使用指南

N32G43x&N32L40x&N32L43x系列BOOT接口指令使用指南

简介

使用指南主要描述N32G43x系列、N32L40x系列、N32L43x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 Nations 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
邮箱：info@nationstech.com 邮编：518057

目录

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

1 BOOT简述

使用指南适用于N32L40x、N32L43x、N32G43x系列芯片，提供了用户下载功能，具体如下：

1) 接口支持：

A. 支持 USART1，具体波特率支持列表见 2.2.1 章节描述

a) N32L40x、N32L43x、N32G43x 系列 MCU 支持波特率协商，接口为 PA9(TX)、PA10(RX)；

B. 支持 USB 接口，使用 DFU 协议下载；

串口自动波特率检测和串口波特率协商区别：

- 串口自动波特率检测：

  上电后，通过上位机串口发送 0x7F，MCU 检测上位发送的数据，识别串口通讯的波特率，该种方式 N32L40x、N32L43x、N32G43x 系列 MCU 不支持；

- 串口波特率协商：

  上电后，上位机与通用 MCU 通过串口通讯时，首先使用 9600bps 的波特率进行通讯，通过 CMD_SET_BR 命令重新设置波特率，返回成功应答后生效，如果指定的波特率不支持，将会返回失败状态， N32L40x、N32L43x、N32G43x 系列，都支持该种方式。

2) 支持 Flash 擦除功能（下载前确保该页已经被擦除）；

3) 支持数据或程序下载功能；

4) 支持下载数据 CRC32 校验；

5) 支持上电 BOOT 自校验；

6) 支持跳转到用户区执行；

7) 支持软件复位芯片操作；

8) 支持 FLASH 分区和分区擦除下载时密钥认证；

9) 支持分区密钥更新；

10) 支持加密下载（AES-128 ECB）

本文档详细描述了通用MCU芯片BOOT的功能、实现及使用介绍。

2 BOOT流程及命令处理

BOOT程序支持通过USART/USB接口下载用户程序和数据。上电时，自动识别使用的接口。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	简要说明
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。

1. 逻辑层指令数据结构

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：

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

< 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。

2. 物理层指令数据结构

1) USB 接口指令数据结构

USB 接口采用 DFU 协议，详情见'DFU_1.1'文档：

- 上位机下发上层指令：

  使用**DFU_DNLOAD**请求下发上层指令数据。

- 上位机**获取**下层应答指令：

  使用**DFU_GETSTATUS**请求获取下层应答指令数据。

2) 串口指令数据结构：

- 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}）。

- 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}）。

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

2.2 命令说明

2.2.1 CMD_ SET_BR

该命令仅用于支持波特率协商的BOOT版本，修改串口波特率，仅串口下载时有效。

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 ~ 4.5Mbps；
- 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)：

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

- N32L40x、N32L43x、N32G43x 系列 MCU BOOT V1.1 版本串口波特率支持：

时钟参数 (MHz)		波特率											
		2400	**4800**	**9600**	**14400**	**19200**	**38400**	**57600**	**115200**	**128000**	**256000**	**576000**	**923076**
外部时钟	4	√	√	√	√	√	√	√	√	√	√	√	√
	6	√	√	√	√	√	√	√	√	√	√	√	√
	8	√	√	√	√	√	√	√	√	√	√	√	√
	12	√	√	√	√	√	√	√	√	√	√	√	√
	16	√	√	√	√	√	√	√	√	√	√	√	√
	24	√	√	√	√	√	√	√	√	√	√	√	√
	32	√	√	√	√	√	√	√	√	√	√	√	√
内部时钟	8	√	√	√	√	√	√	√	√	√	√	√	√

- N32L40x、N32L43x、N32G43x 系列 MCU BOOT V1.2 版本串口波特率支持：

时钟参数 (MHz)		波特率															
		2400	**4800**	**9600**	**14400**	**19200**	**38400**	**57600**	**115200**	**128000**	**256000**	**576000**	**923076**	**1M**	**1.5M**	**2M**	**2.25M**	**3M**
外部时钟	4	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
	6	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
	8	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
	12	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
	16	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
	24	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
	32	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
内部时钟	8	√	√	√	√	√	√	√	√	√	√	√	√	√	/	/	/	/

