User guide

N32G43x&N32L40x&N32L43x Series BOOT interface instruction user Guide

Introduction

The user guide mainly describes the BOOT interface instructions of N32G43x series, N32L40x series and N32L43x series MCU, which is easy to download and develop by using the National technology BOOT Loader.

Content

1 BOOT brief introductions

User Guide applicable to N32L40x, N32L43x, N32G43x series chips, provides users with the download function, details are as follows:

1) Interface support:

   A. USART1 is supported. For details about the baud rate, see 2.2.1

      a) N32L40x, N32L43x, N32G43x series MCU support baud rate negotiation, interface is PA9(TX), PA10(RX);

   B. Support USB interface, using DFU protocol download;

   Serial port automatic baud rate detection and serial port baud rate negotiation:

   - Serial port automatic baud rate detection:

     After power-on, 0x7F is sent through the serial port of the upper computer. MCU detects the data sent by the upper computer and identifies the baud rate of serial port communication. This method is not supported by N32L40x, N32L43x, and N32G43x series MCU.

   - Serial port baud rate negotiation:

     After power-on, when the upper computer communicates with the universal MCU through the serial port, the baud rate of 9600bps will be used first for communication. Then the CMD_SET_BR command is used to reset the baud rate, and the response will take effect after success. If the specified baud rate is not supported, the state will return to failure. The N32L40x, N32L43x, and N32G43x series all support this mode.

2) Support Flash erasure (make sure the page has been erased before downloading);
3) Support data or program download function;
4) Support download data CRC32 verification;
5) Support power-on BOOT self-verification.
6) Jump to the user area for execution.
7) Support software reset chip operation;
8) Support FLASH partition and partition eraser download key authentication;

9) Support partition key update;

10) Support encrypted download (AES-128 ECB)

This document describes in detail the functions, implementation and user of the universal MCU chip BOOT.

2 BOOT Process and command processing

The BOOT program supports downloading user programs and data through USART/USB ports.During power-on, the interface is automatically identified.The following describes the command processing process.

2.1 Commands and data structures

2.1.1 Command list

Table2.1 Command definition

Name of the command	Key value	Description
CMD_SET_BR	0x01	Set the baud rate of the serial port (Valid only when serial ports are used)
CMD_GET_INF	0x10	Read chip model index, BOOT version number, chip ID
CMD_GET_RNG	0x20	Get random number
CMD_KEY_UPDATE	0x21	Update the encryption download key or partition authentication key
CMD_FLASH_ERASE	0x30	Erase FLASH
CMD_FLASH_DWNLD	0x31	Download user programs to FLASH
CMD_DATA_CRC_CHECK	0x32	CRC verification download user program
CMD_OPT_RW	0x40	Read/configure option bytes (including read protection level, FLASH page write protection, datA0/1 configuration, USER configuration)
CMD_USERX_OP	0x41	Get the partition USERX size and set the partition USERX size
CMD_SYS_RESET	0x50	The system reset

2.1.2 Data structure

This section describes some conventions described in the following sections. "<>" represents fields that must be included, and "()" represents fields that must be included according to parameters.

1. **Logical layer instruction data structure**

1) Upper instruction structure:

<CMD_H + CMD_L + LEN + Par> + (DAT).

CMD_H indicates the level-1 command field, and CMD_L indicates the level-2 command field.LEN indicates the length of data to be sent.Par represents a four-byte command parameter;DAT represents the specific data sent from the upper level instruction to the lower level;

2) Lower response structure:

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

CMD_H indicates the level-1 command field, and CMD_L indicates the level-2 command field. The command fields at the lower level are the same as those at the upper level.LEN indicates the length of data to be sent.DAT indicates the specific data that the lower layer replies to the upper layer.CR1+CR2 indicates the command execution result returned to the upper layer. If the level-1 and level-2 command fields do not belong to any command, BOOT replies CR1=0xBB and CR2 = 0xCC.

2. Physical layer instruction data structure

1) USB interface instruction data structure

USB interface adopts DFU protocol, see 'DFU_1.1' for details:

- The upper computer issues the upper instruction:

  Use the **DFU_DNLOAD** request to deliver the upper-layer instruction data.

- The upper computer gets the lower response command:

  Use the **DFU_GETSTATUS** request to get the underlying reply instruction data.

2) Serial command data structure:

- The upper computer issues the upper instruction:

  STA1 + STA2 + {superstructure} + XOR.

  STA1 and STA2 are the start bytes of commands sent through the serial port. STA1=0xAA and STA2=0x55.The chip is used to identify the serial port data stream sent by the host computer.

  XOR represents the XOR operation value of the previous command byte (STA1 +

STA2 + {superstructure}).

- The upper computer receives the lower response:

STA1 + STA2 + {lower response structure} + XOR.

STA1 and STA2 are the start bytes of commands sent through the serial port. STA1=0xAA and STA2=0x55.It is used for the host computer to identify the chip and send serial port data stream

XOR represents the XOR operation value of the previous command byte (STA1 + STA2 + {underlying reply structure}).

2.2 Command description

2.2.1 CMD_ SET_BR

This command is used only for the BOOT version that supports baud rate negotiation and changes the baud rate over a serial port.

Upper-level instructions:

bit / byte	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x01 Level-1 command field							
1(CMD_L)	0x00 Level-2 command field							
2~3(LEN)	Length of sent data: 0x00, 0x00							
4~7(Par)	Par[0~3] : Set baud rate parameters							
(DAT)	None							

- Par[0~3], the serial port baud rate negotiation value can be set to the maximum, the setting range is 2.4Kbps ~ 4.5Mbps;
- Reserved value: 0x00;

Underlying response:

bit / byte	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x01 Level-1 command field							
1(CMD_L)	0x00 Level-2 command field							
2~3(LEN)	Length of sent data: 0x00, 0x00							

(DAT)	None
4(CR1)	Status byte 1
5(CR2)	Status byte 2

- Status bytes (CR1 and CR2) are divided into the following types according to command execution:

1. Return success: status flag bit (0xA0, 0x00).
2. Return failure: status flag bits (0xB0, 0x00).

The following are the baud rate values supported by baud rate negotiation (√ indicates that baud rate negotiation is supported, and / indicates that baud rate negotiation is not supported) :

