RH850/U2B Group

R01AN6435EJ0100
Rev.1.00

Code Flash　Application Note

Summary

This application note summaries the internal-flash rewriting program operation example for RH850/U2Bx by user program. As the interface by the user program, the RS-CANFD is used. The internal-flash rewriting program is on the user mat.

Although the task examples and application examples described in this application note have been confirmed to operate, be sure to confirm the operation before using them.

Application

This document is applicable for RH850/U2Bx.

[Note] Self-programing Function Activation

In this application note, enable the following setting on CS+ for rewriting the internal-flash ROM.

(1) Select "*****(Debag Tool)" from the project tree.

(2) Select the Tab of "Setting for Connection".

(3) Set "Yes" to "Perform flash self programing" of "Flash".

Contents

1. Specification

1.1 Entire Specification

- In this application note, perform the user mat rewriting of the internal flash memory (hereinafter referred to ROM) by the user program.
- The operation mode is booted by the normal operation mode. The boot mat is booted by the user mat.
- Use Block 6 (H’00018000) to (H’0001BFFF) as the ROM rewriting area.
- The data used for ROM writing uses the RS-CANFD (ch0), and it is stored to the internal RAM.
- When ROM rewriting target device receives the specification ID and data by using the RS-CANFD from the external device, it performs the corresponded ROM rewriting processes. in this application note, the combinations of these specification IDs and Data are called as “CANFD Command”.
- The start command, write data request command, write data download command, and write end command are used as the CANFD command.
- The internal ROM rewrite program is previously stored to the user mat and transferred to the internal RAM.

Figure 1-1 shows the system configuration diagram.

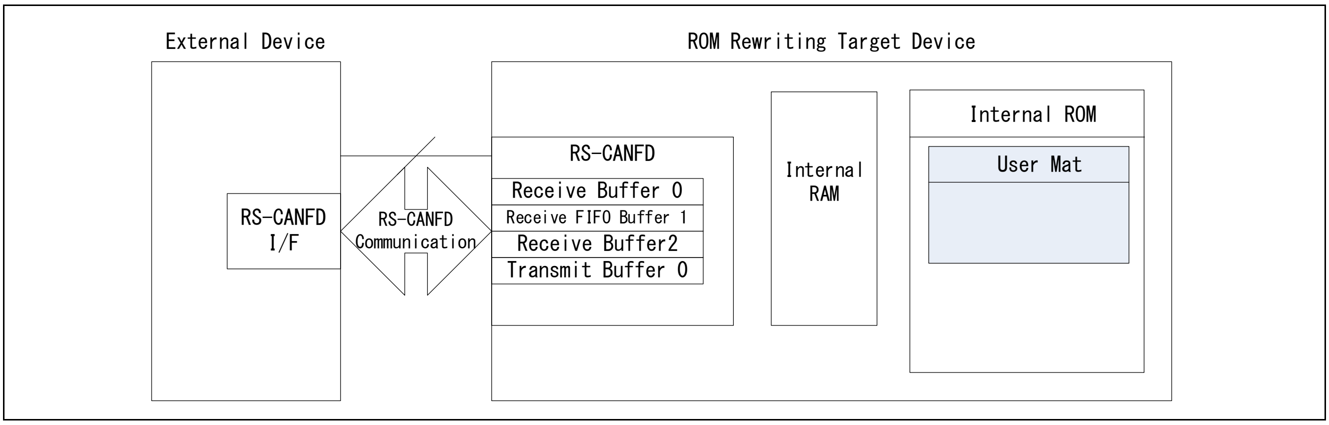


Figure 1-1 System Configuration

1.2 RS-CANFD Communication Specification

- Channel 0 is used.
- Set the normal bit rate 1Mbps and the data bit rate 2Mbps as the communication speed.
- Set the CANFD frame as the communication frame.
- For storing each CAFD Commands (start command, writing data download command, and write end command) that is transmitted from the external device, set “3” to the number of the receive rules for channel 0.
- Set ID (H’100) and the data length (1 byte) to the start command. Set ID (H’101) to the write data request command. Set ID (H’111) and the data length (64 byte) to the write data download command. Set ID (H’131) and the data length (4 byte) to the writing end command.

1.3 CANFD Command Specification

- ROM rewrite processing is started by transmitting the start command from the external device to the ROM rewrite target device.
- ROM rewrite data is requested by transmitting the write data request command from ROM rewrite target device to the external device.
- Write data download command transmits the write data from the external device to ROM rewrite target device.
- Write end command terminates ROM rewriting to transmit the command from the external device to ROM rewrite target device.
- CANFD command transmitted from external device is stored to the receive buffer. Set the register so that the start command is stored to the receive buffer 0 (1 Byte), the write data download command is stored to the receive FIFO buffer 1 (64 Bytes), and the write end command is stored to the receive buffer 2 (4 Bytes).

Figure 1-1 shows the CANFD command specification.

Table 1-1 CANFD Command Specification

Buffer	Channel	Command Name	Transmission/Reception	Standard ID	Data Length	Data
0	1	Start Command	Reception	H’100	1Byte	H’11
0	1	Write Data Request Command	Transmission	H’101	1Byte	H’22
1	1	Write Data Download Command	Reception	H’111	64Byte	Download the ROM write data 512 bytes (64Byte x 8)
2	1	Write End Command	Reception	H’131	4Byte	H’FFFFFFFF

1.4 Entire Sequence

Figure 1-2 to Figure 1-3 shows the entire sequence.

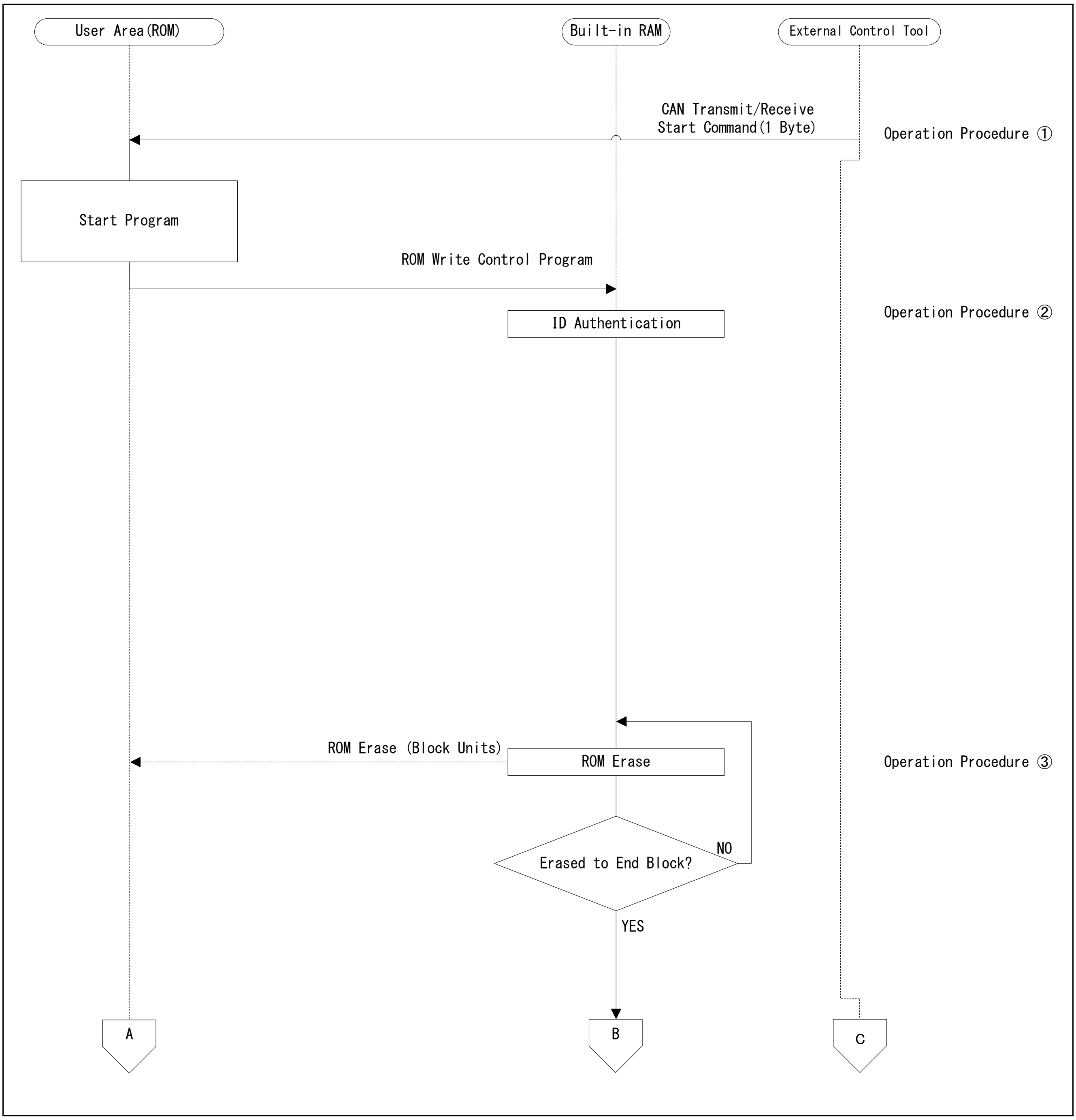


Figure 1-2 Entire Sequence (1)

