PM0019
Programming Manual

AT32 Bootloader SPI Protocol

Introduction

This user manual describes the SPI protocol used in the AT32 MCU bootloader, detailing the supported commands and their operating procedure. For more information about the SPI hardware resources and requirements for your device bootloader, refer to the document PM0007_AT32_Bootloader_Program_Manual.

Contents

1 SPIx bootloader code sequence 7

2 Bootloader command set 9

3 Bootloader command description 10

3.1 Get Command 10

3.1.1 Flow chart on host and device sides 10

3.1.2 Data transmit on host side 11

3.2 Get Version command 12

3.2.1 Flowchart on host and device sides 12

3.2.2 Data transmit on host side 14

3.3 Get Device ID command 14

3.3.1 Flowchart on host and device sides 15

3.3.2 Data transmit on host side 16

3.4 Read Memory command 17

3.4.1 Flowchart on host and device sides 18

3.4.2 Data transmit on host side 20

3.5 Jump command 20

3.5.1 Flowchart on host and device sides 21

3.5.2 Data transmit on host side 23

3.6 Write Memory command 23

3.6.1 Flowchart on host and device sides 24

3.6.2 Data transmit on host side 26

3.7 Erase command 26

3.7.1 Flowchart on host and device sides 28

3.7.2 Data transmit on host side 30

3.8 Erase and Program Protect command 30

3.8.1 Flowchart on host and device sides 31

3.8.2 Data transmit on host side 32

3.9 Erase and Program Unprotect 33

3.9.1 Flowchart on host and device sides 33

3.9.2 Data transmit on host side 34

3.10 Access Protect command 34
3.10.1 Flowchart on host and device sides 35
3.10.2 Data transmit on host side 36
3.11 Access Unprotect command 37
3.11.1 Flowchart on host and device sides 37
3.11.2 Data transmit on host side 38
3.12 Firmware CRC command 39
3.12.1 Flowchart on host and device sides 39
3.12.2 Data transmit on host side 42
3.13 Enable sLib 43
3.13.1 Flowchart on host and device sides 44
3.13.2 Data transmit on host side 46
3.14 Disable sLib 46
3.14.1 Flowchart on host and device sides 47
3.14.2 Data transmit on host side 49
3.15 Get sLib status 49
3.15.1 Flowchart on host and device sides 50
3.15.2 Data transmit on host side 52
3.16 Reset Device 52
3.16.1 Flowchart on host and device sides 53
3.16.2 Data transmit on host side 54
3.17 Advanced Access Protect 55
3.17.1 Flowchart on host and device sides 55
3.17.2 Data transmit on host side 56

4 Revision history 57

List of tables

Table 1 List of erase type 27
Table 2 Document revision history 57

List of figures

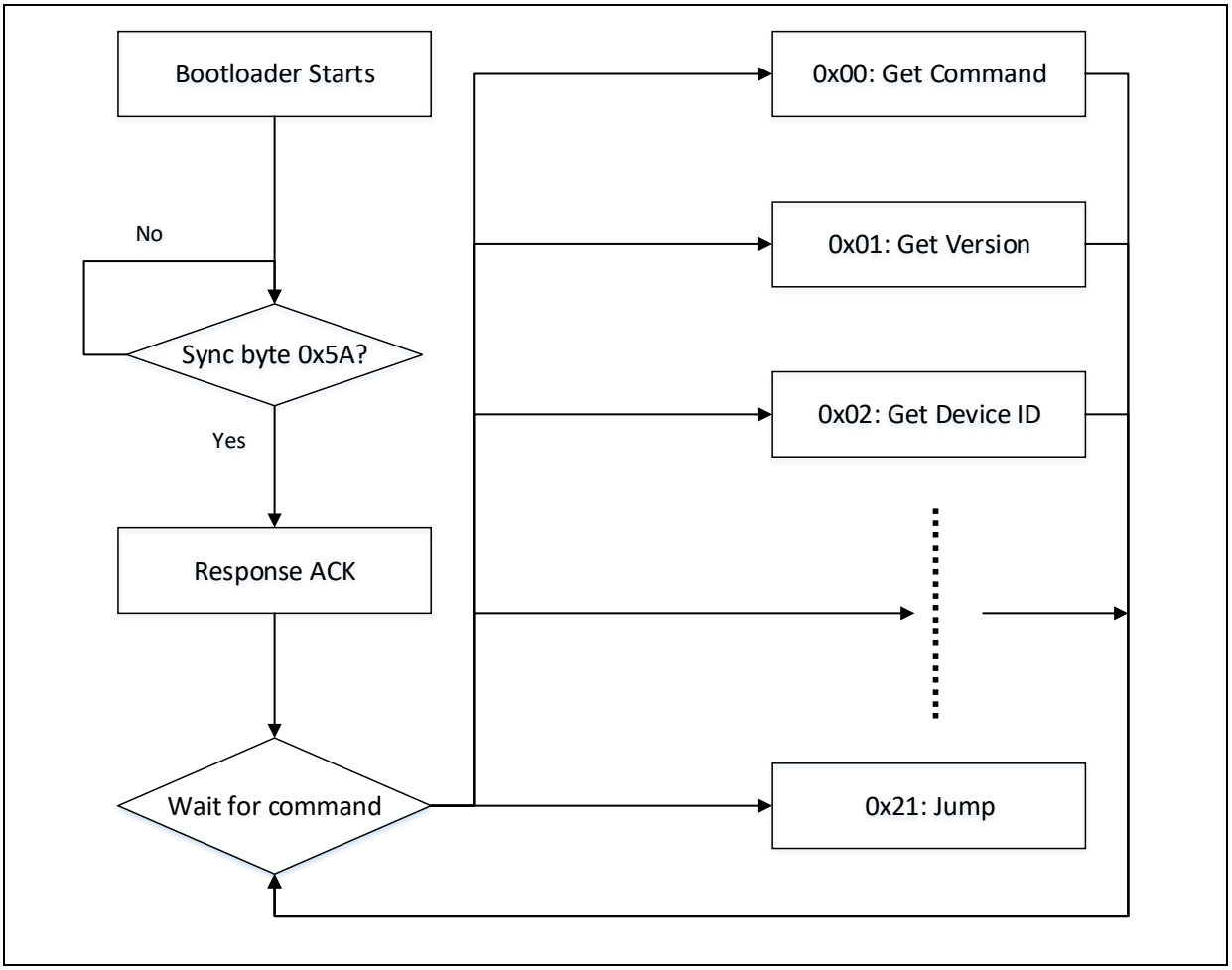
Figure 1 Bootloader Main Loop 7
Figure 2 Get ACK procedure (host side) 8
Figure 3 Synchronization connection timing 8
Figure 4 SPI command timing 8
Figure 5 Get Commands: host side 10
Figure 6 Get Commands: device side 11
Figure 7 Get Version: host side 12
Figure 8 Get Version: device side 13
Figure 9 Get Device ID: host side 15
Figure 10 Get Device ID: device side 16
Figure 11 Read Memory: host side 18
Figure 12 Read Memory: device side 19
Figure 13 Jump: host side 21
Figure 14 Jump: device side 22
Figure 15 Write Memory: host side 24
Figure 16 Write Memory: device side 25
Figure 17 Erase: host side 28
Figure 18 Erase: device side 29
Figure 19 Erase and Program Protect: host side 31
Figure 20 Erase and Program Protect: device side 32
Figure 21 Erase and Program Unprotect: host side 33
Figure 22 Erase and Program Unprotect: device side 34
Figure 23 Access Protect: host side 35
Figure 24 Access Protect: device side 36
Figure 25 Access Unprotect: host side 37
Figure 26 Access Unprotect: device side 38
Figure 27 Firmware CRC: host side 40
Figure 28 Firmware CRC: device side 41
Figure 29 Enable sLib: host side 44
Figure 30 Enable sLib: device side 45
Figure 31 Disable sLib: host side 47
Figure 32 Disable sLib: device side 48
Figure 33 Get sLib status: host side 50
Figure 34 Get sLib status: device side 51

Figure 35 Reset Device: host side 53
Figure 36 Reset Device: device side 54
Figure 37 Advanced Access Protect: host side 55
Figure 38 Advanced Access Protect: device side 56

1 SPIx bootloader code sequence

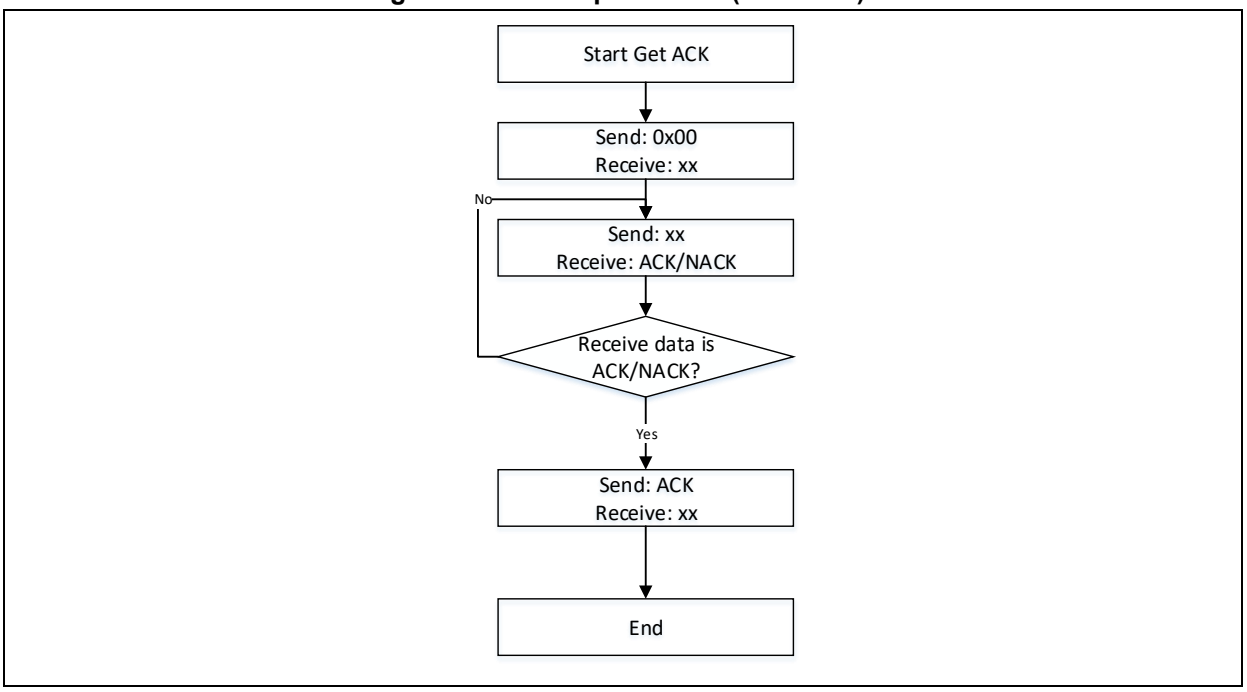
Once the SPI programming mode is entered, the SPIC as a slave device must have its CS pin connected to the ground. In this mode, the bootloader begins to scan the MOSI pin, waiting to receive a synchronization byte (0x5A), at the same time, it sends a synchronization byte (0xA5) via the MISO pin to the host. The reception of the 0xA5 byte by the host indicates a connection success. Meanwhile, the MCU waits for an ACK response to the host, as described in Figure 2. After the ACK completion, the MCU gets ready to receive host commands.

Figure 1 Bootloader Main Loop



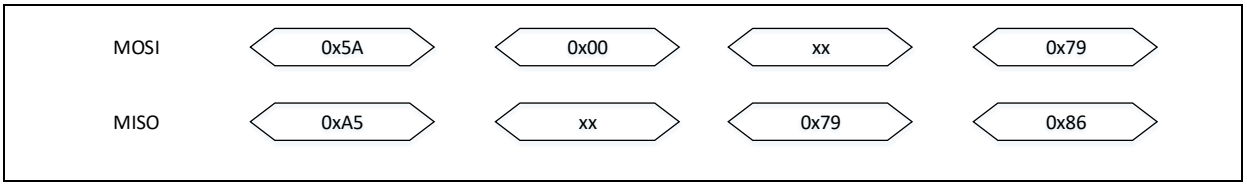
Get ACK procedure for host side: ACK = 0x79, NACK = 0x1F.

Figure 2 Get ACK procedure (host side)



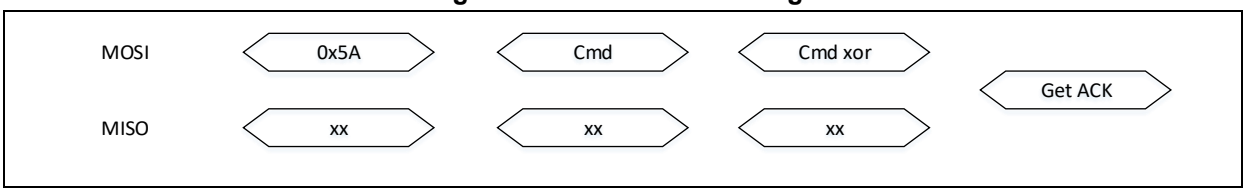
Synchronization byte inspection procedure: the host first sends a synchronization byte (0x5A), and the device sends back a 0xA5 byte. After this operation, the host waits for an ACK, as described in Figure 2.

Figure 3 Synchronization connection timing



To send a SPI command, the host must first send a synchronization byte (0x5A) and then a 2-byte command and command checksum, as described in Figure 4.

Figure 4 SPI command timing



Note: The minimum timing between bytes sent over the SPI is *15us*.

2 Bootloader command set

The number of the supported commands depends on the product series. However, for the same command set such as read, write or erase, they are entirely compatible across all the AT32 MCU series.

Bootloader commands

Command	Code	Description	Supported AT32 MCU series
Get Commands	0x00	Get the allowed commands supported by the device	Bootloader that supports SPI feature
Get Version	0x01	Get the protocol version of the bootloader	Bootloader that supports SPI feature
Get Device ID	0x02	Get the device ID.	Bootloader that supports SPI feature
Read memory	0x11	Read data of the memory starting from an address specified by the application	Bootloader that supports SPI feature
Jump	0x21	Jump to memory address executable application	Bootloader that supports SPI feature
Write memory	0x31	Write data to memory starting from an address specified by the application	Bootloader that supports SPI feature
Erase	0x44	Erase memory	Bootloader that supports SPI feature
Erase and program protect	0x63	Enable erase/program protection	Bootloader that supports SPI feature
Erase and program unprotect	0x73	Disable erase/program protection	Bootloader that supports SPI feature
Access Protect	0x82	Enable access protection	Bootloader that supports SPI feature
Access Unprotect	0x92	Disable access protection	Bootloader that supports SPI feature
Firmware CRC	0xAC	Compute a CRC value on a given memory area	Bootloader that supports SPI feature
Enable sLib	0xD0	Enable sLib	Bootloader that supports SPI feature
Disable sLib	0xD1	Disable sLib	Bootloader that supports SPI feature
Get sLib Status	0xD2	Get sLib status	Bootloader that supports SPI feature
Reset Device	0xD4	Reset device	Bootloader that supports SPI feature
Advanced Access Protect	0xD6	Enable advanced access protection	Bootloader that supports SPI feature and advanced access protection

3 Bootloader command description

This chapter describes how to use each of the bootloader commands from the point of the host side and the device side.

3.1 Get Command

This command is used to get the protocol version and the supported commands. The number of the supported commands depends on the MCU series.
When the bootloader receives the command, it transmit an “ACK” byte to the host. Then the bootloader sends the number of bytes (one byte) to the host, the protocol version and the supported commands and after that, transmits an ACK byte.
This command is allowed and executed when the access protection is enabled.

3.1.1 Flow chart on host and device sides

Figure 5 Get Commands: host side

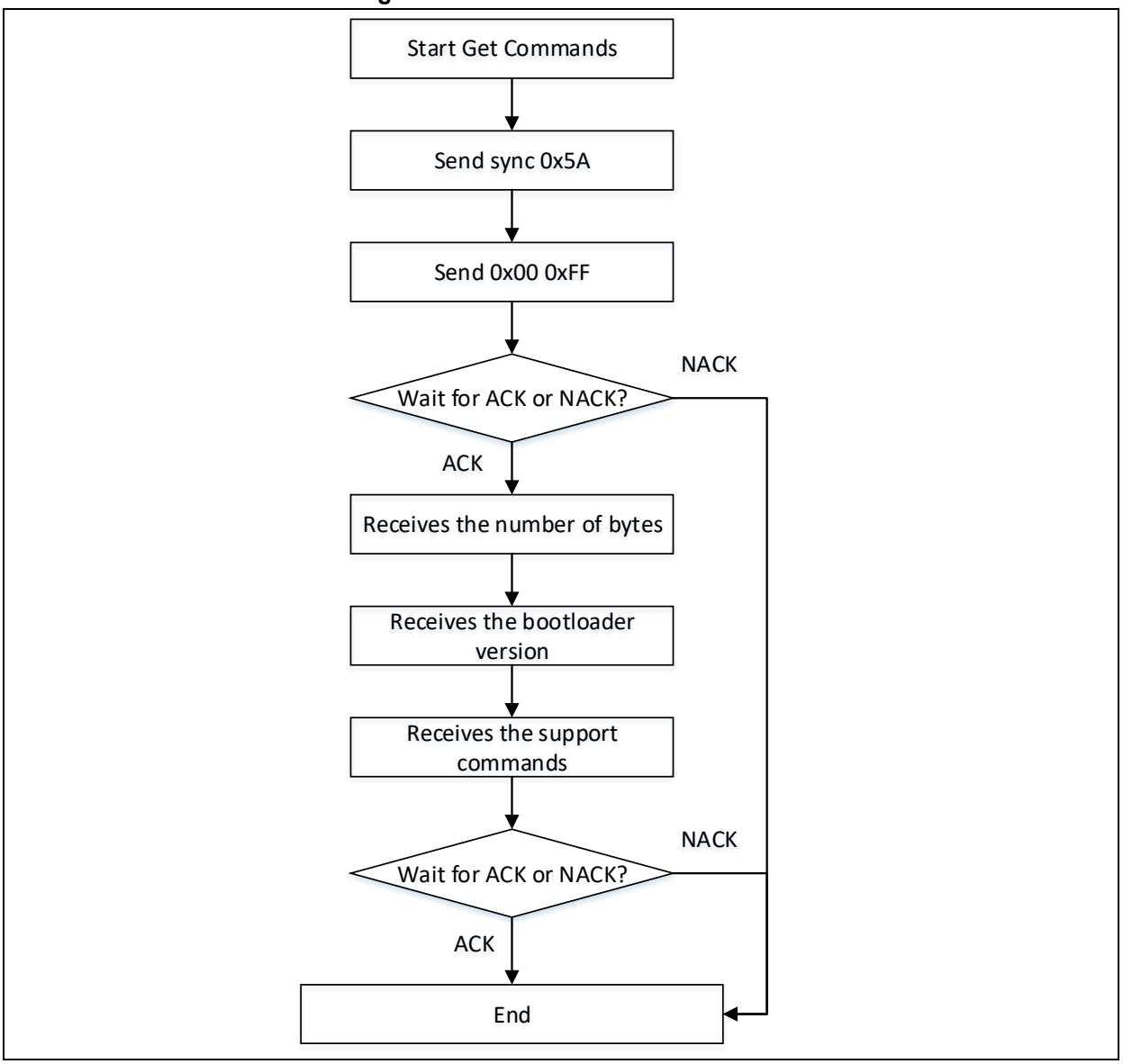
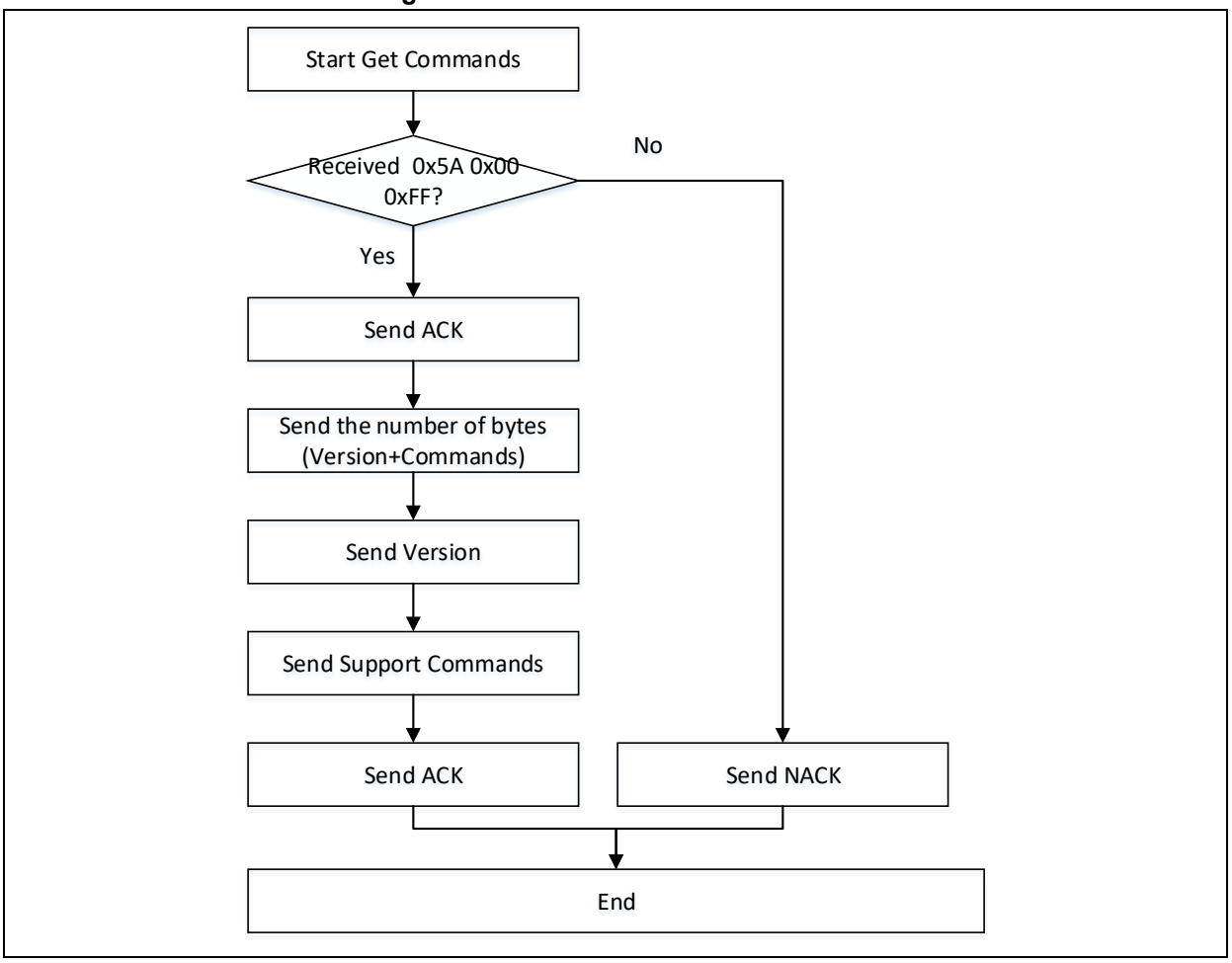


