



**STM32F101xx, STM32F102xx and STM32F103xx
system memory boot mode**

Introduction

This application note describes the bootloader stored in the system memory of the STM32F101xx, STM32F102xx and STM32F103xx Flash-memory-based microcontrollers. All STM32F10xxx in production include the bootloader detailed in this application note.

The bootloader is used to program the application into the internal Flash memory. For more information about the Flash module organization, refer to the STM32F101xx, STM32F102xx and STM32F103xx Flash programming manual (PM0042).

The specifications cover the architectural model of the bootloader for the STM32F10xxx family, but the low-level communication software supports all the microcontroller families that implement the bootloader.

Contents

1	Bootloader description	5
1.1	Bootloader introduction	5
1.2	Bootloader activation	5
1.3	Hardware requirements	6
1.4	Bootloader code sequence	7
1.5	Choosing the USART baud rate	8
1.5.1	Minimum baud rate	8
1.5.2	Maximum baud rate	8
1.6	Exiting System memory boot mode	8
2	Bootloader command set	9
2.1	Get command	10
2.2	Get Version & Read Protection Status command	12
2.3	Get ID command	14
2.4	Read Memory command	15
2.5	Go command	18
2.6	Write Memory command	21
2.7	Erase Memory command	25
2.8	Write Protect command	27
2.9	Write Unprotect command	29
2.10	Readout Protect command	31
2.11	Readout Unprotect command	33
3	Bootloader version evolution	34
	Revision history	35

List of tables

Table 1. Boot pin configuration 5

Table 2. STM32F10xxx configuration in System memory boot mode 6

Table 3. Bootloader commands 9

Table 4. Bootloader versions 34

Table 5. Document revision history 35

List of figures

Figure 1.	Bootloader for STM32F10xxx with USART1	7
Figure 2.	Get command: host side	10
Figure 3.	Get command: device side	11
Figure 4.	Get Version & Read Protection Status command: host side	12
Figure 5.	Get Version & Read Protection Status command: device side	13
Figure 6.	Get ID command: host side	14
Figure 7.	Get ID command: device side	14
Figure 8.	Read Memory command: host side	16
Figure 9.	Read Memory command: device side	17
Figure 10.	Go command: host side	19
Figure 11.	Go command: device side	20
Figure 12.	Write Memory command: host side	22
Figure 13.	Write Memory command: device side	23
Figure 14.	Erase Memory command: host side	25
Figure 15.	Erase Memory command: device side	26
Figure 16.	Write Protect command: host side	27
Figure 17.	Write Protect command: device side	28
Figure 18.	Write Unprotect command: host side	29
Figure 19.	Write Unprotect command: device side	30
Figure 20.	Readout Protect command: host side	31
Figure 21.	Readout Protect command: device side	32
Figure 22.	Readout Unprotect command: host side	33
Figure 23.	Readout Unprotect command: device side	33

1 Bootloader description

1.1 Bootloader introduction

The bootloader is stored in the internal boot ROM memory (system memory), and its main task is to download the application program to the internal Flash memory through a USART1 communication interface.

The main features of the bootloader are the following:

- it uses an embedded communication peripheral to download the code (peripherals are handled in polling mode)
- it transfers and updates the Flash memory code, the data, and the vector table sections

1.2 Bootloader activation

The bootloader is automatically activated by configuring the BOOT0 and BOOT1 pins in the specific “System memory” configuration (see [Table 1](#)) and then by applying a reset.

Depending on the used pin configuration, the Flash memory, system memory or SRAM is selected as the boot space, as shown in [Table 1](#) below.

Table 1. Boot pin configuration

Boot mode selection pins		Boot mode	Aliasing
BOOT1	BOOT0		
X	0	User Flash memory	User Flash memory is selected as the boot space
0	1	System memory	System memory is selected as the boot space
1	1	Embedded SRAM	Embedded SRAM is selected as the boot space

[Table 1](#) shows that the STM32F10xxx enters the System memory boot mode if the BOOT pins are configured as follows:

- BOOT0 = 1
- BOOT1 = 0

The values on the BOOT pins are latched on the fourth rising edge of SYSCLK after a reset.

Table 2. STM32F10xxx configuration in System memory boot mode

Feature/Peripheral	State	Comment
Clock source	HSI enabled	The system clock is equal to 24 MHz using the PLL
USART1_RX pin	Input	PA10 pin: USART1 receives
USART1_TX pin	Output	PA9 pin: USART1 transmits
SysTick timer	Enabled	Used to automatically detect the serial baud rate from the host.
USART1	Enabled	Once initialized the USART1 configuration is: 8-bits, even parity and 1 Stop bit
RAM	-	512 bytes starting from address 0x2000 0000 are used by the bootloader firmware
System memory	-	2 Kbytes starting from address 0x1FFF F000, contain the bootloader firmware
IWDG	-	The independent watchdog (IWDG) prescaler is configured to its maximum value and is periodically refreshed to prevent watchdog reset (in case the hardware IWDG option was previously enabled by the user)

- Note:**
- 1 The system clock is derived from the embedded internal high-speed RC, no external quartz is required for the bootloader code.
 - 2 After downloading the application binary, if you choose to execute the Go command, the peripheral registers used by the bootloader (shown in the above table) are not initialized to their default reset values before jumping to the user application. They should be reconfigured in the user application if they are used. So, if the IWDG is being used in the application, the IWDG prescaler value has to be adapted to meet the requirements of the application (since the prescaler was set to its maximum value by the bootloader).

1.3 Hardware requirements

The hardware required to put the STM32F10xxx into System memory boot mode consists of any circuitry, switch or jumper, capable of holding the BOOT0 pin high and the BOOT1 pin low during reset.

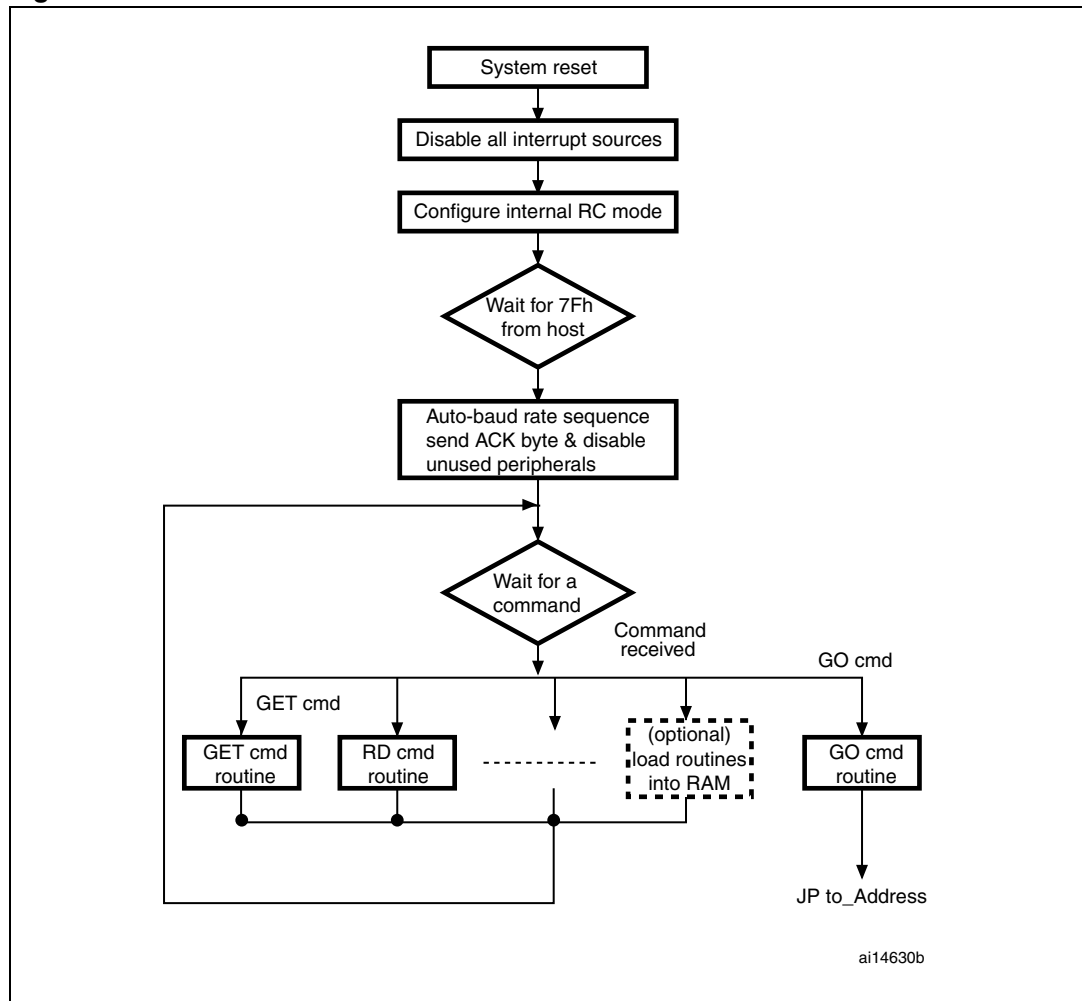
To connect to the STM32F10xxx during System memory boot mode, an RS232 serial interface (example, ST3232 RS232 transceiver) has to be directly linked to the USART1_RX (PA10) and USART1_TX (PA9) pins.

Note: USART1_CK, USART1_CTS and USART1_RTS pins are not used, therefore user can use these pins for other peripherals or GPIOs.

For more details about hardware recommendations, refer to application note AN2586: “STM32F10xxx hardware development: getting started”, available from the STMicroelectronics website: www.st.com.

1.4 Bootloader code sequence

Figure 1. Bootloader for STM32F10xxx with USART1



Once the System memory boot mode is entered and the STM32F10xxx has been configured as described above, the bootloader code begins to scan the PA10 pin (USART1_RX line), waiting to receive 0x7F data: one start bit, 0x7F data bits, even parity bit and one stop bit.

The duration of this data byte is measured using the SysTick timer. The count value of the timer is then used to calculate the corresponding baud rate factor with respect to the current system clock.

Next, the code initializes the serial interface accordingly. Using this calculated baud rate, an acknowledge byte (0x79) is returned to the host, which signals that the STM32F10xxx is ready to receive user commands.

1.5 Choosing the USART baud rate

The calculation of the serial baud rate for USART1, from the length of the first byte that is received, is used to operate the bootloader within a wide range of baud rates. However, the upper and lower limits have to be kept, in order to ensure proper data transfer.

For a correct data transfer from the host to the STM32F10xxx, the maximum deviation between the internal initialized baud rate for USART1 and the real baud rate of the host should be below 2.5%. The deviation (f_B , in percent) between the host baud rate and the STM32F10xxx baud rate can be calculated using the formula below:

$$f_B = \left| \frac{\text{STM32Fxxx baud rate} - \text{Host baud rate}}{\text{STM32Fxxx baud rate}} \right| \times 100\%, \text{ where } f_B \leq 2.5\%.$$

This baud rate deviation is a nonlinear function depending on the CPU clock and the baud rate of the host. The maximum of the function (f_B) increases with the host baud rate. This is due to the smaller baud rate prescale factors, and the implied higher quantization error.

1.5.1 Minimum baud rate

The lowest tested baud rate (B_{Low}) is 1200. Baud rates below B_{Low} would cause the SysTick timer to overflow. In this event, USART1 would not be correctly initialized.

1.5.2 Maximum baud rate

B_{High} is the highest baud rate for which the deviation still does not exceed the limit. All baud rates between B_{Low} and B_{High} are below the deviation limit. The highest tested baud rate (B_{High}) is 115 200.