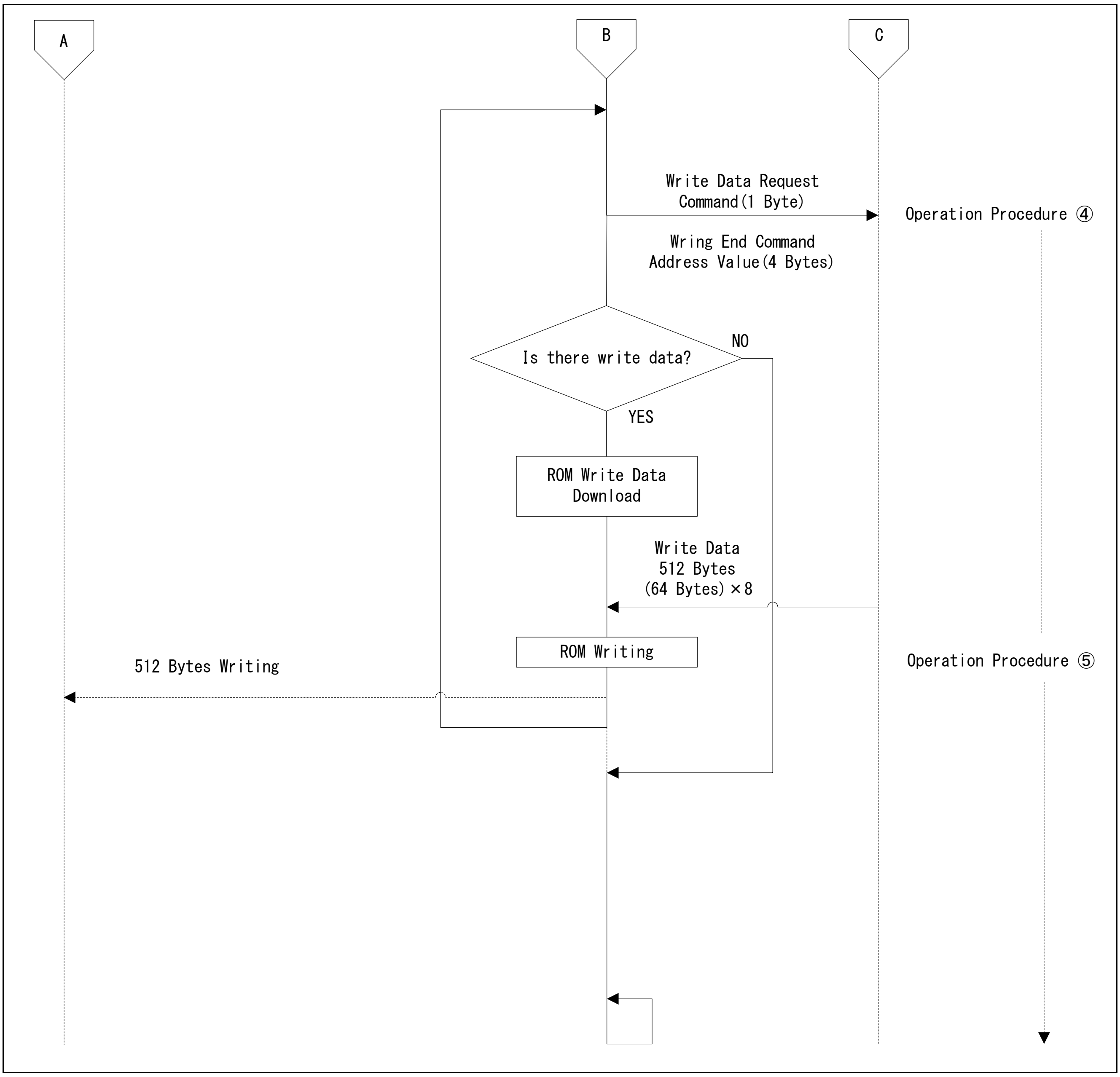


Figure 1-3　Entire Sequence (2)

1.5 Used Functions

- CANFD Interface (RS-CANFD)
- FACI
- Pin

1.6 Operation Mode

In this application note, the microcomputer operation mode in ROM rewriting is performed in the normal operation mode. The normal operation mode can select the boot mat from the user boot mat or the user mat, however, the user mat is used in this application note. The user boot mat is not used.

The operation mode selection method is set in the mode pin. The option byte setting is set by using Renesas Flash Programmer for RH850 families.

Table 1-2 shows the operation mode selection.

Table 1-2 Operation Mode Selection

Pin Setting Value			Option Byte Setting Value		Operation Mode	Boot Mat
FLMD1	FLMD0	TRST	STMSEL1	STMSEL0		
0	0	0	0	0	Normal operation mode	User mat

2. Flash Rewriting

2.1 Flash Memory Related Module

The flash memory erasing/writing can execute the erasing/writing for using the sequencer (flash sequencer) for the flash memory via P-Bus.

The flash sequencer is configured by FCU and FACI. FCU executes the basic control of the flash memory rewriting. FACI controls FCU according to the FACI command received via P-Bus. The products that mount the data flash memory for ICUM are mounted another pair of sequencers. These sequencers individually control the data flash memory for ICUM. When operating the reset transfer, FACI transfers the data from the flash memory to the IDCTRL/option byte storing register. In IDCTRL, the ID transferred to the flash memory and CUSTIDAIN0 to 7 registers in IDCTRL are compared.

Figure 2-1 shows the configuration diagram of the flash memory related module.

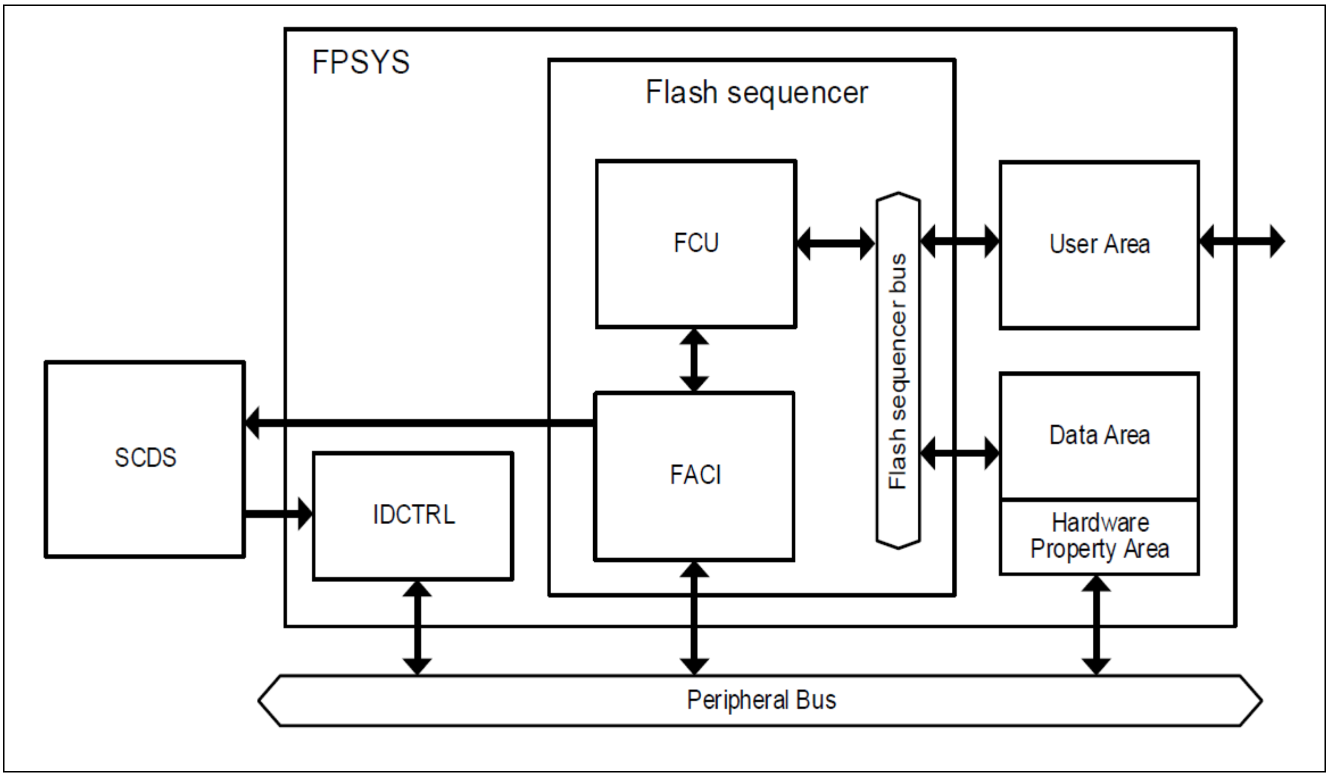


Figure 2-1 Flash Memory Related Module Configuration

2.2 Register Explanation

The following shows the using registers explanations in ROM erasing/writing by the user program.

- Common Use Register in ROM Erase/Write Processing

・ID Authentication Register

CUSTIDAIN Register 0 to 7 (CUSTIDAIN0 to 7)

CUSTIDAIN is for inputting the ID that is used for the authentication of the code flash/configuration setting protection. ID is authenticated by comparing 256 bits ID previously set to the security setting area in flash memory with CUSTIDAIN0 to CUSTIDAINID7 registers values. The ID stored in the security setting area of flash memory can be set by the setting command of the security setting FACI. CUSTIDAIN must be inputted starting with the lowest register number.

Flash P/E Mode Entry Register (FENTRYR_0)

FENTRYR_0 register specifies the programing/erasing mode of the code flash or the data flash. Set either the FENTRYD or FENTRYC bit to 1 to specify the code flash or data flash write/erase mode so that the flash sequencer accepts FACI commands. When setting the register to the values other than 0000H, 0001H, and 0080H, ILGLERR bit in FSTATR_0 register is set, and the flash sequencer will be command lock status. When SUINIT bit is set to 1, FENTRY_0 value is initialized. It is also initialized by resetting.

Flash Access Error Interrupt Enable Register (FAEINT_0)

FAEINT_0 register is for enabling/disabling the flash access error (FLERR) interrupt request occurrence.

FACI Command Processing Start Address Register (FSADDR_0)

FSADDR_0 register specifies and issues the start address in the target area of the command processing when executed the FACI command (programing, multi-programing, DMA programing, block erase, area erase, blank check, or the setting of configuration setting, block protection setting, and security setting). If SUINIT bit in FSUINITR_0 is set to “1”, FSADDR_0 value is initialized. Also, the reset initialize.

- Use Register in Error Processing

Flash Status Register (FSTATR_0)

FSTATR_0 register is for checking the flash sequencer status.

Flash Access Status Register (FASTAT_0)

FASTAT_0 register is for showing the access violation of the Code Flash/Data Flash memory.

Table 2-1 shows ROM erase/write register setting example.

Table 2-1 ROM Erase/Write Register Setting Example

Register Name	Setting Value	Function
CUSTIDAIN register 0 to 7 (RHSIFIDIN0~7)	Write H’0FFFFFFF to CUSTIDAIN0, H’FFFFFFFF to CUSTIDAIN1 to 7 H’0FFFFFFF	Use for inputting ID used for code flash/configuration setting authentication. 31-0 bits : ID for CUSTIDAIN n [31:0] code flash/configuration setting protection authentication
Flash P/E mode entry register (FENTRYR_0)	ROM leading (H’AA00) ROM P/E (H’AA01)	Use for being P/E mode or lead mode. Higher order 8 bits is KEY code : Fixed AA 7 bits: FENTRYD Data Flash P/E Mode Entry 0: Data Flash memory is lead mode. 6 to 1 bit: All reserve bits are ”0”. 0 bit: Code Flash P/E Mode Entry 0: ROM is lead mode. 1: ROM is P/E mode.

Register Name	Setting Value	Function
Flash access interrupt enable register (FAEINT_0)	Error interrupt request disable (H'00)	Set enable/disable of flash access error (FLERR) interrupt request occurrence. 7 bits: CFAEIE Interrupt request is not occurred by 0:CFAE bit = "1". 6 to 5 bits: All reserve bits are "0". 4 bits: CMDLKIE Interrupt request is not occurred by 0:CMDLK bit ="1". 3 bits: DFAEIE Interrupt request is not occurred by 0:DFAE bit = "1". 2 to 1 bit: All reservations are "0". 0 bit: ECRCTIE Interrupt request is not occurred by 0:ECRCT＝"1".
FACI command processing start address register (FSADDR_0)	H'00018000 +H'200 * n (n = 0,1,2,⋯)	FACI command processing start address 31 to 0 bit: FSADDR[31:0]
FHVE15 control register (FHVE15)	Writing/Erasing Enable (H'00000001)	Register for protecting flash write/erase execution. 31 to 1bit: All reservations are "0". 0 bit: FHVE15CNT 0: Write/Erase disable 1: Write/Erase enable
FHVE3 control register (FHVE3)	Writing/Erasing Enable (H'00000001)	Register for protecting flash write/erase execution by software. 31 to 1 bit: All reservations are "0". 0 bit: FHVE3CNT 0: Write/Erase disable 1: Write/Erase enable

Table 2-2 shows the using register in error processing.