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

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							
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、芯片系列化信息							
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]芯片型号索引

产品编号：0x01

- DAT[1] 0xXY，BOOT 命令集版本号(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 代码版本
- DAT[3~50] 48Byte

  DAT[3~18]：16Byte UCID（例：36 01 01 A0 15 50 36 33 50 30 35 30 30 09 7D 22），

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

DAT[19~30]：12Byte Chip ID(UID)（例：36 01 01 50 36 33 50 30 35 09 7D 22）

DAT[31~34]：4Byte DBGMCU_IDCODE（例：01 54 87 F8）

UCID/ UID/ DBGMCU_IDCODE具体定义见《UM_N32G45x系列用户手册》《UM_N32G4FR系列用户手册》《UM_N32WB452系列用户手册》《UM_N32G43x系列用户手册》《UM_N32L40x系列用户手册》《UM_N32L43x系列用户手册》

DAT[35~50]：16Byte (保留)；

- 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)。

2.2.3 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的真随机数							
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)。

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

- 16Byte 的真随机数由芯片生成。
- 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CRC32校验值(旧密钥+新密钥值) + 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(0x00~0x1F)：密钥索引 ID。
- 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。

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

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)	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)
     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、0x21)：旧密钥认证失败次数超过限制；
     6) (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，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。

当使能认证功能，认证擦除前需要使用CMD_KEY_RNG获取随机数，并进行认证。

BOOT提供以页为单位擦除FLASH的功能，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。

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

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)	二级命令字段：擦除分区号							
2~3(LEN)	发送数据长度							
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USER1/2/3分区认证的密钥认证值，仅用于使能认证情况							

- CMD_L：擦除分区号
  1. 0x00 = USER1；
  2. 0x01 = USER2；
  3. 0x02 = USER3；
- LEN 发送数据长度：0x10(LEN[0])、0x00(LEN[1])，LEN = LEN[0] + (LEN[1]<<8)。
- 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）

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

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)。
     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)：擦除 FLASH 页被 RDP 保护；
     5) (0xB0、0x31)：擦除 FLASH 页被 WRP 保护；
     6) (0xB0、0x32)：擦除 FLASH 页被分区保护；
     7) (0xB0、0x34)：擦除 FLASH 地址范围越界（指超出 FLASH 大小）；
     8) (0xB0、0x37)：擦除 FLASH 失败。
     9) (0xB0、0x3F)：更新管理信息失败；
     10) (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，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。

当使能认证或加密时，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。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。

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

上层指令：

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
1(CMD_H)	0x31一级命令字段							
2(CMD_L)	二级命令字段：下载分区号							
3~4(LEN)	发送数据长度							
5~8(Par)	下载FLASH的起始地址							
8~23+N(DAT)	DAT[0:15]：16字节USER1/2/3分区认证的密钥认证值 DAT[16~16+N]：下载的具体数据（加密或者非加密） DAT[N+1~N+4]：非加密数据的 4Byte CRC32校验值							

- CMD_L：下载分区号
  1. 0x00 = USER1；
  2. 0x01 = USER2；
  3. 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 | Par[2]<<16 | Par[3]<<24。
- DAT[0:15]，Reserved。
- DAT[16~16+N]：下载的具体数据
  1. USB：最大 128 个字节，15<=N<=143，N+1 必须为 16 的倍数。
  2. USART：最大 128 个字节，15<=N<=143，N+1 必须为 16 的倍数。

DAT[N+1~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							

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

- 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；
     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。

当使能认证时，CRC校验前需要使用CMD_KEY_RNG获取随机数，并进行认证。

上层指令:

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

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							
8~31(DAT)	DAT[0:15]：16字节USER1/2/3分区认证的密钥认证值 DAT[16:19]：校验起始地址 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. 0x01 = USER2；
  3. 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]：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							

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

- 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）。

上层指令:

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)								
8~27(DAT)	选项字节配置20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：0x14(LEN[0])、0x00(LEN[1])，LEN = LEN[0] + (LEN[1]<<8)。

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

- DAT[0~19]：选项字节配置 20 个字节

RDP、nRDP、USER、nUSER、Data0、nData0、Data1、nData1、WRP0、nWRP0、WRP1、nWRP1、WRP2、nWRP2、WRP3、nWRP3、RDP2、nRDP2、Reserved、nReserved；

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							
4~23(DAT)	选项字节配置20个字节							
24(CR1)	状态字节1							
25(CR2)	状态字节2							

- LEN 发送数据长度：0x14(LEN[0])、0x00(LEN[1])，LEN = LEN[0] + (LEN[1]<<8)。
- DAT[0~19]：当前选项字节配置 20 个字节

RDP、nRDP、USER、nUSER、Data0、nData0、Data1、nData1、WRP0、nWRP0、WRP1、nWRP1、WRP2、nWRP2、WRP3、nWRP3、RDP2、nRDP2、Reserved、nReserved；

- 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. 校验失败：状态标志位(CR1, CR2)
     1) (0xB0、0x00)：返回失败；

2.2.9 CMD_ USERX_OP

该命令用于读取或者配置分区USER1/2/3大小，分区配置完成后对应的分区自动使能封口。分区USER1/2/3大小只能配置一次，软件会判断NVR的MMU分区是否有配置过（在判断NVR值时，加流程变量或者随机延时）。

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

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

口，再配置一下USER1。USER1 + USER3的大小必须为整个FLASH的大小；

2.如果需要分三个区，先配置USER3（配置完自动封口），再配置USER2（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 + USER2 + 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USER1/2/3							
	Par [1]：分区USER1/2/3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 USER1/2/3 大小配置。
  2. 0x01：配置分区 USER1/2/3 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. 0x01：分区 USER2。
  3. 0x02：分区 USER3。
- Par [1]：
  1. CMD_L = 0x00：0x00。
  2. CMD_L = 0x01：分区 USER1/2/3 大小配置

  分区大小的输入范围：0x1(16KB) … 0x1F(496KB)、0x20(512KB)，USER1 + USER2 + USER3 = 512KB；用户区USER1/2/3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

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

量（比如FLASH的容量为512K，则末地址为0x0800_0000 + 512*0x800 = 0x0808_0000）。

如果USER1分区了，则USER1的分区地址范围为0x0800_0000 ~ (0x0800_0000 + USER1_Size*0x4000)。

如果USER3分区了，则USER3的分区地址范围为(0x0808_0000 – USER3_Size*0x4000) ~ 0x0800_8000（例如FLASH末地址为0x0808_0000）。

USER2的分区地址，首地址为USER1的末地址，末地址为USER3的首地址。如果USER1没有分区，则USER2的首地址需要由USER2_Size确定。

- Par [2]：

  1. CMD_L = 0x00：0xFF。
  2. CMD_L = 0x01：0x00~0x1F 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：

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

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(DAT)	DAT[0]：分区USER1/2/3							
	DAT[1]：分区USER1/2/3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. 0x01：分区 USER2。
  3. 0x02：分区 USER3。
- DAT[1]：读取的当前分区 USER1/2/3 大小

  分区大小的输出范围：0x0(0KB)、0x1(16KB) … 0x1F(496KB)、0x20(512KB)，

  0x0表示未配置分区大小，USER1 + USER2 + USER3 = 512KB；
- 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)。

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

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；

4) (0xB0、0x3B)：分区大小配置错误，必须满足 USER1 + USER2 + USER3 = FLASH 容量，USER1/2/3 配置最少为 0x01(16KB)；

5) (0xB0、0x3C)：分区配置顺序错误，必须先配置 USER1 或者 USER3；

6) (0xB0、0x3D)：分区密钥索引 ID 配置失败或者已经配置；

7) (0xB0、0x3E)：分区认证和加密下载使能配置失败或者已经配置；

8) (0xB0、0x3F)：更新管理信息失败；

2.2.10CMD_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：

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

1. 返回成功：状态标志位(0xA0、0x00)。
2. 返回失败：状态标志位(0xB0、0x00)。

2.3 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过限制；
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；
16) (0xB0、0x3B)：分区大小配置错误，必须满足 USER1 + USER2 + USER3 = FLASH 容