- N32L40x, N32L43x, N32G43x series MCU BOOT V1.1

Clock parameters (MHz)		**Baud rate**											
		2400	**4800**	**9600**	**14400**	**19200**	**38400**	**57600**	**115200**	**128000**	**256000**	**576000**	**923076**
External clock	**4**	√	√	√	√	√	√	√	√	√	√	√	√
	6	√	√	√	√	√	√	√	√	√	√	√	√
	8	√	√	√	√	√	√	√	√	√	√	√	√
	12	√	√	√	√	√	√	√	√	√	√	√	√
	16	√	√	√	√	√	√	√	√	√	√	√	√
	24	√	√	√	√	√	√	√	√	√	√	√	√
	32	√	√	√	√	√	√	√	√	√	√	√	√
Internal clock	8	√	√	√	√	√	√	√	√	√	√	√	√

- N32L40x, N32L43x, N32G43x series MCU BOOT V1.2

Clock parameters (MHz)		**Baud rate**																
		2400	**4800**	**9600**	**14400**	**19200**	**38400**	**57600**	**115200**	**128000**	**256000**	**576000**	**923076**	**1M**	**1.5 M**	**2M**	**2.25 M**	**3M**
External clock	4	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
	6	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
	8	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
	12	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
	16	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
	24	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
	32	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	/	√
Internal clock	8	√	√	√	√	√	√	√	√	√	√	√	√	√	/	/	/	/

2.2.2 CMD_GET_INF

The command reads the BOOT version number, chip model index, chip ID, and chip serialization information.

Upper-level instructions:

bit byte	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x10 Level-1 command field							
1(CMD_L)	0x00 Level-2 command field							
2~3 (LEN)	Length of sent data							
4~7(Par)	Reserved							
(DAT)	None							

- Reserved value: 0x00.
- LEN Send data length: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] +(LEN[1]<<8).

Underlying response:

bit byte	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x10 Level-1 command field							
1(CMD_L)	0x00 Level-2 command field							
2~3 (LEN)	The length of the data							
4~54(DAT)	BOOT version number, chip model index, chip ID, and chip serialization							
55(CR1)	Status byte 1							
56(CR2)	Status byte 2							

- The procedure byte (CMD_H) corresponds to the upper instruction (CMD_H).
- LEN is the data length: 0x33(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- DAT[0] Chip model index

Product number: 0x01

- DAT[1] 0xXY, BOOT command set version number (BCD code)

  0x10: indicates the command set version used by BOOT, indicating that V1.0 command set version is used
- DAT[2] : BOOT code version
- DAT[3~50] 48Byte

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

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

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

UCID/ UID/ DBGMCU_IDCODE For details, see UM_N32G45x Series User Manual, UM_N32G4FR Series User Manual, UM_N32WB452 Series User Manual, UM_N32G43x Series User Manual, UM_N32L40x Series User Manual, UM_N32L43x Series User Manual

DAT[35~50] : 16 bytes (reserved);

- Status bytes (CR1 and CR2) are divided into the following types according to command execution:

1. Return success: status flag bit (0xA0, 0x00).
2. Return failure: status flag bits (0xB0, 0x00).

2.2.3 CMD_KEY_RNG

Gets the random number of the key that the user needs to verify.

Upper-level instructions:

byte bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x20 Level-1 command field							
1(CMD_L)	0x00 Level-2 command field							
2~3(LEN)	Length of sent data							
4~7(Par)	Reserved							
(DAT)	None							

- Reserved value: 0x00;
- LEN Send data length: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).

Underlying response:

byte bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x20 Level-1 command field							
1(CMD_L)	0x00 Level-2 command field							
2~3(LEN)	Length of sent data							
4~19(DAT)	A truly random number of 16Bytes							
20(CR1)	Status byte 1							
21(CR2)	Status byte 2							

- LEN Send data length: 0x10(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- The true random number of 16 bytes is generated by the chip.
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:

1. Return success: status flag bit (0xA0, 0x00).
2. Return failure: status flag bits (0xB0, 0x00).

2.2.4 CMD_KEY_UPDATE

The user can update the encryption download key and partition authentication key. Before updating, the user needs to use CMD_KEY_RNG to obtain a random number. The random number is used by the upper computer to produce a 16Bytes old key authentication value, which is then sent to the BOOT by using the CMD_KEY_UPDATE command. This verifies whether to update the key.The new key needs to be decrypted with the old key.

Upper-level instructions:

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x21 Level-1 Command field							
1(CMD_L)	Secondary command field: KEY index ID							
2~3(LEN)	Length of sent data							
4~7(Par)	Reserved value: 0x00							
8~55(DAT)	DAT[0~15] : 16Bytes old key authentication value							
	DAT[16~31] : indicates the new encryption value of 16 bytes							
	DAT[32~47] : indicates the CRC32 encryption value 4Bytes CRC32 check value (old key + new key) + 12Bytes fill the value 0x00 The 16Bytes of data are then encrypted with the old key							

- CMD_L: indicates the ID of the key index to be updated
  1. ID(0x00-0x1f) : indicates the ID of the key index.
- LEN Send data length: 0x30(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Reserved value: 0x00.
- DAT[32~47] : indicates the CRC32 parity value.
- DAT[0~15] : a 16-bit random number obtained by CMD_KEY_RNG and an authentication value generated by the old key.
- DAT[16-31] : indicates a new key encrypted with the old key. BOOT indicates a new key decrypted with the old key and then saved.

Underlying response:

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x21 Level-1 Command field							

1(CMD_L)	Secondary command field: key ID
2~3(LEN)	Length of sent data
(DAT)	None
4(CR1)	Status byte 1
5(CR2)	Status byte 2

- LEN Send data length: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:

1. Return success: status flag bit (0xA0, 0x00).
2. Return failure: status flag bits (CR1, CR2)
   1) (0xB0, 0x00) : return failed.
   2) (0xB0, 0x10) : The key index ID range is incorrect.
   3) (0xB0, 0x11) : The CRC check of the new key is incorrect.
   4) (0xB0, 0x20) : Authentication of the old key fails.
   5) (0xB0, 0x21) : The number of old key authentication failures exceeds the limit.
   6) (0xB0, 0x3F) : Failed to update the management information.

2.2.5 CMD_FLASH_ERASE

BOOT erases the FLASH by page. The page address number and page number can be specified by the user. The erasure space cannot exceed the entire FLASH space and at least one page can be erased.

If the authentication function is enabled, the CMD_KEY_RNG command is used to obtain a random number and perform authentication before erasing the authentication function.