Table 2-2 Use Register in Error Processing

Register Name	Function
Flash status register (FSTATR_0)	Register for checking flash sequencer condition. 31-30 bits: All reserve bits are ”0”. 29 bits: ERCDTCT Erase Counter ECC 2 Bit Error Detection Observation Bit 0: 2 bits error is not detected. 1: 2 bits error is detected. 28 bits: ERCCRCT Erase Counter ECC 1 Bit Error Detection Observation Bit 0: 1 bit error is not detected. 1: 1 bit error is detected. 27 bits: SWTDTCT Switch/Tag Area ECC 2 Bits Error Detection Observation Bit 0: 2 bits error is not detected. 1: 2 bits error is detected. 26 bits: SWTCRCT Switch/Tag Area ECC 1 Bit Error Detection Observation Bit 0: 1 bit error is not detected. 1: 1 bit error is detected. 25 bits: SECDTCT Security Setting Area ECC 2 Bits Error Detection Observation Bit 0: 2 bits error is not detected. 1: 2 bits error is detected. 24 bits: SECCRCT Security Setting Area ECC 1 Bit Error Correction Observation Bit 0: 2 bits error is not corrected. 1: 2 bits error is corrected. 23 bits: ILGCOMERR Illegal Command Error When flash sequencer is command lock status, this bit will be “1”. [Setting Condition] When error detected. [Clear Condition] Completed status clear or forced stoppage command processing. 22 bits: FESETERR FENTRY Setting Error When flash sequencer is command lock status, this bit will be “1”. [Setting Condition] When error detected. [Clear Condition] Completed status clear or forced stoppage command processing. 21 bits: SECERR Security Error When flash sequencer is command lock status, this bit will be “1”. [Setting Condition] When error detected. [Clear Condition] Completed status clear or forced stoppage command processing. 20 bits: OTERR Other Errors When flash sequencer is command lock status, this bit will be “1”.

Register Name	Function
	[Setting Condition] When error detected. [Clear Condition] Completed status clear or forced stoppage command processing. 19 bits: Reserve Bit 18 bits: EBFULL FDMYECC Buffer Full 0: ECC buffer is empty. 1: ECC buffer is full. 17 bits: BPLDTCT Block Protection Area 2 Bits Error Detection Monitor (OTP Setting) 0: 2 bits error is not detected. 1: 2 bits error is detected. 16 bits: BPLCRCT Block Protection Area 1 Bit Error Correction Monitor (OTP Setting) 0: 1 bit error correction is not occurred. 1: 1 bit error correction is occurred. 15 bits: FRDY Flash Ready Bit 0: In command processing of program, DMA program, block erase, P/E suspend, P/E resume, forced end, blank check, configuration setting, block protection setting, and security setting. 1: Above processing is not executed. 14 bits: ILGLERR Illegal Command Error Bit 0: Flash sequencer does not detect illegal FACI command and illegal flash memory access. 1:Flash sequencer detects illegal FACI command and illegal flash memory access. 13 bits: ERSERR Erase Error Bit 0: Erase processing is normally end. 1: Error is occurred in erase processing 12 bits: PRGERR Write Error Bit 0: Write processing is normally end. 1: Error is occurred in write processing 11 bits: SUSRDY Suspend Ready Bit 0: Disable P/E suspend command acceptance 1: Enable P/E suspend command acceptance 10 bits: DBFULL Data Buffer Full 0: Data buffer is empty. 1: Data buffer is full. 9 bits: ERSSPD Erase Suspend Status Bit 0: Status other than the following 1: In erase suspend processing or erase suspending 8 bits: PRGSPD Write Suspend Status Bit 0: State other than the following 1: In write suspend processing or write suspending

Register Name	Function
	7 bits: Reserve bit 6 bits: FHVEERR Flash Write Erase Protect Error 0: Error is not occurred. 1: Error is occurred. 5 bits: CFGDTCT 2 Bits Error Detection Monitor 0: 2 bits error is not detected. 1: 2 bits error is detected. 4 bits: CFGCRCT 1 Bits Error Correction Monitor 0: 1 bit error is not detected. 1: 1 bit error is detected. 3 bits: TBLDTCT 2 Bits Error Detection Monitor 0: 2 bits error is not detected. 1: 2 bits error is detected. 2 bits: TBLCRCT 1 Bits Error Correction Monitor 0: 1 bit error is not detected. 1: 1 bit error is detected. 1 to 0 bit: Reserve bit
Flash Access Data Register (FASTAT_0)	Register for showing the access illegal existence of Code Flash memory/Data Flash memory. 7 bits: CFAE Code Flash Memory Access violation Bit 0: No access violation 1: Access violation 6 to 5 bits: All reserve bits are ”0”. 4 bits: CMDLK Command Lock Bits 0: Flash sequencer is not command lock status. 1:Flash sequencer is command lock status. 3 bits: Data Flash Access Error Indicates whether the data flash access error has occurred. When this bit is 1, ILGLERR bits of FSTATR_n is set to 1, and flash sequencer is became command lock status. 0: Data flash access error is not occurred. 1: Data flash access error is occurred. [Setting Condition] Command is issued as following setting in data flash programing/erase mode. (1) If FACI command is issued to invert the data area or data area of another FACI. In FACI0, 20 to 0 of FSADDR_0 register are: 03 0000H to 1F FFFFH (Data flash 192KB + 32KB * 2) 01 0000H to 1F FFFFH (Date flash 64KB + 32KB * 2) (In FACI1 data area (ICUM) or opposite data area) In FACI1, 20 to 0 of FSADDR_1 register are 00 0000H to 02 FFFFH or 03 8000H to 1F FFFFH (Data flash192KB + 32KB * 2) 00 0000H～00 FFFFH or 01 8000H～1F FFFFH (Date flash 64KB + 32KB * 2) (In FACI0 data area or opposite data area)

Register Name	Function
	(2) When the configuration setting command is issued outside the configuration setting area. In FACI0, 20 to 0 of FSADDR_0 register are: 00 0000H to 12 003FH or 12 0100H to 1F FFFFH. In FACI1, 20 to 0 of FSADDR_1 register are: 00 0000H～FF FFFFH (All possible values) (3) When the setting command of the block protection setting is issued outside the block protection area. In FACI0, 20 to 0 of FSADDR_0 register are: 00 0000H to 12 203FH or 12 2100H to 1F FFFFH. In FACI1, 20 to 0 of FSADDR_1 register are: 00 0000H to FF FFFFH (All possible values) (4) When the setting command of the security setting is issued outside the security setting area. In FACI0, 20 to 0 of FSADDR_0 register are: 00 0000H to 10 003FH or 10 0200H to 1F FFFFH。 In FACI1, 20 to 0 of FSADDR_1 register are: 00 0000H to FF FFFFH (All possible values) [Clear Condition] (1) After reading 1 form this bit, 0 is written. (2) Completed status clear or forced suspend command processing. 2 to 1 bits: All reserve bits are ”0”. 0 bit: Error Correction Shows that a 1-bit error was corrected when the flash sequencer read the flash memory(configuration setting area, block protect area, security setting area, overwrite parameter/table, and OTP setting). 0: 1 bit error is not corrected. 1: 1 bit error is corrected. [Clear Condition] When SECCRCT, BPLCRCT, and CFGCRCT bit in FSTATR_n is 1 or TBLCRCT in FSTATR_n is 1, flash sequencer starts status clear or forced suspend command processing.
ID 認証ステータスレジスタ (IDST)	Register for ID authentication result. 31 to 7 bits: All reserve bits are ”0”. 6 bits: CUSTIDRC　Customer ID C Authentication Status 0: ID match (Security release status) 1: No ID match (Security lock status) 5 bits: CUSTIDRB　Customer ID B Authentication Status 0: ID match (Security release status) 1: No ID match (Security lock status) 4 bits: CUSTIDRA　Customer ID A Authentication Status 0: ID match (Security release status) 1: No ID match (Security lock status) 3 bits: CTESTIDR　C-TEST ID Authentication Status 0: ID match (Security release status) 1: No ID match (Security lock status) 2 bits: OCDIDR　OCD ID Authentication Status 0: ID match (Security release status)

Register Name	Function
	1: No ID match (Security lock status) 1 bits: DFIDR Data-Flash ID Authentication Status 0: ID match (Security release status) 1: No ID match (Security lock status)0 bits: SPIDR Serial-Programming ID Authentication Status 0: ID match (Security release status) 1: No ID match (Security lock status)

2.3 ROM Erasing/Writing by User Program

Use FCU farmwear built-in microcomputer for ROM erasing/writing by user program. FCU farmwear executes the processing corresponding to the command by issuing FACI command to FCU farmwear. ROM erasing/writing is executed on internal RAM.

The following shows the software processing required for executing ROM erasing/writing. Table 2-3 shows FACI command for erasing, and Table 2-4 shows FACI command for writing.

(1) Jump to ROM rewrite control program copied to RAM.

(2) Program for controlling FCU farmwear. FCU is possible to use to release security lock by ID authentication.

(Hereafter, both programs are written as ROM rewrite control program.)

Table 2-3 FACI Command for Erasing

Command	Bus Cycles	1st Cycle		2nd Cycle	
		Address	Data	Address	Data
Block erase	2	H’FFA20000	H’20	H’FFA20000	H’D0

Table 2-4 FACI Command for Writing

Command	Bus Cycles	1st Cycle		2nd Cycle	
		Address	Data	Address	Data
Program	131	H’FFA20000	H’E8	H’FFA20000	H’80

3rd Cycle		4th to 130th cycle		131th Cycle	
Address	Data	Address	Data	Address	Data
H’FFA20000	ROM write data (1st word)	H’FFA20000	ROM write data (2nd to 128th word)	H’FFA20000	H’D0

2.4 ROM Erasing

ROM erasing executes the erasing in block units specified in the memory map. For ROM erasing, by writing the erasing FACI command to the FACI command issuing area, CPU issues the FACI command for ROM erasing to FCU, and FCU erases the erase target block.

Figure 2-2 shows code flash memory map.

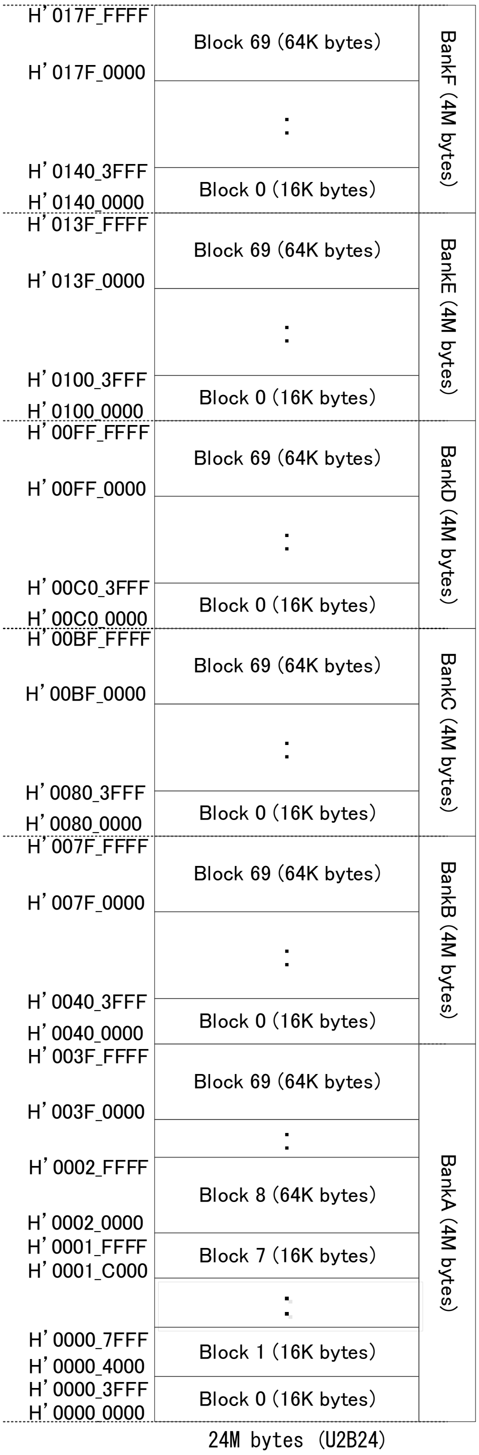


Figure 2-2 Code Flash Memory Map (Single Map Mode, User Area)

- ROM Erasing Procedure

(1) Set the leading address of erase block to FSADDR_0 register. Set FENTRYR_0 corresponding to the erase target (Code Flash/Data Flash).