Figure 6 Get Commands: device side



3.1.2 Data transmit on host side

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0x00	
3		0xFF	
	1	ACK/NACK	When an NACK is received, it represents the end of the command (Get ACK procedure).
	2	n	It represents the number of data to be received.
	3	*	The protocol version of the bootloader
	4	0x00	First command: Get Commands
	5	0x01	Second command: Get Version
	…	…	…
	n+2	*	N command
	n+3	ACK	End of command (Get ACK procedure)

3.2 Get Version command

This command is used to get the version of the bootloader. When the device receives the command, it transmits an ACK byte to the host. After the transmission of the ACK byte, the device sends the bootloader protocol version (1 byte) and the bootloader version code (BID, two bytes). After this operation, the device transmits the ACK byte to the host signaling the end of the command.

This command is allowed and executed when the access protection is enabled.

3.2.1 Flowchart on host and device sides

Figure 7 Get Version: host side

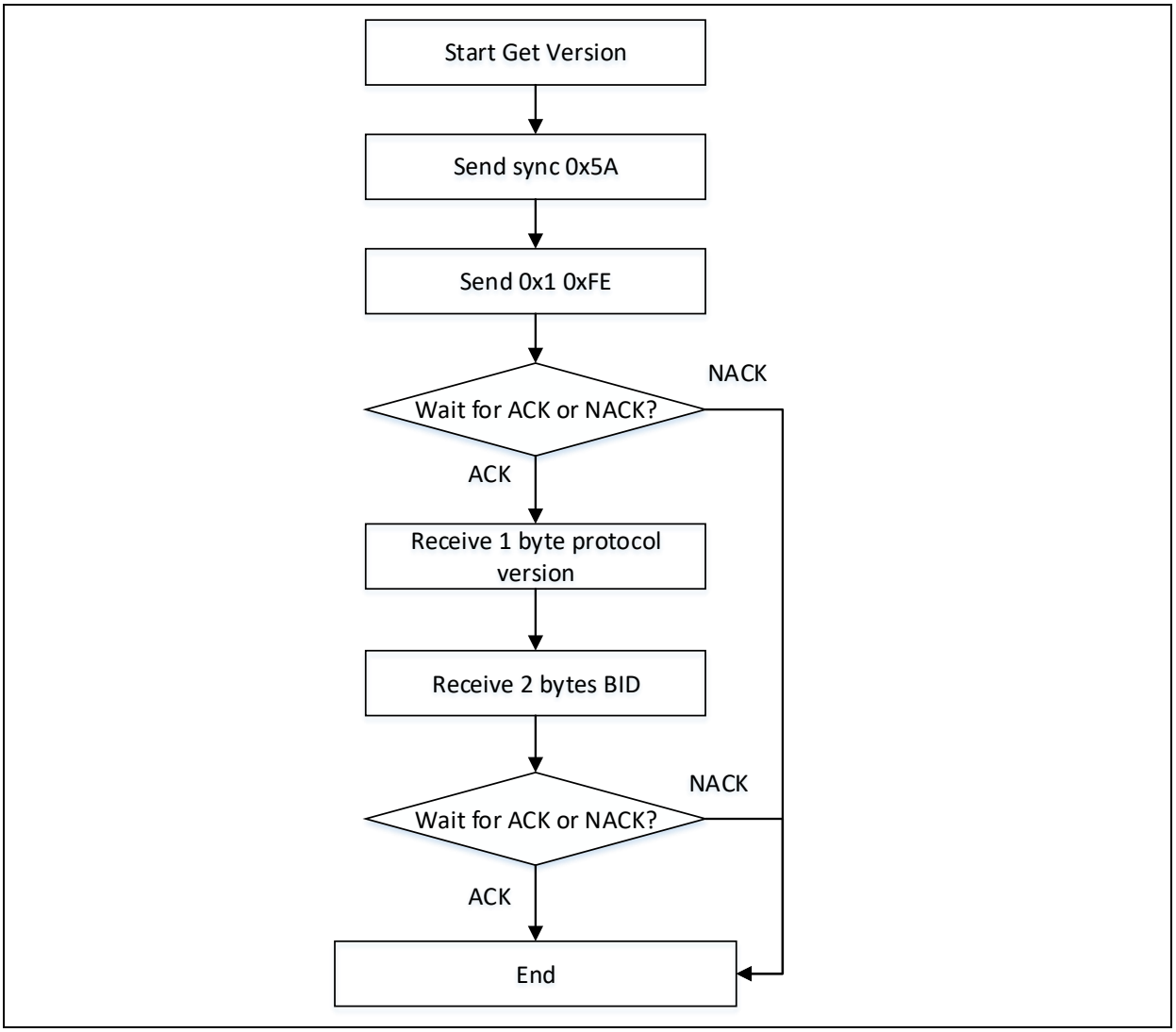
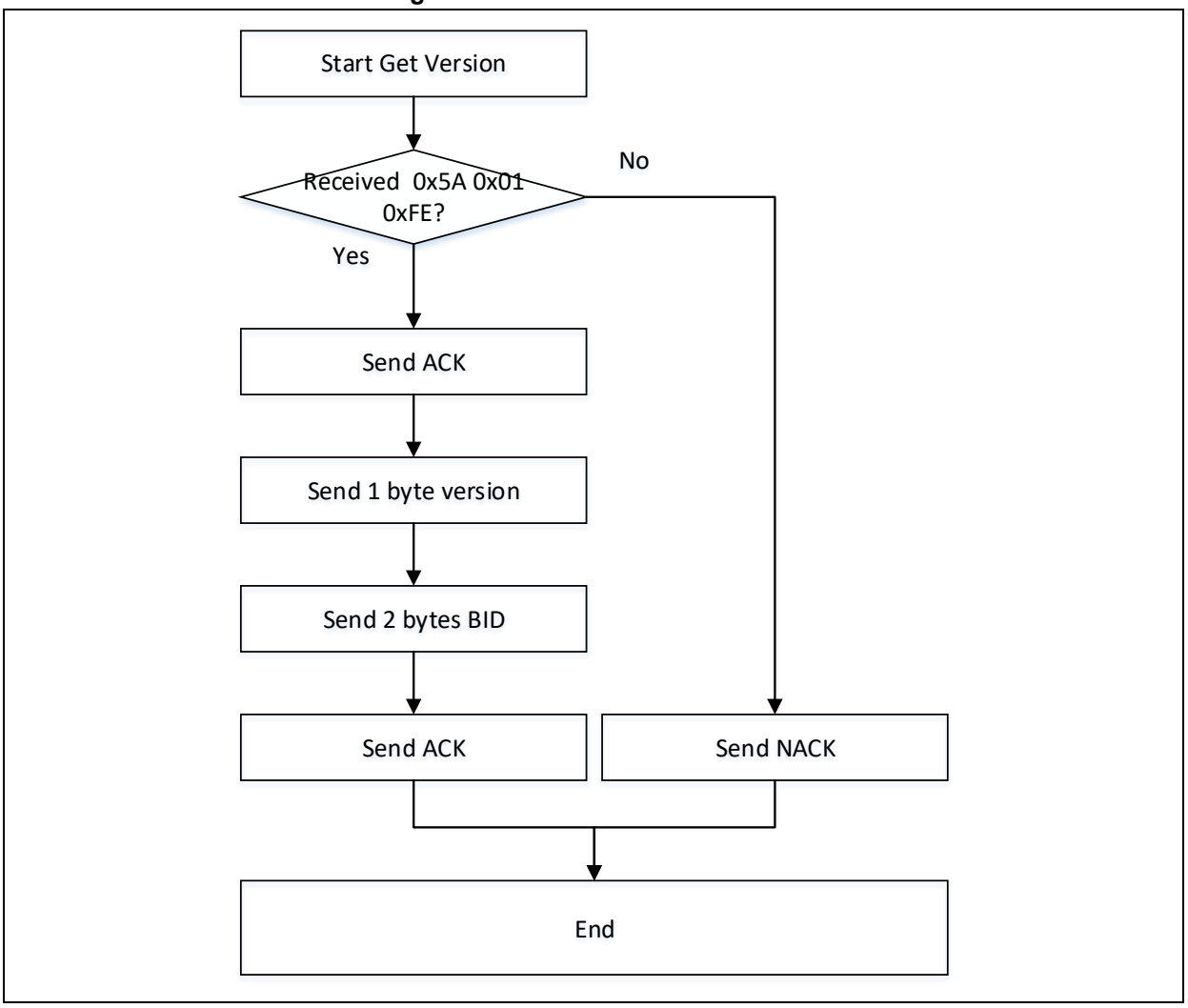


Figure 8 Get Version: device side



3.2.2 Data transmit on host side

Send	Receive	Data	Description
1		0x5A	
2		0x01	
		0xFE	
	1	ACK/NACK	When an NACK is received, it represents the end of the command (get ACK procedure).
	2	*	Bootloader protocol version
	3	*	Bootloader version ID (BID）
	4	*	Bootloader version ID（BID）
	5	ACK	End of command (get ACK procedure)

3.3 Get Device ID command

This command is used to get the identification code of the device. This ID data includes a 4-byte product ID and a 1-byte project ID. The “project ID” is used to identify which MCU series is being used, and the “product ID” is used to get the exact part number of the current MCU series in use. When the device receives this command, it transmits an “ACK” byte to the host. After the transmission of the ACK byte, the device sends a 1-byte data length indicating the number of data to be transmitted-- the value is the transmitted length minus 1 (for example, the transmitted data size is 5, then the value is 4), then sends another 4-byte product ID and 1-byte project ID. After this operation, the device transmits an ACK byte to the host.
This command is allowed and executed when the access protection is enabled.

3.3.1 Flowchart on host and device sides

Figure 9 Get Device ID: host side

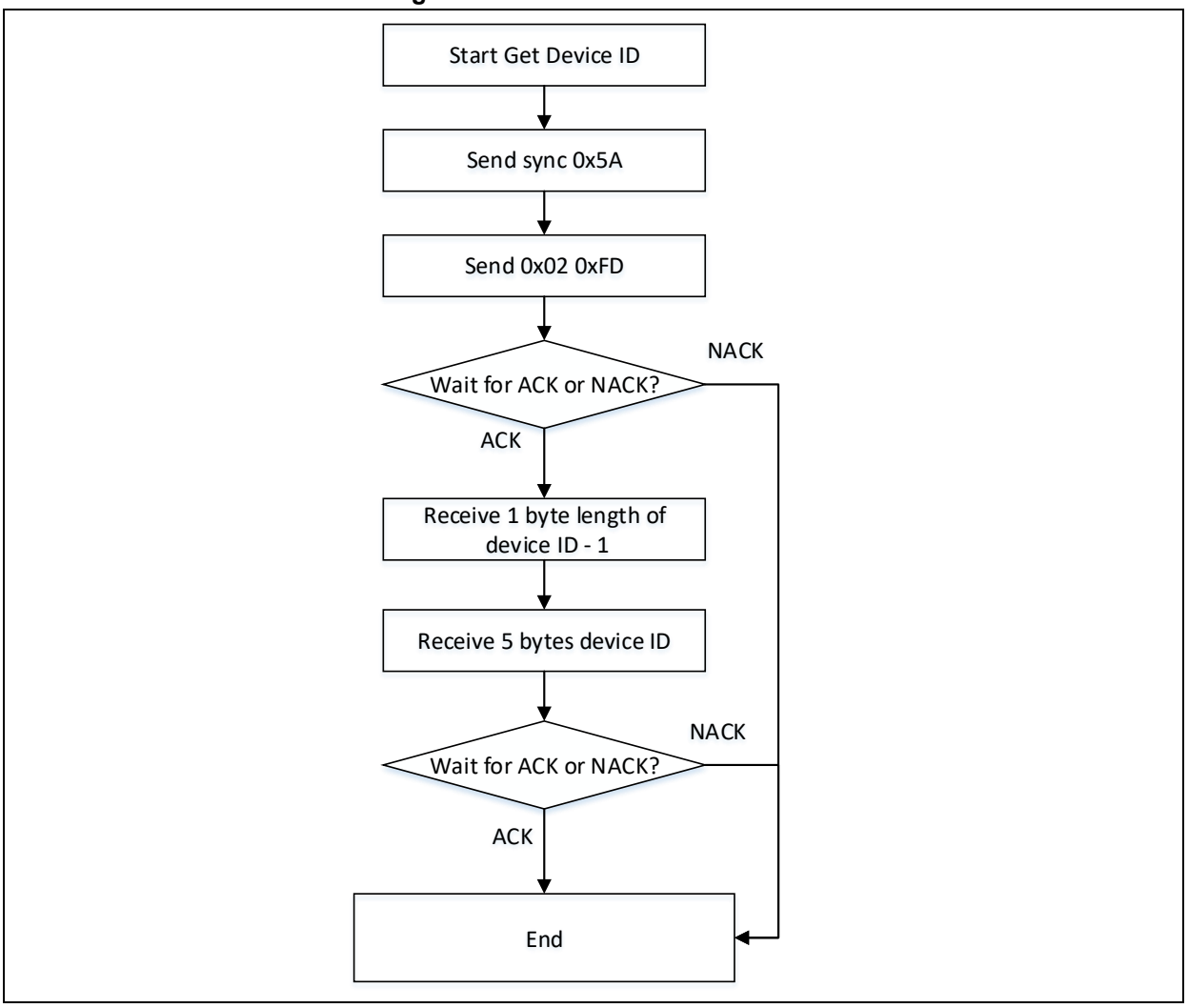
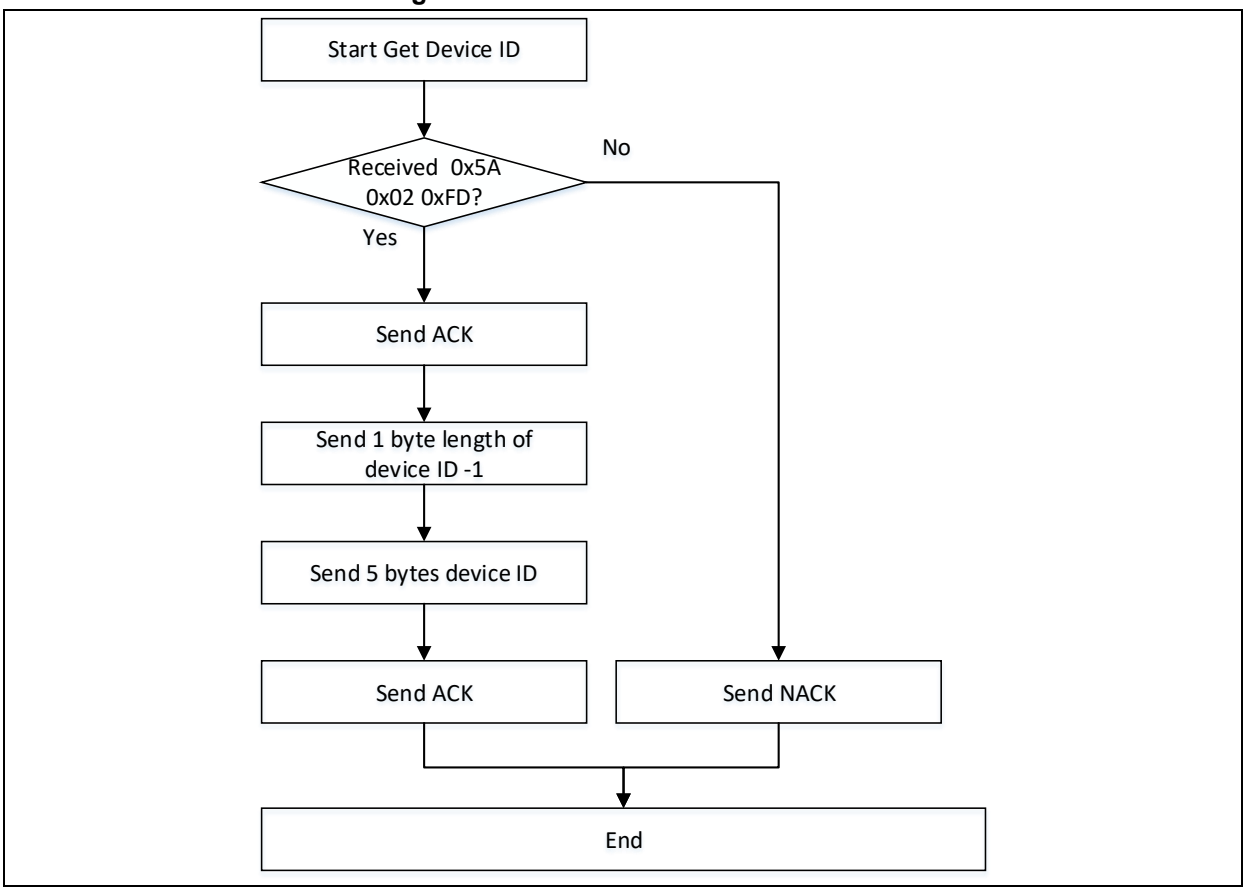


Figure 10 Get Device ID: device side



3.3.2 Data transmit on host side

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0x02	
3		0xFD	
	1	ACK/NACK	When an NACK is received, it represents the end of the command (Get ACK procedure).
	2	0x04	Device ID length minus 1
	3	*	Product ID [8-15]
	4	*	Product ID [0-7]
	5	*	Product ID [24-31]
	6	*	Product ID [16-23]
	7	*	Project ID
	8	ACK	End of command (Get ACK procedure).

3.4 Read Memory command

This command is used to read data from any valid memory address (refer to the product datasheets) in SRAM, boot memory and in the user system data area.
When the device receives the command, if the access protection is not enabled, it transmits the ACK byte to the host. After the transmission of the ACK byte, the device waits for an address (four bytes) and a checksum byte. If the Checksum is correct and the valid is valid, the devices transmits an ACK byte, and then waits for the number of bytes to be read (1 byte) and for a checksum byte. The number of byte to read is the actual read data length -1(for example, to read 10 bytes, the value here is 9). If the checksum is correct, the devices sends an ACK before starting to send the needed data.
This command is not allowed and executed when the access protection is enabled.