1.6 Exiting System memory boot mode

System memory boot mode must be exited in order to execute a program in a normal User mode. The STM32F10xxx may exit this mode by applying a hardware reset. At the time of reset, the BOOT pins (BOOT0 and BOOT1) must be set at the proper levels to enter the desired user mode (see [Table 1](#)). Following the reset, the CPU starts code execution from the boot memory located at the bottom of the memory address space starting from 0x0000 0000.

2 Bootloader command set

The supported commands are listed in [Table 3](#) below. Each command is further described in this section.

Table 3. Bootloader commands

Command ⁽¹⁾	Command code	Command description
Get ⁽²⁾	0x00	Gets the version and the allowed commands supported by the current version of the bootloader
Get Version & Read Protection Status ⁽²⁾	0x01	Gets the bootloader version and the Read Protection status of the Flash memory
Get ID ⁽²⁾	0x02	Gets the chip ID
Read Memory	0x11	Reads up to 256 bytes of memory starting from an address specified by the user
Go	0x21	Jumps to the user application code located in the internal Flash memory or in SRAM
Write Memory	0x31	Writes up to 256 bytes to the RAM or Flash memory starting from an address specified by the user
Erase	0x43	Erases from one to all the Flash memory pages
Write Protect ⁽³⁾	0x63	Enables the write protection for some sectors
Write Unprotect ⁽³⁾	0x73	Disables the write protection for all Flash memory sectors
Readout Protect ⁽²⁾	0x82	Enables the read protection
Readout Unprotect ⁽²⁾	0x92	Disables the read protection

1. If a denied command is received or an error occurs during the command execution, the bootloader sends NACK byte and goes back to command checking.
2. Read protection – When the RDP (read protection) option is active, only this limited subset of commands is available. All other commands are NACKed and have no effect on the device. Once the RDP has been removed, the other commands become active.
3. On the STM32F10xxx, the sector size is 4 KBytes so, depending on the product, this could be 4 pages (when the page is 1 Kbyte) or 2 pages (when the page is 2 KBytes) for the Write Protect and Write Unprotect commands.

Communication safety

All communications from the programming tool (PC) to the device are verified by:

1. checksum: all received bytes are XORed. A byte containing the computed XOR of all previous bytes is added to the end of each communication (checksum byte). By XORing all received bytes, data + checksum, the result at the end of the packet must be 0x00.
2. for each command the host sends a byte and its complement (XOR = 0x00)
3. UART: parity check active (even parity)

Each packet is either accepted (ACK answer) or discarded (NACK answer):

- ACK = 0x79
- NACK = 0x1F

2.1 Get command

The Get command allows the user to get the version of the bootloader and the supported commands. When the bootloader receives the Get command, it transmits the bootloader version and the supported command codes to the host, as described in [Figure 2](#).

Figure 2. Get command: host side

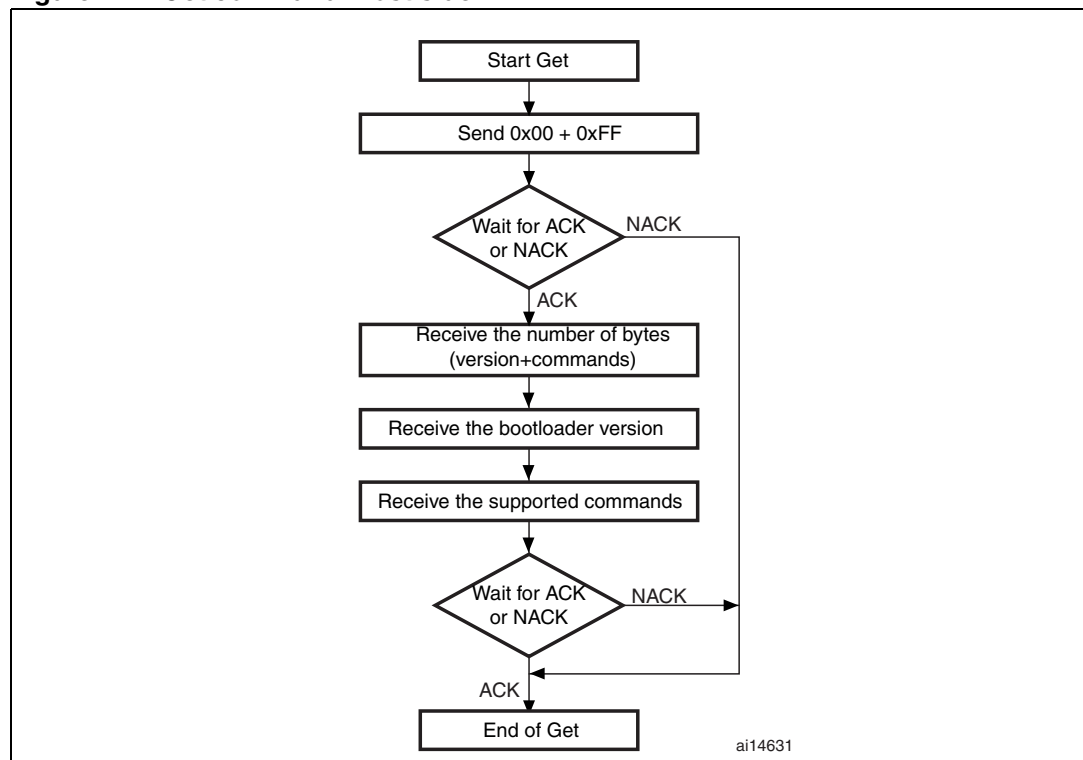
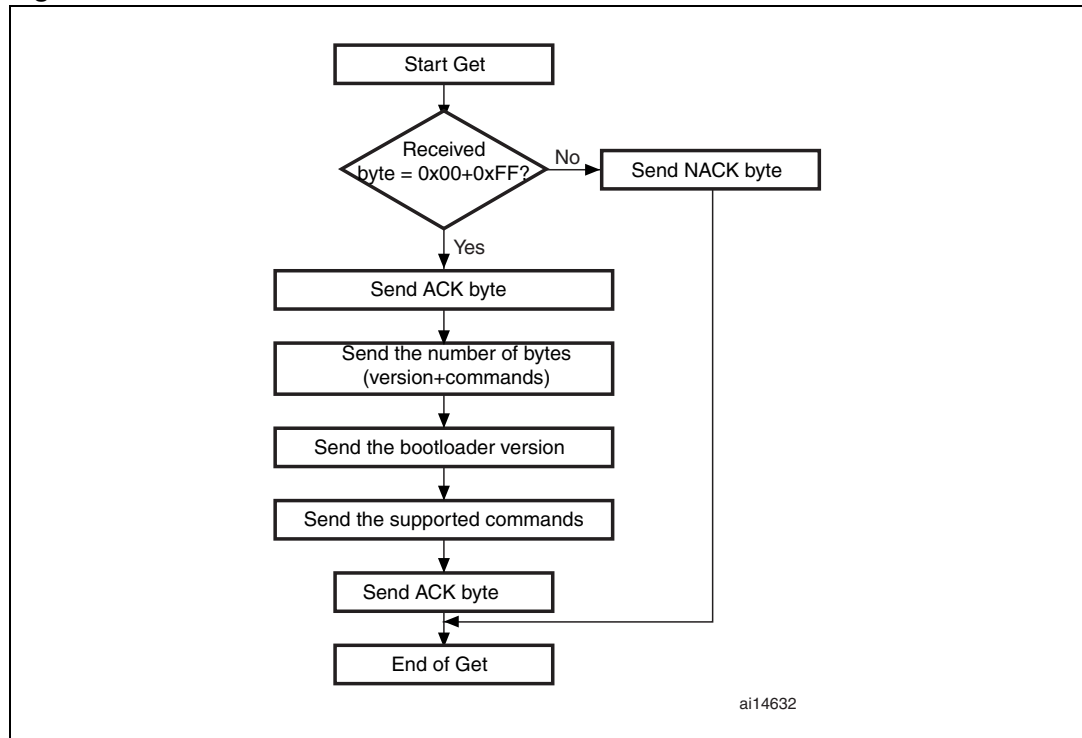


Figure 3. Get command: device side

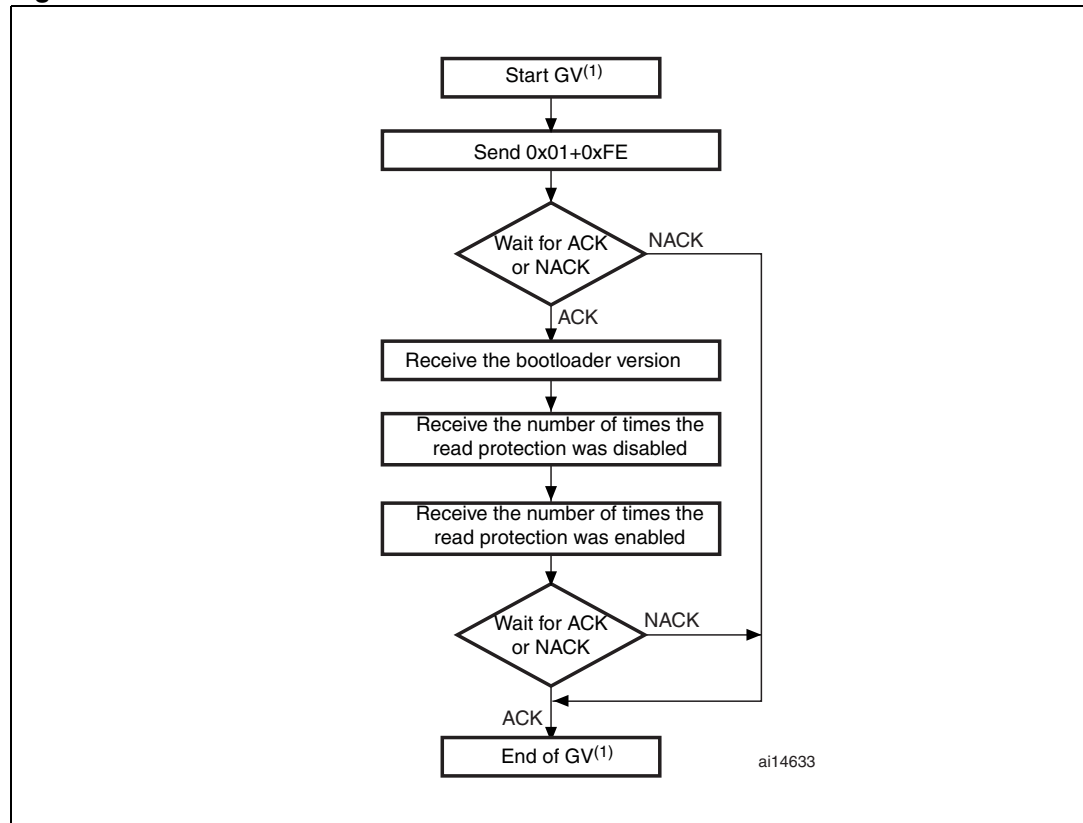
The STM32F10xxx sends the bytes as follows:

- Byte 1: ACK
- Byte 2: N = 11 = the number of bytes to follow – 1 except current and ACKs.
- Byte 3: Bootloader version (0 < Version < 255): 0x21 = Version 2.1
- Byte 4: 0x00 – Get command
- Byte 5: 0x01 – Get Version and Read Protection Status
- Byte 6: 0x02 – Get ID
- Byte 7: 0x11 – Read Memory command
- Byte 8: 0x21 – Go command
- Byte 9: 0x31 – Write Memory command
- Byte 10: 0x43 – Erase command
- Byte 11: 0x63 – Write Protect command
- Byte 12: 0x73 – Write Unprotect command
- Byte 13: 0x82 – Readout Protect command
- Byte 14: 0x92 – Readout Unprotect command
- Last byte (15): ACK