(2) Write FACI command [H'20] to the FACI command issuing area.

(3) Write FACI command [H'D0] to the FACI command issuing area. (Erase processing start)

(4) Erasing completion can be checked by FRDY bit in FSTATR_0. (If the erasing time is long[*2.1], it is regarded as the error and the forced end command is issued.)

(5) After completing the erasing, check CMDLK bit in FASTAT_0.

[Note] *2.1 For the timeout decision time of (4) , refer to "RH850/U2Bx Flash Memory User's Manual: Hardware Interface".

Figure 2-3 shows ROM Erase Flowchart.

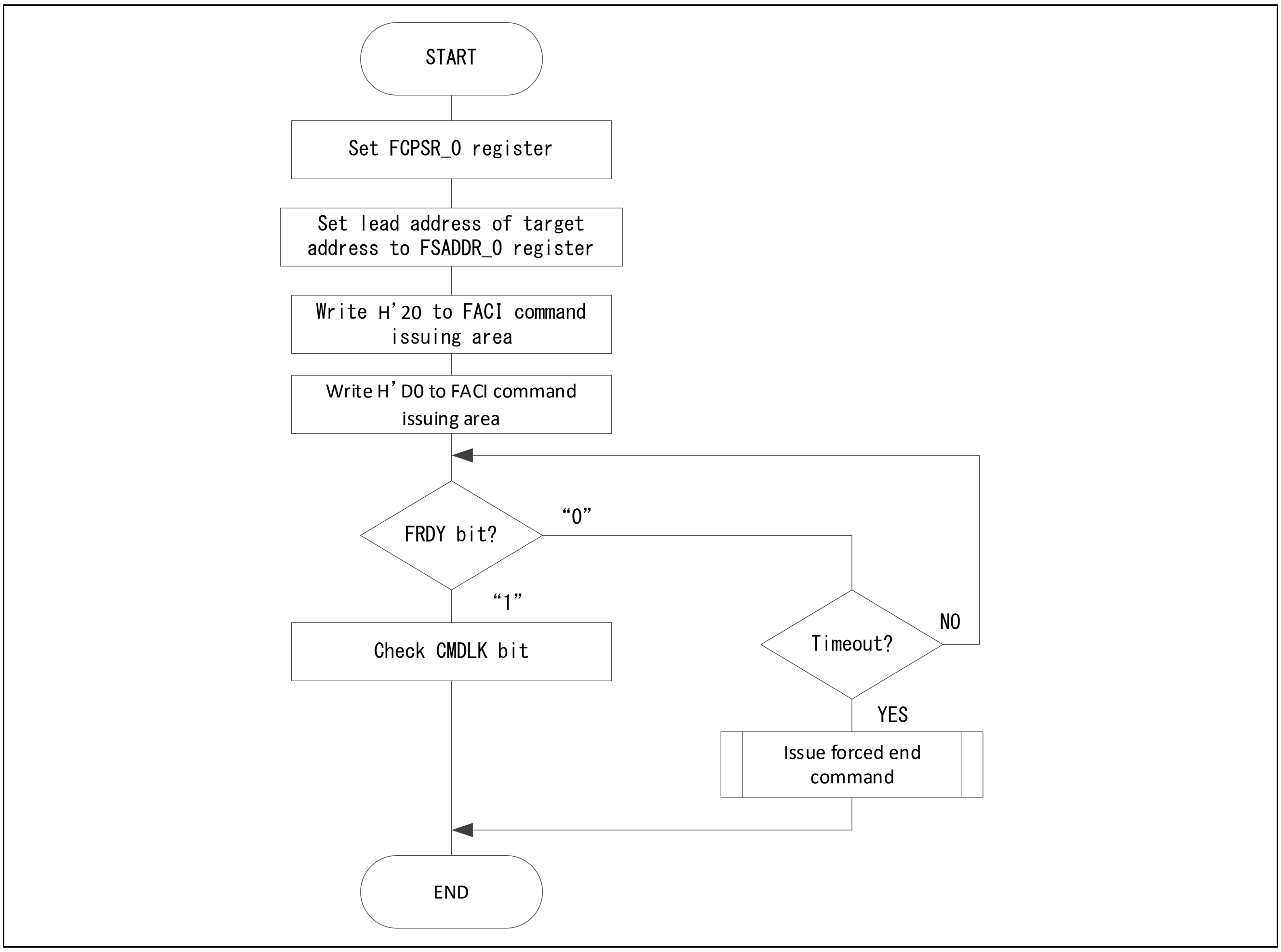

START
Set FCPSR_0 register
Set lead address of target address to FSADDR_0 register
Write H'20 to FACI command issuing area
Write H' D0 to FACI command issuing area
FRDY bit?
"0"
"1"
Check CMDLK bit
Timeout?
NO
YES
Issue forced end command
END

Figure 2-3 ROM Erase Flowchart

2.5 ROM Writing

In ROM writing, by writing FACI command for writing to FACI command area, CPU issues FACI command for FACI command to FCU, and FACI writes in 512 bytes form the specified write destination address.

● ROM Writing Procedure

(1) Specify a head address of the write destination to FSADDR_0 register. Set FENTRYR_0.

(2) Write FACI command [H’E8] to FACI command issuing area.

(3) Write FACI command [H’80] (Code Flash memory writing) to FACI command issuing area.

(4) Write ROM write data in 32 bits size to FACI command issuing area.

(5) Write the write data for 512 bytes to ROM write data.

(6) Write FACI command [H’D0] to FACI command issuing area. (write processing start)

(7) Write completion can be checked by FRDY bit in FSTATR_0. (If the writing time is long[*2.2], it is regarded as the error and the forced end command is issued.)

(8) After completing the writing, check CMDLK bit in FASTAT_0.

[Note] *2.2 For the timeout decision time of (7) processing, refer to “RH850/U2Bx Flash Memory User’s Manual: Hardware Interface”.

Figure 2-4 shows ROM writing flowchart.

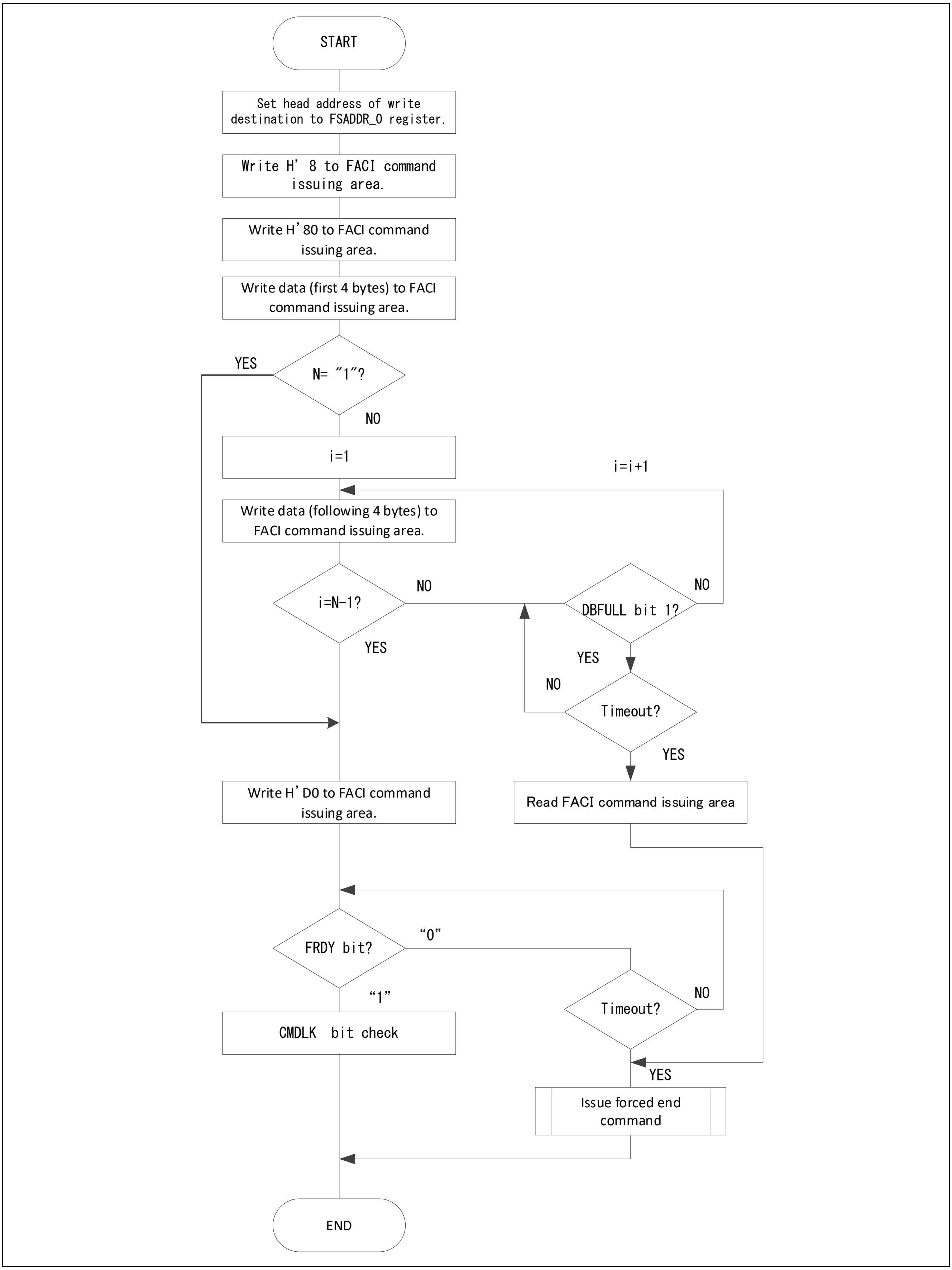

START
Set head address of write destination to FSADDR_0 register.
Write H’ 8 to FACI command issuing area.
Write H’80 to FACI command issuing area.
Write data (first 4 bytes) to FACI command issuing area.
N= ″1″?
YES
NO
i=1
i=i+1
Write data (following 4 bytes) to FACI command issuing area.
i=N-1?
NO
YES
DBFULL bit 1?
NO
YES
Timeout?
NO
YES
Read FACI command issuing area
Write H’D0 to FACI command issuing area.
FRDY bit?
“0”
“1”
CMDLK bit check
Timeout?
NO
YES
Issue forced end command
END

Figure 2-4 ROM Write Flowchart

3. ROM Erasing/Writing using External Device

3.1 Operation Procedure

Operation procedure① to ⑤ are corresponded to “1.4 Entire Sequence”.