3.4.1 Flowchart on host and device sides

Figure 11 Read Memory: host side

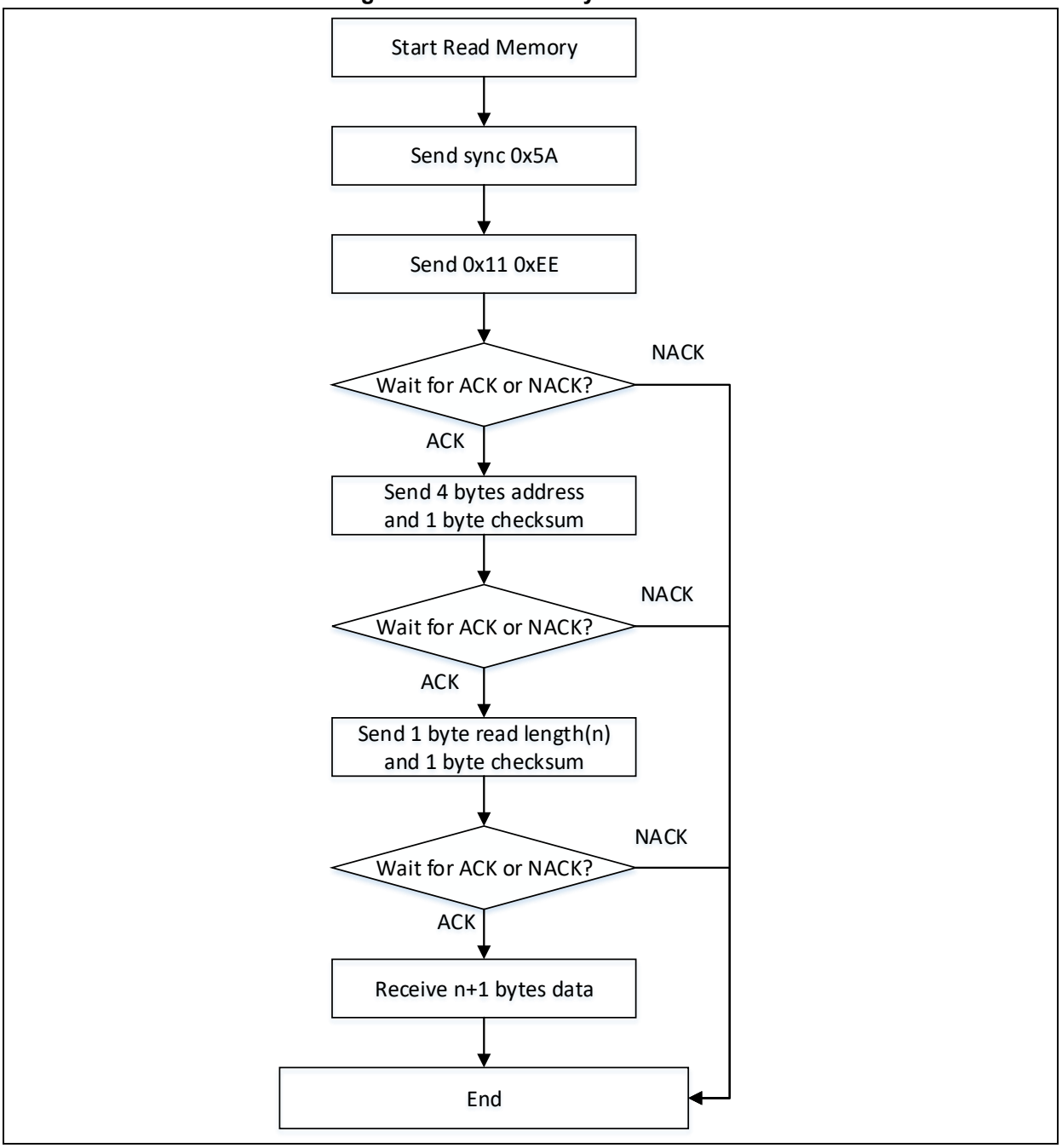
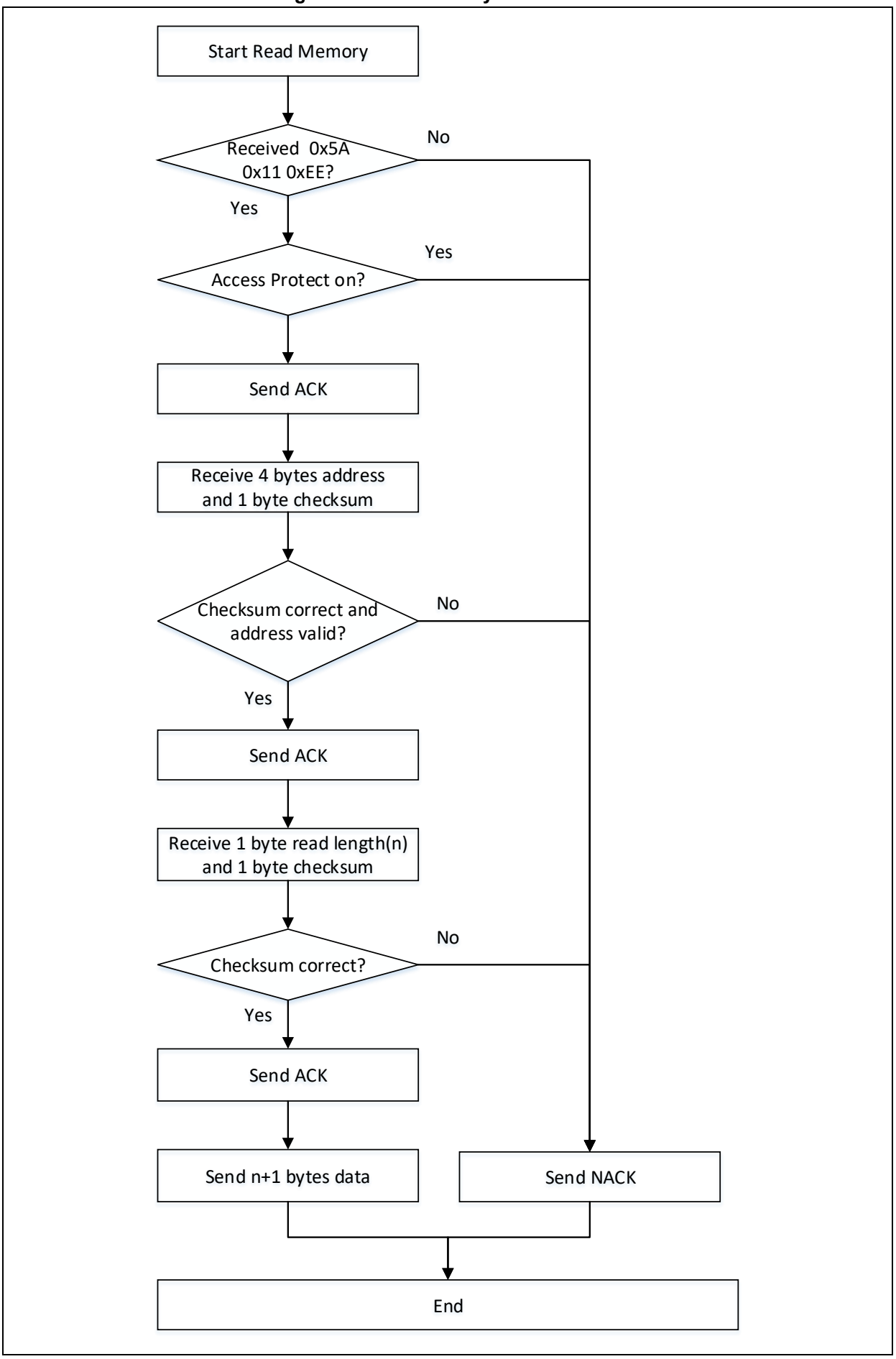


Figure 12 Read Memory: device side



3.4.2 Data transmit on host side

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0x11	
3		0xEE	
	1	ACK/NACK	When an NACK is received, it represents that the access protection is enabled, and the end of the command (Get ACK procedure).
4		*	Address MSB
5		*	
6		*	
7		*	Address LSB
8		*	Checksum：XOR（address byte3~byte6）
	2	ACK/NACK	When an NACK is received, it represents the end of the command (Get ACK procedure).
9		*	Read data length -1 (n)
10		*	Checksum：0xFF XOR byte8
	3	ACK/NACK	When an NACK is received, it represents the end of the command (Get ACK procedure)
	4	*	Destination address data
	…	…	Destination address data
	4+n+1	*	Destination address data

3.5 Jump command

This command is used to execute the code in a specified address. It can jump to main memory or SRAM to execute code. The address must be valid, which depends on the MCU series.
When the device receives the command, if the access protection is not enabled, it transmits the ACK byte to the host. After the transmission of the ACK byte, the device waits for an address (four bytes) and a checksum byte, then it checks the received address. If the address is valid and the checksum is correct, the devices transmits an ACK byte, and jumps to the memory location.
This command is not allowed and executed when the access protection is enabled.

3.5.1 Flowchart on host and device sides

Figure 13 Jump: host side

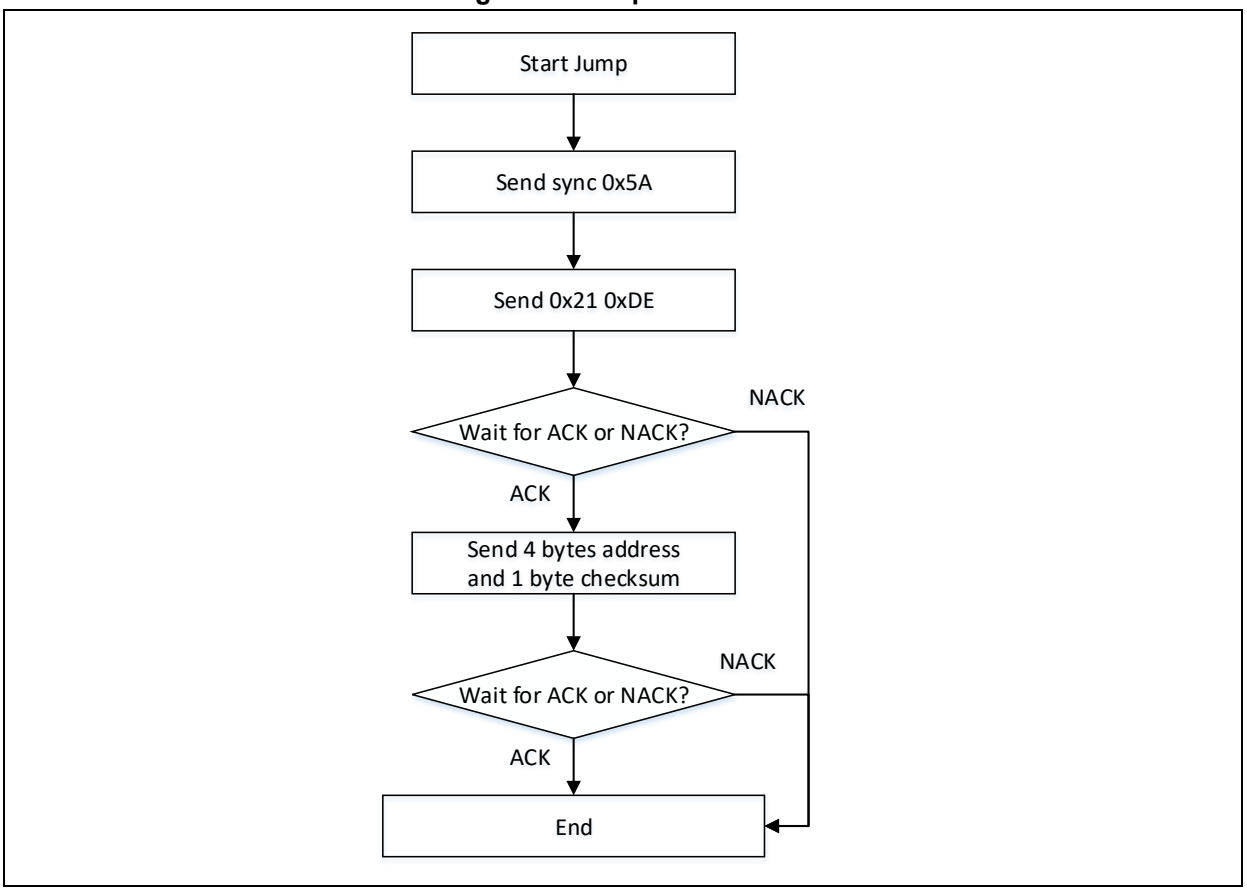
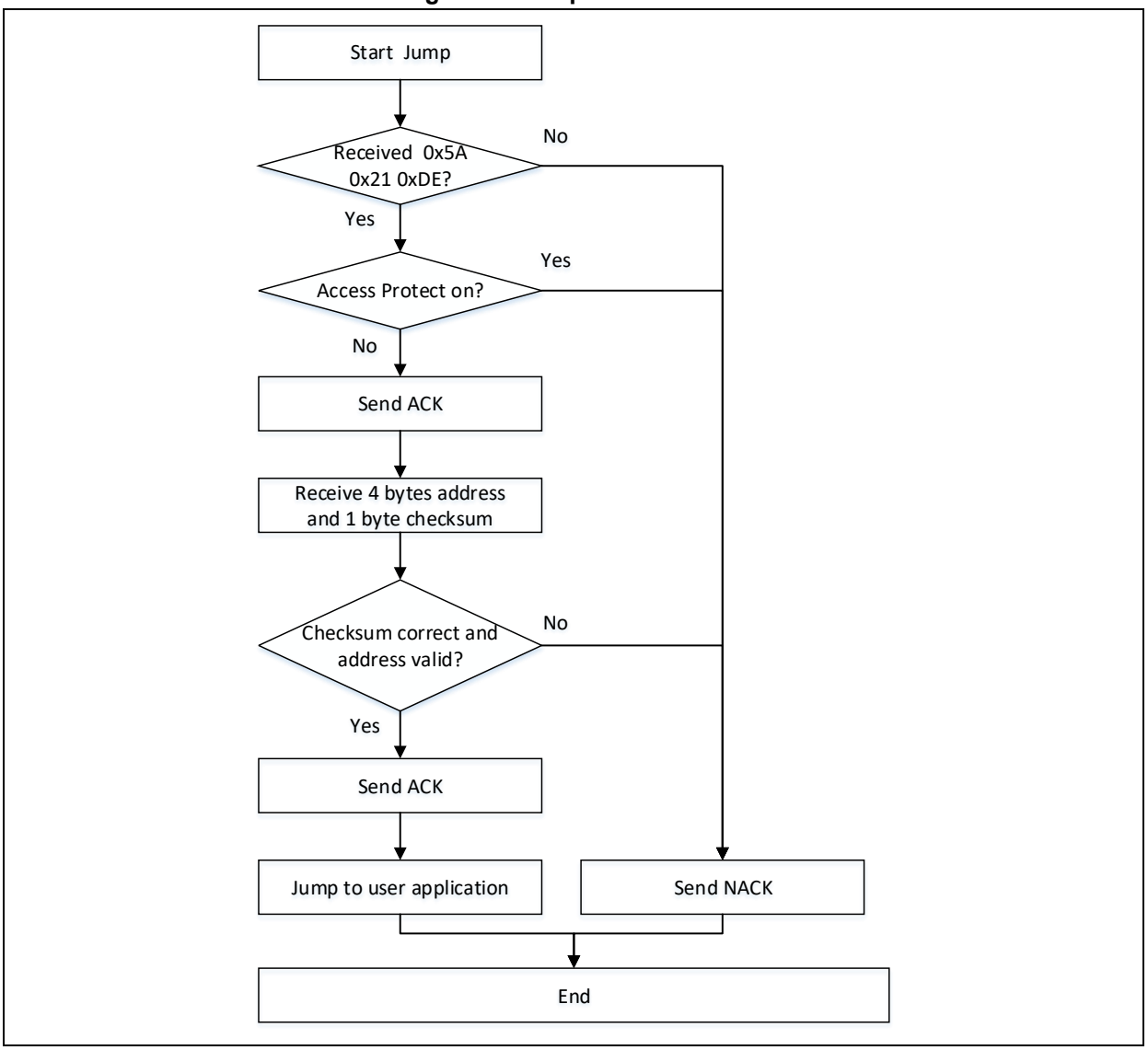


Figure 14 Jump: device side



3.5.2 Data transmit on host side

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0x21	
3		0xDE	Jump
	1	ACK/NACK	When an NACK byte is received, it indicates that the access protection is enabled, and the end of the command (Get ACK procedure).
4		*	Address MSB
5		*	
6		*	
7		*	Address LSB
8		*	Checksum：XOR（address byte3~byte6）
	2	ACK/NACK	End of the command (Get ACK procedure).

3.6 Write Memory command

This command is used to write data to any valid memory address (depending on the product series) such as Flash memory, SRAM, or user system data area.

If the Write Memory command is issued to the Flash memory, all bytes are erased before writing the new values.

The size of the user system data area depends on the product series:

- User system data area smaller than 256 bytes
  Only a single Write Memory command is issued by the host to write data to the user system data area. When the device receives the command, it erases all bytes in the user system data area before writing to it and then performing a system reset.
- User system data area greater than 256 bytes
  Multiple Write Memory commands are issued by the host to write data to the user system data area.
  When the device receives the command, if the received address to write is the start address of the user system data area, the address is erased before written.
  If it is not the start address of the user system data area, no erase operation is performed and data are directly written.
  After the write operation (after all of data are written), a system reset is performed automatically.

Note: No system reset is performed following the write operation, instead it asks the host to send a Reset command.

When the device receive the “Write Memory” command, if the access protection is not enabled, it transmits the ACK byte to the host. After the transmission of the ACK byte, the device waits for an address (four bytes) and a checksum byte. If the received address is valid and the checksum is correct, the device transmits an ACK byte. After the transmission of the ACK byte, the device waits for an address (one byte) and a checksum byte. The value is the actual written length minus 1 (for example, to write 10 bytes, the value here is 9). If the checksum is correct, the device writes data to the received address and then transmits an ACK byte to the host.

This command is not allowed and executed when the access protection is enabled.