BOOT erases the FLASH by page. The page address number and page number can be specified by the user. The erasure space cannot exceed the entire FLASH space and at least one page can be erased.

Upper-level instructions:

bit / byte	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x30 Level-1 command field							
1(CMD_L)	Level-2 command field: Erase partition number							
2~3(LEN)	Length of sent data							
4~7(Par)	Page address number 2 bytes: 0 to 255 Page Number 2 bytes :1 to 256							

8~23(DAT)	DAT[0~15] : 16 bytes User1/2/3 partition authentication key authentication value, used only when authentication is enabled

- CMD_L: erases the partition number
  1. 0 x00 = USER1;
  2. 0 x01 = USER2;
  3. 0 x02 = USER3;
- LEN Send data length: 0x10(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- The erase address and range consist of four bytes in the Par field

  Par[0~1] : page address number 2 bytes (0~255)

  Page address = Par [0] + (Par [1]<<8);

  Par[2~3] : Page number 2 bytes (1~256)

  Page count = Par [2] + (Par [3]<<8);

  The beginning address of page 0 is 0x0800_0000. The number of subsequent pages is incremented by 1, and the first address is incremented by 0x800.

  Such as:

  The beginning address of page 1 is 0x0800_0000 + 1*0x800 = 0x0800_0800

  The beginning address of page 2 is 0x0800_0000 + 2*0x800 = 0x0800_1000

  The entire address range erased

  For example, the page address is 0x01 and the number of pages is 0x02

  Erasing address range:

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

  That is, (first address of the page number) to (First address of the page number + number of pages x page size)

Underlying response:

bit / byte	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x30 Level-1 command field							
1(CMD_L)	Secondary command field: Erase area							
2~3(LEN)	Length of sent data							
(DAT)	None							
4(CR1)	Status byte 1							
5(CR2)	Status byte 2							

- LEN Send data length: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).

- Status bytes (CR1 and CR2) are divided into the following types according to command execution:

1. Return success: status flag bit (0xA0, 0x00).
2. Return failure: status flag bits (CR1, CR2).
   1) (0xB0, 0x00) : return failed.
   2) (0xB0, 0x20) : Key authentication fails.
   3) (0xB0, 0x21) : The number of key authentication failures exceeds the limit.
   4) (0xB0, 0x30) : The erased FLASH page is protected by RDP.
   5) (0xB0, 0x31) : The erased FLASH page is protected by WRP.
   6) (0xB0, 0x32) : deletes the FLASH page to be partitioned.
   7) (0xB0, 0x34) : Erasing the FLASH address range exceeds the threshold (indicates that the FLASH size exceeds the threshold).
   8) (0xB0, 0x37) : Failed to erase the FLASH.
   9) (0xB0, 0x3F) : Failed to update the management information.
   10) (0xB0, 0x3F) : Failed to update the management information.

2.2.6 CMD_FLASH_DWNLD

This command provides the user to download the code into the specified FLASH, and the data length must be 16 bytes aligned (less than 0x00 automatically added by the upper computer), which is provided by the upper-layer command.

When authentication or encryption is enabled, the CMD_KEY_RNG command is used to obtain a random number before authentication or encryption is enabled.For partition authentication and encryption download, you need to provide the partition number.To encrypt the downloaded data, decrypt the data into plaintext by encrypting the download key (that is, the key used for partition authentication) and write the data into the FLASH.

Upper-level instructions:

bit / byte	b7	b6	b5	b4	b3	b2	b1	b0
1(CMD_H)	0x31 Level-1 command field							
2(CMD_L)	Secondary command field: Download partition number							
3~4(LEN)	Length of sent data							
5~8(Par)	Start address for downloading the FLASH							
8~23+N(DAT)	DAT[0~15] : 16 bytes Key authentication value for user1/2/3 partition authentication DAT[16~16+N] : Specific data downloaded (encrypted or unencrypted)							

	DAT[N+1~N+4] : indicates the 4 byte CRC32 check value of unencrypted data

- CMD_L: indicates the number of the download partition
  1. 0x00 = USER1;
  2. 0x01 = USER2;
  3. 0x02 = USER3;
- LEN[0]), 0xXX(LEN[1]), LEN = LEN[0] + (LEN[1]<<8)
- Par [0 ~ 3]: download the starting Address of the FLASH, synthetic rules to Address = Par [0] 8 | | Par [1] < < Par [2] | Par [3] < < < < 16 to 24.
- DAT [0~15], Reserved.
- DAT[16~16+N] : Specific data to be downloaded
  1. USB: a maximum of 128 bytes, 15<=N<=143, N+1 must be a multiple of 16.
  2. USART: contains a maximum of 128 bytes. 15<=N<=143. N+1 must be a multiple of 16.

DAT[N+1 to N+4] : 4Byte CRC32 check value of unencrypted data

Underlying response:

bit byte	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x31 Level-1 command field							
1(CMD_L)	Secondary command field: Download partition number							
2(LEN)	Length of sent data							
(DAT)	None							
3(CR1)	Status byte 1							
4(CR2)	Status byte 2							
5(XOR)	Xor result							

- LEN Send data length: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:
  1. Download success: status flag bit (0xA0, 0x00).
  2. Download failed: status flag bit (CR1, CR2).
     1) (0xB0, 0x00) : return failed.
     2) (0xB0, 0x20) : Key authentication fails.
     3) (0xB0, 0x21) : The number of key authentication failures exceeds the limit.
     4) (0xB0, 0x30) : The downloaded FLASH address is protected by RDP.
     5) (0xB0, 0x31) : The downloaded FLASH address is protected by WRP.

6) (0xB0, 0x32) : The downloaded FLASH address is protected by a partition.

7) (0xB0, 0x33) : Download FLASH address range across partitions;

8) (0xB0, 0x34) : The address range of the downloaded FLASH exceeds the threshold.

9) (0xB0, 0x35) : Download FLASH start address is not 16-byte alignment;

10) (0xB0, 0x36) : The downloaded FLASH data length is not a multiple of 16.

11) (0xB0, 0x37) : Programming the FLASH fails.

12) (0xB0, 0x3F) : The management information fails to be updated.

2.2.7 CMD_DATA_CRC_CHECK

This command is used to check whether the downloaded data is correct. Considering the download speed and low probability of download failure, the CRC check is performed after the downloaded data is complete. The upper-layer command must provide the CRC value, start address, and check length of the downloaded data.