3.1.1 ① User Area/RAM Transfer (ROM/RAM Transfer)

After starting the reset, “Write Control Program (ROM)” stored to the user area is transferred[*3.1] to RAM. Subsequent processing is executed on RAM.

Figure 3-1 shows ROM erase/write start operation.

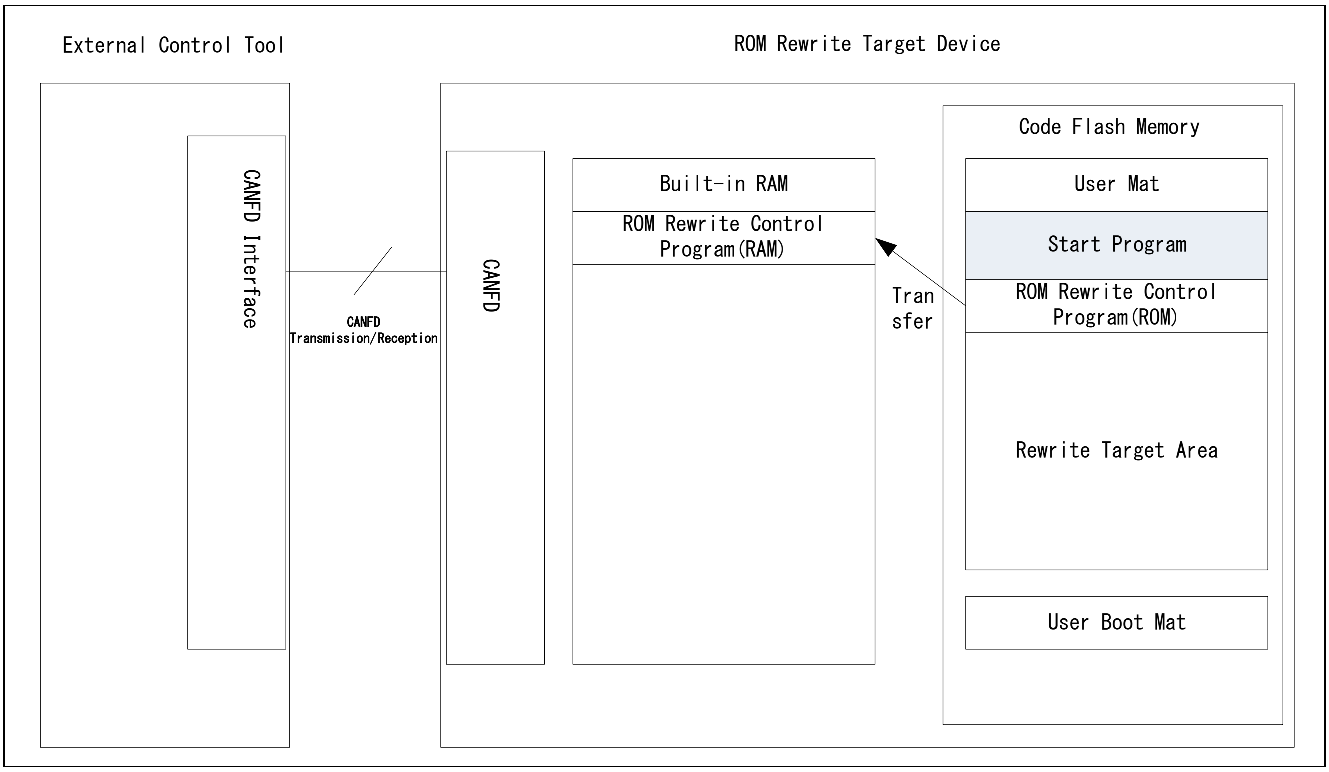


Figure 3-1 ROM Erase/Write Start Operation

[Note] *3.1 Program is transferred to RAM from ROM (User Mat).

Function Explanation

Table 3-1 “main() Function”

Function Name	Overview
main()	Program starting. After receiving start command, “Built-in RAM/ROM Rewrite Control Program” is executed.

Figure 3-2 shows the flowchart of “main() Function”.

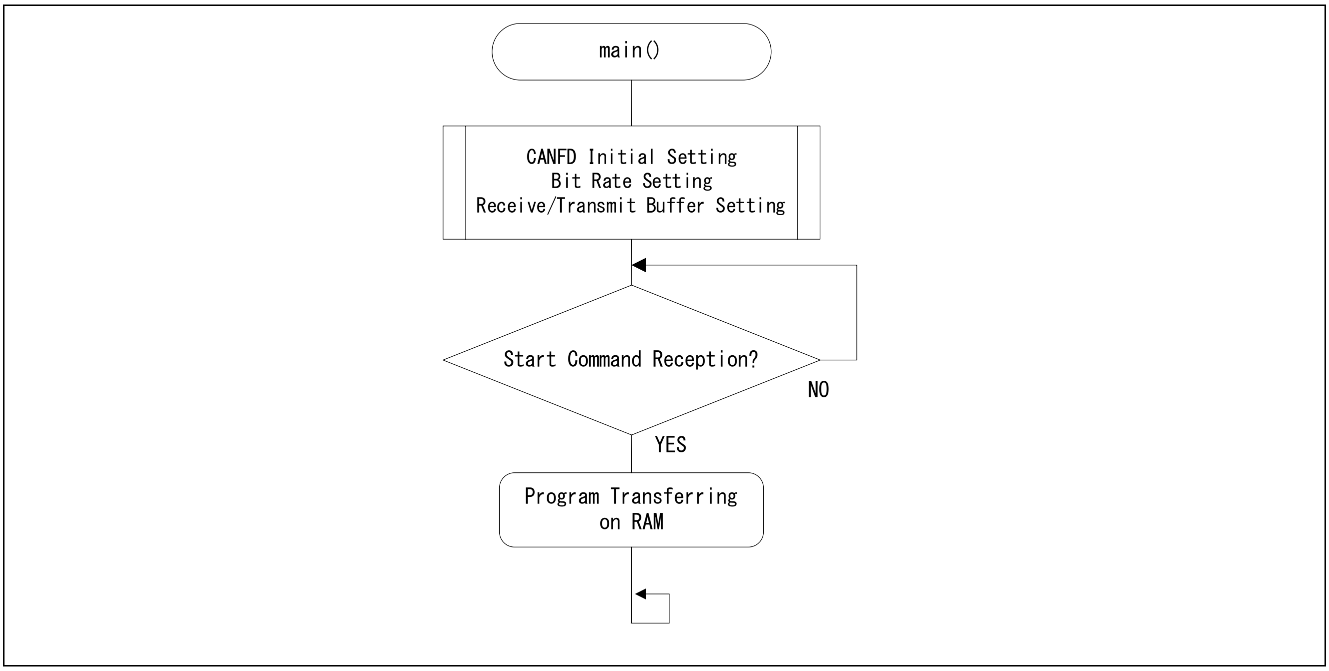


Figure 3-2 “main() Function” Flowchart

“Operation Procedure ①”

3.1.2 ② ID Authentication

Execute “ID Authentication Function” in “ROM Rewrite Control Program (RAM)”. ID authentication is executed by comparing 256 bits ID previously set to specialized area in flash memory with RHSIFIDIN0 to 7 values.

In this application note, ID setting is “0” for first byte, “ F” for other bytes. When changing ID setting, Renesas Flash Programmer for RH850 family or the configuration setting command.

Function Name

Table 3-2 “FCU_ID() Function”

Function Name	Overview
FCU_ID()	Execute comparison with ID set to specialized area in flash memory and ID authentication.

Figure 3-3 shows the flowchart of “FCU_ID() Function”.

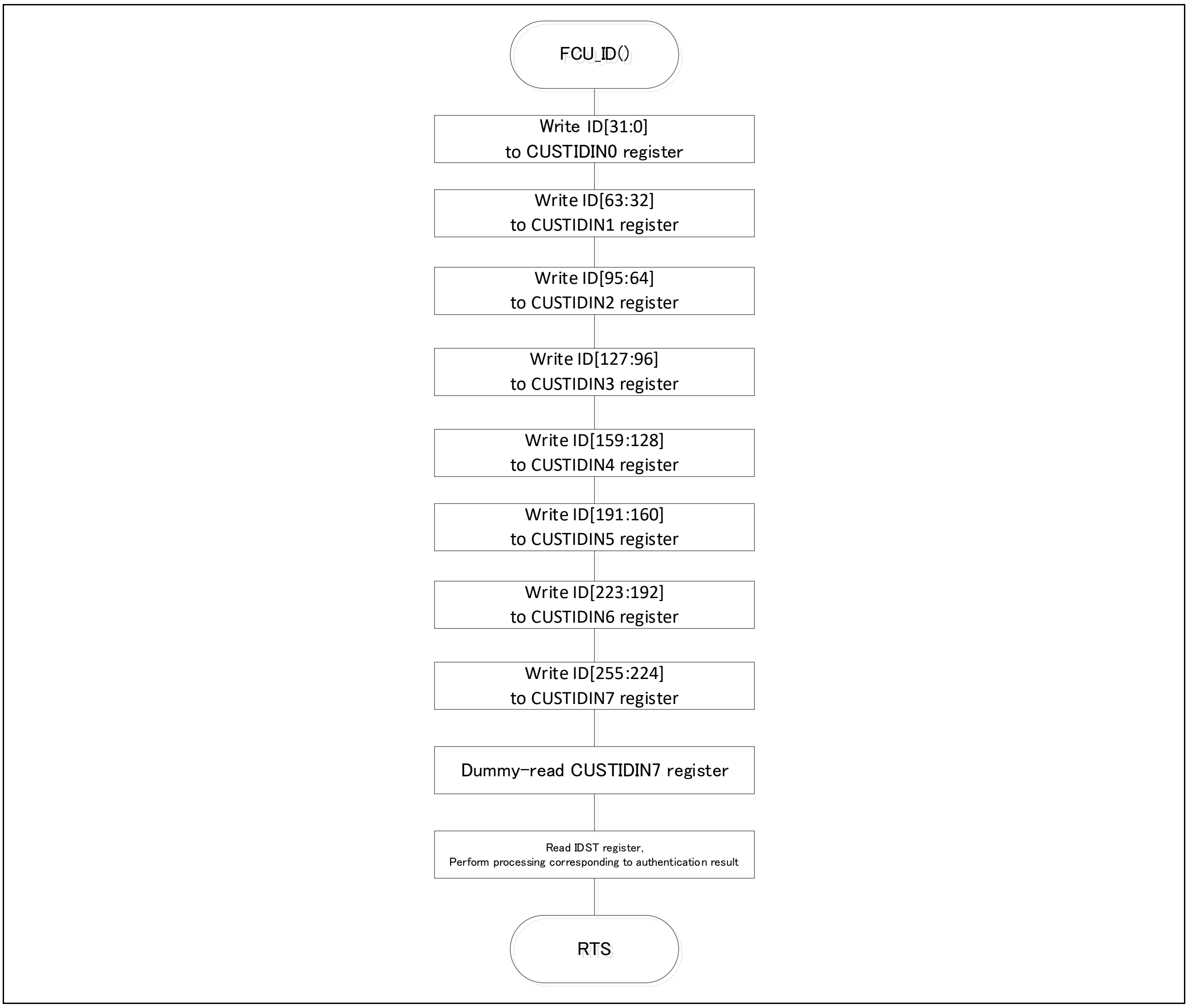


Figure 3-3 “FCU_ID() Function” Flowchart

“Operation Procedure ②”

3.1.3 ③ ROM Erasing

After ID authentication, execute “ROM Erase Function” in “ROM Rewrite Control Program (RAM)”.