3.6.1 Flowchart on host and device sides

Figure 15 Write Memory: host side

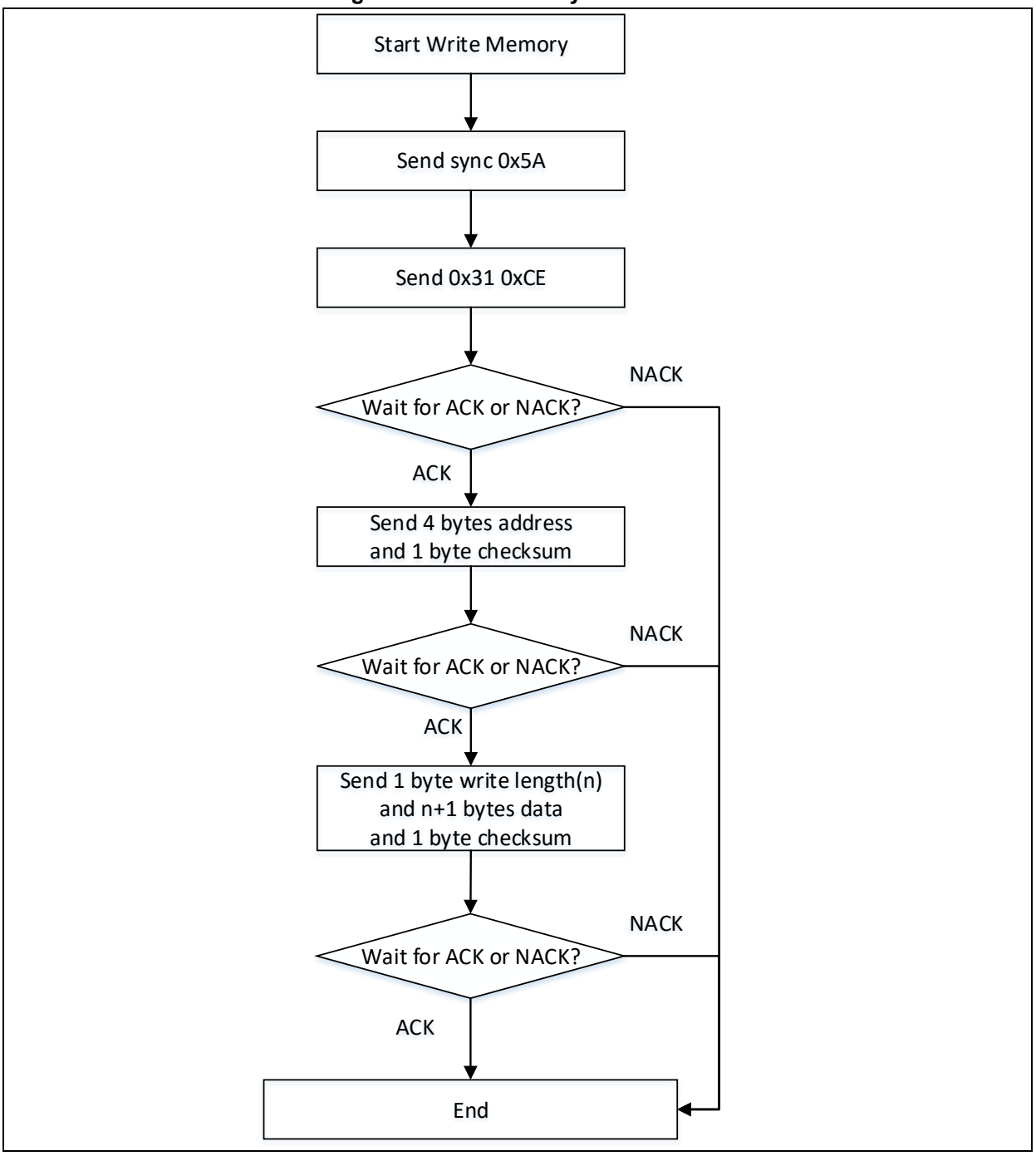
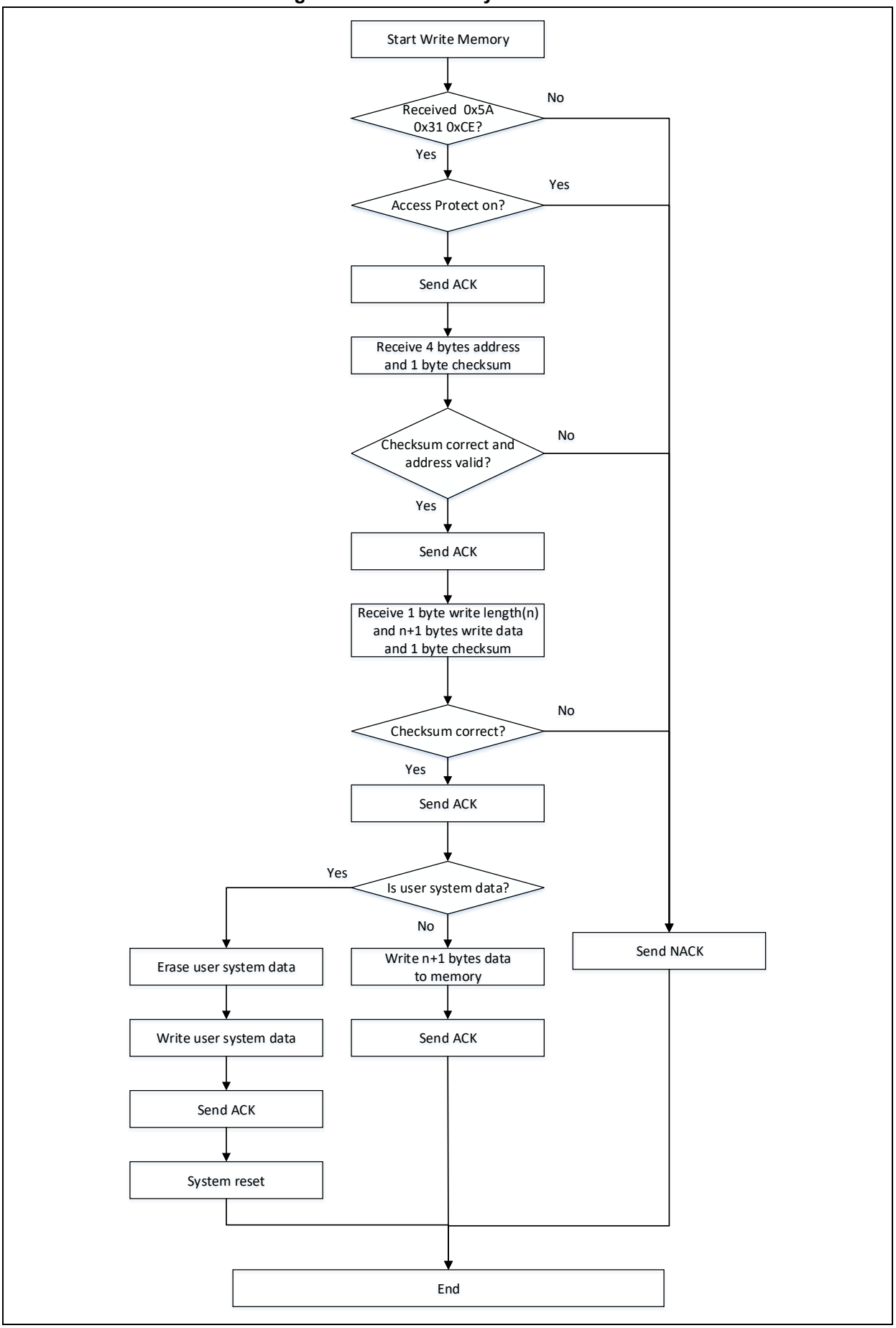


Figure 16 Write Memory: device side



3.6.2 Data transmit on host side

Send	Transmit	Data	Description
1		0x5A	Synchronization byte
2		0x31	
3		0xCE	Write memory
	1	ACK/NACK	When an NACK byte is received, it indicates the access protection is enabled, and the end of the command (Get ACK procedure).
4		*	Address MSB
5		*	
6		*	
7		*	Address LSB
8		*	Checksum：XOR（address byte3~byte6）
	2	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
9		*	The number of data to be written n – 1
10		*	Write data
…		…	Write data
10+n		*	Write data
			Checksum: XOR byte8 - byte9+n
	3	ACK/NACK	End of command (Get ACK procedure).

3.7 Erase command

This command allows the host to erase Flash memory pages. It supports sector erase (sector size depends on the product series) and mass erase.

For those products that contain bank 1 and bank 2, this command can be used to erase bank 1 and bank 2.

Note that this command is used to erase any valid memory address, depending on the product series.

When the device receives the command, if the access protection is not enabled, it transmits the ACK byte to the host. After the transmission of the ACK byte, the devices receives two bytes data and check which erase operation is performed based on the received data type.

- If it is Sector erase, the received data indicates the number of the sectors to be erased. Then the device receives the index of N sectors to be erased. After receiving the index, the device starts erasing the corresponding sector and then transmits an ACK byte to the host.
- If it is mass erase or bank erase, the device directly performs erase operation and then transmits the ACK byte to the host after the erase operation.

This command is not allowed and executed when the access protection is enabled.

Table 1 List of erase type

Erase type	Erase index	Erase area
Sector erase	0x00 0x00	Sector0
	0x00 0x01	Sector1
	…	…
	0x80 00	Bank3 Sector0
	0x80 01	Bank3 Sector1
	…	…
	0x8F 0xFF	Bank3 Sector4096
Mass erase	0xFF 0xFF	All Flash
Bank erase	0xFF 0xFE	Bank1 Erase
	0xFF 0xFD	Bank2 Erase
	0xFF 0xFC	Bank3 Erase

Note: the sector size is dependent on the product series.

3.7.1 Flowchart on host and device sides

Figure 17 Erase: host side

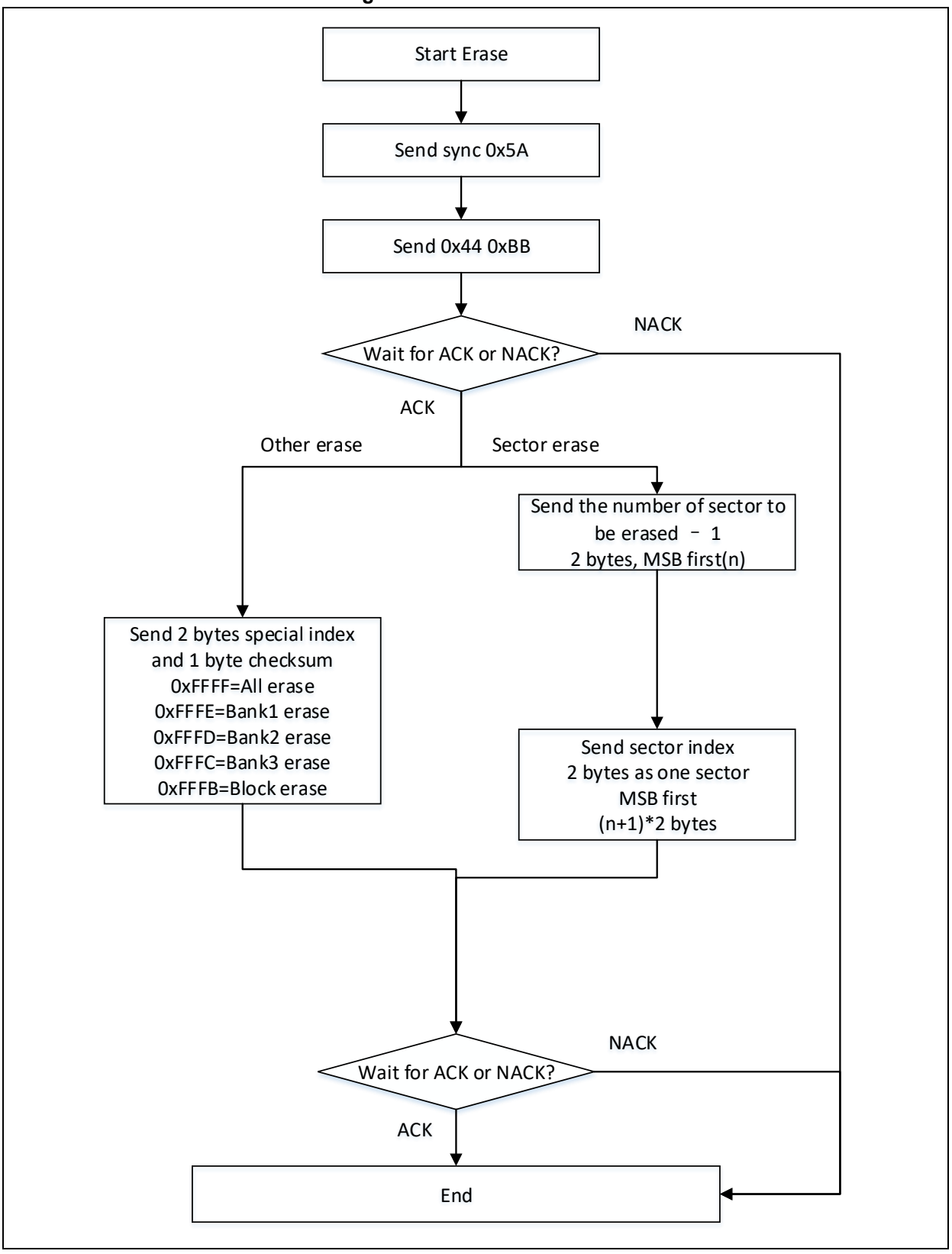
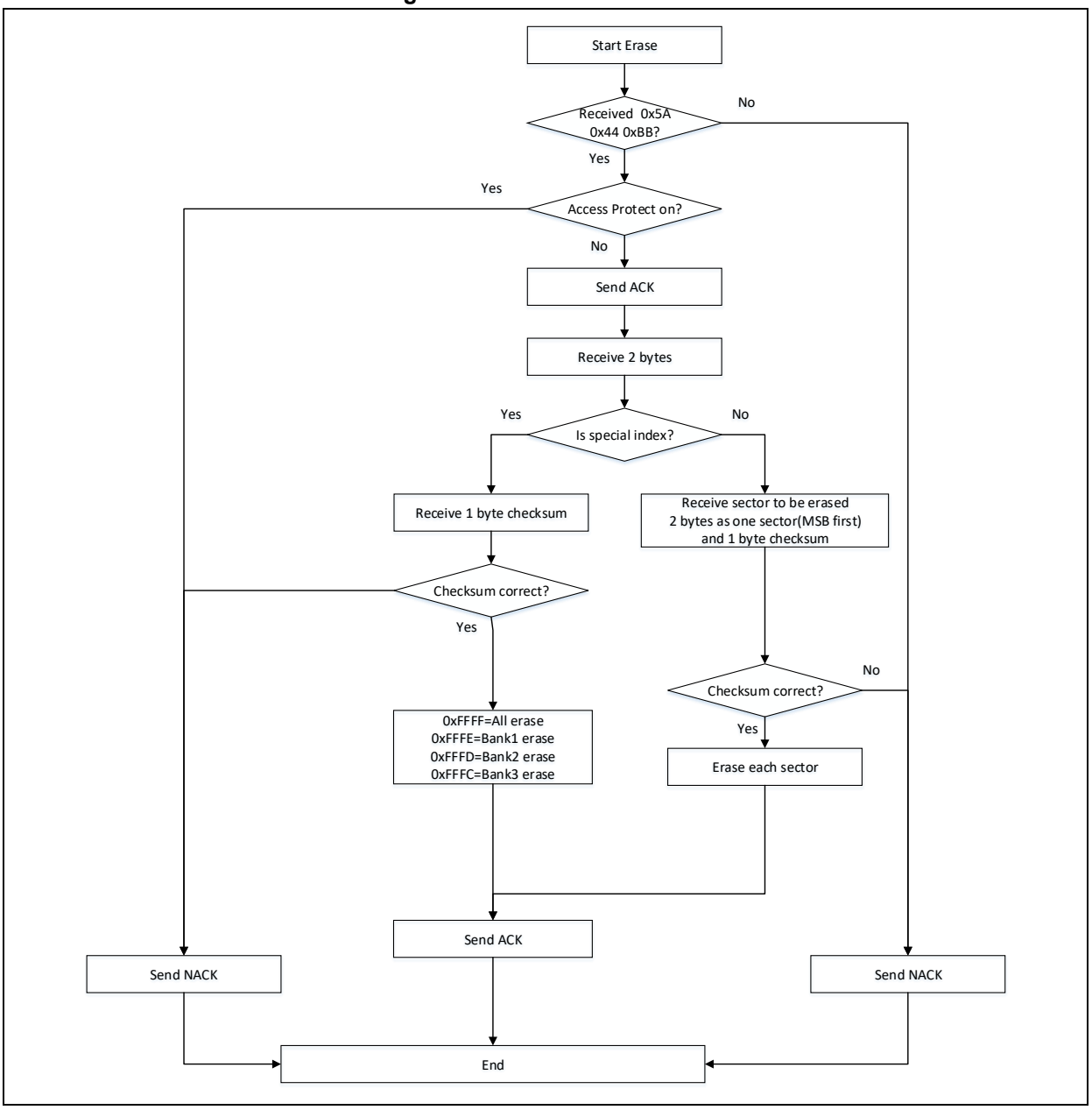


Figure 18 Erase: device side



3.7.2 Data transmit on host side

Sector erase

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0x44	
3		0xBB	Erase
	1	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
4		*	Erase sector number – 1 (n) MSB
5		*	Erase sector number– 1 (n) LSB
6		*	First Sector index (MSB)
7		*	First Sector index (LSB)
…		*	X Sector index (MSB)
…		*	X Sector index (LSB)
8+2(n+1)		*	Checksum：XOR（byte 3~6+2(n+1)）
	2	ACK	End of the command (Get ACK procedure).

Bank or mass erase

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0x44	
3		0xBB	Erase
	1	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
4		0xFF	Mass erase or Bank erase index (MSB)
5		*	Mass erase (0xFF) or Bank erase (0xFE, 0xFD, 0xFC) index (LSB)
6		*	Checksum: XOR (byte 3~4)
	2	ACK	End of the command (Get ACK procedure).

3.8 Erase and Program Protect command

This command is used to enable erase/program protection for the specified sectors.
When the device receives the command, if the access protection is not enabled, it transmits an ACK byte to the host. After the transmission of the ACK byte, it waits for one-byte length-1 (n), and then receives the index bit corresponding to the erase/program protection (n+1 bytes) ---refer to the corresponding product datasheet for more details about the bit definition --- and a checksum byte. If the checksum is correct, the device erases the user system data area (those data other than erase/program protect bytes are reserved), and writes the settings for erase/program protection, and transmits the ACK byte to the host before performing a system reset.

Note: The index bit (0, 1, 2…n) for erase/program protection corresponds to the bit (0-N) of the erase/program protection byte of the user system data area. See the corresponding product sheet for more details about the user system data area.

This command is not allowed and executed when the access protection is enabled.

3.8.1 Flowchart on host and device sides

Figure 19 Erase and Program Protect: host side

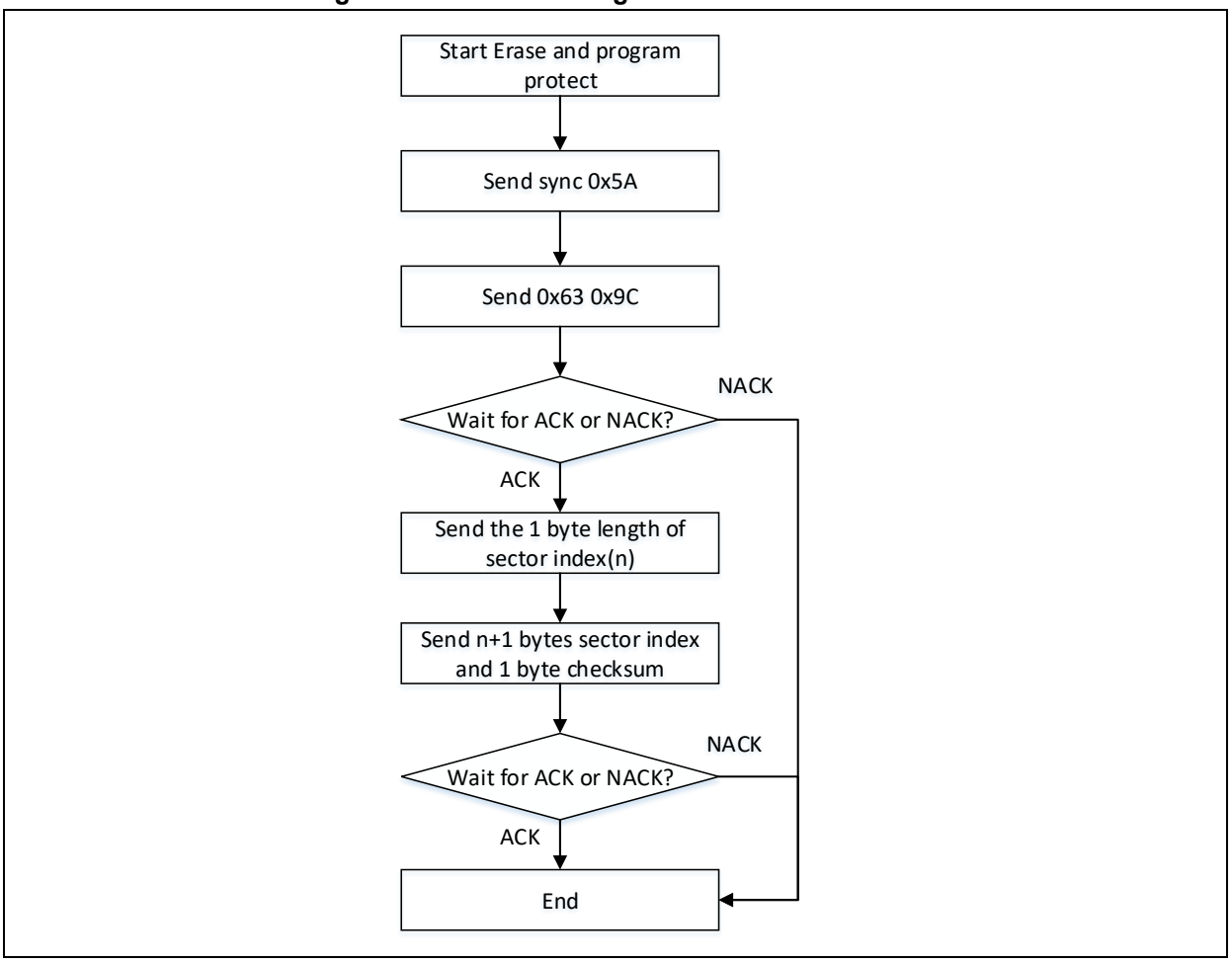
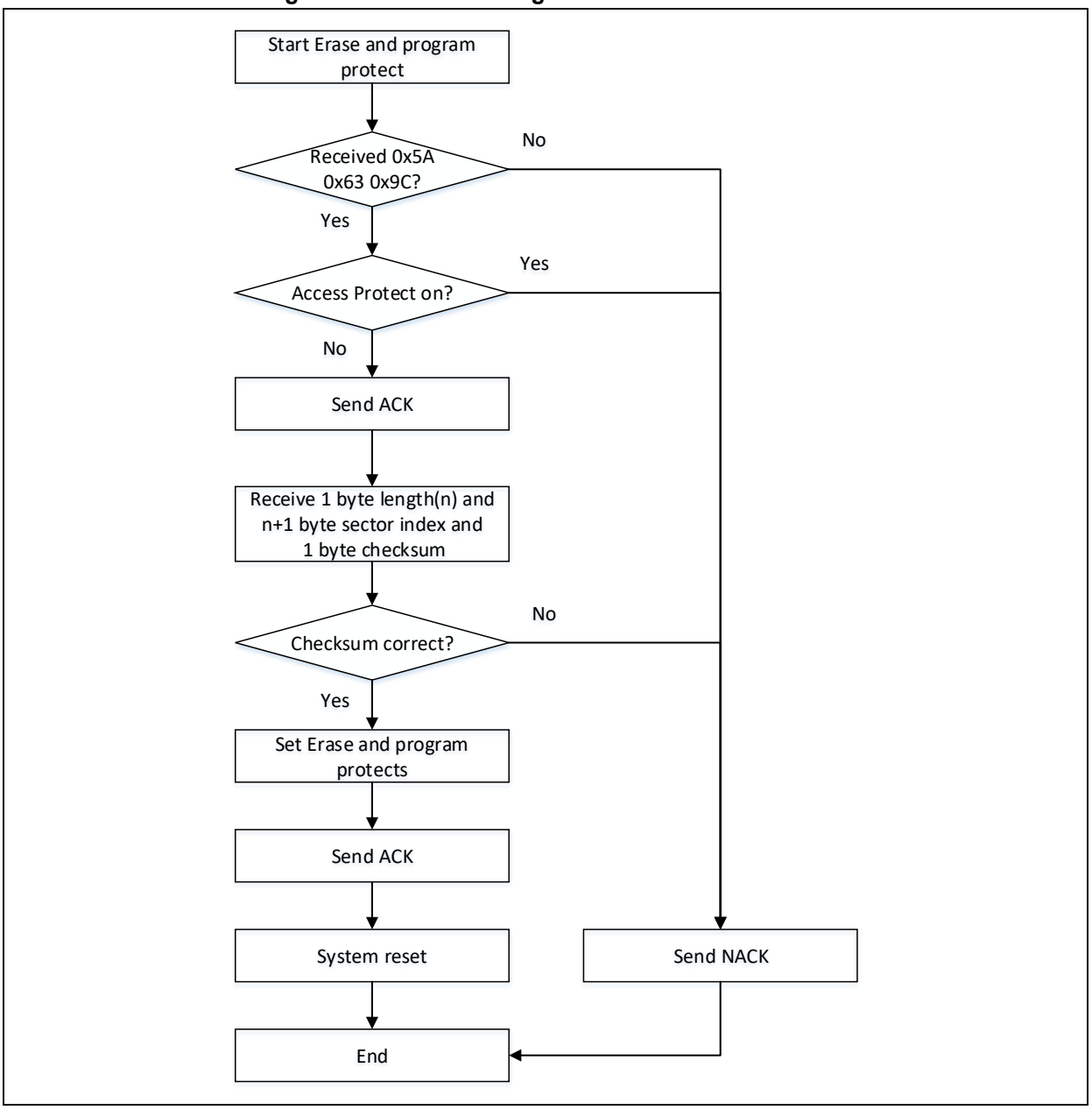