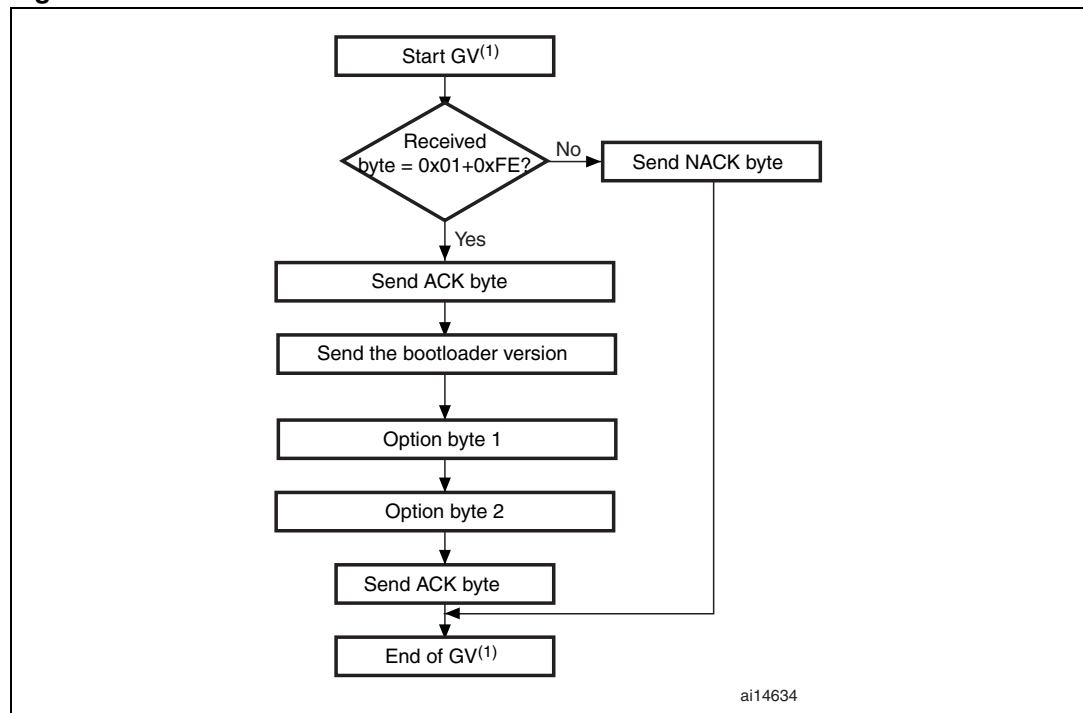
2.2 Get Version & Read Protection Status command

The Get Version & Read Protection Status command is used to get the bootloader version and the read protection status. When the bootloader receives the command, it transmits the information described below (version, read protection: number of times it was enabled and disabled) to the host.

Figure 4. Get Version & Read Protection Status command: host side



1. GV = Get Version & Read Protection Status.

Figure 5. Get Version & Read Protection Status command: device side

1. GV = Get Version & Read Protection Status.

The STM32F10xxx sends the bytes as follows:

Byte 1: ACK

Byte 2: The version of the bootloader ($0 < \text{Version} \leq 255$): 0x21 = Version 2.1

Byte 3: Option byte 1: 0x00 to keep the compatibility with generic bootloader protocol

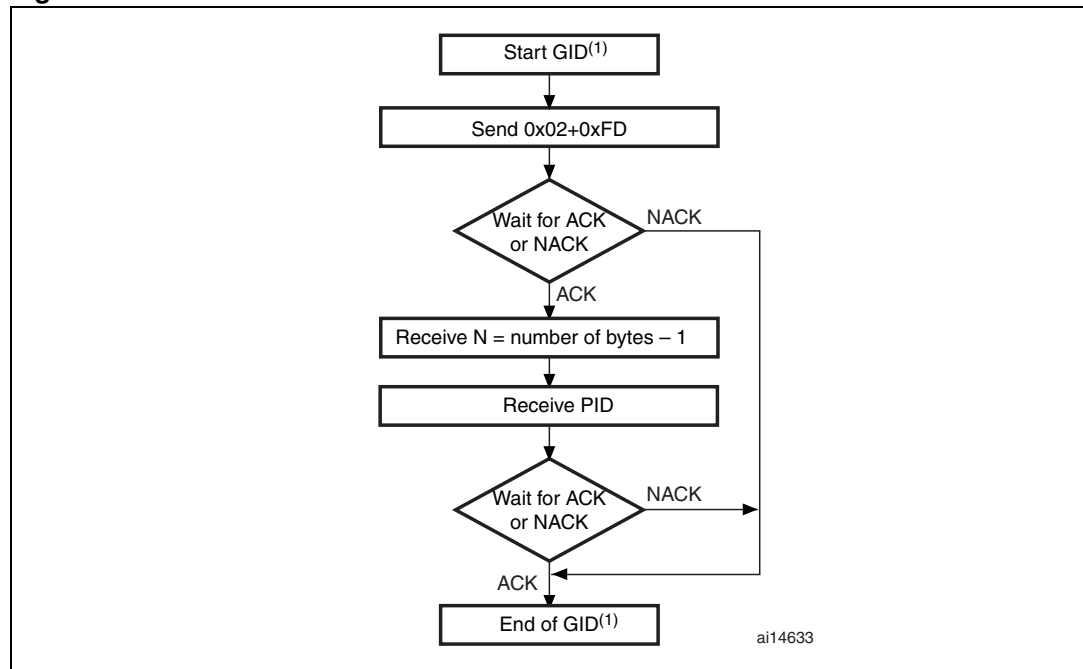
Byte 4: Option byte 2: 0x00 to keep the compatibility with generic bootloader protocol

Byte 5: ACK

2.3 Get ID command

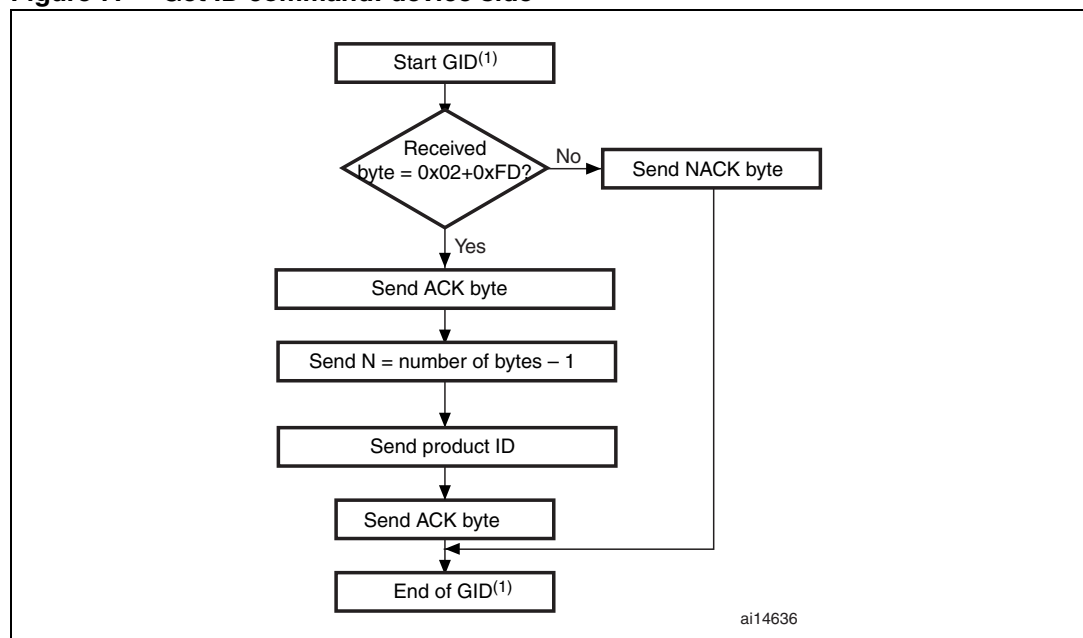
The Get ID command is used to get the version of the chip ID (identification). When the bootloader receives the command, it transmits the product ID to the host.

Figure 6. Get ID command: host side



1. GID = Get ID.

Figure 7. Get ID command: device side



1. GID = Get ID.

The STM32F10xxx sends the bytes as follows:

Byte 1: ACK

Byte 2: N = the number of bytes – 1 (N = 1 for STM32F10xxx), except for current byte and ACKs.

Bytes 3-4: PID⁽¹⁾ byte 3 = 0x04, byte 4 = 0x1X

Byte 5: ACK

1. PID: is the product ID, which may be 0x0410, 0x0412 or 0x0414 according to the STM32F10xxx product.

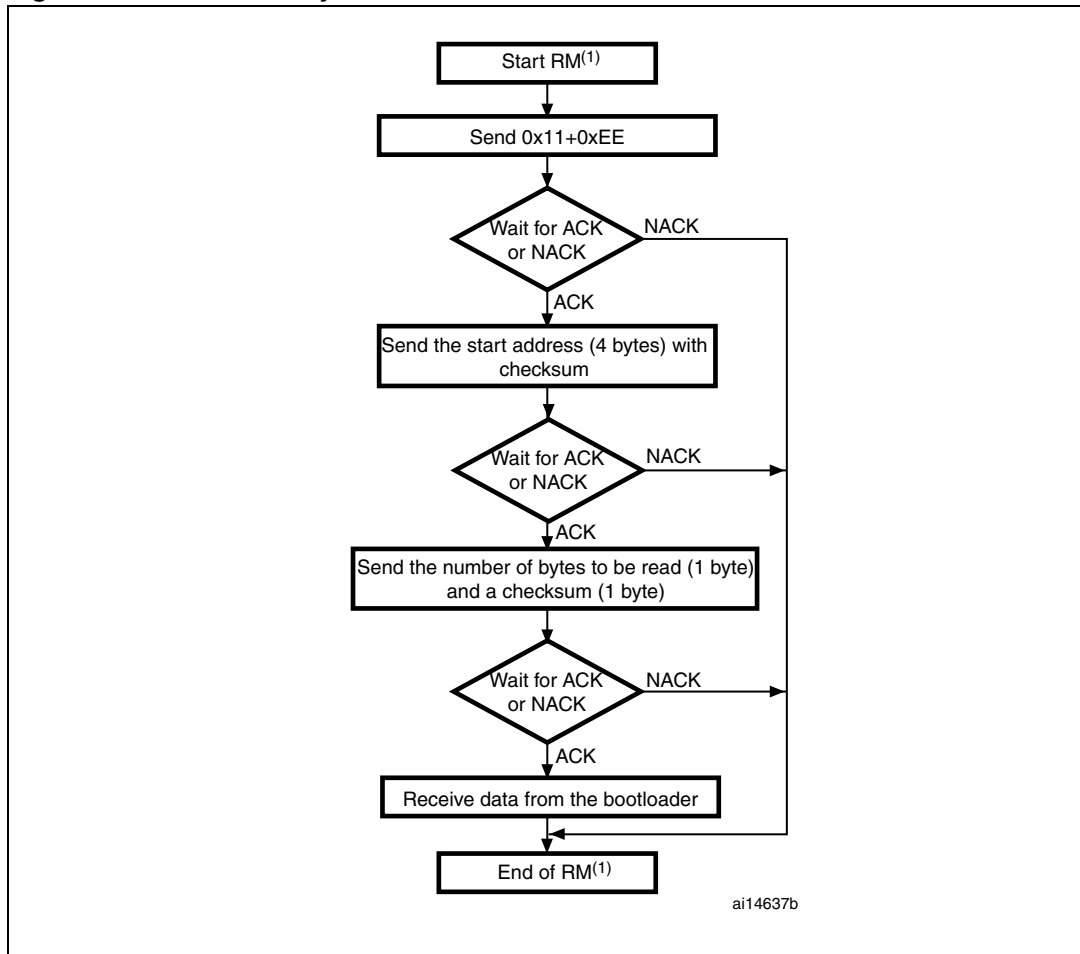
2.4 Read Memory command

The Read Memory command is used to read data from any memory address in RAM, Flash memory and information block (System memory or option byte areas).