Issue the block erase command to FACI command issuing area, and erase ROM rewrite specified area.

Function Explanation

Table 3-3 “ROM_ERASE() Function”

Function Name	Overview
ROM_ERASE()	Erase ROM rewrite specified area.

Figure 3-4 shows the flowchart of “ROM_ERASE() Function”

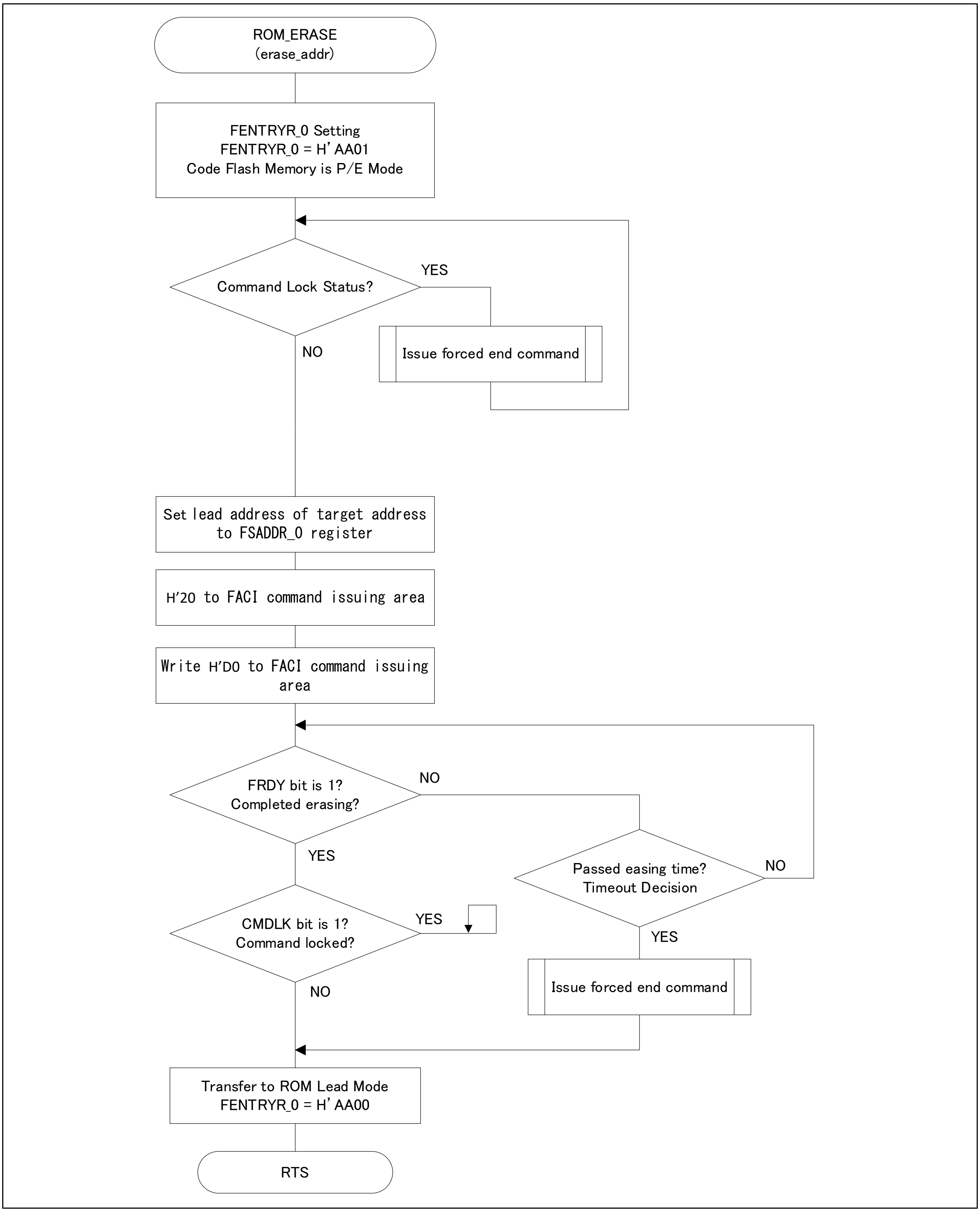


Figure 3-4 “ROM_ERASE() Function” Flowchart

“Operation Procedure ③”

3.1.4 ④ ROM Write Data Download

After completing the ROM erasing, transmit the write data request command to the external device, execute "ROM Write Data Download Function" in "ROM Rewrite Control Program (RAM)". The external device received the write data request transmits the write data 512 bytes to the microcomputer by the write data download command. In "ROM Write Data Download Function", the received write data is stored to RAM.

If the writing end command is received, the write data request command transmission and "ROM Write Data Download Function" execution are not performed, and the flash rewrite is end.

Function Explanation

Table 3-4 "ROM_WE_DL() Function"

Function Name	Overview
ROM_WE_DL()	Download write data from external device.

Figure 3-5 shows the flowchart of "ROM_WE_DL() Function".

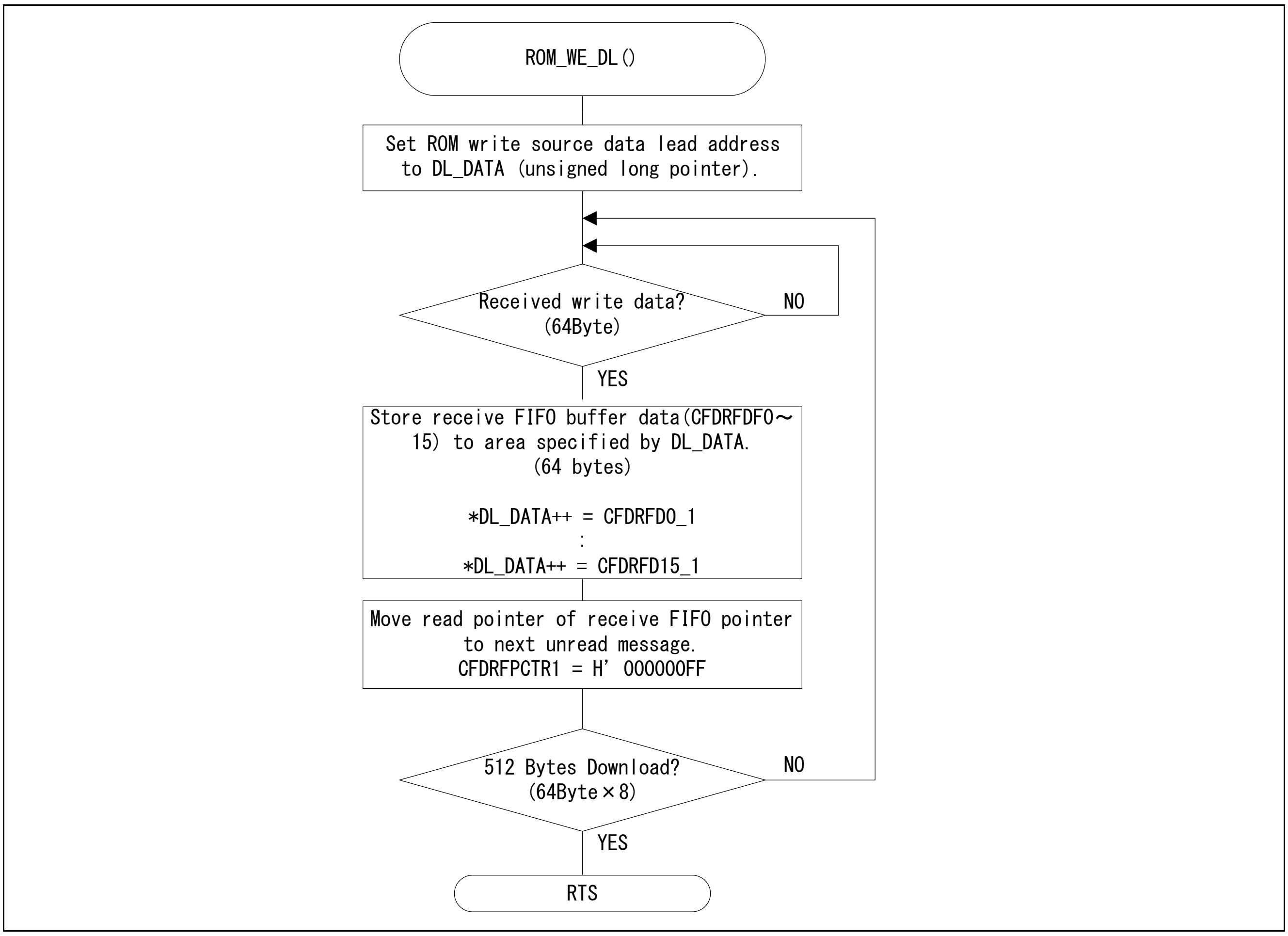

ROM_WE_DL()
Set ROM write source data lead address to DL_DATA (unsigned long pointer).
Received write data? (64Byte)
NO
YES
Store receive FIFO buffer data(CFDRFDF0～15) to area specified by DL_DATA. (64 bytes)
*DL_DATA++ = CFDRFD0_1
:
*DL_DATA++ = CFDRFD15_1
Move read pointer of receive FIFO pointer to next unread message.
CFDRFPCTR1 = H' 000000FF
512 Bytes Download? (64Byte×8)
NO
YES
RTS

Figure 3-5 "ROM_WE_DL() Function" Flowchart

"Operation Procedure ④"

3.1.5 ⑤ ROM Writing

Write the write data that received from the external device in the CAN communication to ROM by using “ROM Write Function” in “ROM Rewrite Control Program (RAM)”

Issue the program command to FACI command issuing area, and write to the ROM rewrite specification area.

Function Explanation

Table 3-5 “ROM_WRITE() Function”

Function Name	Overview
ROM_WRITE()	Write to ROM rewrite specification area. (in 512 bytes)

Figure 3-6 shows the flowchart on “ROM_WRITE() Function”.