Figure 20 Erase and Program Protect: device side



3.8.2 Data transmit on host side

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0x63	Erase and program protect
3		0x9C	Erase and program protect
	1	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
4		*	Protection byte-1 (n)
…		…	The index to be protected
5+n+1		*	Checksum：XOR（byte 3~4+n+1）
	2	ACK	End of the command (Get ACK procedure).

3.9 Erase and Program Unprotect

This command is used to disable the erase/program protection of memory.
When the device receives the command, if the access protection is not enabled, it transmits the ACK byte to the host. After the transmission of the ACK byte, the device disables the erase/program protection of all the flash memory sectors. After the unprotection operation, the device transmits the ACK byte and performs a system reset.
This command is not allowed and executed when the access protection is enabled.

3.9.1 Flowchart on host and device sides

Figure 21 Erase and Program Unprotect: host side

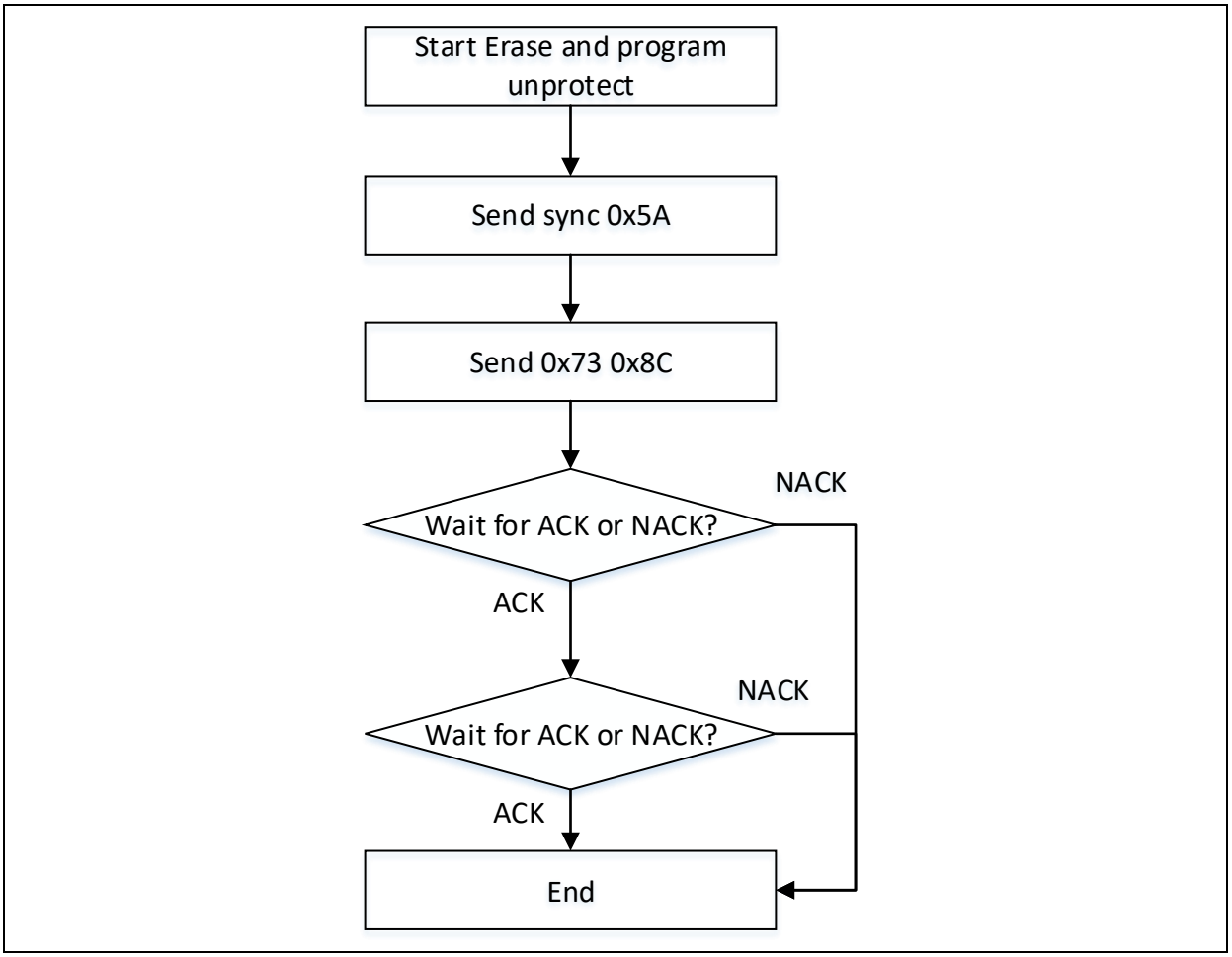
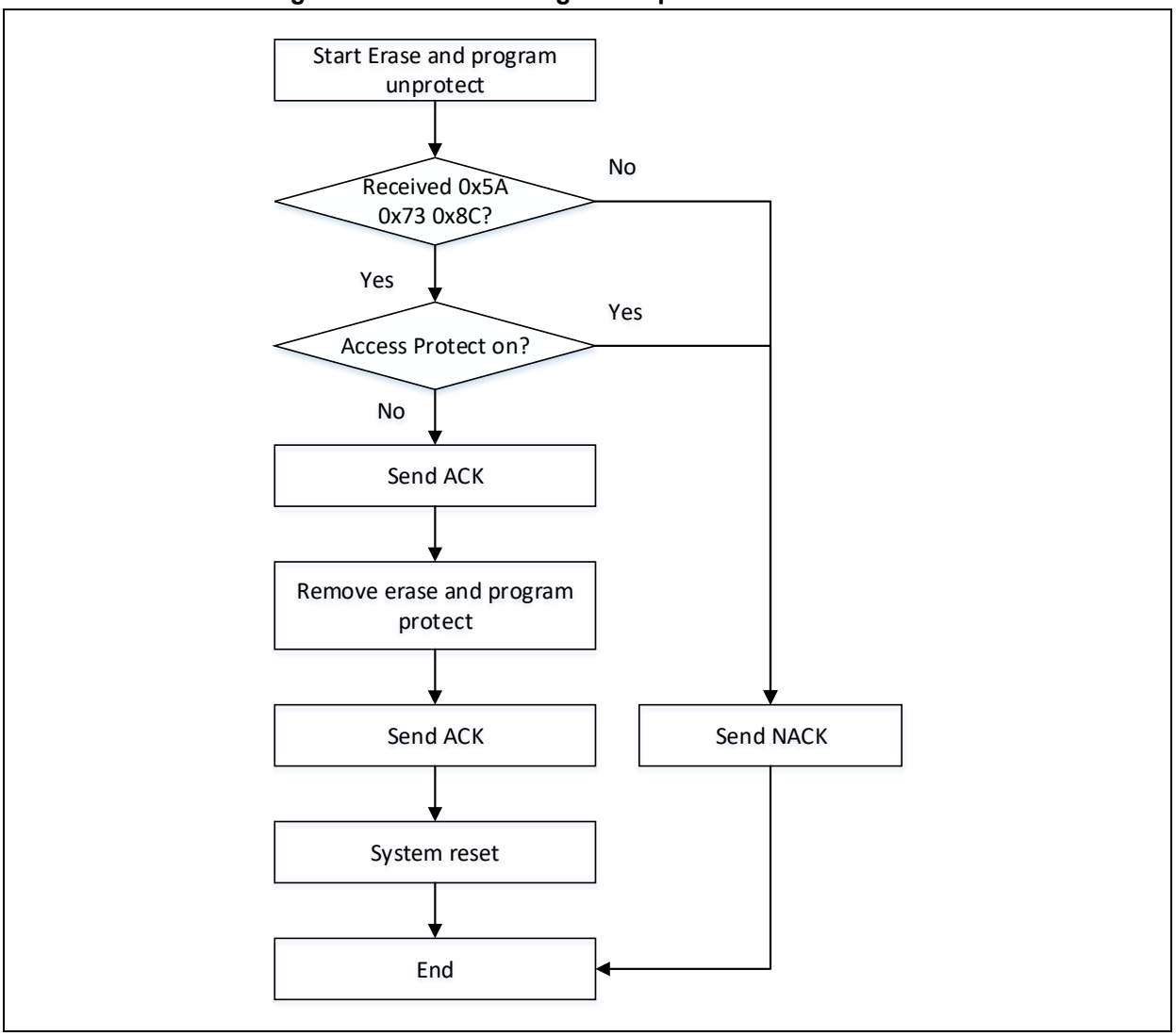


Figure 22 Erase and Program Unprotect: device side



3.9.2 Data transmit on host side

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0x73	Erase and program unprotect
3		0x8C	Erase and program unprotect
	1	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
	2	ACK	End of the command (Get ACK procedure).

3.10 Access Protect command

This command is used to enable the flash memory access protection. After this command is enabled, it is not allowed to read data from flash memory.

When the device receives the command, if the access protection is not enabled, it transmits the ACK byte to the host. After the transmission of the ACK byte, the device enables the access protection for the flash memory. After the protection operation, the device transmits the ACK byte to the host and then performs a system reset.

This command is not allowed and executed when the access protection is enabled.

3.10.1 Flowchart on host and device sides

Figure 23 Access Protect: host side

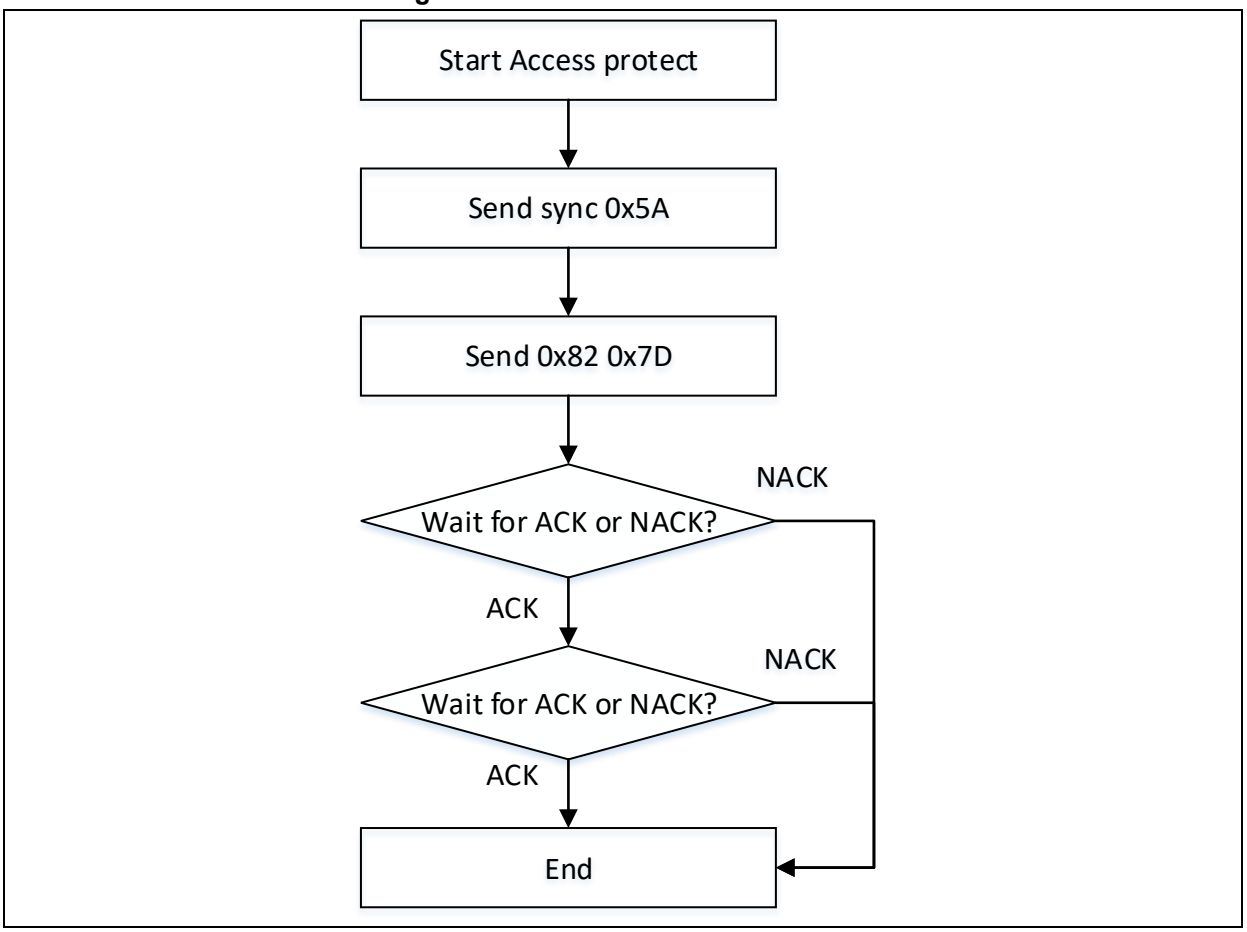
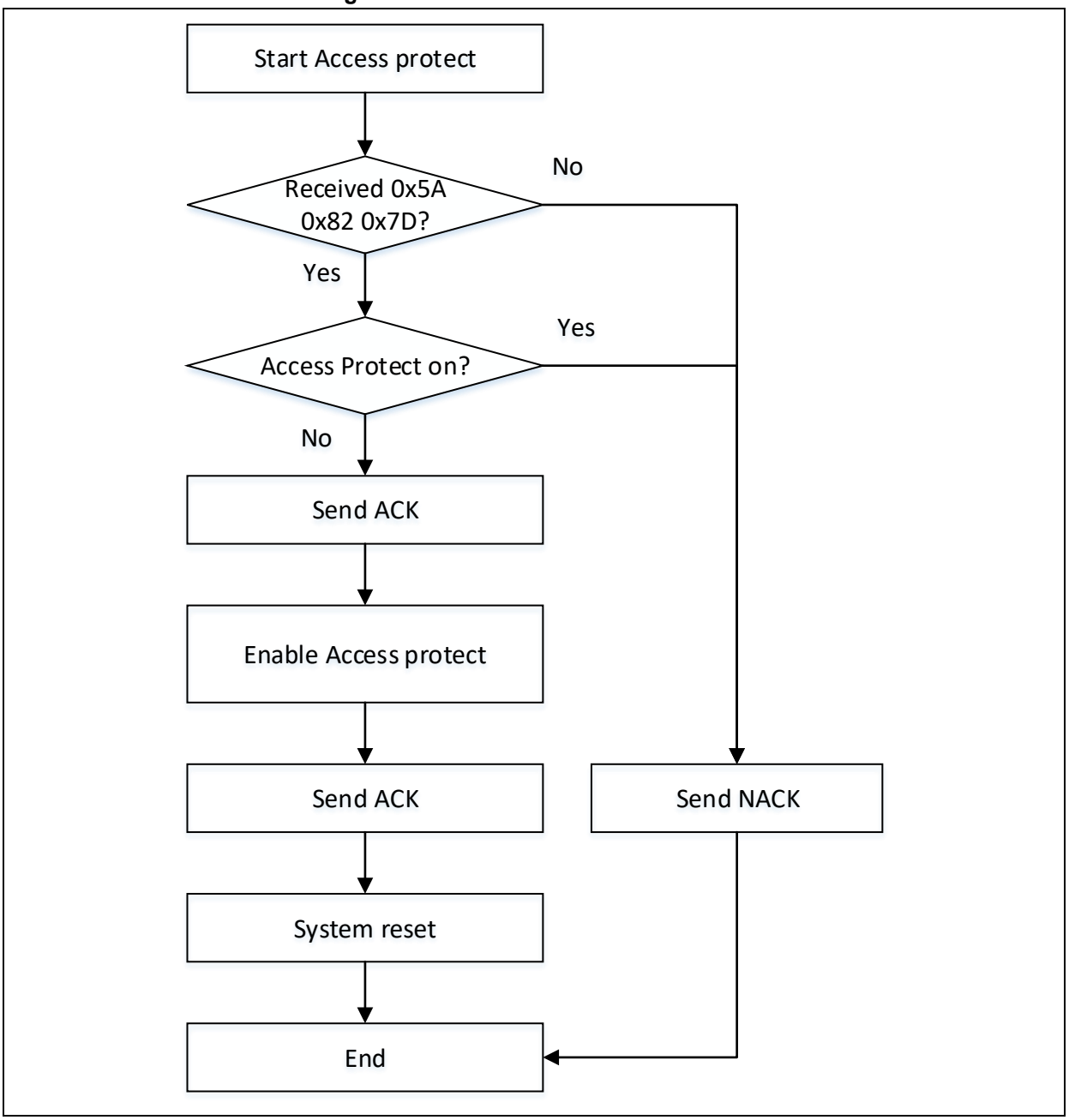


Figure 24 Access Protect: device side



3.10.2 Data transmit on host side

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0x82	Access protect
3		0x7D	Access protect
	1	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
	2	ACK	End of the command (Get ACK procedure).

3.11 Access Unprotect command

This command is used to disable the flash memory access protection. If the device is in Access protection mode, this command operation induces a mass erase of the flash memory.
When the device receives the command, it transmits the ACK byte to the host. After the transmission of the ACK byte, the devices disables the access protection of the flash memory. After the unprotection operation, the device transmits the ACK byte to the host and then performs a system reset.