When authentication is enabled, the CMD_KEY_RNG command is used to obtain a random number and perform authentication before CRC verification.

Upper-level instructions:

bit byte	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x32 Level-1 command field							
1(CMD_L)	Level-2 command field: Parity partition number							
2~3(LEN)	Length of sent data							
4~7(Par)	32-bit CRC check value							
8~31(DAT)	DAT[0~15] : 16 bytes Key authentication value for user1/2/3 partition authentication DAT[16~19] : indicates the start IP address of the verification DAT[20~23] : parity length (in bytes, minimum length 2KB)							

- CMD_L: indicates the verification partition number
  1. 0x00 = USER1;
  2. 0x01 = USER2;
  3. 0x02 = USER3;
- LEN Send data length: 0x18(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Par[0 ~ 3]: 32 bit CRC checksum value, the synthetic rules for CRC32 = Par[0] | Par[1]<<8 | Par[2]<<16 | Par[3]<<24.
- DAT[0:15] : authentication key authentication value
- DAT[16~19]: check the starting Address, the synthesis rules to Address = DAT [16] | DAT

[17] < < 8 | DAT [18] < < 16 | DAT [19] < < 24, the Address can only be in the range of the FLASH.

- DAT[20~23]: check length, its synthesis rules for CRC_LEN = DAT [20] | DAT [21] < < 8 | DAT [22] < < 16 | DAT [23] < < 24, CRC_LEN is only within the effective range, length is larger than 2 KB, and is a multiple of 16.

Underlying response:

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x32 Level-1 command field							
1(CMD_L)	Level 2 command field: Parity partition number							
2~3(LEN)	Length of sent data							
(DAT)	None							
4(CR1)	Status byte 1							
5(CR2)	Status byte 2							

- LEN Send data length: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:

1. Verification succeeded: status flag bit (0xA0, 0x00).
2. Check failure: status flag bits (CR1, CR2)

   1) (0xB0, 0x00) : return failed.
   2) (0xB0, 0x20) : CRC verification key authentication fails.
   3) (0xB0, 0x21) : The number of CRC key authentication failures exceeds the limit.
   4) (0xB0, 0x32) : indicates that CRC check addresses are protected by partitions.
   5) (0xB0, 0x33) : indicates that the ADDRESS range of CRC check is across partitions.
   6) (0xB0, 0x34) : Indicates that the ADDRESS range of CRC check exceeds the threshold.
   7) (0xB0, 0x35) : indicates that CRC addresses are not aligned with 16 bytes.
   8) (0xB0 or 0x36) : indicates that the CRC check length is not a multiple of 16 or less than 2KB.
   9) (0xB0, 0x38) : CRC verification fails.
   10) (0xB0, 0x3F) : The management information fails to be updated.

2.2.8 CMD_OPT_RW

This command is used for option byte read and write (including read protection level, FLASH page write protection, datA0/1 configuration, and USER configuration).

Upper-level instructions:

bit / byte	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x40 Level-1 command field							
1(CMD_L)	Secondary command field							
2~3(LEN)	Length of sent data							
4~7(Par)								
8~27(DAT)	Option byte configures 20 bytes							

- CMD_L Secondary command field:
  1. 0x00: Gets option bytes.
  2. 0x01: Configuration option byte.
  3. 0x02: Configuration option byte, reset again.
- LEN Send data length: 0x14(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- DAT[0~19] : Option byte 20 bytes

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

1. CMD_L = 0x00: all values are 0x00.
2. CMD_L = 0x01/0x02: Configuration option bytes are the values to be written.

Underlying response:

bit / byte	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x40 Level-1 command field							
1(CMD_L)	Secondary command field							
2~3(LEN)	Length of sent data							
4~23(DAT)	Option byte configures 20 bytes							
24(CR1)	Status byte 1							
25(CR2)	Status byte 2							

- LEN Send data length: 0x14(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- DAT[0~19] : The current option contains 20 bytes

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

- Status bytes (CR1 and CR2) are divided into the following types according to command execution:

1. Return success: status flag bit (0xA0, 0x00).
2. Check failure: status flag bits (CR1, CR2)
   1) (0xB0, 0x00) : return failed.

2.2.9 CMD_ USERX_OP

This command is used to read or configure the size of the user1/2/3 partition. After the partition is configured, the partition is automatically sealed.The user1/2/3 partition can be configured only once. The software determines whether the NVR MMU partition has been configured (process variables or random delay are added to determine the NVR value).

The recommended configuration process is as follows:

1. If you need to divide two areas, configure USER3 (automatic sealing is complete).If you want to also seal USER1, configure USER1 again.The size of USER1 + USER3 must be the size of the entire FLASH;

2. To divide three zones, configure USER3 (automatic sealing is configured) and then USER2 (automatic sealing is configured).If you want to also seal USER1, configure USER1 again.The size of USER1 + USER2 + USER3 must be the size of the entire FLASH.

Upper-level instructions:

byte \ bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x41 Level-1 command field							
1(CMD_L)	Secondary command field							
2~3(LEN)	Length of sent data							
4~7(Par)	Par[0] : Partition User1/2/3							
	Par [1] : Partition user1/2/3 size							
	Par [2] : Partition authentication key index ID							
	Par [3] : Partition authentication and encryption download enable configuration							
DAT	None							

- CMD_L Secondary command field:

    1. 0x00: Read partition user1/2/3 size configuration.
    2. 0x01: Partition user1/2/3 size, key ID, and partition authentication/encryption download are enabled.

- LEN Send data length: 0x00(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- Par[0] : Partition number

    1. 0x00: partition USER1.
    2. 0x01: partition USER2.
    3. 0x02: partition USER3.

- Par [1] :

1. CMD_L = 0x00:0x00.
2. CMD_L = 0x01: partition user1/2/3 size configuration

Input range for partition size: 0x1(16KB)... 0x1F(496KB), 0x20(512KB), USER1 + USER2 + USER3 = 512KB;The user area user1/2/3 size is automatically sealed after configuration.

Partition size and address determined

The start address of the partition is 0x0800_0000, and the end address of the partition is the start address plus the total FLASH capacity (for example, if the FLASH capacity is 512 KB, the end address is 0x0800_0000 + 512*0x800 = 0x0808_0000).

If USER1 is partitioned, the partition address of USER1 ranges from 0x0800_0000 to (0x0800_0000 + USER1_Size*0x4000).