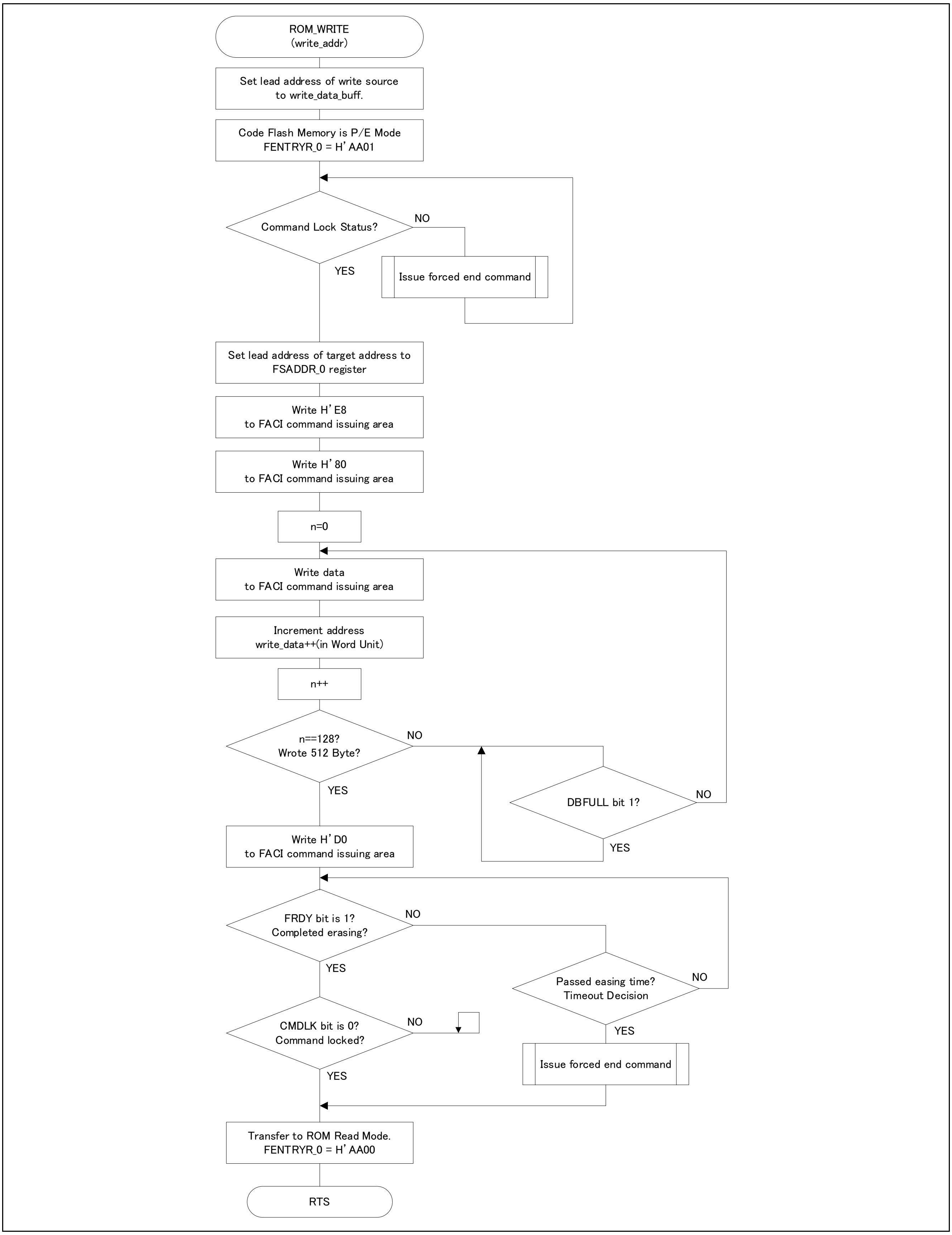

ROM_WRITE
(write_addr)
Set lead address of write source to write_data_buff.
Code Flash Memory is P/E Mode FENTRYR_0 = H’AA01
Command Lock Status?
NO
YES
Issue forced end command
Set lead address of target address to FSADDR_0 register
Write H’E8 to FACI command issuing area
Write H’80 to FACI command issuing area
n=0
Write data to FACI command issuing area
Increment address write_data++(in Word Unit)
n++
n==128? Wrote 512 Byte?
NO
YES
DBFULL bit 1?
NO
YES
Write H’D0 to FACI command issuing area
FRDY bit is 1? Completed erasing?
NO
YES
Passed easing time? Timeout Decision
NO
YES
Issue forced end command
CMDLK bit is 0? Command locked?
NO
YES
Transfer to ROM Read Mode. FENTRYR_0 = H’AA00
RTS

Figure 3-6 “ROM_WRITE() Function” Flowchart

“Operation Procedure ⑤”

3.1.6 ⑥ ROM_WE_MAIN Function

Main routine of “ROM Rewrite Control Program”. “ROM Rewrite Control Program” storing in the user mat are transferred and performed to the internal RAM.

”ROM Rewrite Control Program” performs each function call of ID authentication, ROM erasing, ROM Write Data Download, and ROM writing.

Function Explanation

Table 3-6 “ROM_WE_MAIN() Function”

Function Name	Overview
ROM_WE_MAIN()	Main routine of “ROM Rewrite Control Program”. (Perform on RAM) Perform each function call for ROM rewriting.

Figure 3-7 shows the flowchart of “ROM_WE_MAIN() Function”.

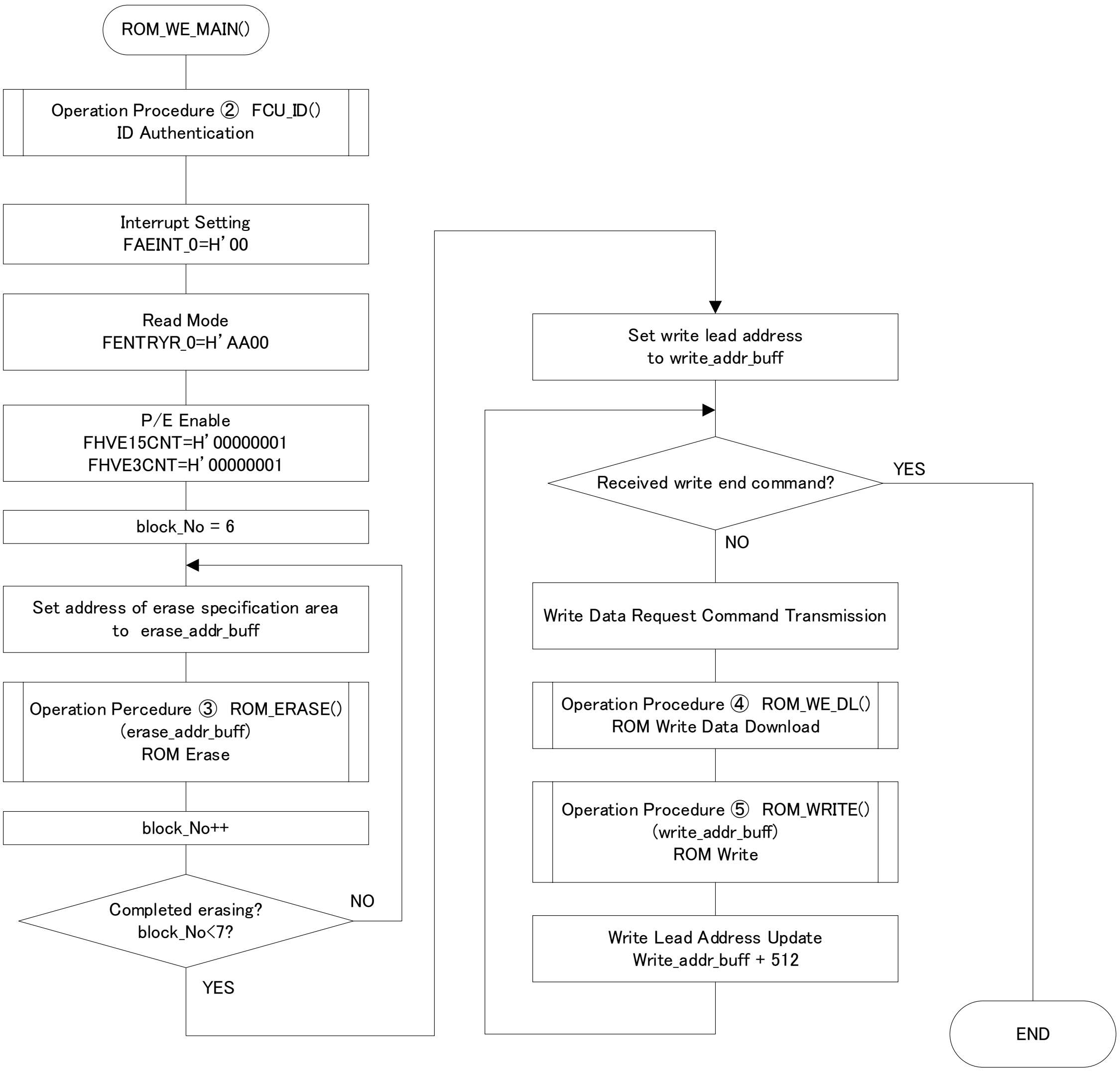


Figure 3-7 “ROM_WE_MAIN() Function” Flowchart

“Including Operation Procedure ②③④⑤”

3.1.7 Writing without RAM Transmission

After the reset starting, if the ROM area to be written is a different bank from the "Write Control Program (ROM)" stored in the user area, the writing is enabled to RAM without transmitting to “Write Control Program (ROM)”. Therefore, the processing is executed on ROM after this. In this time, “Write Control Program (ROM)” is in Bank A, and the ROM area of the writing target is in Bank B.

The program executes “ROM_WE_MAIN Function” after the start command reception without transferring to RAM. Each routine is only targeting address.

Figure 3-8 shows the ROM erase/write starting operation.

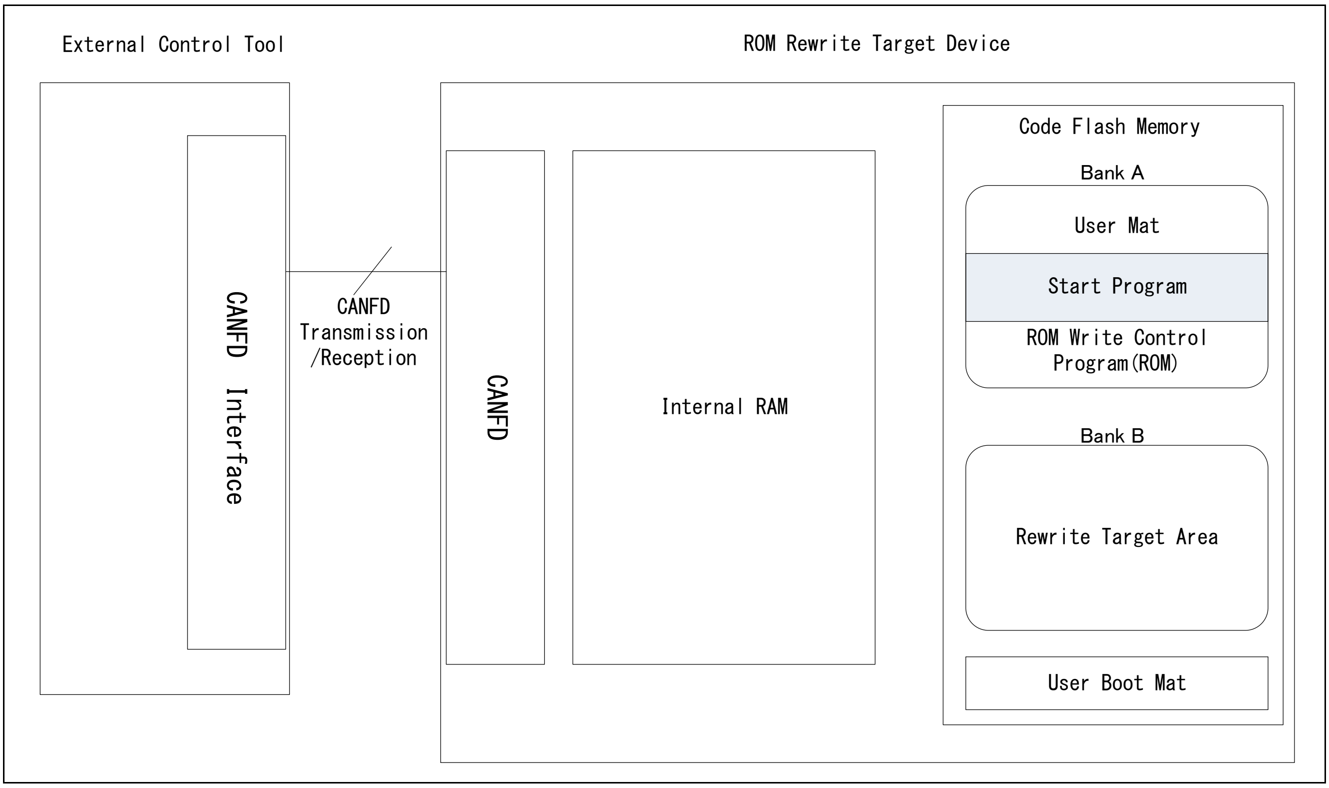


Figure 3-8 ROM Erase/Write Starting Operation

Function Explanation

Table 3-7　“main() Function”

Function Name	Overview
main()	Program starts. After receiving the start command, “ROM Rewrite Control Program” is executed.