When the bootloader receives the Read Memory command, it transmits the ACK byte to the user. After the transmission of the ACK byte, the bootloader waits for an address (4 bytes, byte 1 is the address MSB and byte 4 is the LSB) and a checksum byte, then it checks the received address. If the address is valid and the checksum is correct, the bootloader transmits an ACK byte, otherwise it transmits a NACK byte and aborts the command.

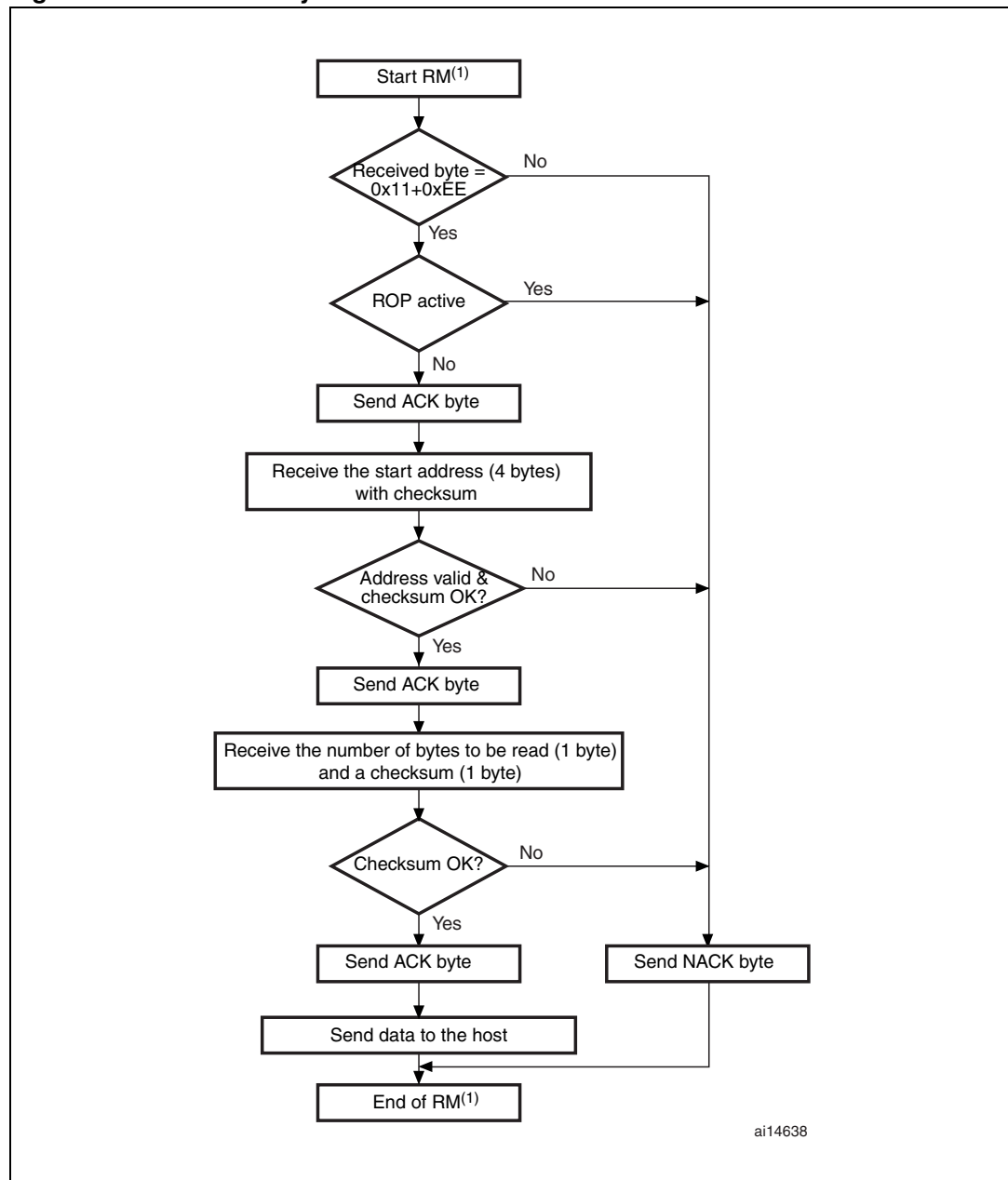
When the address is valid and the checksum is correct, the bootloader waits for the number of bytes to be transmitted – 1 (N bytes) and for its complemented byte (checksum). If the checksum is correct it then transmits the needed data ((N + 1) bytes) to the user, starting from the received address. If the checksum is not correct, it sends a NACK before aborting the command.

Figure 8. Read Memory command: host side



1. RM = Read Memory.

Figure 9. Read Memory command: device side



1. RM = Read Memory.

The host sends the bytes to the STM32F10xxx as follows:

Bytes 1-2: 0x11+0xEE

Wait for ACK

Bytes 3 to 6: start address

- byte 3: MSB
- byte 6: LSB

Byte 7: Checksum: XOR (byte 3, byte 4, byte 5, byte 6)

Wait for ACK

Byte 8: The number of bytes to be read – 1 ($0 < N \leq 255$);

Byte 9: Checksum: XOR byte 8 (complement of byte 8)

2.5 Go command

The Go command is used to execute the downloaded code or any other code by branching to an address specified by the user. When the bootloader receives the Go command, it transmits the ACK byte to the user. After the transmission of the ACK byte, the bootloader waits for an address (4 bytes, byte 1 is the address MSB and byte 4 is LSB) and a checksum byte, then it checks the received address. If the address is valid and the checksum is correct, the bootloader transmits an ACK byte, otherwise it transmits a NACK byte and aborts the command.

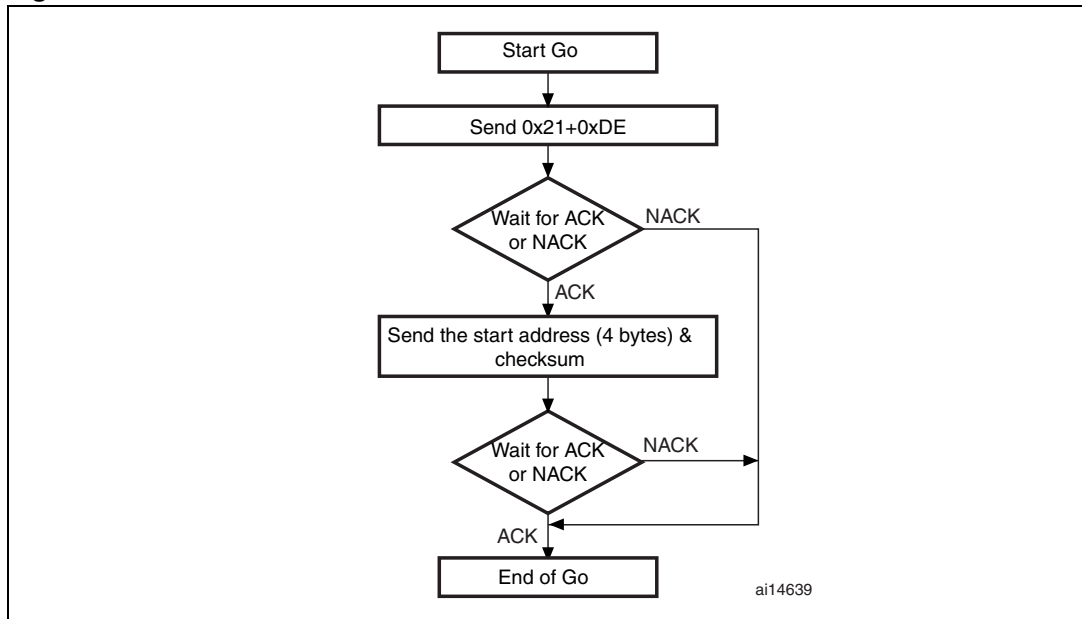
When the address is valid and the checksum is correct, the bootloader firmware:

- initializes the user application's main stack pointer
- jumps to the memory location programmed in the received address + 4 (which corresponds to the address of the application's reset handler)

For example if the received address is 0x0800 0000, the bootloader will jump to the memory location programmed at address 0x0800 0004.

In general, the host should send the base address where the application to jump to is programmed.

Figure 10. Go command: host side

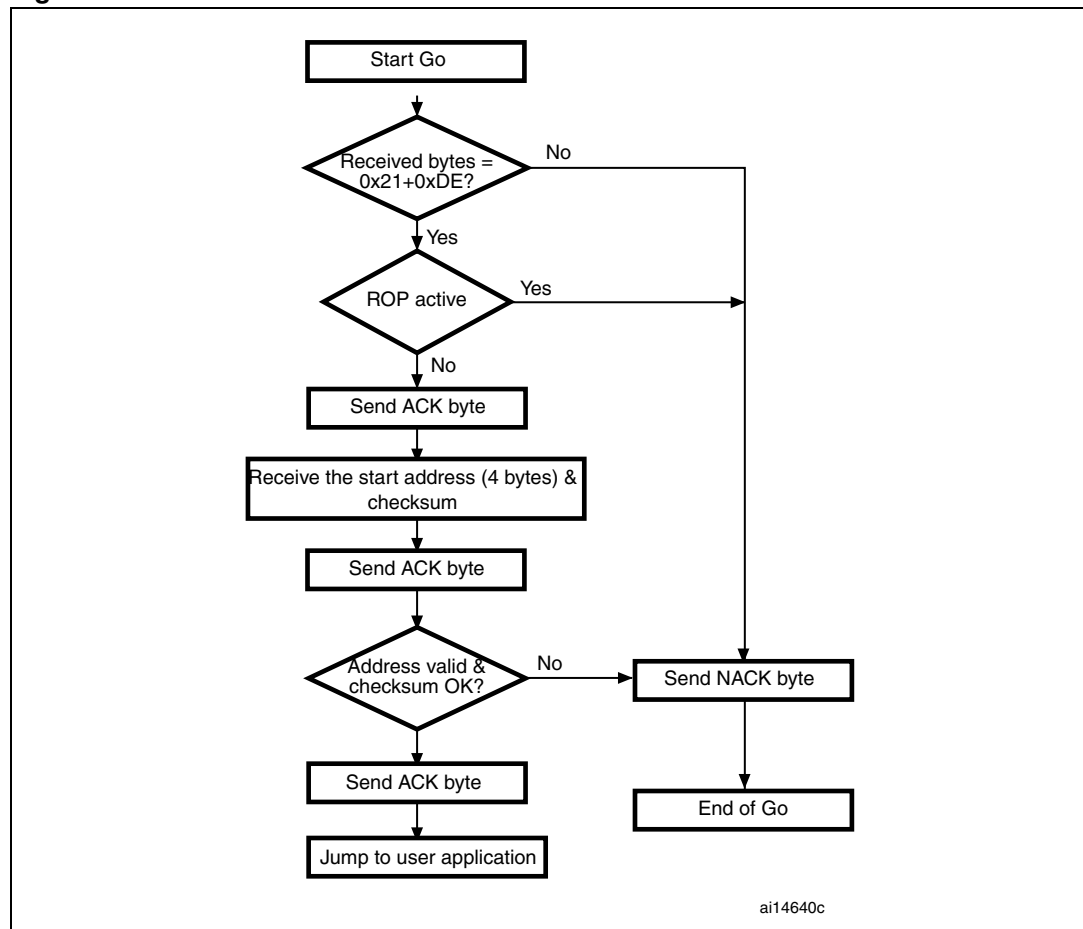


Note: Valid addresses are RAM (starting from 0x2000 0200 to the end of the RAM) or Flash memory (starting from 0x800 0000 to the end of the Flash memory) addresses. All other addresses are considered not valid and will be NACKed by the device.