3.11.1 Flowchart on host and device sides

Figure 25 Access Unprotect: host side

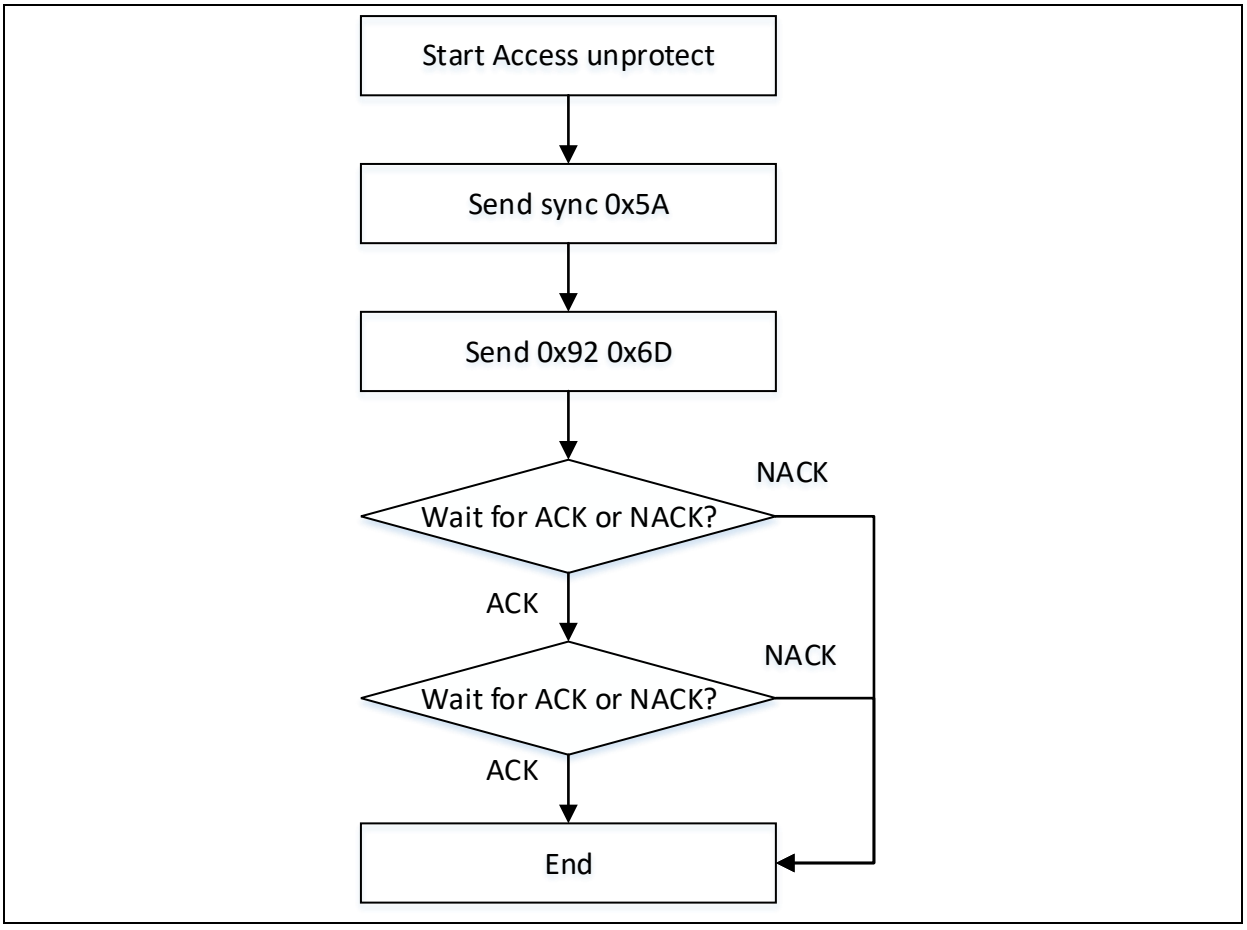
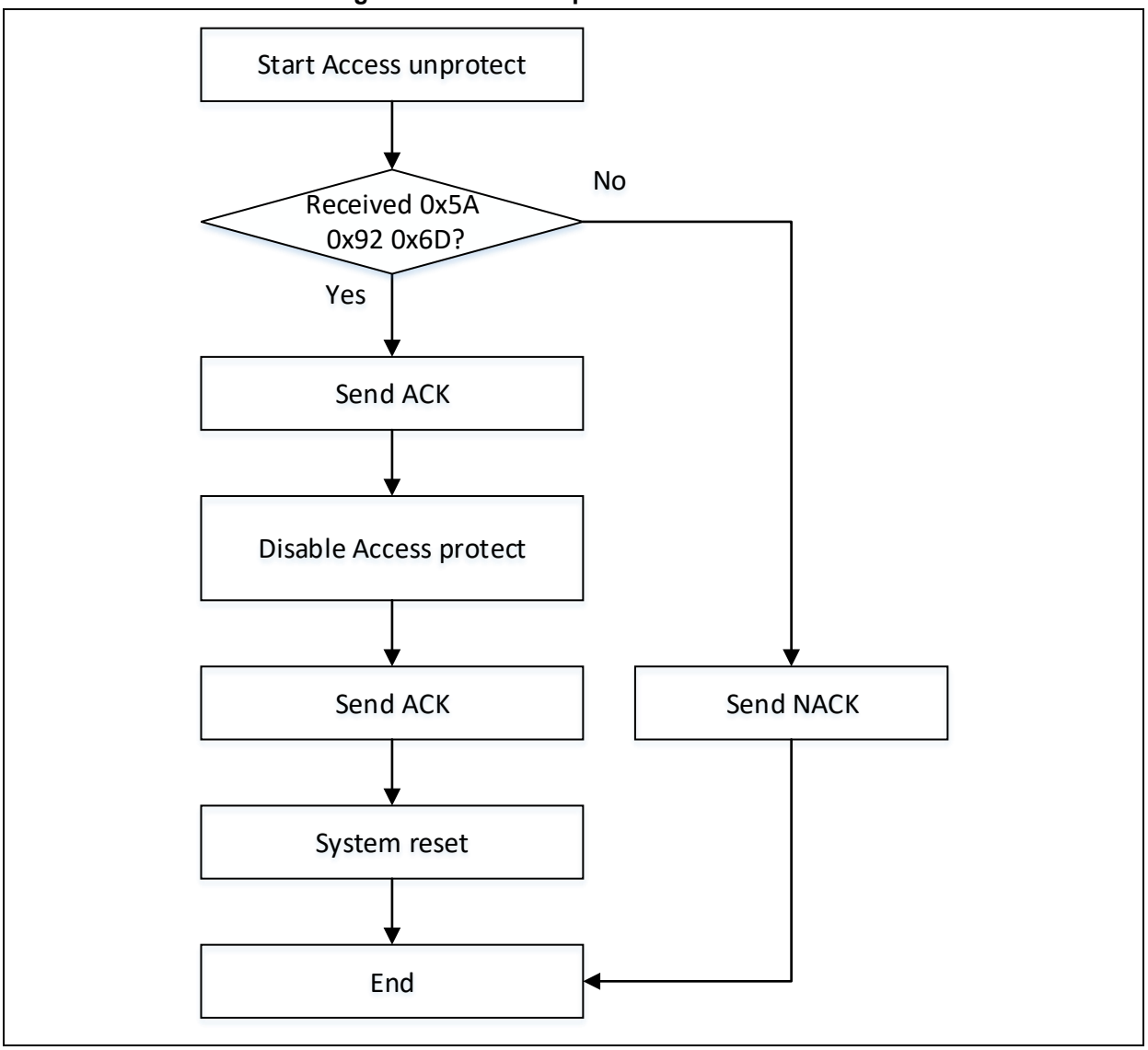


Figure 26 Access Unprotect: device side



3.11.2 Data transmit on host side

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0x92	Access unprotect
3		0x6D	Access unprotect
	1	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
	2	ACK	End of the command (Get ACK procedure).

3.12 Firmware CRC command

This command is used to check whether memory data is correct. The memory area is specified by the host but must be expressed in sector unit and its start address must be aligned with a sector. When the device receives the command, it transmits the ACK byte to the host. After the transmission of the ACK byte, the device waist for the start address (four bytes) and a checksum byte. If the received address and the checksum are all valid, the device transmits the ACK byte to the host. Then the device waits for the number of sectors (two bytes) to be computed -1 (n) and a checksum byte. If the checksum is correct, the device transmits an ACK byte to the host and starts computing CRC value. After the computing operation, the device sends back a four-byte CRC value to the host.

The Firmware CRC adopts the MPEG-2 CRC algorithm.

3.12.1 Flowchart on host and device sides

Figure 27 Firmware CRC: host side

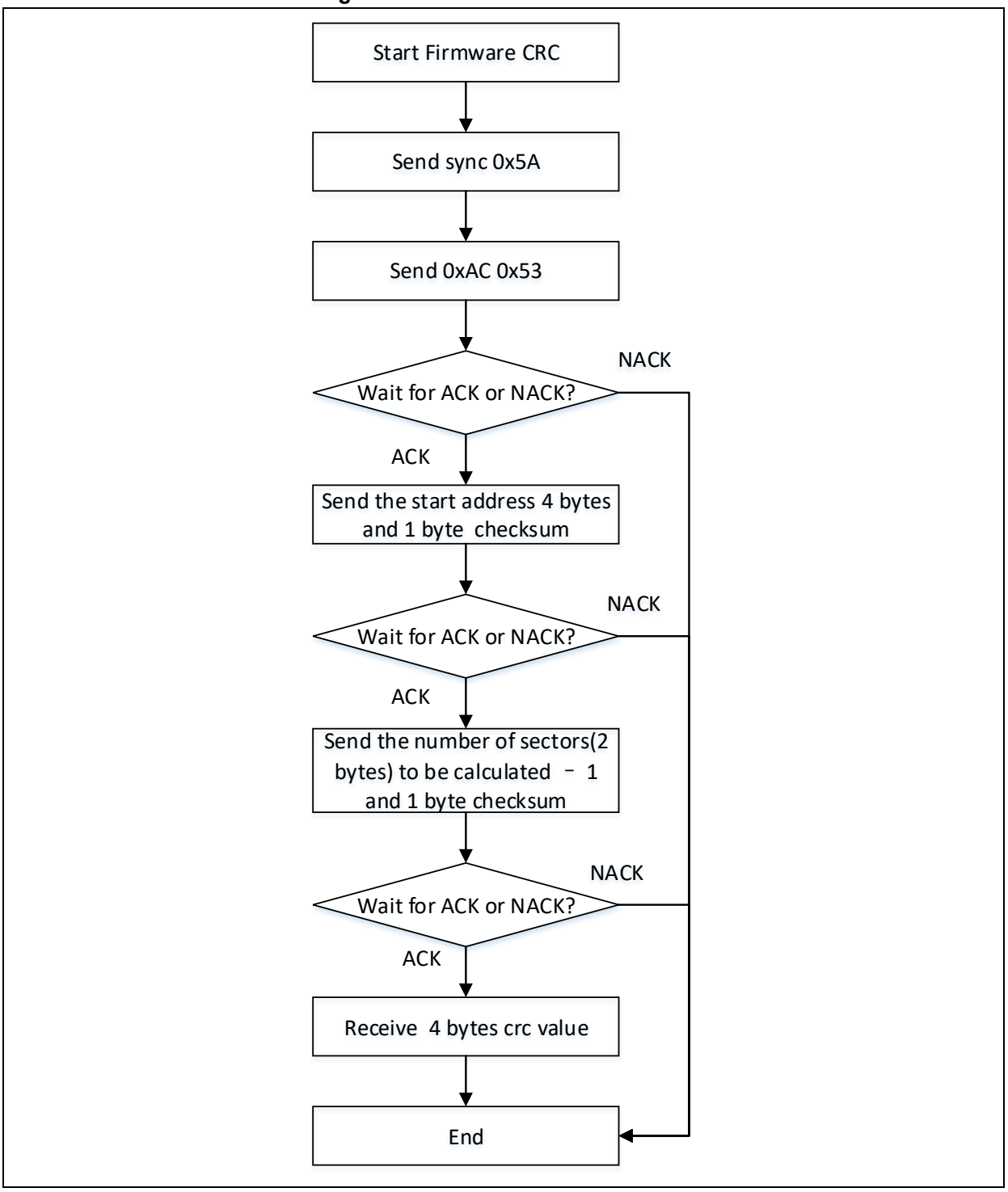
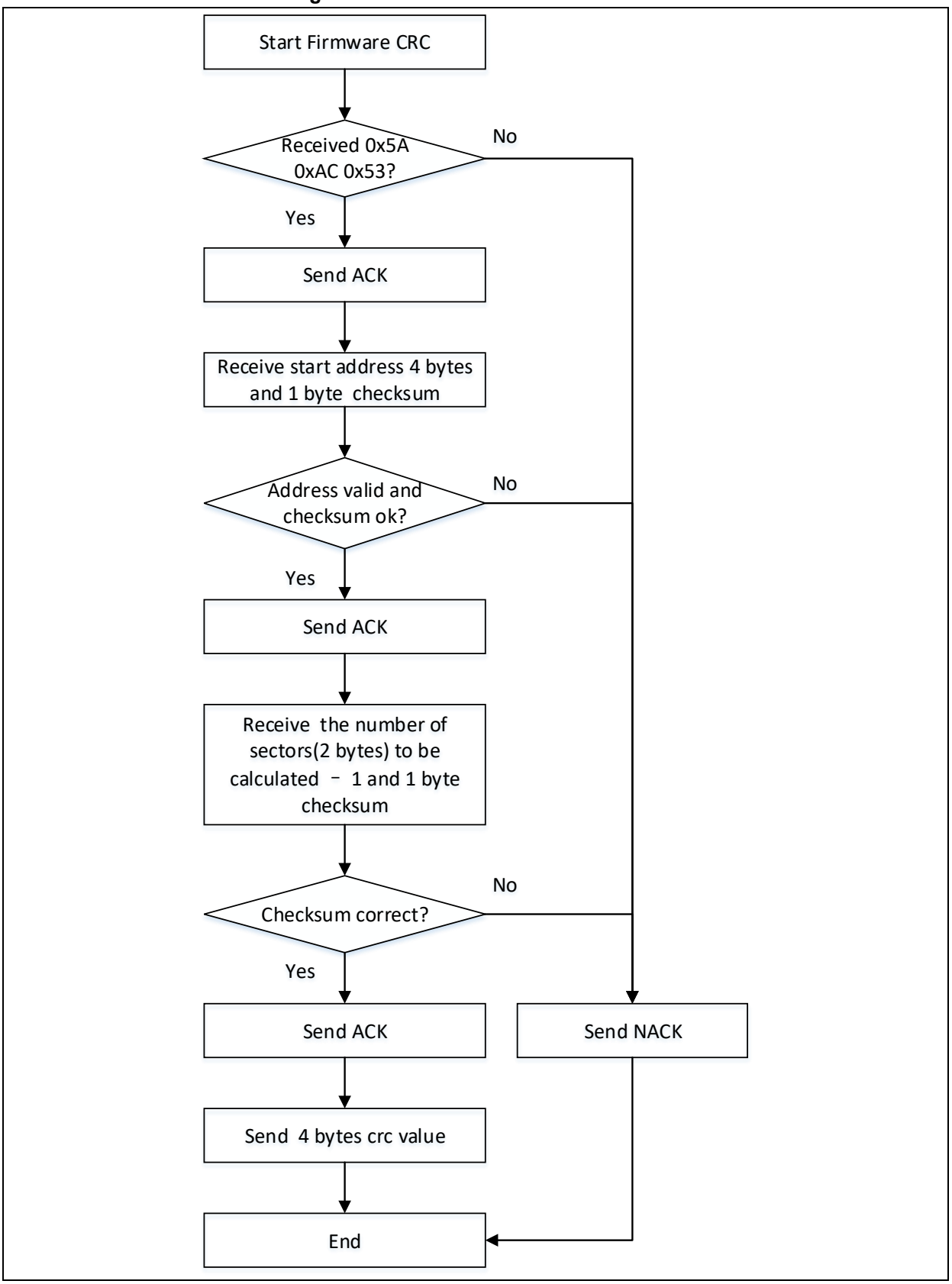


Figure 28 Firmware CRC: device side



3.12.2 Data transmit on host side

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0xAC	Firmware CRC
3		0x53	Firmware CRC
	1	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
4		*	Address （MSB）
5		*	Address
6		*	Address
7		*	Address （LSB）
8		*	Checksum XOR (byte 3~6)
	2	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
9		*	Number of sectors – 1 MSB（n）
10		*	Number of sectors – 1 LSB（n）
11		*	Checksum = XOR byte 8~9
	3	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
	4	*	CRC value (MSB)
	5	*	CRC value
	6	*	CRC value
	7	*	CRC value (LSB)

3.13 Enable sLib

This command is used to enable security library (also called sLib). Refer to the sLib use manual for more details about it.

When the device receives the command, if the access protection is not enabled, it transmits an ACK byte to the host. After the transmission of the ACK byte, the device waits for the sLib password (four bytes), sLib start sector (two bytes), sLib data/instruction start sector (two bytes), sLib end sector (two bytes) and a checksum byte. If the checksum is valid, the device configures sLib, and waits for 1ms before sending back the setting status (one byte). After this operation, the device transmits the ACK byte to the host.

Note that a system reset has to be done for the sLib settings to take into account.

This command is not allowed and executed when the access protection is enabled.

sLib state:

- 1: sLib is enabled
- 0: sLib configuration success

3.13.1 Flowchart on host and device sides

Figure 29 Enable sLib: host side

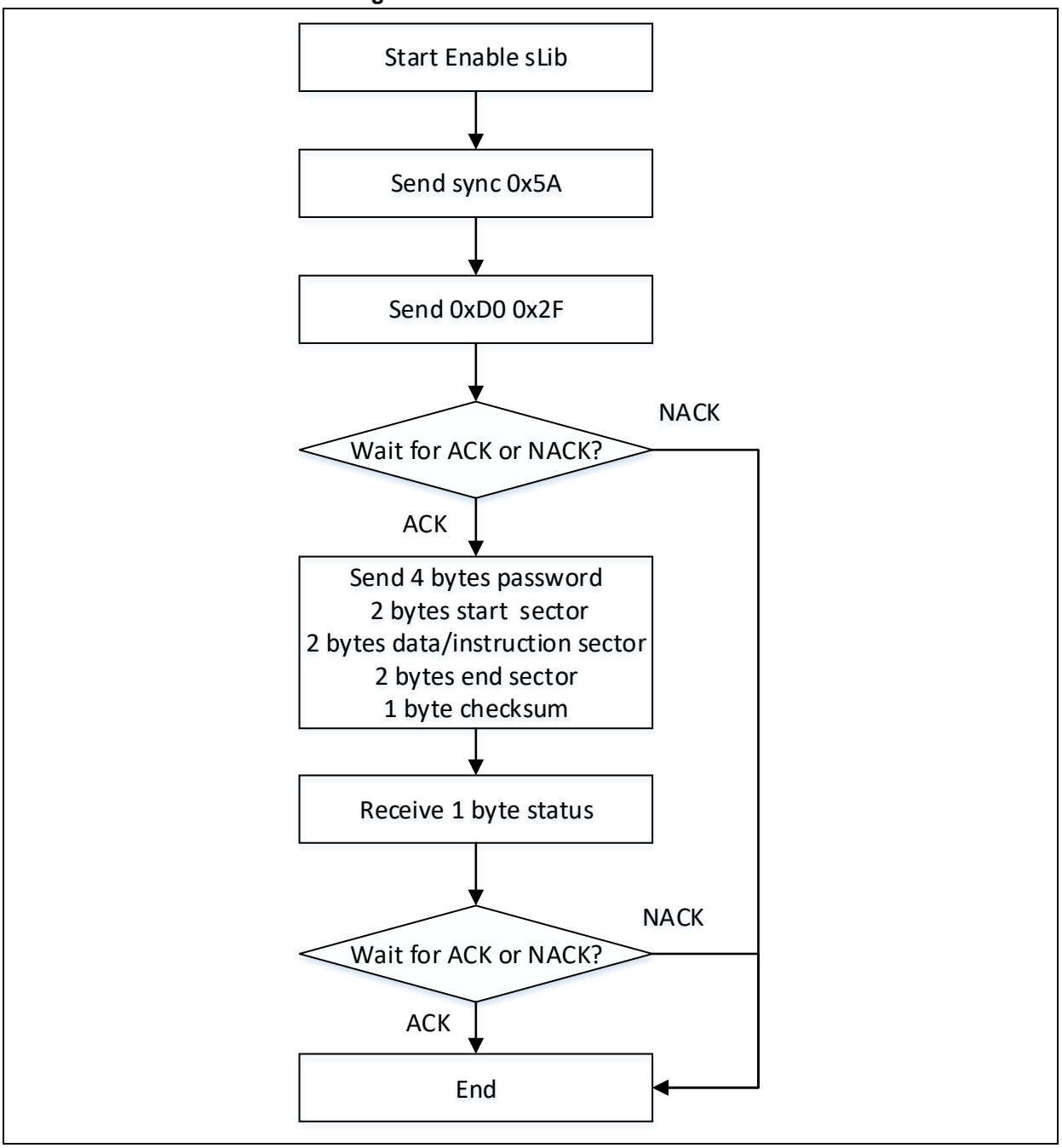
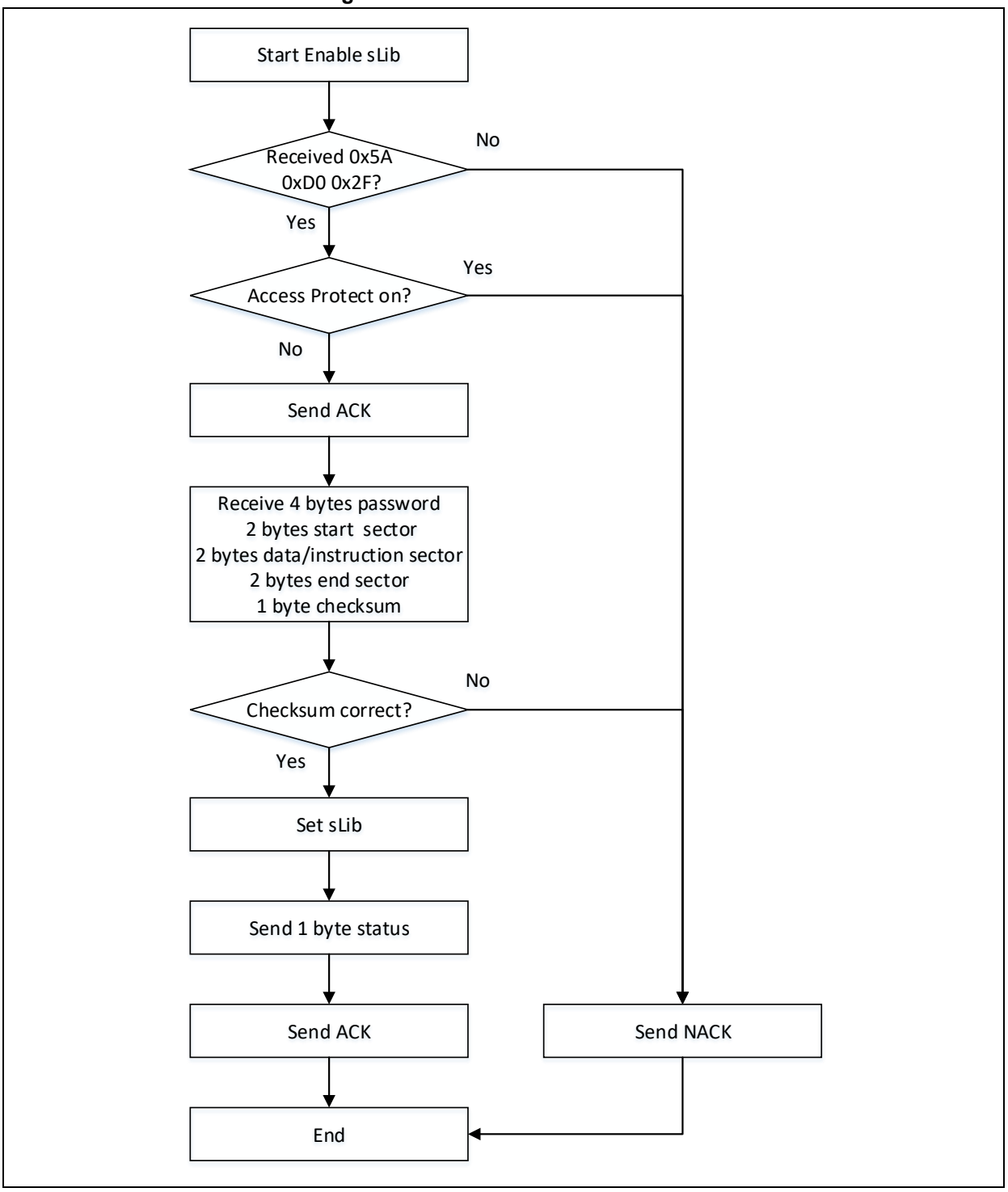


Figure 30 Enable sLib: device side



3.13.2 Data transmit on host side

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0xD0	Enable sLib
3		0x2F	Enable sLib
	1	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
4		*	Password (MSB)
5		*	Password
6		*	Password
7		*	Password（LSB）
8		*	sLib start sector（MSB）
9		*	sLib start sector（LSB）
10		*	sLib data/instruction start sector（MSB）
11		*	sLib data/instruction start sector（LSB）
12		*	sLib end sector（MSB）
13		*	sLib end sector（LSB）
14		*	Checksum XOR byte (3~12)
	2	0/1	sLib configuration state
	3	ACK	End of the command (Get ACK procedure)

3.14 Disable sLib

This command is used to disable sLib. This operation induces mass erase of the memory.
When the device receives the command, if the access protection is not enabled, it transmits an ACK byte to the host. After the transmission of the ACK byte, the device waits for the password (four bytes) and a checksum byte. If the checksum is valid, the device erases sLib, and returns the current state (one bytes). After the operation, the device transmits the ACK byte to the host.
sLib disable state:

- 1: sLib password wrong
- 0: sLib is disabled.

This command is not allowed and executed when the access protection is enabled.

3.14.1 Flowchart on host and device sides

Figure 31 Disable sLib: host side

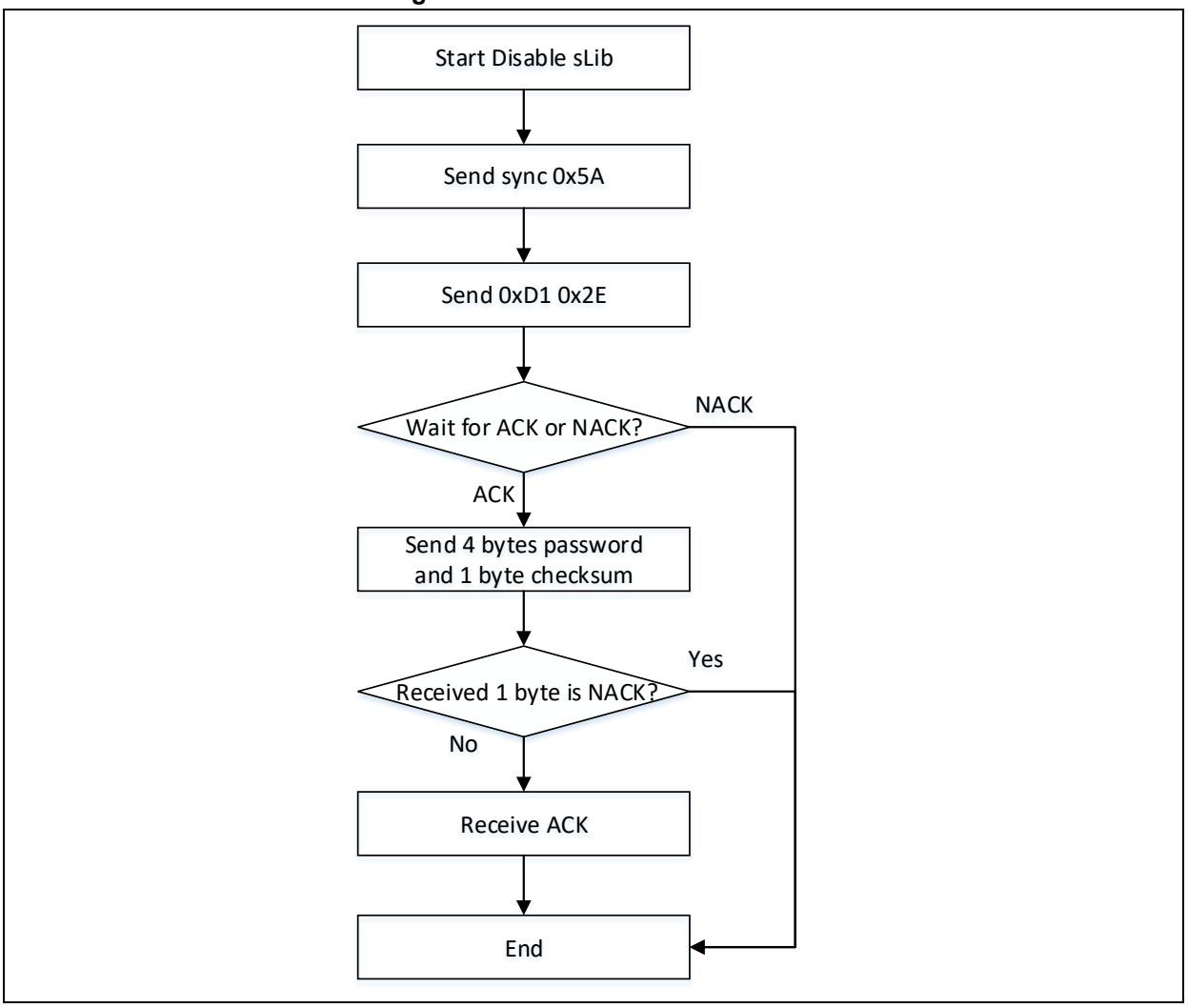
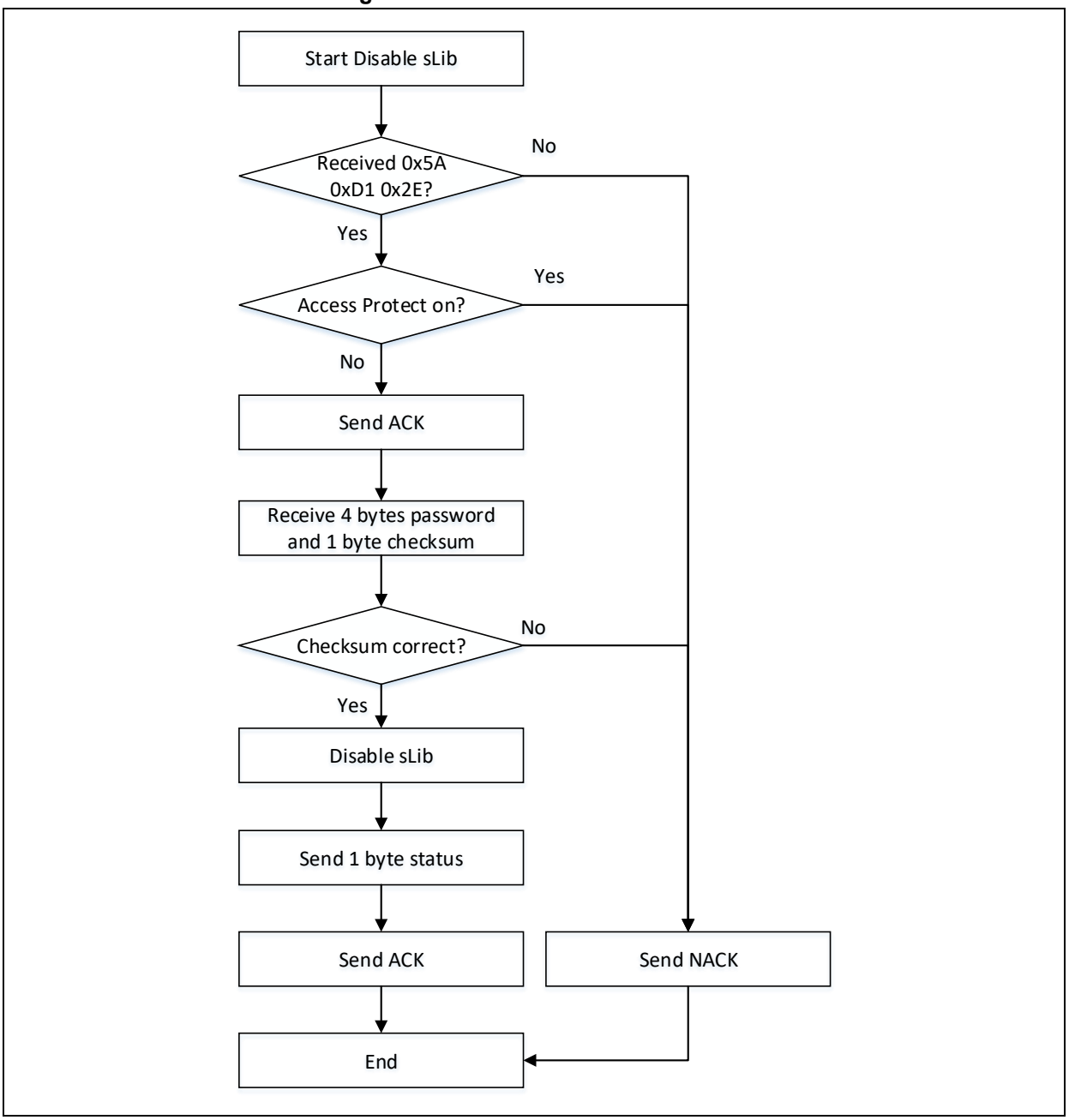


Figure 32 Disable sLib: device side



3.14.2 Data transmit on host side

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0xD1	Disable sLib
3		0x2E	Disable sLib
	1	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
4		*	Password（MSB）
5		*	Password
6		*	Password
7		*	Password（LSB）
	2	0/1	sLib disable state (100ms is required to get the sLib status)
	3	ACK	End of the command (Get ACK procedure).

3.15 Get sLib status

This command is used to get the current sLib state. It returns the corresponding sLib register value. For more details about the sLib, see the corresponding product datasheet.

When the device receives the command, it transmits the ACK byte to the host. After the transmission of the ACK byte, the device sends the values of the SLIB_STS0 register (four bytes), the SLIB_STS1 register (four bytes), and SLIB_MISC_STS register (four bytes). After the operation, the device transmits the ACK byte to the host.

Note: For AT32F403A, AT32F407 and AT32F413 series, this command is not allowed and executed when the access protection is enabled. For other product series, this command is still active when the access protection is enabled.

3.15.1 Flowchart on host and device sides

Figure 33 Get sLib status: host side

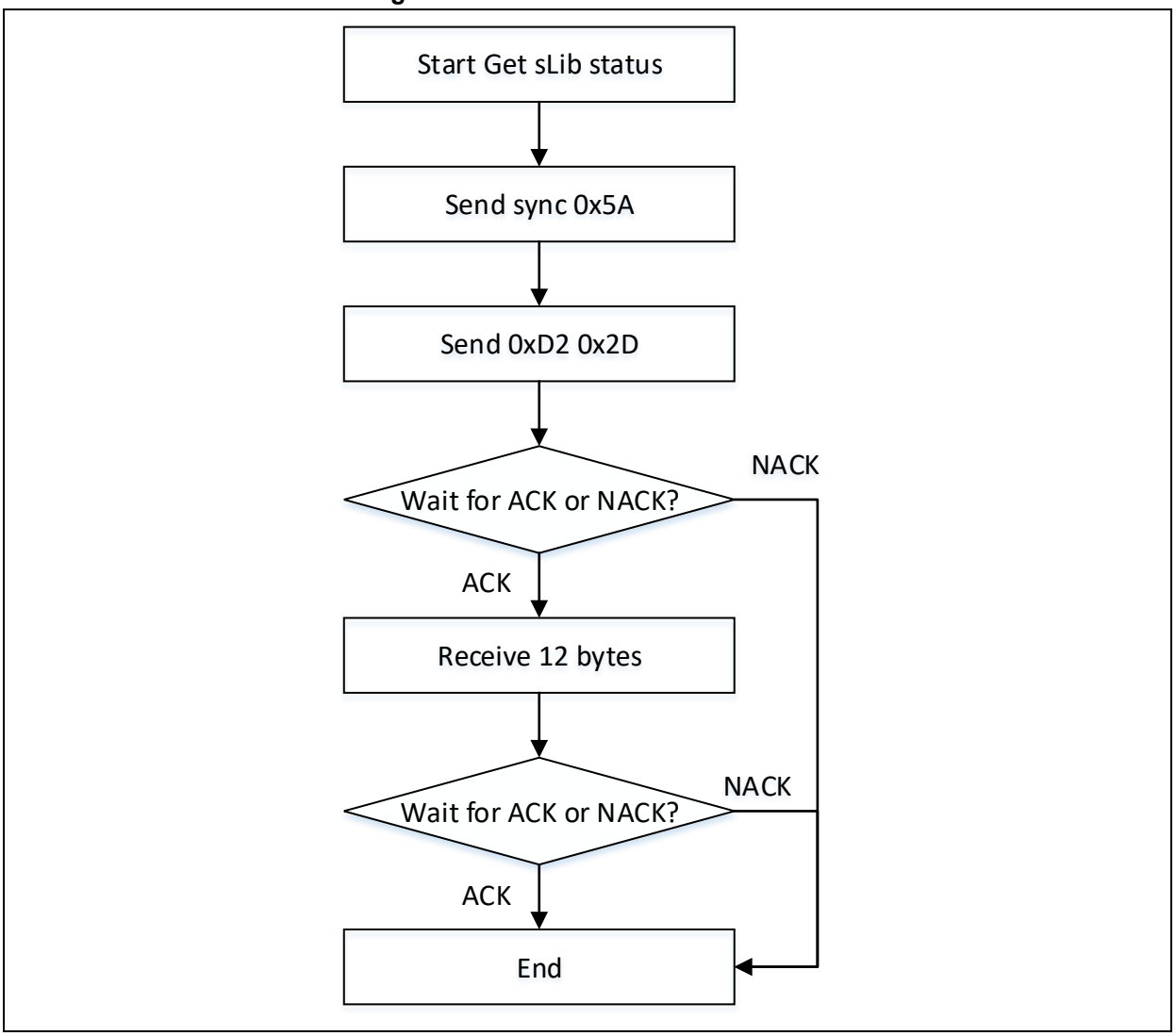
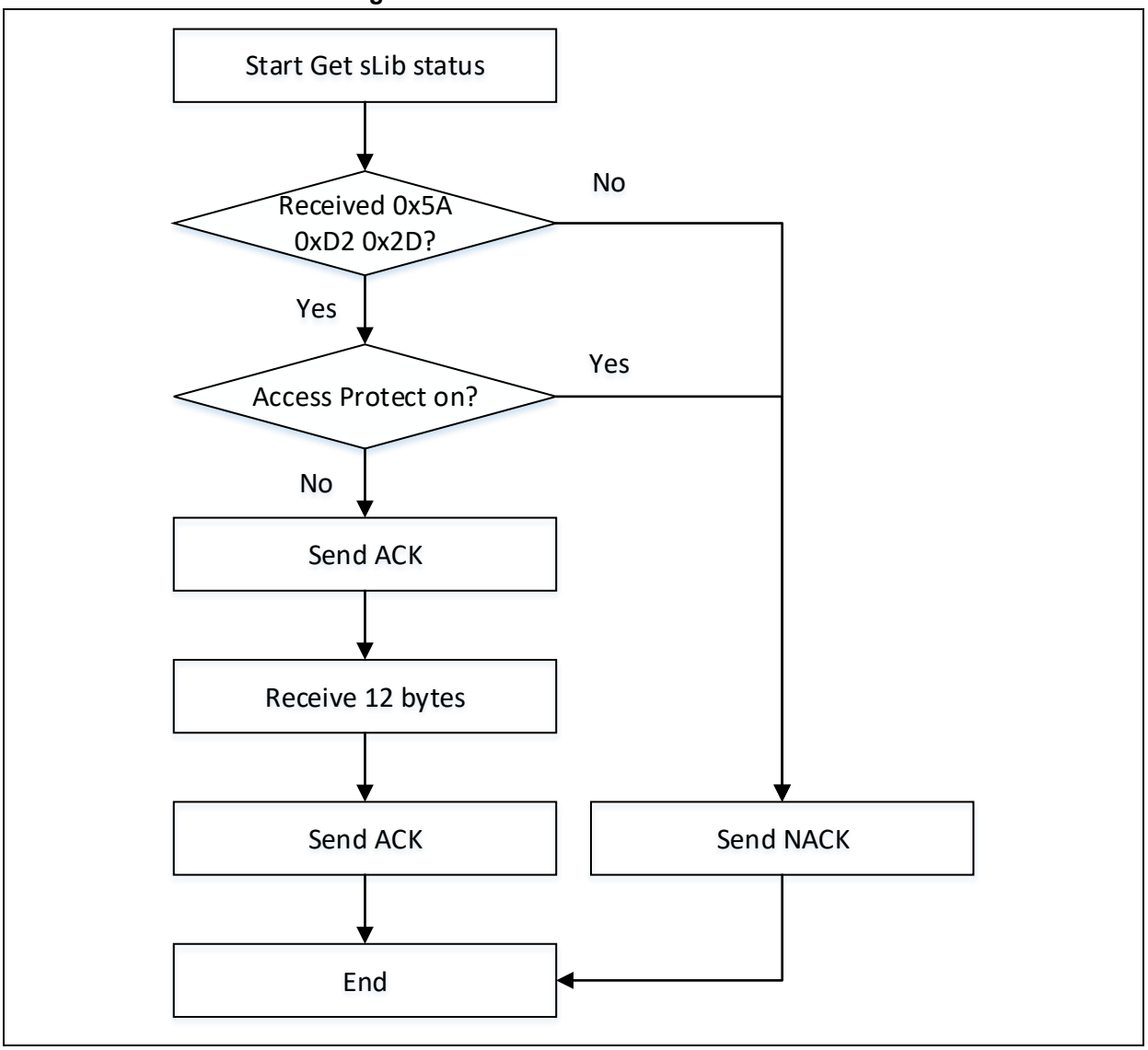


Figure 34 Get sLib status: device side



3.15.2 Data transmit on host side

AT32F435xx/AT32F437xx:

Send	Receive	Data	Description
1		0x5A	Synchronization byte
2		0xD2	Get sLib status
3		0x2D	Get sLib status
	1	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
	2	*	SLIB_STS0（MSB）
	3	*	SLIB_STS0
	4	*	SLIB_STS0
	5	*	SLIB_STS0（LSB）
	6	*	SLIB_STS1（MSB）
	7	*	SLIB_STS1
	8	*	SLIB_STS1
	9	*	SLIB_STS1（LSB）
	10	*	SLIB_MISC_STS（MSB）
	11	*	SLIB_MISC_STS
	12	*	SLIB_MISC_STS
	13		SLIB_MISC_STS（LSB）
	14	ACK	End of the command (Get ACK procedure)

3.16 Reset Device

This command is used to enable a system reset.