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

量；

17) (0xB0、0x3C)：分区配置顺序错误，必须先配置 USER1 或者 USER3；

18) (0xB0、0x3D)：分区密钥索引 ID 配置失败或者已经配置；

19) (0xB0、0x3E)：分区认证和加密下载使能配置失败或者已经配置；

20) (0xB0、0x3F)：更新管理信息失败；

21) (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 Nations 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
邮箱：info@nationstech.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USER1/2/3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。

上位机支持软件复位命令和跳转USER1复位程序入口地址执行命令。

进BOOT：进入BOOT，此时可以与PC TOOL通过USART1接口或者USB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真随机数；
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；
10. 跳转USER1复位程序入口地址，跳转到下载到USER1分区代码的复位程序入口地址；

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

3.1.1 擦除命令控制流程图

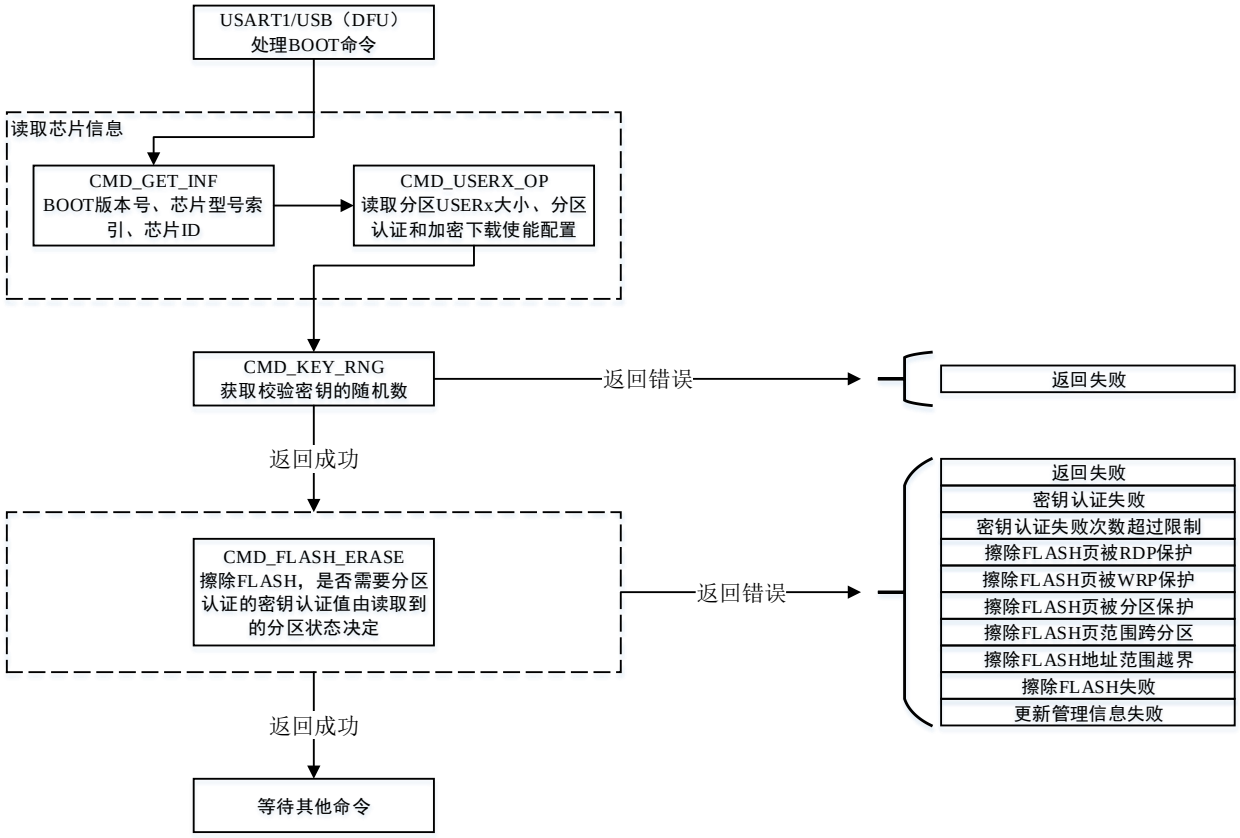

Figure3.1 擦除命令控制流程图

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USER1/2/3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 Nations 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
邮箱：info@nationstech.com 邮编：518057

