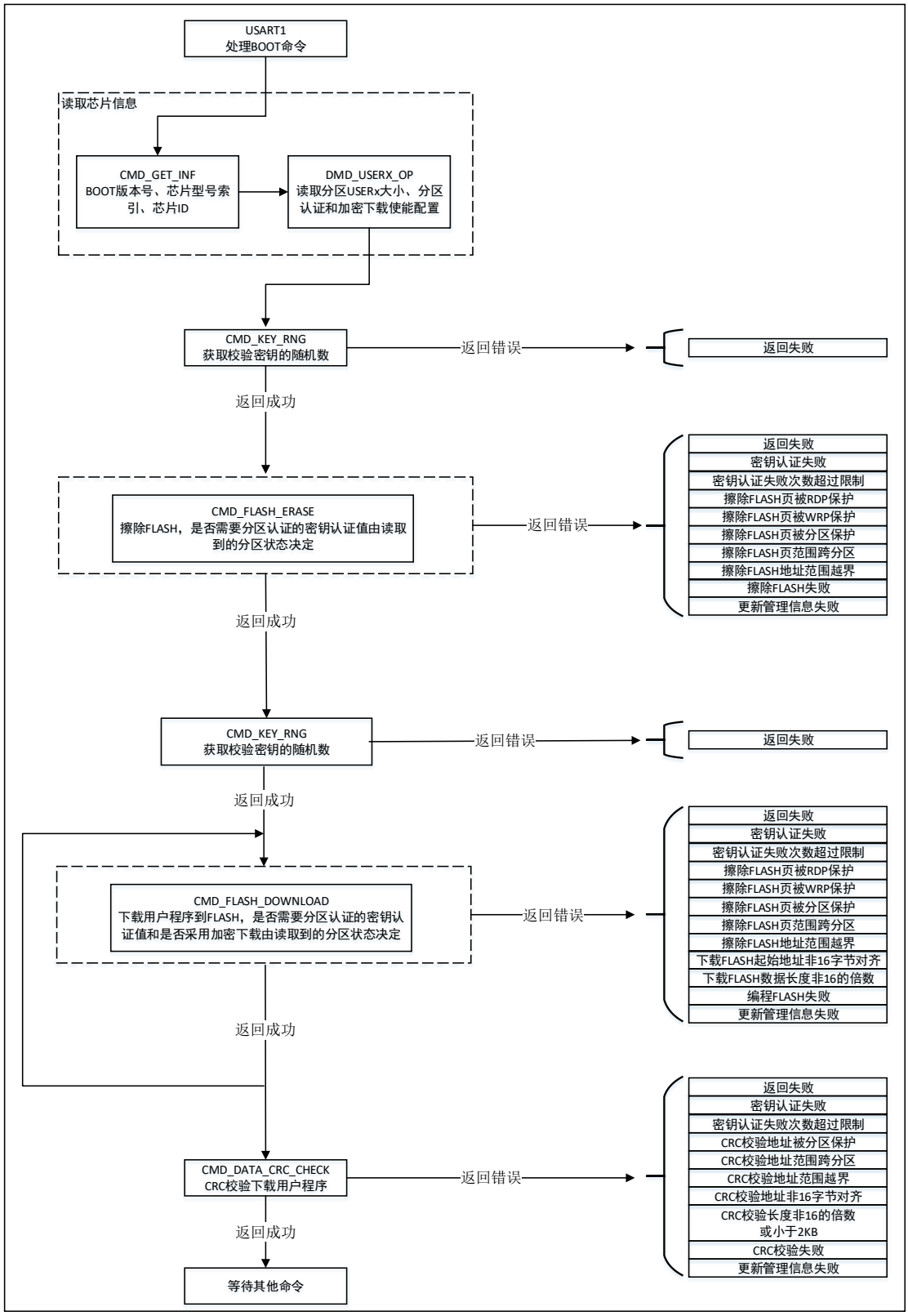


3.1.2. 下载命令控制流程图

分区认证加密下载前获取一个随机数，上位机用此随机数生成 16 字节 USER1/3 分区认证的密钥认证值。连续下载时，第一次之后的下载命令使用的随机数用第一次的随机数派生算法生成，不用再次获取新的随机数。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