If USER3 is partitioned, the partition address of USER3 ranges from (0x0808_0000 - USER3_Size*0x4000) to 0x0800_8000 (for example, the last FLASH address is 0x0808_0000).

The initial address of the partition of USER2 is the last address of USER1 and the first address of USER3.If USER1 has no partition, the first address of USER2 needs to be determined by USER2_Size.

- Par [2] :

1. CMD_L = 0x00:0xFF.
2. CMD_L = 0x01:0x00~0x1F Encrypted Download/Partition authentication key index ID, 0xFF indicates that the index ID is not configured. If the corresponding USERX is not configured with an ID, the value of Par[3] is not judged.

- Par [3] :

Enable configuration of partition authentication and encrypted download, 0xXY

X = 0 - If zone authentication is not enabled, set this parameter to 1.

X = 1 - If zone authentication is enabled, the value cannot be 0.

Y = 0 - If encrypted download is not enabled, set this parameter to 1.

Y = 1 - Encrypted download is enabled and cannot be set to 0.

1. CMD_L = 0x00: read status, retain value 0x00;
2. CMD_L = 0x01: configuration status, configuration value 0xXY;

Underlying response:

byte bit	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x41 Level-1 command field							

1(CMD_L)	Secondary command field
2~3(LEN)	Length of sent data
4~7(DAT)	DAT[0] : partition user1/2/3
	DAT[1] : partition user1/2/3 size
	DAT [2] : Indicates the configuration status of the partition authentication key index ID
	DAT [3] : Read partition authentication and encryption download enable configuration
8(CR1)	Status byte 1
9(CR2)	Status byte 2

- LEN Send data length: 0x02(LEN[0]), 0x00(LEN[1]), LEN = LEN[0] + (LEN[1]<<8).
- DAT[0] : indicates the partition number
  1. 0x00: partition USER1.
  2. 0x01: partition USER2.
  3. 0x02: partition USER3.
- DAT[1] : Read the current partition user1/2/3 size

  Partition size output range: 0x0(0KB), 0x1(16KB)... 0x1F (496 KB), 0x20 (512 KB). 0x0 indicates that the partition size is not configured. USER1 + USER2 + USER3 = 512KB.
- DAT [2].
  1. 0x00, the ID has been configured.
  2. 0xFF, ID is not configured
- DAT [3] :

  Read partition authentication and encryption download enable configuration, 0xXY

  X = 0 - If zone authentication is not enabled, set this parameter to 1.

  X = 1 - If zone authentication is enabled, the value cannot be 0.

  Y = 0 - If encrypted download is not enabled, set this parameter to 1.

  Y = 1 - Encrypted download is enabled and cannot be set to 0.
- Status bytes (CR1 and CR2) are divided into the following types according to command execution:
  1. Return success: status flag bit (0xA0, 0x00).
  2. Return failure: status flag bit (0x70, 0x00)
     1) (0xB0, 0x00) : return failed.

2) (0xB0, 0x10) : The key index ID range is incorrect.
3) (0xB0, 0x3A) : The partition size has been configured and cannot be configured again.
4) (0xB0, 0x3B) : the partition size is incorrectly configured. USER1 + USER2 + USER3 = FLASH capacity. The minimum value for user1/2 /2/3 is 0x01(16KB).
5) (0xB0, 0x3C) : The partition configuration sequence is incorrect and USER1 or USER3 must be configured first.
6) (0xB0, 0x3D) : The partition key index ID fails to be configured or has been configured.
7) (0xB0, 0x3E) : The configuration of zone authentication and encryption download fails or has been configured.
8) (0xB0, 0x3F) : Failed to update the management information.

2.2.10CMD_SYS_RESET

This command is used to reset the BOOT program.

Upper-level instructions:

bit byte	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x50 Level-1 command field							
1(CMD_L)	0x00 Level-2 command field							
2~3(LEN)	Length of sent data							
4~7(Par)	Reserved							
(DAT)	None							

- Reserved value: 0x00;

Underlying response:

bit byte	b7	b6	b5	b4	b3	b2	b1	b0
0(CMD_H)	0x50 Level-1 command field							
1(CMD_L)	0x00 Level-2 command field							
2~3(LEN)	Length of sent data							
(DAT)	None							
4(CR1)	Status byte 1							
5(CR2)	Status byte 2							

- Status bytes (CR1 and CR2) are divided into the following types according to command execution:

1. Return success: status flag bit (0xA0, 0x00).
2. Return failure: status flag bits (0xB0, 0x00).

2.3 Returns the status word description

2.3.1 Returns the success status word

Return success: status flag bit (0xA0, 0x00).It indicates that the command delivered by the upper layer is successfully executed. The returned success status contains the returned value of the read, update, and configuration commands.

2.3.2 Returns the failure status word

Return failure: status flag bits (0xB0, 0x00).Indicates that the command delivered by the upper layer fails to be executed due to other reasons (such as incorrect command acceptance format or timeout). Failure status is returned.

2.3.3 Return other status word

The following return status words also return failure. The second byte status word indicates a different error type.

1) (0xB0, 0x10) : The key index ID range is incorrect.
2) (0xB0, 0x11) : The CRC check of the new key is incorrect.
3) (0xB0, 0x20) : Key authentication fails.
4) (0xB0, 0x21) : The number of key authentication failures exceeds the limit.
5) (0xB0, 0x30) : Eraser/download FLASH page protected by RDP;
6) (0xB0, 0x31) : Erasing/downloading FLASH pages is protected by WRP.
7) (0xB0, 0x32) : Erase/download /CRC addresses are protected by partitions.
8) (0xB0, 0x33) : erase/download /CRC check address range across partitions;
9) (0xB0, 0x34) : The address range of erase/download /CRC is out of bounds (indicating that the size of the FLASH exceeds the limit).
10) (0xB0, 0x35) : The start address of erase/download /CRC is not 16-byte alignment;
11) (0xB0, 0x36) : Indicates that the length of the downloaded /CRC data is not a multiple of 16.Data length indicates the length of erasing FLASH, or the length of downloading code to FLASH, or the length of checking FLASH CRC values;
12) (0xB0, 0x37) : Erasing or downloading the FLASH program fails.
13) (0xB0, 0x38) : CRC verification fails.
14) (0xB0, 0x39) : A partition has been configured and the read protection level cannot be changed from L1 to L0.