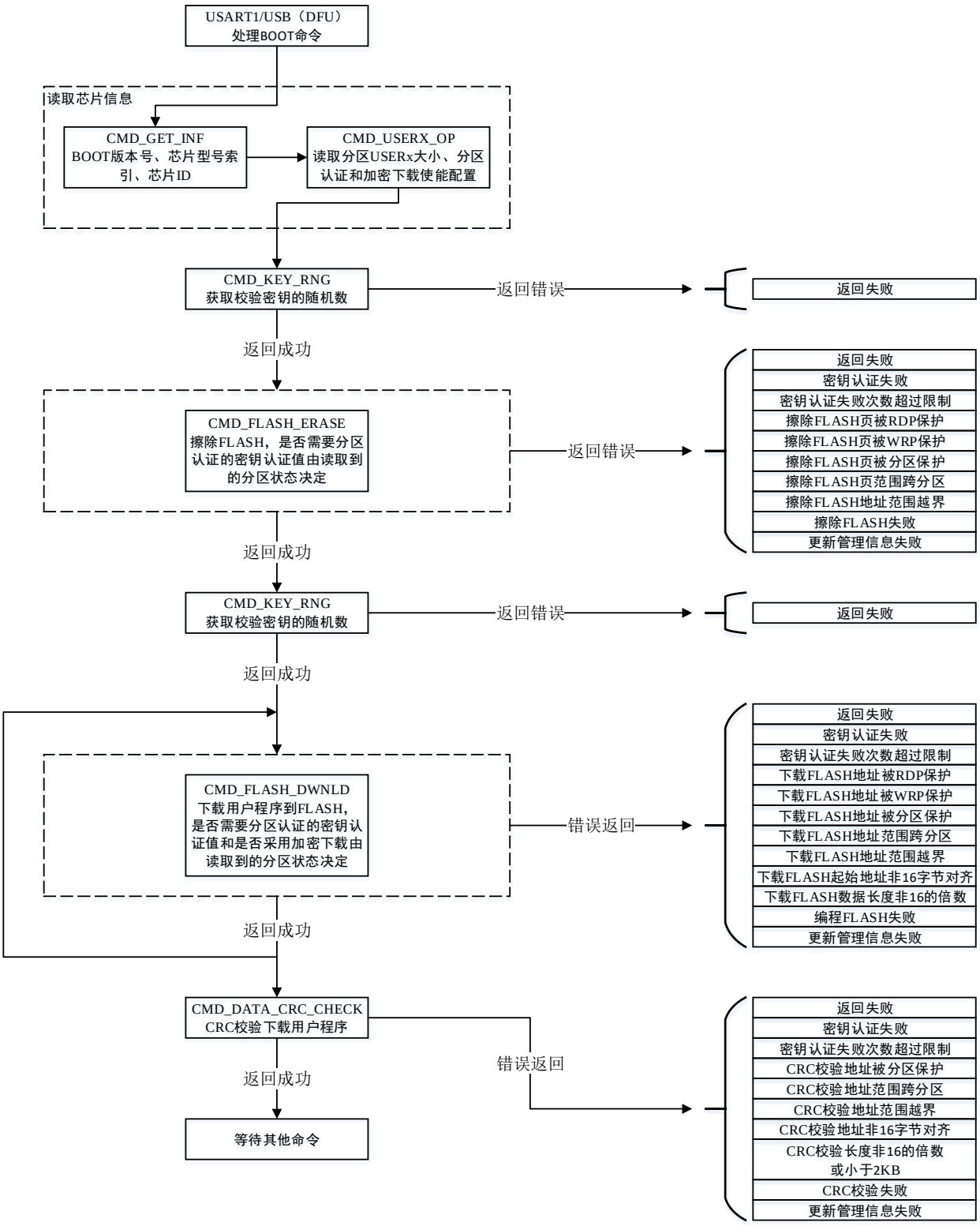

Figure3.2 下载命令控制流程图

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

3.1.3 更新密钥命令控制流程图

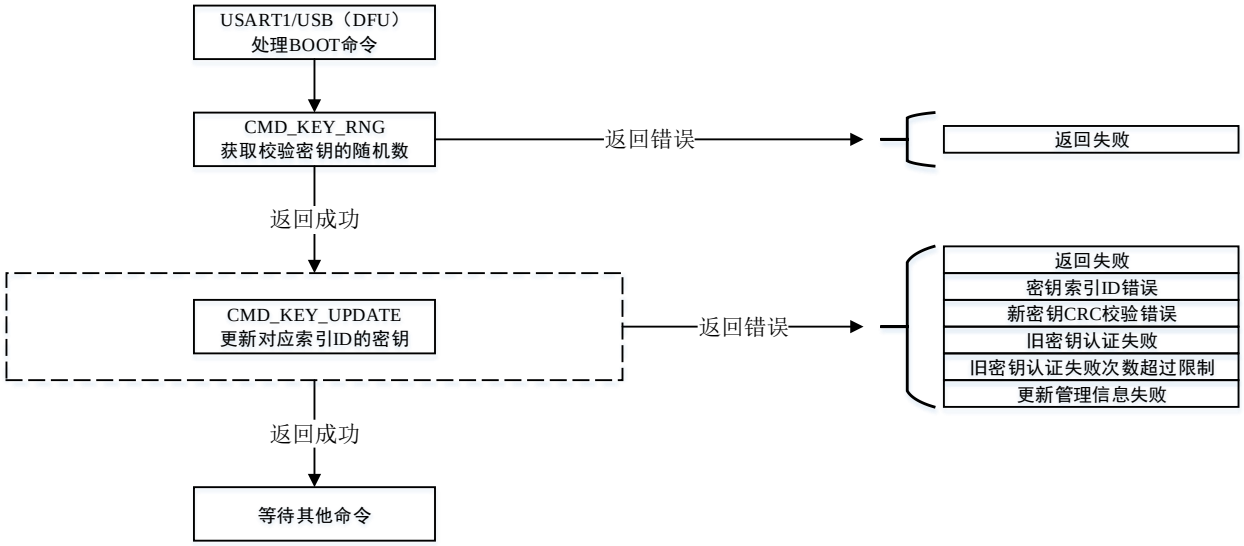

Figure3.3 更新密钥命令控制流程图

3.1.4 分区操作命令控制流程图

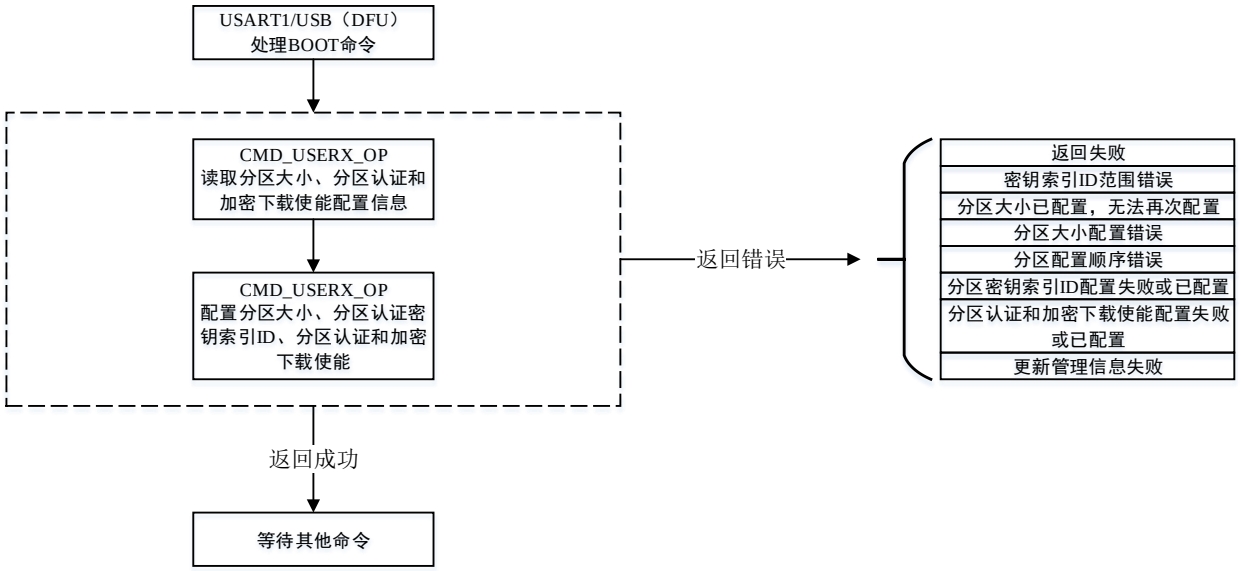

Figure3.4 分区操作命令控制流程图

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