When an application is loaded into RAM and then a jump is made to it, the program must be configured to run with an offset of at least 0x200 to avoid overlapping with the first 0x200 RAM memory used by the bootloader firmware.

Jump to the application works only if the user application sets the vector table to point to the application address.

Figure 11. Go command: device side



The host sends the bytes as follow to the STM32F10xxx:

Byte 1: 0x21

Byte 2: 0xDE

Wait for ACK

Byte 3 to Byte 6: start address

byte3: MSB

byte6: LSB

Byte 7: checksum: XOR (byte 3, byte 4, byte 5, byte 6)

2.6 Write Memory command

The Write Memory command is used to write data to any memory address of RAM (starting from 0x2000 0200), Flash memory, or Option byte area. Refer to the STM32F101xx, STM32F102xx and STM32F103xx Flash programming manual. When the bootloader receives the Write Memory command, it transmits the ACK byte to the user. After the transmission of the ACK byte, the bootloader waits for an address (4 bytes, byte 1 is the address MSB and byte 4 is the LSB) and a checksum byte, it then checks the received address. For the Option byte area, the start address must be 0x1FFFF800 to avoid writing inopportunely in this area.

If the received address is valid and the checksum is correct, the bootloader transmits an ACK byte, otherwise it transmits a NACK byte and aborts the command. When the address is valid and the checksum is correct, the bootloader:

- gets a byte, N, which contains the number of data bytes to be received
- receives the user data ((N + 1) bytes) and the checksum (XOR of N and of all data bytes)
- programs the user data to memory starting from the received address
- at the end of the command, if the write operation was successful, the bootloader transmits the ACK byte; otherwise it transmits a NACK byte to the user and aborts the command

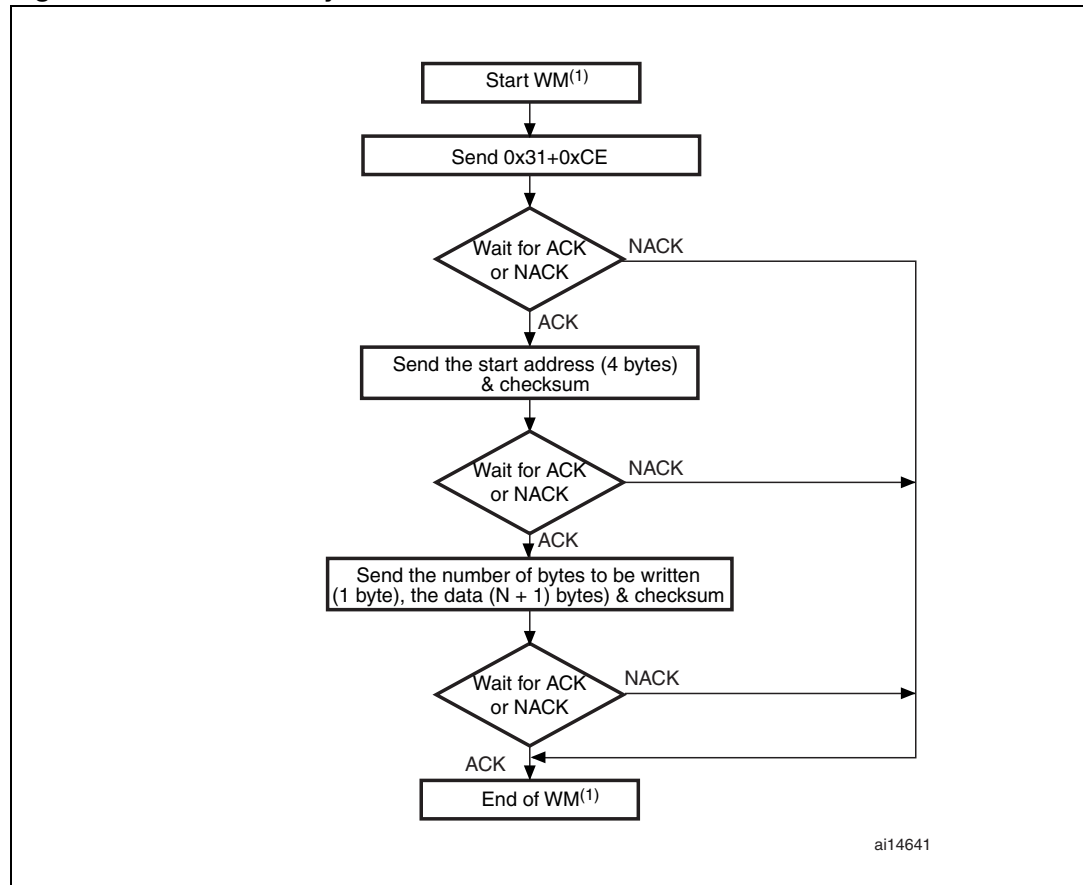
The maximum length of the block to be written for the STM32F10xxx is 256 bytes.

If the Write Memory command is issued to the Option byte area, all options are erased before writing the new values and, at the end of the command, the bootloader generates a system reset to take into account the new configuration of the option byte.

Note: When writing to the RAM, care must be taken to avoid overlapping with the first 512 bytes (0x200) in RAM because they are used by the bootloader firmware.

No error is returned when write operations are performed on write-protected sectors.

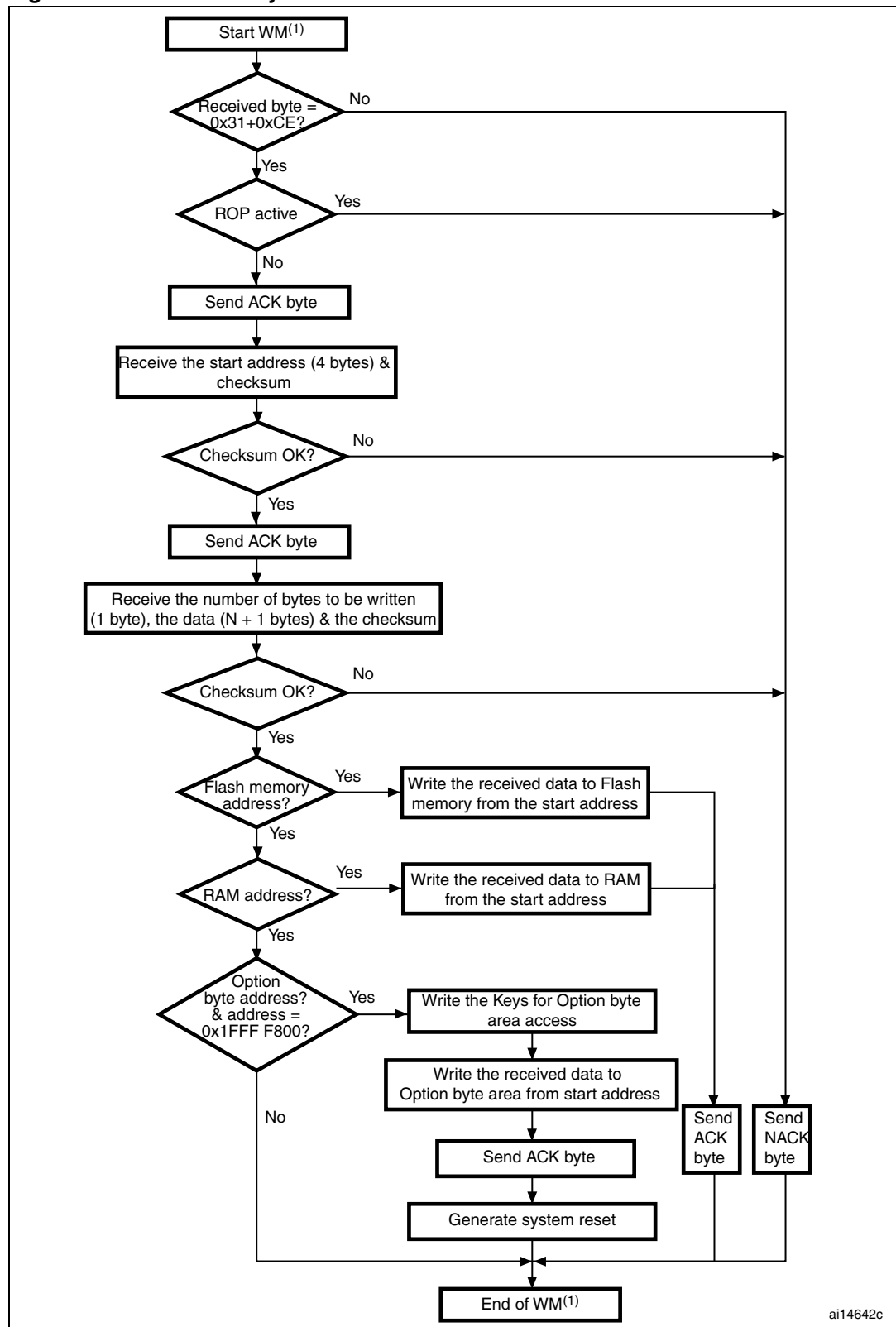
Figure 12. Write Memory command: host side



1. WM = Write Memory.

Note: *If the start address is invalid, the command is NACKed by the device.*

Figure 13. Write Memory command: device side



1. WM = Write Memory.

The host sends the bytes to the STM32F10xxx as follows:

Byte 1: 0x31

Byte 2: 0xCE

Wait for ACK

Byte 3 to byte 6: start address

byte 3: MSB

byte 6: LSB

Byte 7: Checksum: XOR (Byte3, Byte4, Byte5, Byte6)

Wait for ACK

Byte 8: Number of bytes to be received ($0 < N \leq 255$)

N +1 data bytes: (Max 256 bytes)

Checksum byte: XOR (N, N+1 data bytes)