15) (0xB0, 0x3A) : The partition has been configured and cannot be configured again.
16) (0xB0, 0x3B) : The partition size is incorrect. USER1 + USER2 + USER3 = FLASH capacity.
17) (0xB0, 0x3C) : The partition configuration sequence is incorrect and USER1 or USER3 must be configured first.
18) (0xB0, 0x3D) : The partition key index ID fails to be configured or has been configured.
19) (0xB0, 0x3E) : The configuration of zone authentication and encryption download fails or has been configured.
20) (0xB0, 0x3F) : Failed to update the management information.
21) (0xBB, 0xCC) : The level 1 and level 2 command fields do not belong to any command.

3 BOOT Instructions

3.1 Upper computer control process

Upper computer support user erasing FLASH area, user code download, download code integrity check.By reading partition information, the upper computer automatically identifies the address range of erasing, downloading and checking entered by the user and requires authentication.

Upper computer supports users to choose whether to enable encryption download to protect user code.

Upper computer supports the user to read and configure the partition user1/2/3 size.The partition size cannot be changed after being configured.

Upper computer supports users to update the security key (used for partition authentication and encryption download).

Upper computer supports user update option byte reading and modification.

Upper computer supports software reset command and jump USER1 reset program entry address execution command.

Enter BOOT: After you log in to the BOOT, you can interact with the PC TOOL through the USART1 or USB port.

Chip firmware integrity check: Select BOOT from the system storage area, and BOOT automatically verifies the integrity. If the verification fails, an infinite loop will be entered, and subsequent functions cannot be used.

Command set interaction: The PC TOOL sends different commands based on the command set supported by the BOOT to use corresponding functions.

1. Read BOOT version number, chip model index, chip ID;
2. Get 16byte true random number;
3. Update the security key (for partition authentication and encrypted download);
4. Erase FLASH;
5. Download user programs to FLASH;
6. CRC verification of downloaded user programs;
7. Read/configure option bytes (including read protection level, FLASH page write protection, datA0/1 configuration, USER configuration);
8. Get partition USERX size, set partition USERX size;
9. System reset, you can reset the BOOT program to run again;
10. Jump to USER1 reset program entry address, jump to the reset program entry address downloaded to USER1 partition code;

3.1.1 Erase command control flow chart

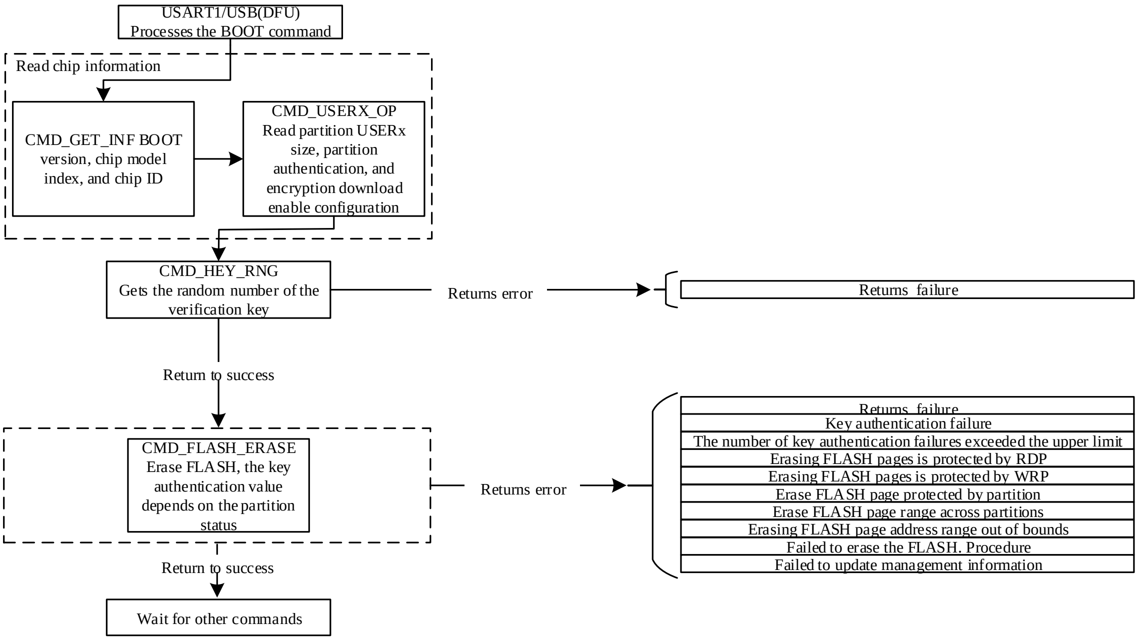
USART1/USB(DFU)
Processes the BOOT command
Read chip information
CMD_GET_INF BOOT version, chip model index, and chip ID
CMD_USERX_OP Read partition USERx size, partition authentication, and encryption download enable configuration
CMD_HEY_RNG Gets the random number of the verification key
Returns error
Returns failure
Return to success
CMD_FLASH_ERASE Erase FLASH, the key authentication value depends on the partition status
Returns error
Returns failure
Key authentication failure
The number of key authentication failures exceeded the upper limit
Erasing FLASH pages is protected by RDP
Erasing FLASH pages is protected by WRP
Erase FLASH page protected by partition
Erase FLASH page range across partitions
Erasing FLASH page address range out of bounds
Failed to erase the FLASH. Procedure
Failed to update management information
Return to success
Wait for other commands

Figure3.1 flowchart of erasing command control

3.1.2 Download the command control flow chart

Partition authentication encryption obtains a random number before downloading, and the host computer uses this random number to generate the key authentication value of 16-byte USER1/2/3 partition authentication.In the case of continuous download, the random number used in the subsequent download command is generated by the random number deriving algorithm of the first time instead of obtaining a new random number.