3.1.5 选项字节读写命令控制流程图

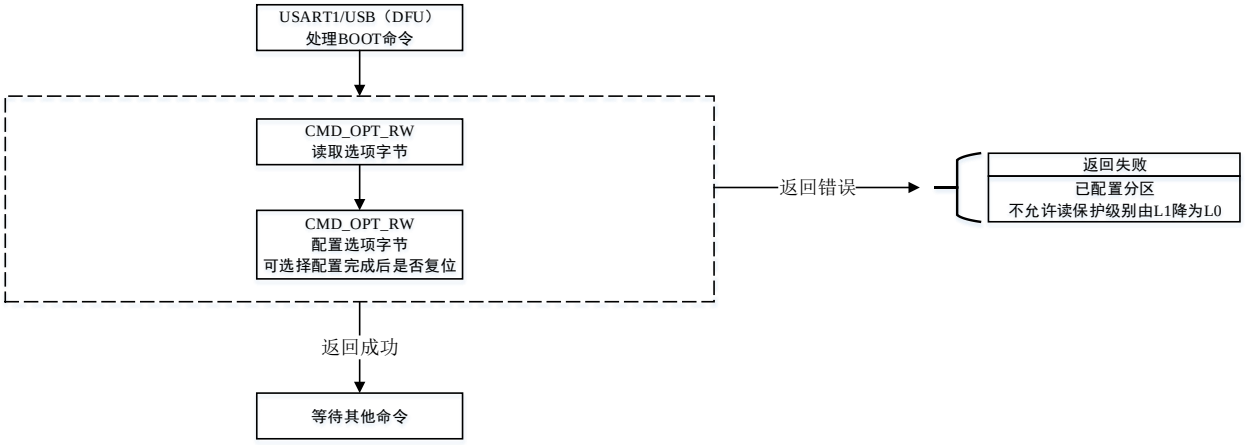

Figure3.5 选项字节读写命令控制流程图

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.com 邮编：518057

4 历史版本

版本	日期	备注
V1.0	2020-04-09	创建文档
V1.1	2020-08-04	1. 增加 USB 接口无晶振模式的控制字； 2. 增加 UART 接口超时功能； 3. 增加 NVR MSI 写接口；
V1.2	2020-12-21	1. 修改 NVR 数据编程未清除错误标注的问题； 2. 修改 NVR 封口后无法读 NVR 的 BUG； 3. 增加 HIS 检测超时机制 4. 优化代码空间
V1.3	2022-7-6	1. 删除 2.2.11 CMD_APP_GO 章节

国民技术股份有限公司 Nations 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
邮箱：info@nationstech.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 Nations 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
邮箱：info@nationstech.com 邮编：518057