2.7 Erase Memory command

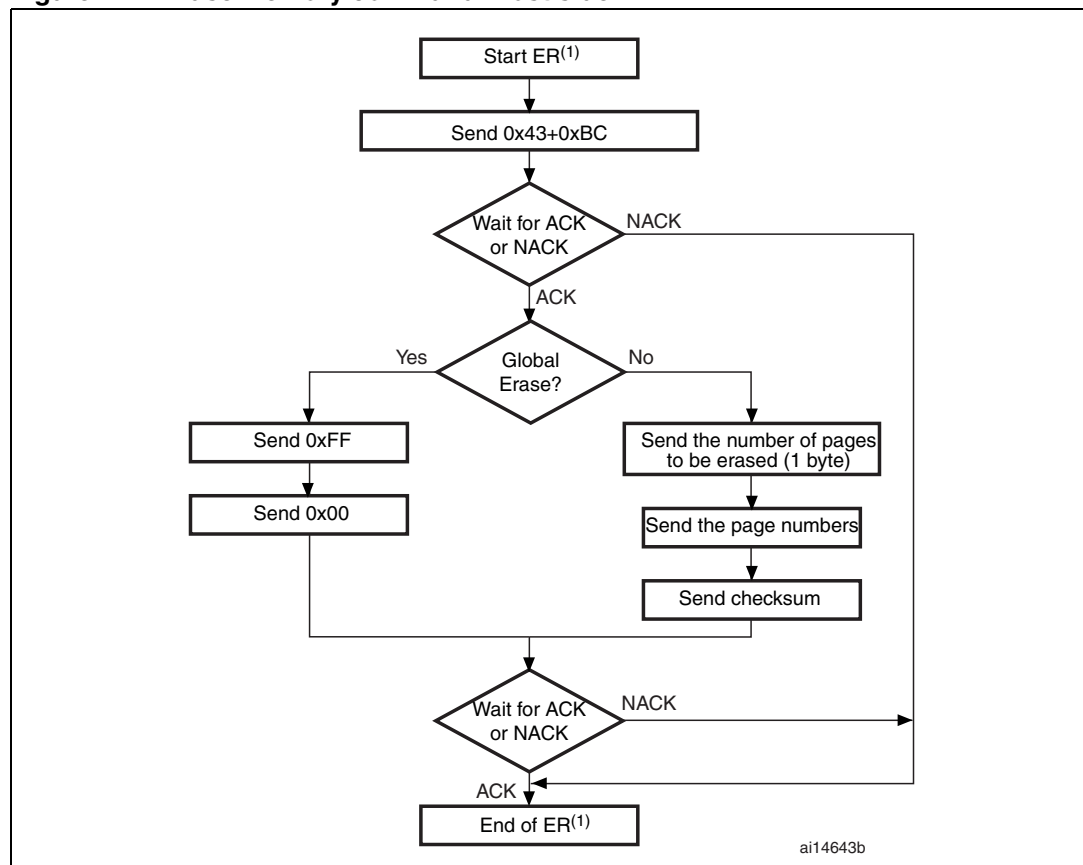
The Erase Memory command allows the host to erase Flash memory pages. When the bootloader receives the Erase Memory command, it transmits the ACK byte to the host. After the transmission of the ACK byte, the bootloader receives one byte (number of pages to be erased), the Flash memory page codes and a checksum byte; if the checksum is correct then bootloader erases the memory and sends an ACK byte to the host, otherwise it sends a NACK byte to the host and the command is aborted.

Erase Memory command specifications:

- the bootloader receives one byte that contains N, the number of pages to be erased – 1.
N = 255 is reserved for global erase requests. For $0 \leq N \leq 254$, N + 1 pages are erased.
- the bootloader receives (N + 1) bytes, each byte containing a page number

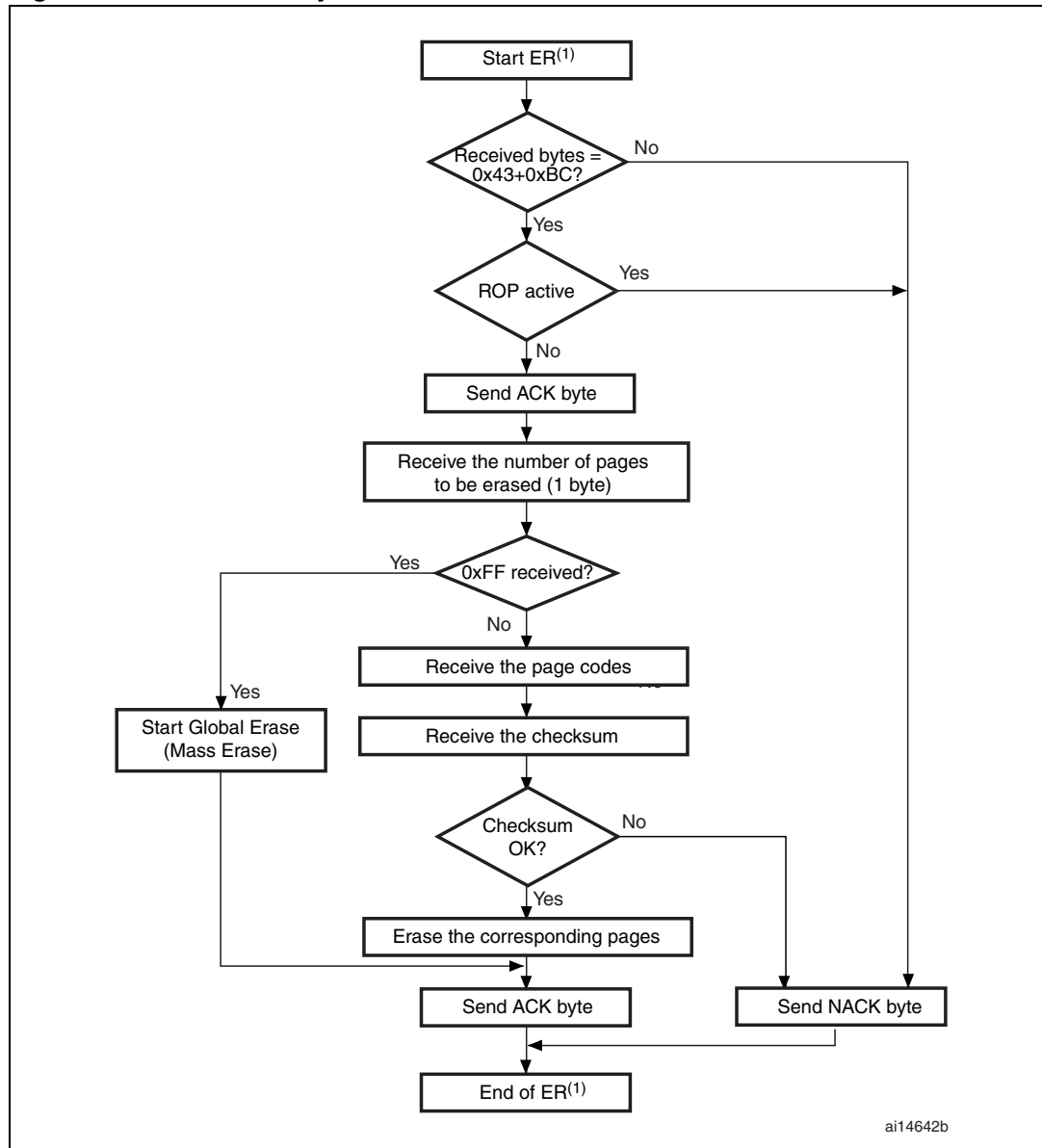
Note: No error is returned when erase operations are performed on write-protected sectors.

Figure 14. Erase Memory command: host side



1. ER = Erase Memory.

Figure 15. Erase Memory command: device side



1. ER = Erase Memory.

Note: After sending the erase memory command and its checksum, if the host sends 0xFF followed by data $\neq 0x00$, the mass erase is not performed but an ACK is send by the device.

The host sends the bytes to the STM32F10xxx as follows:

Byte 1: 0x43

Byte 2: 0xBC

Wait for ACK

Byte 3: 0xFF or number of pages to be erased – 1 ($0 \leq N \leq$ maximum number of pages)

Byte 4: 0x00 (in case of global erase) or (N + 1) bytes (page numbers) and then checksum:
XOR (N, N + 1 bytes)

2.8 Write Protect command

The Write Protect command is used to enable the write protection for some or all Flash memory sectors. When the bootloader receives the Write Protect command, it transmits the ACK byte to the host. After the transmission of the ACK byte, the bootloader waits for the number of bytes to be received (sectors to be protected) and then receives the Flash memory sector codes from the user.

If the write protection was enabled successfully, the bootloader transmits the ACK byte, otherwise it transmits a NACK byte to the user and the command is aborted.

At the end of the Write Protect command, the bootloader generates a system Reset to take into account the new configuration of the option byte.

Note: *On the STM32F10xxx, the sector size is 4 Kbytes (4 pages when the page size is 1 Kbyte and 2 pages when the page is 2 Kbytes) for the Write Protect command.*

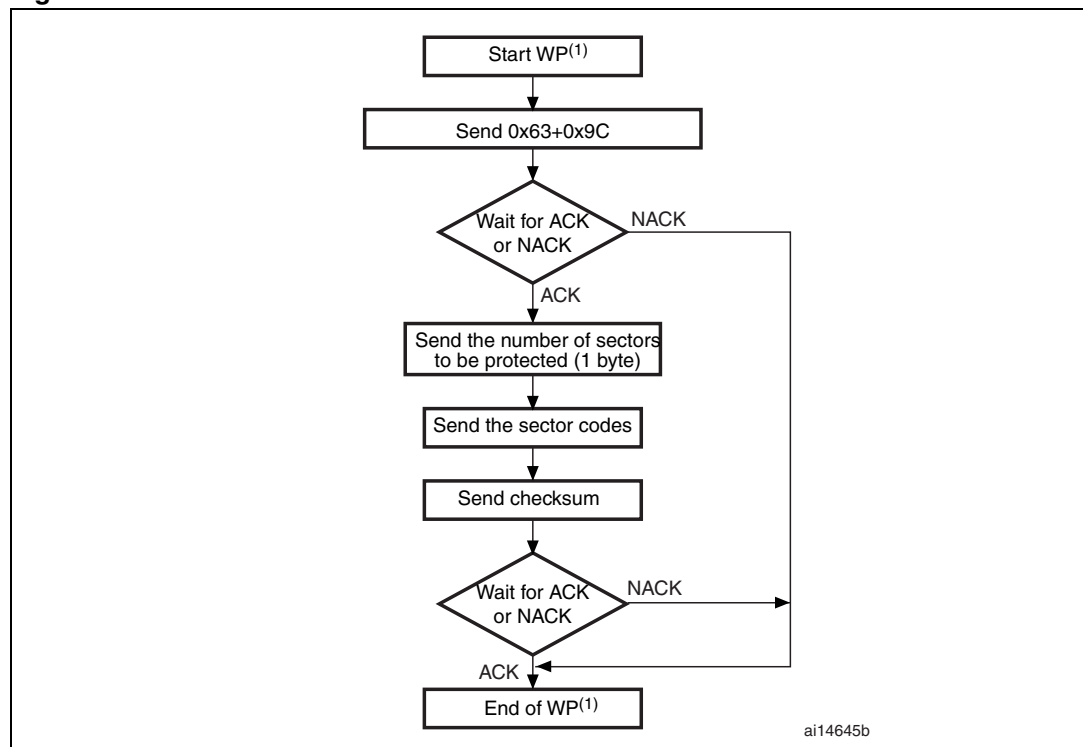
The Write Protect command sequence is as follows:

- the bootloader receives one byte that contains N, the number of sectors to be write-protected – 1 ($0 \leq N \leq 255$)
- the bootloader receives (N + 1) bytes, each byte contains a sector code

Note: *The total number of sectors and the numbers of the sectors to be protected are not checked, this means that no error is returned when a command is passed with a wrong number of sectors to be protected or a wrong sector number.*