When the device receives the command, it transmits the ACK byte to the host in two times and then performs a system reset.

3.16.1 Flowchart on host and device sides

Figure 35 Reset Device: host side

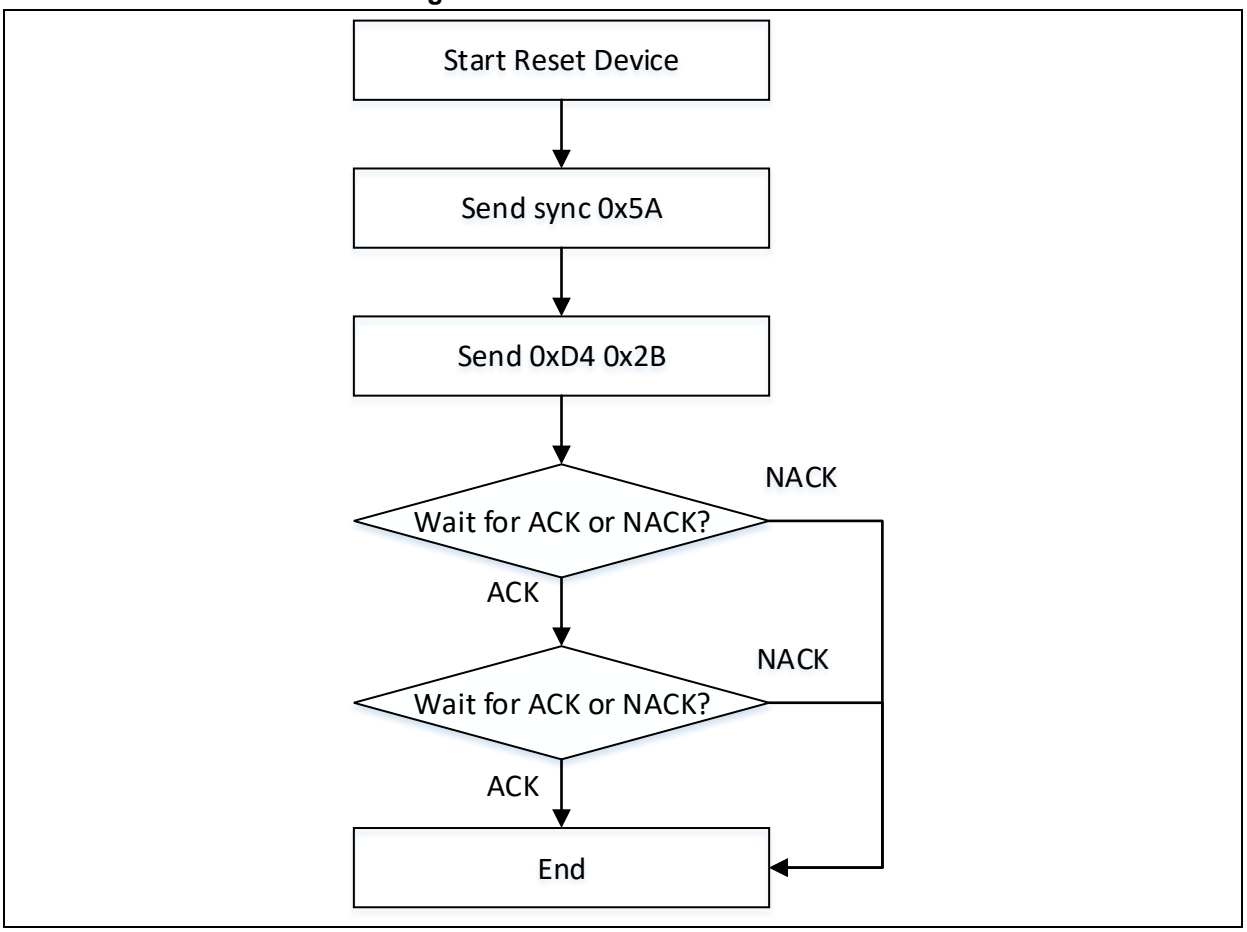
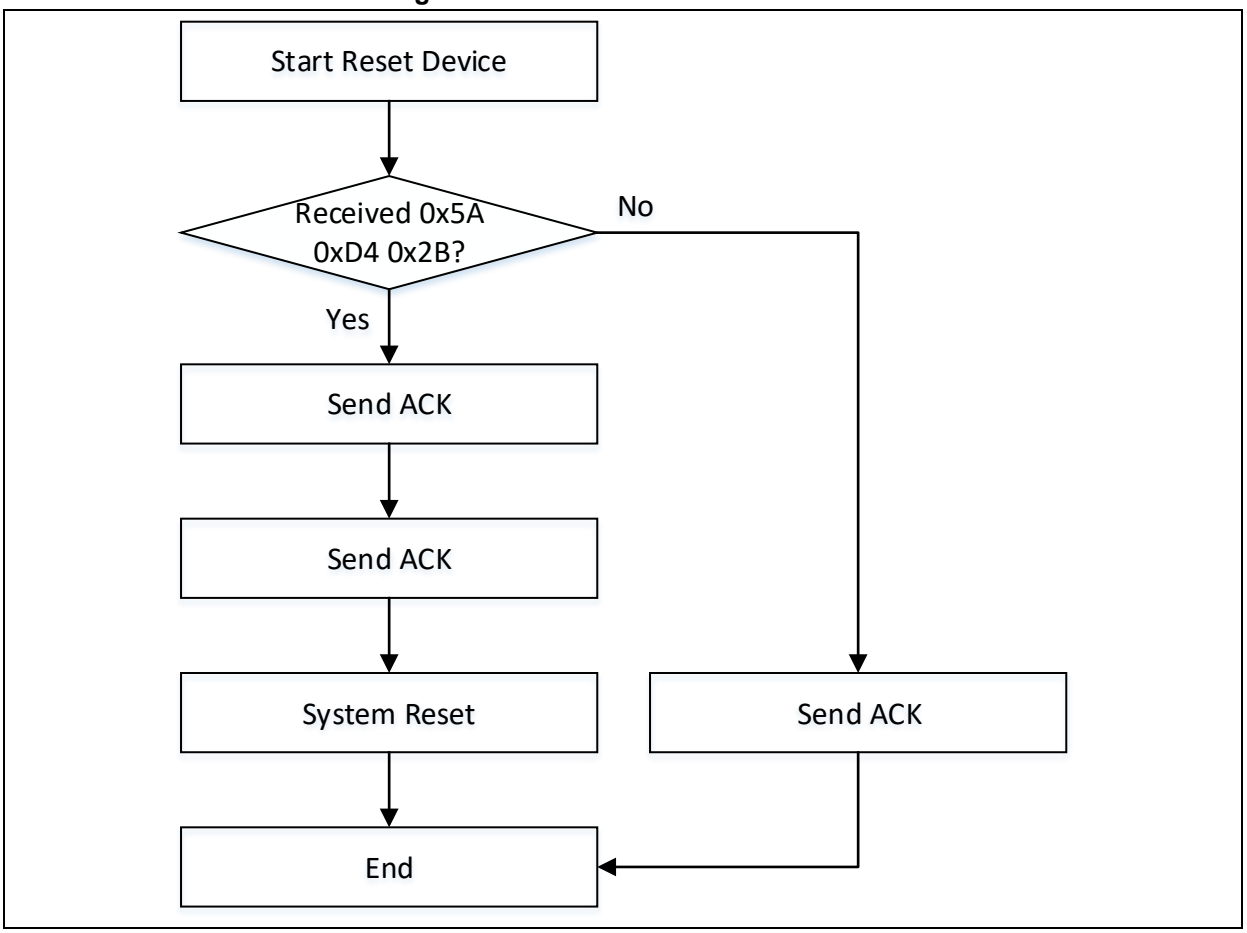


Figure 36 Reset Device: device side



3.16.2 Data transmit on host side

Send	Receive	Data	Description
1		0xD4	Reset Device
2		0x2B	Reset Device
	1	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
	2	ACK	ACK (Get ACK procedure).

3.17 Advanced Access Protect

This command is used to enable advanced access protection. Refer to the corresponding product datasheet for more details about this protection.

When the device receives the command, if the access protection is not enabled, it transmits the ACK byte to the host. After the transmission of the ACK byte, the device waits for the advanced access protection flag (one byte, flag can be any value) and a 1-byte checksum. Then it starts configuring the advanced access protection and transmits the ACK byte to the host before performing a system reset.

This command is not allowed and executed when the access protection is enabled.

Note: the advanced access protection cannot be disabled for some product series. For details, refer to the corresponding user manual.

3.17.1 Flowchart on host and device sides

Figure 37 Advanced Access Protect: host side

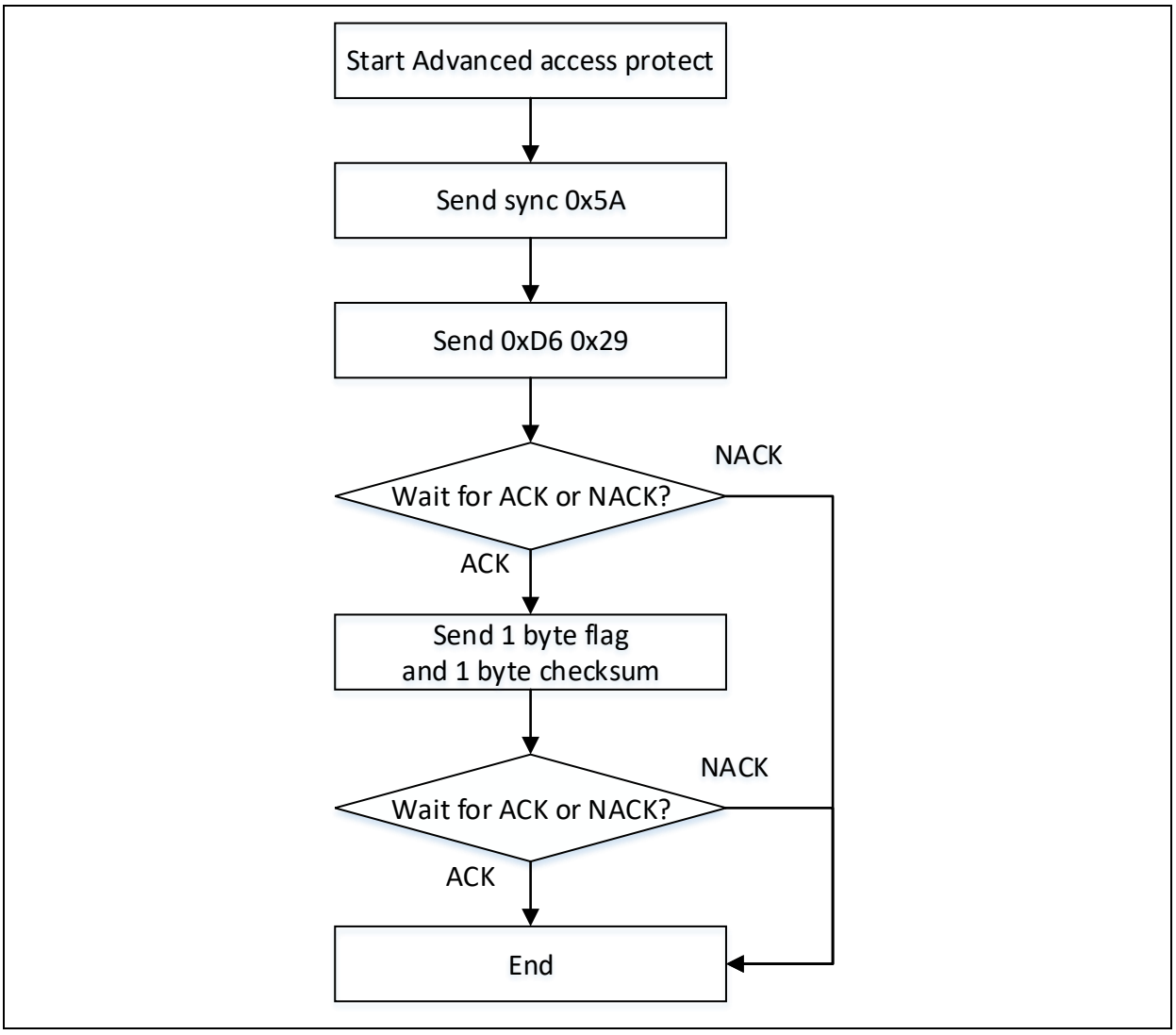
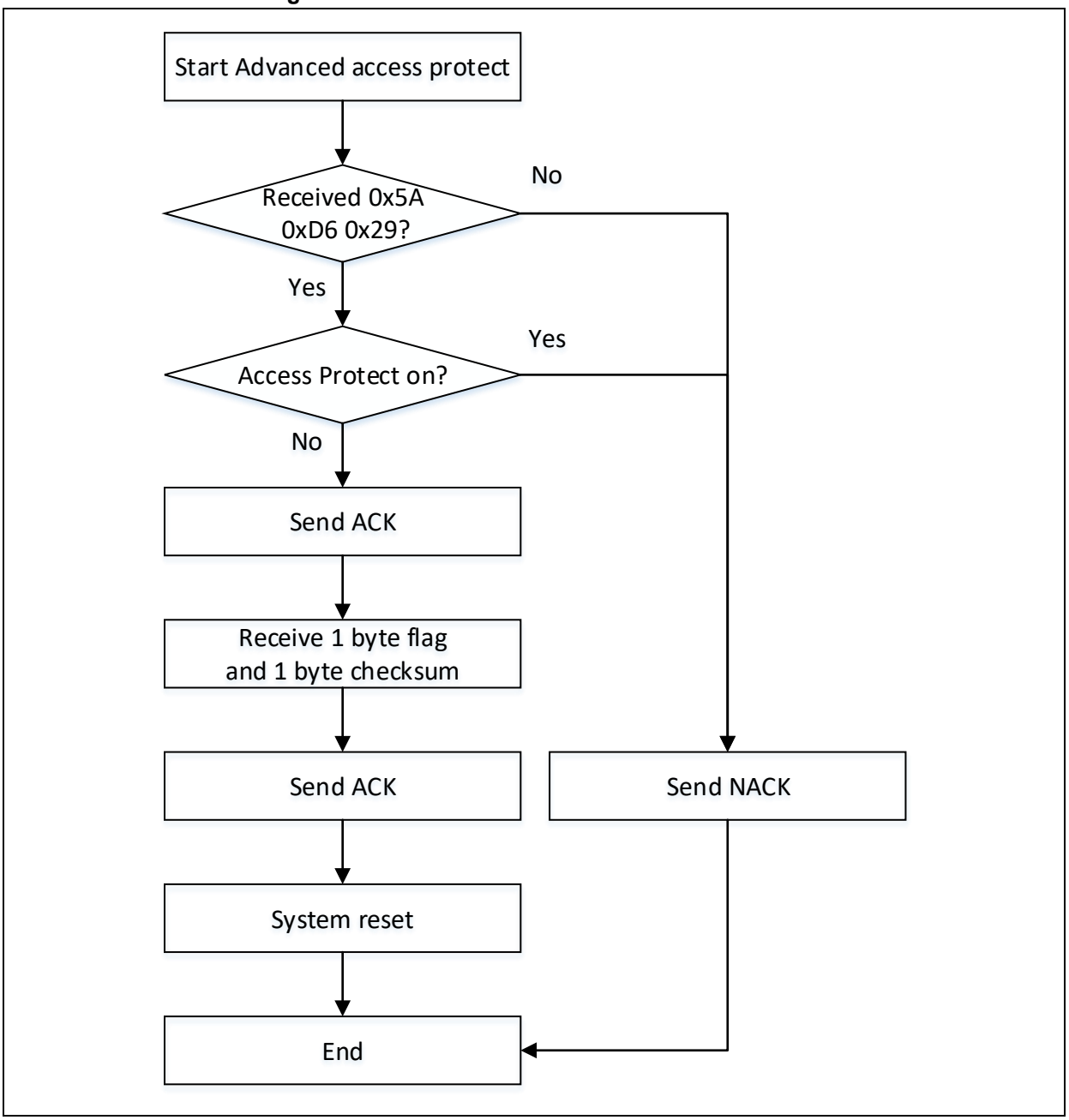


Figure 38 Advanced Access Protect: device side



3.17.2 Data transmit on host side

Send	Receive	Data	Description
1		0xA5	Synchronization byte
2		0xD6	Advanced access protect
3		0x29	Advanced access protect
	1	ACK/NACK	When an NACK byte is received, it indicates the end of the command (Get ACK procedure).
4		*	Flag
5		*	Checksum XOR flag
	2	ACK	End of the command (Get ACK procedure).

4 Revision history

Table 2 Document revision history

Date	Revision	Changes
2023.06.30	2.0.0	Initial release
2024.04.28	2.0.1	1. Update supported product list 2. Update supported command list

IMPORTANT NOTICE – PLEASE READ CAREFULLY

Purchasers are solely responsible for the selection and use of ARTERY's products and services, and ARTERY assumes no liability whatsoever relating to the choice, selection or use of the ARTERY products and services described herein

No license, express or implied, to any intellectual property rights is granted under this document. If any part of this document deals with any third party products or services, it shall not be deemed a license granted by ARTERY for the use of such third party products or services, or any intellectual property contained therein, or considered as a warranty regarding the use in any manner of such third party products or services or any intellectual property contained therein.

Unless otherwise specified in ARTERY's terms and conditions of sale, ARTERY provides no warranties, express or implied, regarding the use and/or sale of ARTERY products, including but not limited to any implied warranties of merchantability, fitness for a particular purpose (and their equivalents under the laws of any jurisdiction), or infringement on any patent, copyright or other intellectual property right.

Purchasers hereby agree that ARTERY's products are not designed or authorized for use in: (A) any application with special requirements of safety such as life support and active implantable device, or system with functional safety requirements; (B) any aircraft application; (C) any aerospace application or environment; (D) any weapon application, and/or (E) or other uses where the failure of the device or product could result in personal injury, death, property damage. Purchasers' unauthorized use of them in the aforementioned applications, even if with a written notice, is solely at purchasers' risk, and Purchasers are solely responsible for meeting all legal and regulatory requirements in such use.

Resale of ARTERY products with provisions different from the statements and/or technical characteristics stated in this document shall immediately void any warranty grant by ARTERY for ARTERY's products or services described herein and shall not create or expand any liability of ARTERY in any manner whatsoever.

© 2024 Artery Technology -All rights reserved