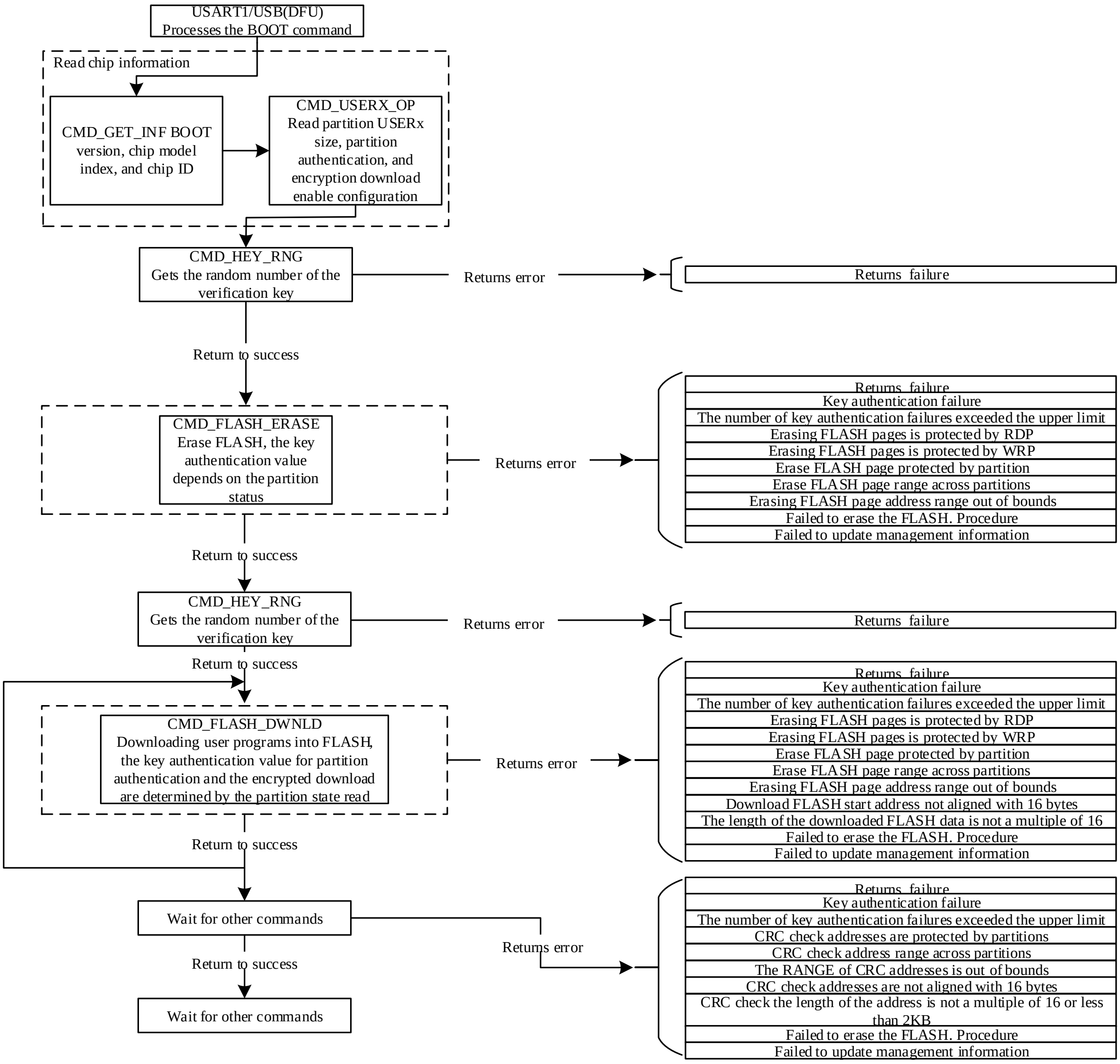
USART1/USB(DFU) Processes the BOOT command
Read chip information
CMD_GET_INF BOOT version, chip model index, and chip ID
CMD_USERX_OP Read partition USERx size, partition authentication, and encryption download enable configuration
CMD_HEY_RNG Gets the random number of the verification key
Returns error
Returns failure
Return to success
CMD_FLASH_ERASE Erase FLASH, the key authentication value depends on the partition status
Returns error
Returns failure
Key authentication failure
The number of key authentication failures exceeded the upper limit
Erasing FLASH pages is protected by RDP
Erasing FLASH pages is protected by WRP
Erase FLASH page protected by partition
Erase FLASH page range across partitions
Erasing FLASH page address range out of bounds
Failed to erase the FLASH. Procedure
Failed to update management information
Return to success
CMD_HEY_RNG Gets the random number of the verification key
Returns error
Returns failure
Return to success
CMD_FLASH_DWNLD Downloading user programs into FLASH, the key authentication value for partition authentication and the encrypted download are determined by the partition state read
Returns error
Returns failure
Key authentication failure
The number of key authentication failures exceeded the upper limit
Erasing FLASH pages is protected by RDP
Erasing FLASH pages is protected by WRP
Erase FLASH page protected by partition
Erase FLASH page range across partitions
Erasing FLASH page address range out of bounds
Download FLASH start address not aligned with 16 bytes
The length of the downloaded FLASH data is not a multiple of 16
Failed to erase the FLASH. Procedure
Failed to update management information
Return to success
Wait for other commands
Returns error
Returns failure
Key authentication failure
The number of key authentication failures exceeded the upper limit
CRC check addresses are protected by partitions
CRC check address range across partitions
The RANGE of CRC addresses is out of bounds
CRC check addresses are not aligned with 16 bytes
CRC check the length of the address is not a multiple of 16 or less than 2KB
Failed to erase the FLASH. Procedure
Failed to update management information
Return to success
Wait for other commands

Figure3.2 flowchart for downloading command control

3.1.3 Update the key command control flow chart

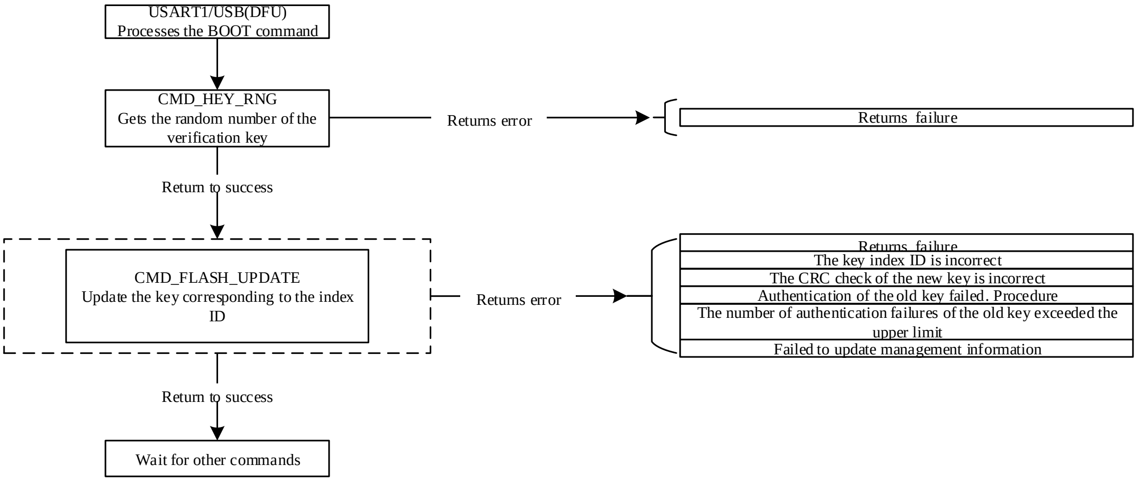
USART1/USB(DFU) Processes the BOOT command
CMD_HEY_RNG Gets the random number of the verification key
Returns error
Returns failure
Return to success
CMD_FLASH_UPDATE Update the key corresponding to the index ID
Returns error
Returns failure
The key index ID is incorrect
The CRC check of the new key is incorrect
Authentication of the old key failed. Procedure
The number of authentication failures of the old key exceeded the upper limit
Failed to update management information
Return to success
Wait for other commands