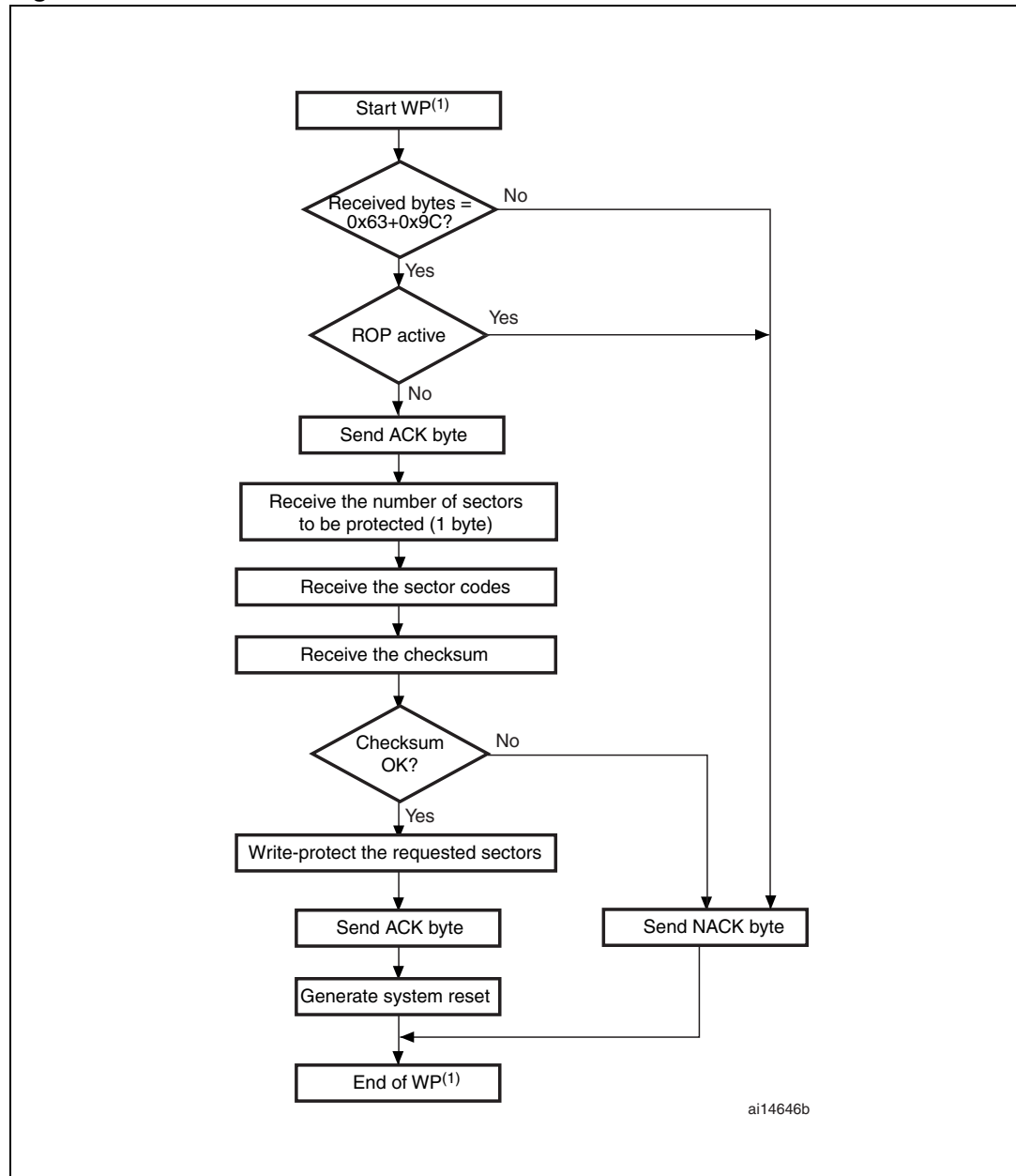
Note: *If a second Write Protect command is executed, the Flash memory sectors that had been protected by the first command become unprotected and only the sectors passed within the second Write Protect command become protected.*

Figure 16. Write Protect command: host side



1. WP = Write Protect.

Figure 17. Write Protect command: device side



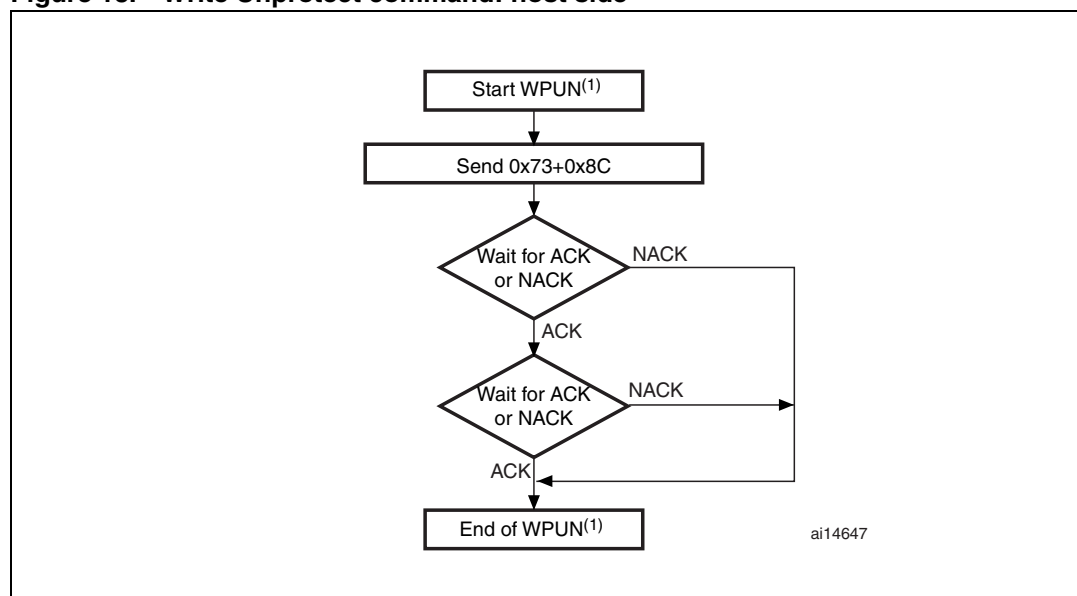
1. WP = Write Protect.

2.9 Write Unprotect command

The Write Unprotect command is used to disable the write protection of all the Flash memory sectors. When the bootloader receives the Write Unprotect command, it transmits the ACK byte to the host. After the transmission of the ACK byte, the bootloader disables the write protection of all the Flash memory sectors. If the unprotection operation was successful the bootloader transmits the ACK byte, otherwise it transmits a NACK byte to the user.

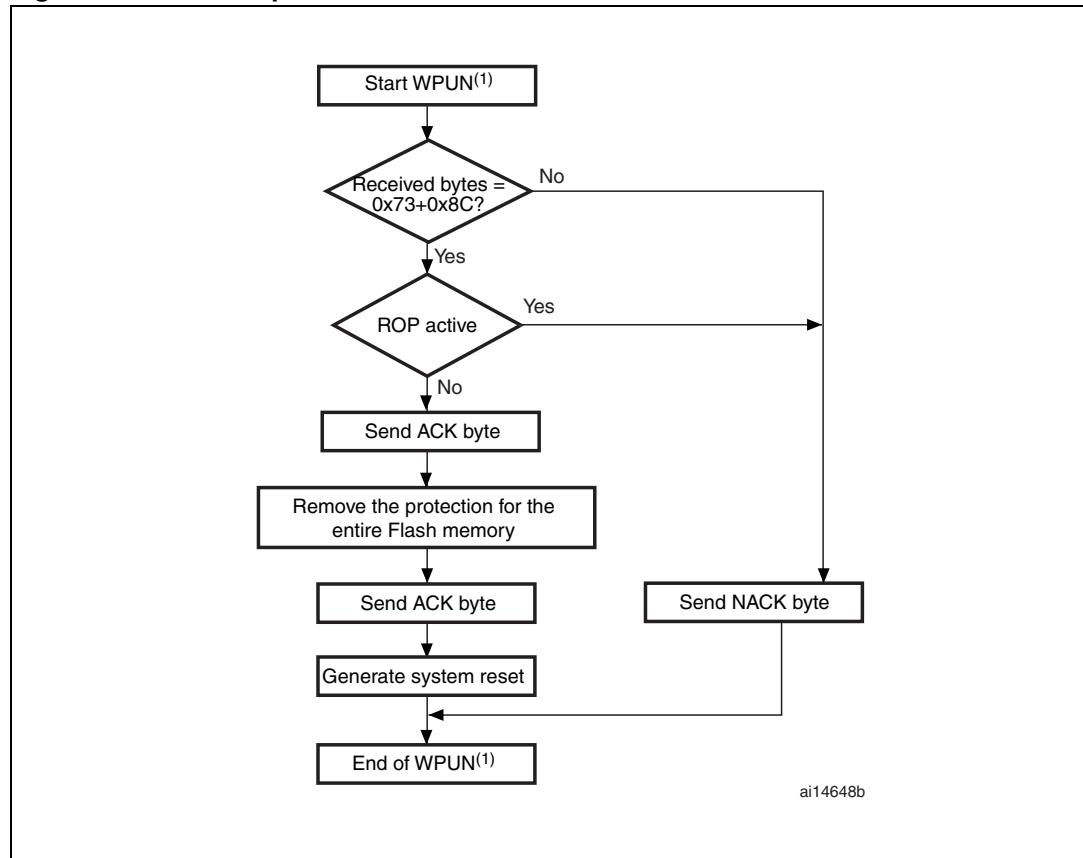
At the end of the Write Unprotect command, the bootloader generate a system Reset to take into account the new configuration of the option byte.

Figure 18. Write Unprotect command: host side



1. WPUN = Write Unprotect.

Figure 19. Write Unprotect command: device side



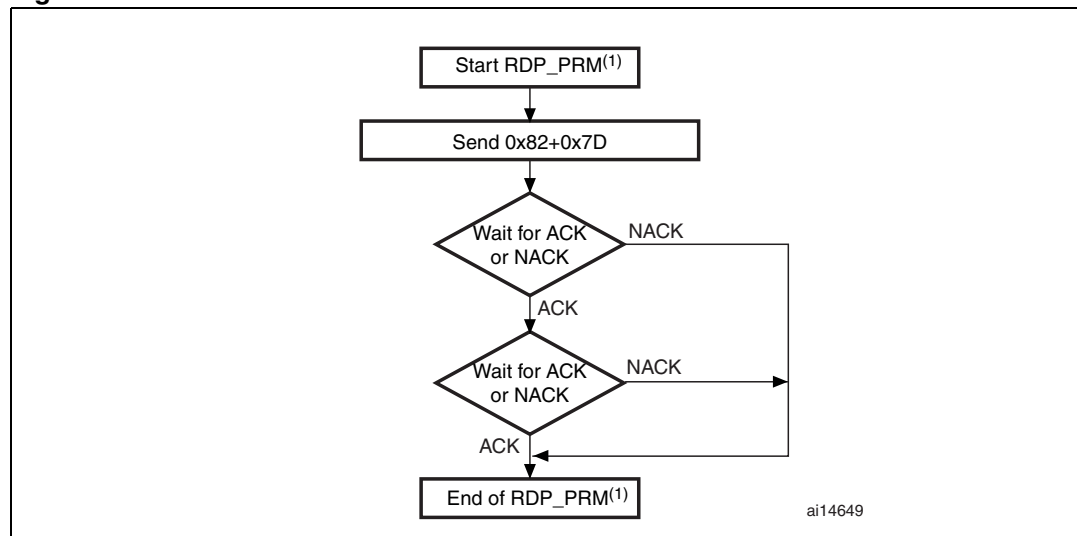
1. WPUN = Write Unprotect.

2.10 Readout Protect command

The Readout Protect command is used to enable the Flash memory read protection. When the bootloader receives the Readout Protect command, it transmits the ACK byte to the host. After the transmission of the ACK byte, the bootloader enables the read protection for the Flash memory. If the protection operation was successful the bootloader transmits the ACK byte, otherwise it transmits a NACK byte to the user.