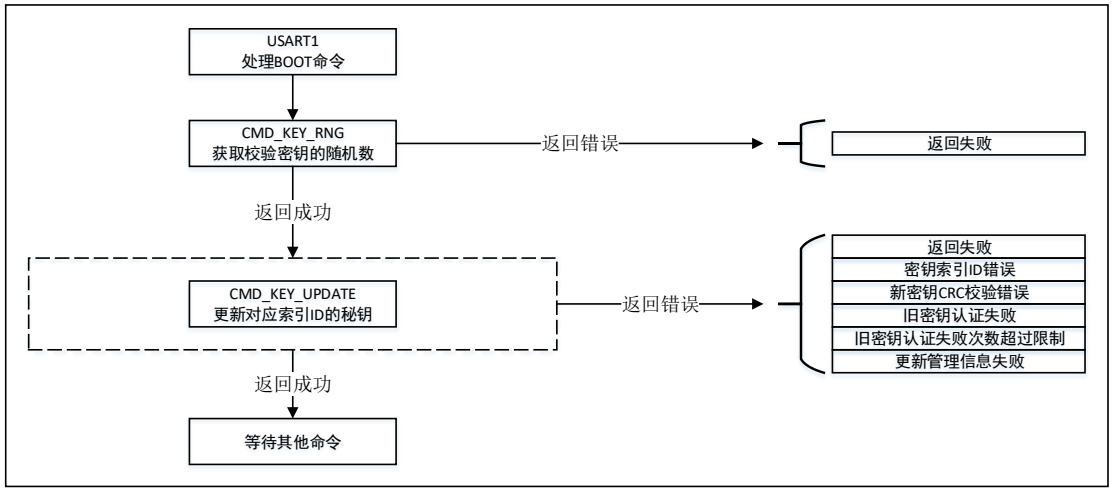
Figure3-2 下载命令控制流程图



3.1.3. 更新密钥命令控制流程图

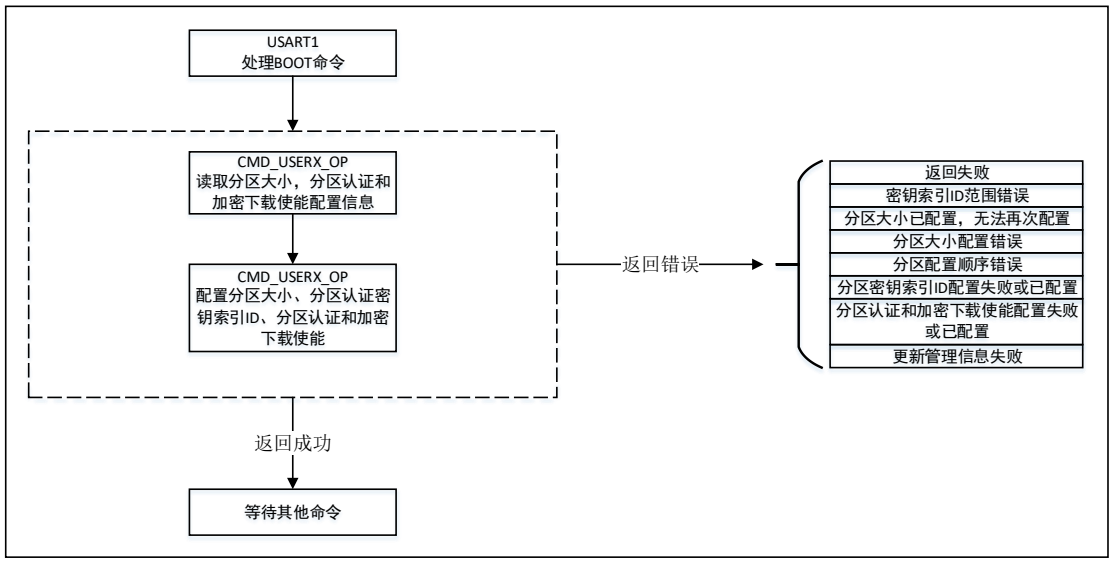
国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

Figure3-3 更新密钥命令控制流程图



3.1.4. 分区操作命令控制流程图

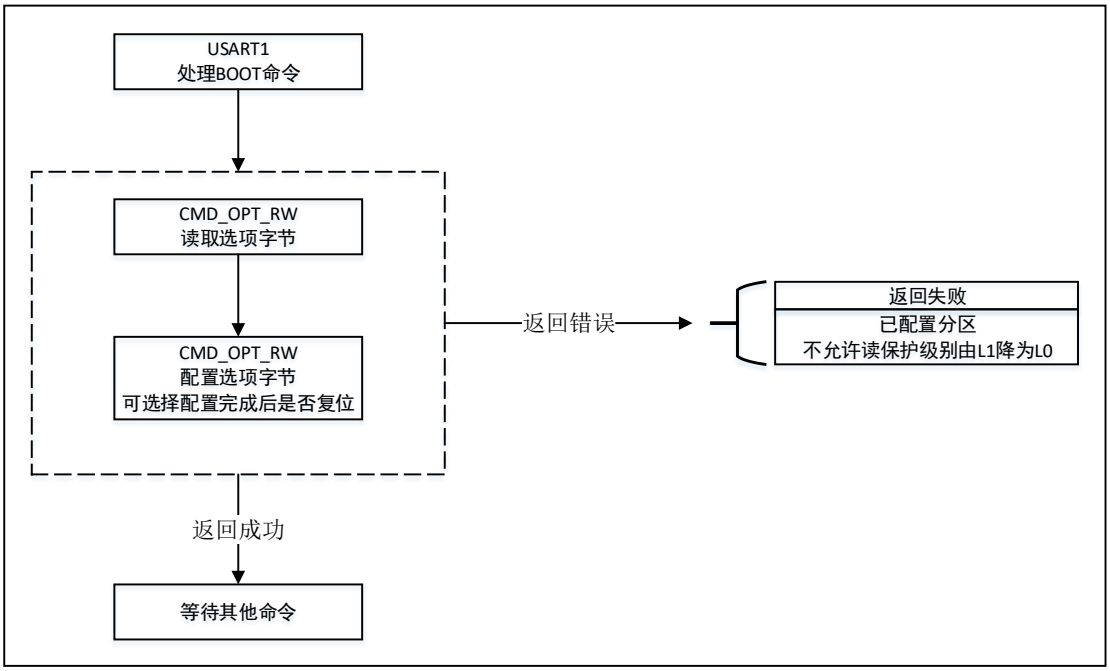
Figure3-4 分区操作命令控制流程图



3.1.5. 选项字节读写命令控制流程图

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

Figure3-5 选项字节读写命令控制流程图



国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

4. 历史版本

版本	修订日期	说明
V1.0.0	2023/5/16	初始版本

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

5. 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。请使用人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责任，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。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057