Figure3.3 command control flowchart for updating a key

3.1.4 Flow chart of partition operation commands

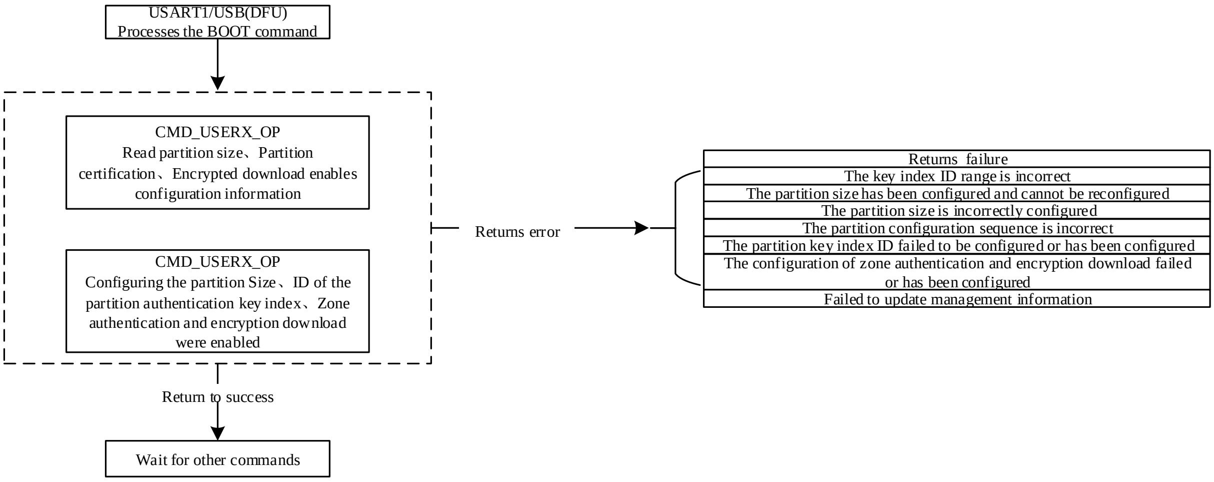
USART1/USB(DFU)
Processes the BOOT command
CMD_USERX_OP
Read partition size、Partition certification、Encrypted download enables configuration information
CMD_USERX_OP
Configuring the partition Size、ID of the partition authentication key index、Zone authentication and encryption download were enabled
Returns error
Returns failure
The key index ID range is incorrect
The partition size has been configured and cannot be reconfigured
The partition size is incorrectly configured
The partition configuration sequence is incorrect
The partition key index ID failed to be configured or has been configured
The configuration of zone authentication and encryption download failed or has been configured
Failed to update management information
Return to success
Wait for other commands

Figure ure3.4 Flow chart of commands for Partition Operations

3.1.5 Option byte read/write command control flowchart

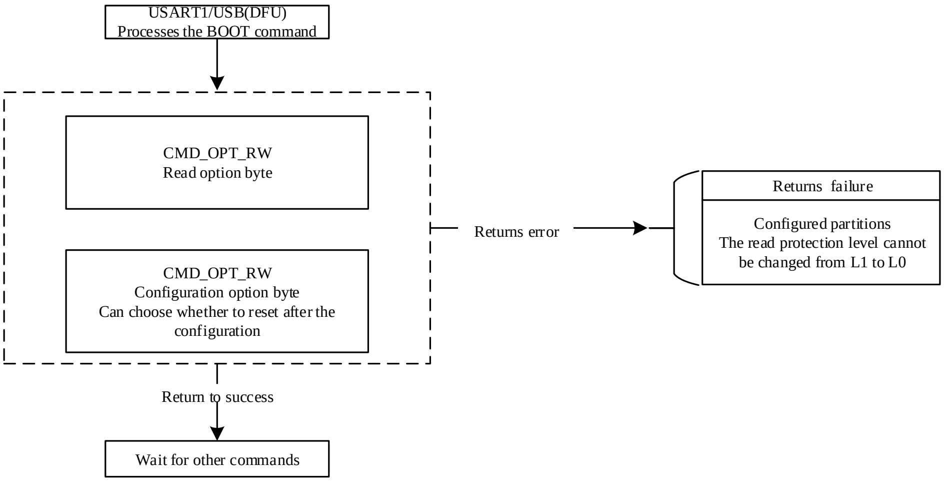
USART1/USB(DFU)
Processes the BOOT command
CMD_OPT_RW
Read option byte
CMD_OPT_RW
Configuration option byte
Can choose whether to reset after the configuration
Returns error
Returns failure
Configured partitions
The read protection level cannot be changed from L1 to L0
Return to success
Wait for other commands

Figure3.5 flowchart of option byte read/write command control

4 Version History

Version	Date	Note
V1.0	2020-04-09	Create a document
V1.1	2020-08-04	1. Add USB interface crystal mode control word; 2. Added the timeout function of the UART interface. 3. Add NVR MSI write interface;
V1.2	2020-12-21	1. Modify the NVR data programming did not clear the error mark problem; 2. Fixed the BUG that NVR cannot be read after NVR sealing; 3. Added a timeout mechanism for HIS detection 4. Optimize code space
V1.3	2022-7-6	1. Deleted chapter 2.2.11 CMD_APP_GO； 2. Fixed some typos.

5 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.