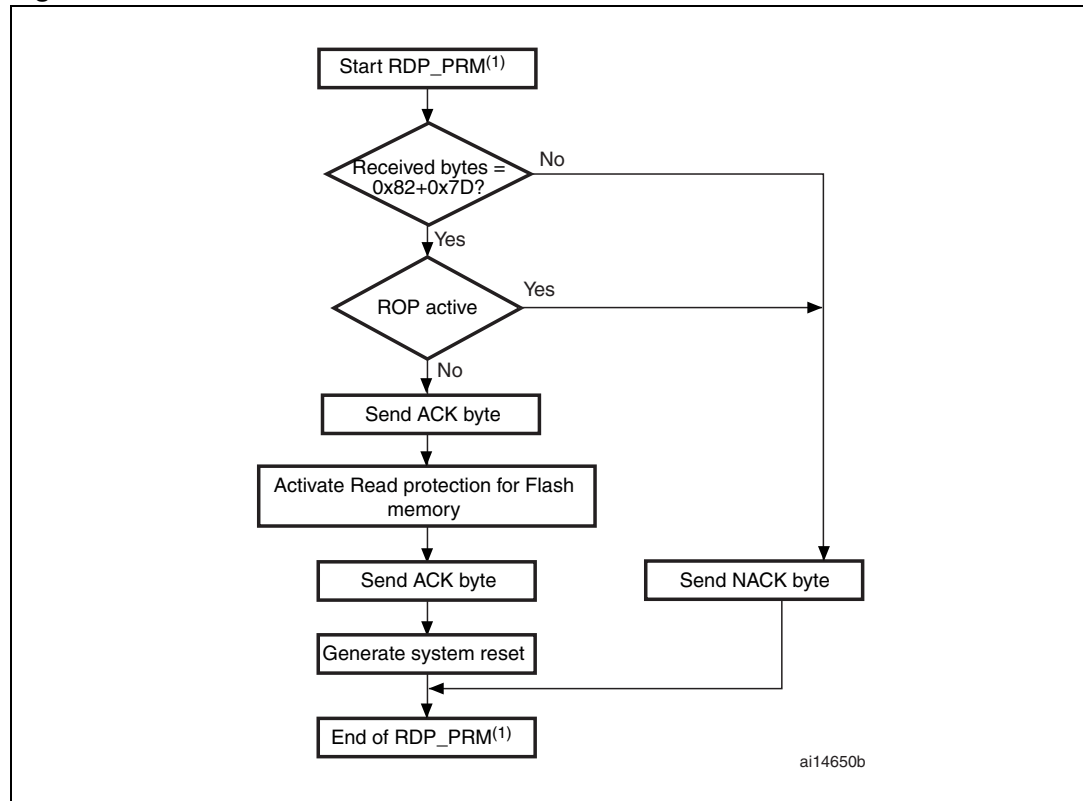
At the end of the Readout Protect command, the bootloader generates a system Reset to take into account the new configuration of the option byte.

Figure 20. Readout Protect command: host side



1. RDP_PRM = Readout Protect.

Figure 21. Readout Protect command: device side



1. RDP_PRIM = Readout Protect.

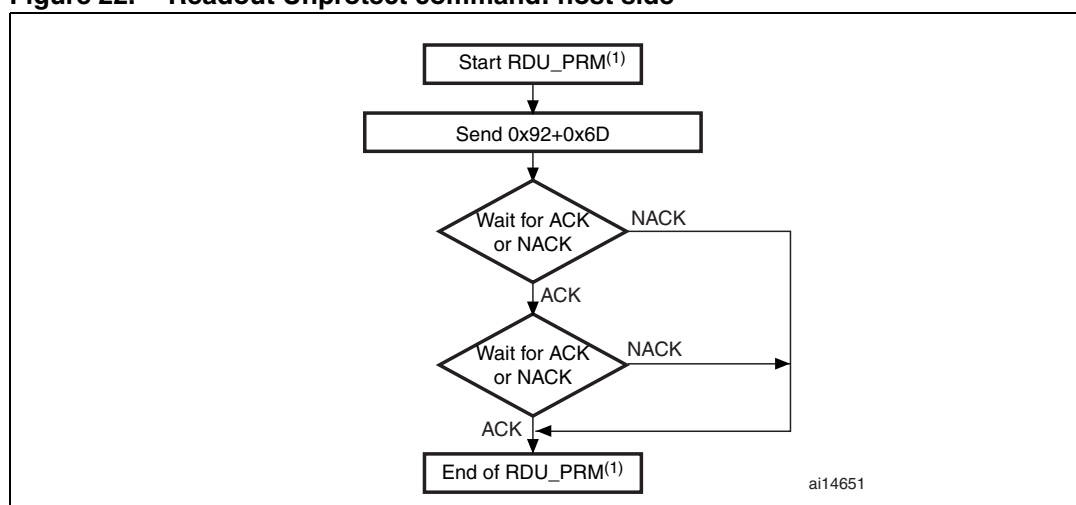
2.11 Readout Unprotect command

The Readout Unprotect command is used to disable the Flash memory read protection. When the bootloader receives the Readout Unprotect command, it transmits the ACK byte to the host. After the transmission of the ACK byte, the bootloader erases all the Flash memory sectors and it disables the read protection for the entire Flash memory. If the erase operation is successful, the bootloader deactivates the RDP. If the RDP deactivation is successful, the bootloader transmits an ACK, otherwise, it transmits a NACK.

If the erase operation is unsuccessful, the bootloader transmits a NACK and the read protection remains active.

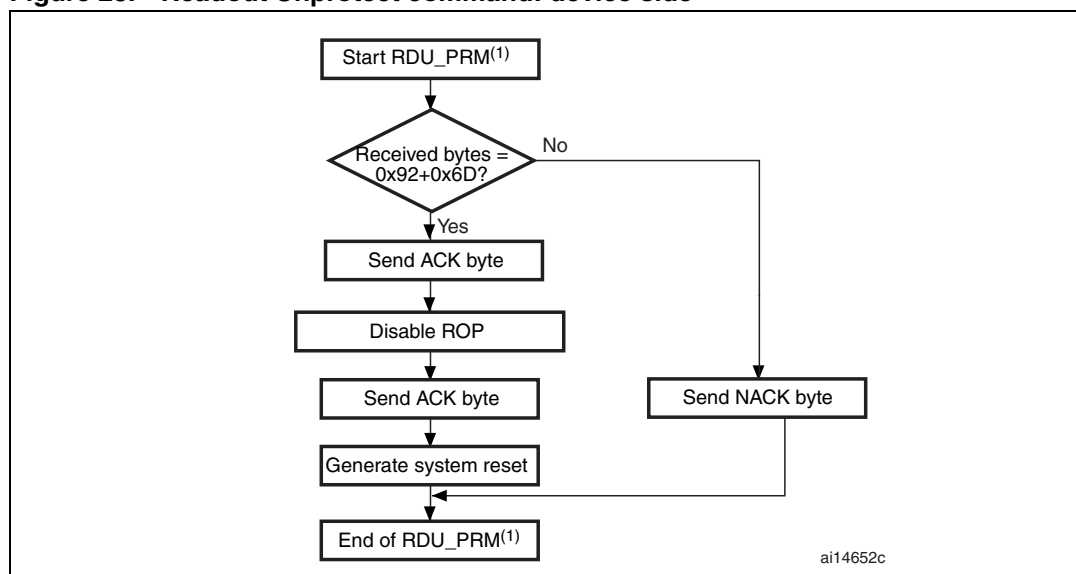
At the end of the Readout Unprotect command, the bootloader generates a system reset to take into account the new configuration of the option byte.

Figure 22. Readout Unprotect command: host side



1. RDU_PRM = Readout Unprotect.

Figure 23. Readout Unprotect command: device side



1. RDU_PRM = Readout Unprotect.

3 Bootloader version evolution

[Table 4](#) lists the bootloader versions.

Table 4. Bootloader versions

Bootloader version number	Description
V2.0	Initial bootloader version.
V2.1	<ul style="list-style-type: none">– Update Go Command to initialize the main stack pointer– Update Go command to return NACK when jump address is in the Option byte area or System memory area– Update Get ID command to return the device ID on two bytes– Update the bootloader version to V2.1
V2.2	<ul style="list-style-type: none">– Update Read Memory, Write Memory and Go commands to deny access with a NACK response to the first 0x200 bytes of RAM memory used by the bootloader– Update Readout Unprotect command to initialize the whole RAM content to 0x0 before ROP disable operation

Revision history

Table 5. Document revision history

Date	Revision	Changes
22-Oct-2007	1	Initial release.
22-Jan-2008	2	<p>All STM32F10xxx in production (rev. B and rev. Z) include the bootloader described in this application note.</p> <p>Modified: Section 1.2: Bootloader activation and Section 1.4: Bootloader code sequence.</p> <p>Added: Section 1.3: Hardware requirements, Section 1.5: Choosing the USART baud rate, Section 1.6: Using the bootloader and Section 1.6: Exiting System memory boot mode.</p> <p>Note 2 linked to Get, Get Version & Read Protection Status and Get ID commands in Table 3: Bootloader commands, Note 3 added.</p> <p>Notion of “permanent” (Permanent Write Unprotect/Readout Protect/Unprotect) removed from document. Small text changes.</p> <p>Bootloader version upgraded to 2.0.</p>
26-May-2008	3	<p>Small text changes. RAM and System memory added to Table 2: STM32F10xxx configuration in System memory boot mode.</p> <p>Section 1.6: Using the bootloader on page 8 removed.</p> <p>Erase modified, Note 3 modified and Note 1 added in Table 3: Bootloader commands on page 9.</p> <p>Byte 3: on page 11 modified.</p> <p>Byte 2: on page 13 modified.</p> <p>Byte 2:; Bytes 3-4: and Byte 5: on page 15 modified, Note 3 modified.</p> <p>Byte 8: on page 18 modified.</p> <p>Notes added to Section 2.5: Go command on page 18.</p> <p>Figure 11: Go command: device side on page 20 modified.</p> <p>Note added in Section 2.6: Write Memory command on page 21.</p> <p>Byte 8: on page 24 modified.</p> <p>Figure 14: Erase Memory command: host side and Figure 15: Erase Memory command: device side modified.</p> <p>Byte 3: on page 26 modified.</p> <p>Table 3: Bootloader commands on page 9.</p> <p>Note modified and note added in Section 2.8: Write Protect command on page 27.</p> <p>Figure 16: Write Protect command: host side, Figure 17: Write Protect command: device side, Figure 19: Write Unprotect command: device side, Figure 21: Readout Protect command: device side and Figure 23: Readout Unprotect command: device side modified.</p>

Table 5. Document revision history (continued)

Date	Revision	Changes
29-Jan-2009	4	This application note also applies to the STM32F102xx microcontrollers. Bootloader version updated to V2.2 (see Table 4: Bootloader versions).
19-Nov-2009	5	IWDG added to Table 2: STM32F10xxx configuration in System memory boot mode . Note 2 added. BL changed bootloader in the entire document. Go command description modified in Table 2: STM32F10xxx configuration in System memory boot mode . Number of bytes awaited by the bootloader corrected in Section 2.4: Read Memory command . Note modified below Figure 10: Go command: host side . Note removed in Section 2.5: Go command and note added. Start RAM address specified and note added in Section 2.6: Write Memory command . All options are erased when a Write Memory command is issued to the Option byte area. Figure 11: Go command: device side modified. Figure 13: Write Memory command: device side modified. Note added and bytes 3 and 4 sent by the host modified in Section 2.7: Erase Memory command . Note added to Section 2.8: Write Protect command .

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST's terms and conditions of sale.

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

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST'S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS EXPRESSLY APPROVED IN WRITING BY AN AUTHORIZED ST REPRESENTATIVE, ST PRODUCTS ARE NOT RECOMMENDED, AUTHORIZED OR WARRANTED FOR USE IN MILITARY, AIR CRAFT, SPACE, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS, NOR IN PRODUCTS OR SYSTEMS WHERE FAILURE OR MALFUNCTION MAY RESULT IN PERSONAL INJURY, DEATH, OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. ST PRODUCTS WHICH ARE NOT SPECIFIED AS "AUTOMOTIVE GRADE" MAY ONLY BE USED IN AUTOMOTIVE APPLICATIONS AT USER'S OWN RISK.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.

Information in this document supersedes and replaces all information previously supplied.

The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

© 2009 STMicroelectronics - All rights reserved

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Philippines - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com