Figure 3-9 shows the “main() Function” flowchart.

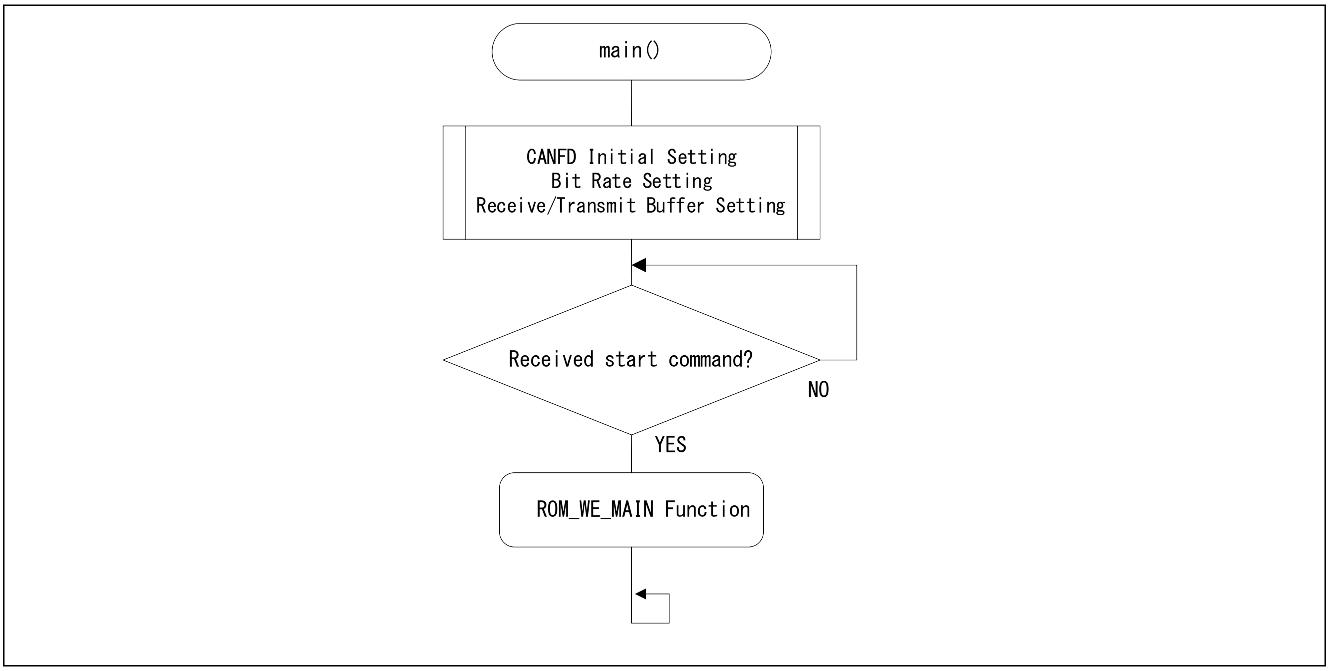


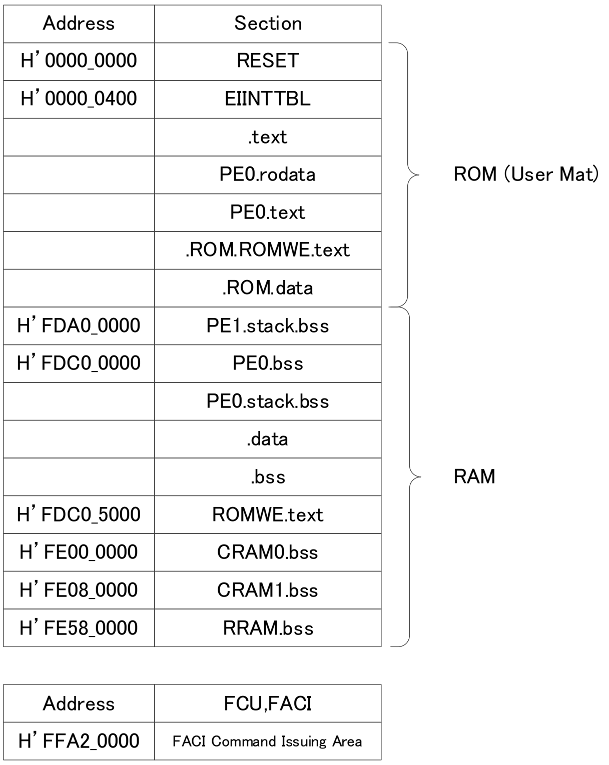
Figure 3-9　“main() Function” Flowchart

4. Detailed Specification

4.1 Address Map

4.1.1 Address Allocation Diagram

Figure 4-1 shows the address allocation diagram.



Address	Section
H’0000_0000	RESET
H’0000_0400	EIINTTBL
	.text
	PE0.rodata
	PE0.text
	.ROM.ROMWE.text
	.ROM.data
H’FDA0_0000	PE1.stack.bss
H’FDC0_0000	PE0.bss
	PE0.stack.bss
	.data
	.bss
H’FDC0_5000	ROMWE.text
H’FE00_0000	CRAM0.bss
H’FE08_0000	CRAM1.bss
H’FE58_0000	RRAM.bss

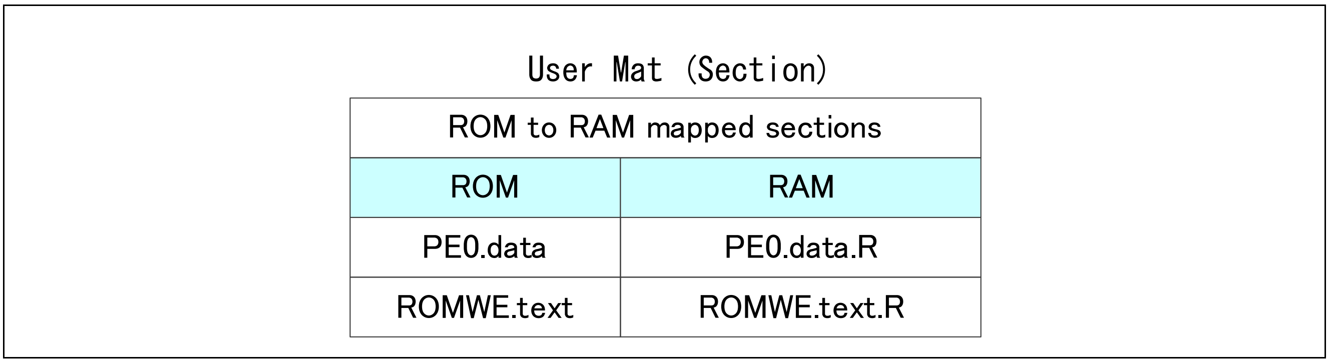
Address	FCU,FACI
H’FFA2_0000	FACI Command Issuing Area

Figure 4-1 Address Allocation Diagram

4.1.2 Link Setting of ROM/RAM Section

In this application note, transfer “ROM Rewrite Control Program” to the internal RAM. Therefore, the link setting between the transmission source (ROM stored ROM Rewrite Control Program) and the transmission destination (Internal RAM) is performed on CS+. By performing this setting, “ROM Rewrite Control Program” is automatically transferred from ROM to RAM in startup.

Figure 4-2 shows the link setting of ROM/RAM section.



User Mat (Section)

ROM to RAM mapped sections	
ROM	RAM
PE0.data	PE0.data.R
ROMWE.text	ROMWE.text.R

Figure 4-2　Link Setting of ROM/RAM Section

Our Company's Website and Inquiry

Website

http://japan.renesas.com/

Inquiry

http://japan.renesas.com/contact/

All trademarks and registered trademarks are the property of their respective owners.

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Precaution against Electrostatic Discharge (ESD)

   A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity. Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.

2. Processing at power-on

   The state of the product is undefined at the time when power is supplied. The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the time when power is supplied. In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the time when power is supplied until the reset process is completed. In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the time when power is supplied until the power reaches the level at which resetting is specified.

3. Input of signal during power-off state

   Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.

4. Handling of unused pins

   Handle unused pins in accordance with the directions given under handling of unused pins in the manual. The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of the LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible.

5. Clock signals

   After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is stabilized. When the clock signal is generated with an external resonator or from an external oscillator during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Additionally, when switching to a clock signal produced with an external resonator or by an external oscillator while program execution is in progress, wait until the target clock signal is stable.

6. Voltage application waveform at input pin

   Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between V_{IL} (Max.) and V_{IH} (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between V_{IL} (Max.) and V_{IH} (Min.).

7. Prohibition of access to reserved addresses

   Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.

8. Differences between products

   Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
4. You shall be responsible for determining what licenses are required from any third parties, and obtaining such licenses for the lawful import, export, manufacture, sales, utilization, distribution or other disposal of any products incorporating Renesas Electronics products, if required.
5. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
6. Renesas Electronics products are classified according to the following two quality grades: “Standard” and “High Quality”. The intended applications for each Renesas Electronics product depends on the product’s quality grade, as indicated below.
   "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.
   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.
   Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user’s manual or other Renesas Electronics document.
7. No semiconductor product is absolutely secure. Notwithstanding any security measures or features that may be implemented in Renesas Electronics hardware or software products, Renesas Electronics shall have absolutely no liability arising out of any vulnerability or security breach, including but not limited to any unauthorized access to or use of a Renesas Electronics product or a system that uses a Renesas Electronics product. RENESAS ELECTRONICS DOES NOT WARRANT OR GUARANTEE THAT RENESAS ELECTRONICS PRODUCTS, OR ANY SYSTEMS CREATED USING RENESAS ELECTRONICS PRODUCTS WILL BE INVULNERABLE OR FREE FROM CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, DATA LOSS OR THEFT, OR OTHER SECURITY INTRUSION (“Vulnerability Issues”). RENESAS ELECTRONICS DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATED TO ANY VULNERABILITY ISSUES. FURTHERMORE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, RENESAS ELECTRONICS DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND ANY RELATED OR ACCOMPANYING SOFTWARE OR HARDWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.
8. When using Renesas Electronics products, refer to the latest product information (data sheets, user’s manuals, application notes, “General Notes for Handling and Using Semiconductor Devices” in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
10. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
12. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
13. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
14. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.
(Note2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

(Rev.5.0-1 October 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit: www.renesas.com/contact/.