RH850/U2B Group

R01AN6438EJ0100
Rev.1.00

OTA Operation Example using GCFU by Single Map Mode

Summary

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

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

Application

This document is applicable for RH850/U2Bx.

[Note 1] Self-programing Function Activation, and Code Flash Memory Mapping

In this application note, enable the following setting on CS+ for performing OTA.

(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”.

(4) Set “Map Mode” = “Single Map Mode” in “Memory”

Contents

1. OTA by Single Map Mode

1.1 Address Translation

1.1.1 Address Translation by GCFU

In single map mode, perform the mapping switching for the programing before/after updating by using the address translation function by GCFU. Code flash can be used efficiently when partially updating the program. Figure 1-1 shows the address translation by GCFU.

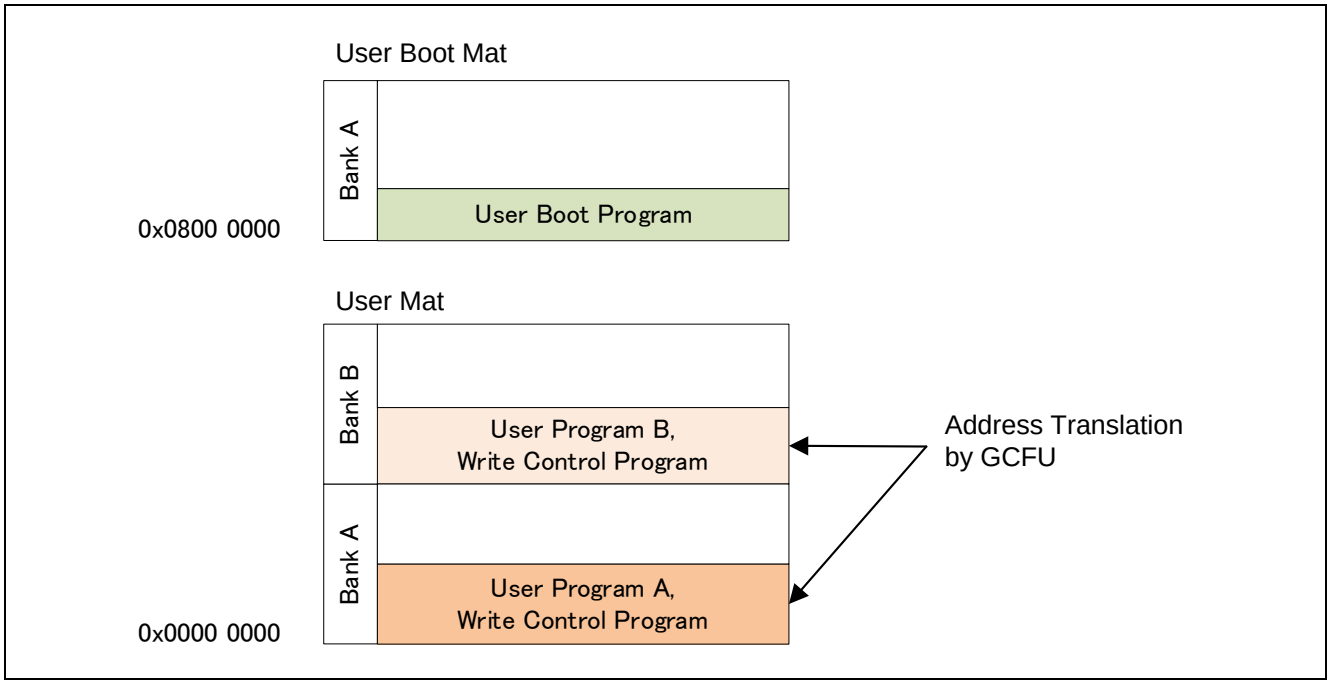

Figure 1-1 Address Translation by GCFU

1.1.2 Flash Access after Address Translation

When translating address by GCFU, the flash is accessed as a logical address from the CPU. FACI does not depend on the address translation in GCFU, therefore it accesses as the physical address. Figure 1-2 shows the memory related bus configuration diagram.

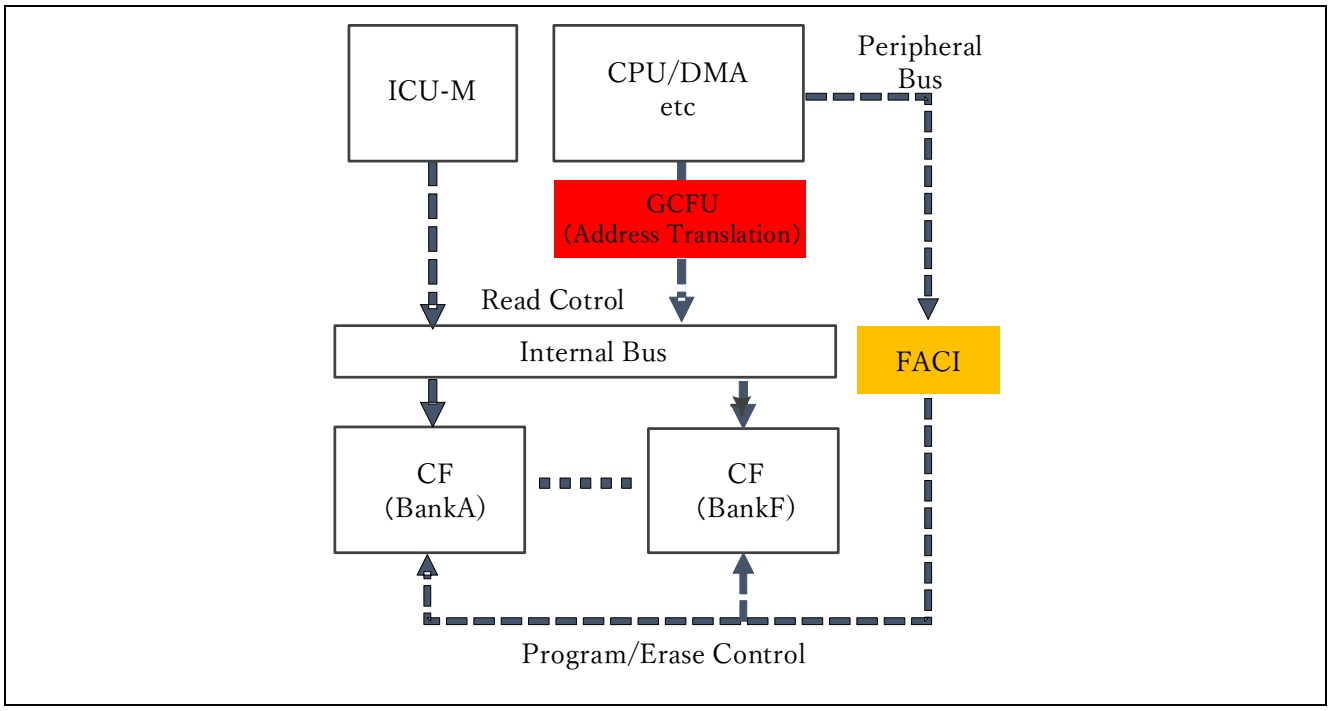

Figure 1-2 Memory Related Bus Configuration Diagram

1.1.3 Restriction when Using GCFU

When translating the address of partial block, the error is occurred if the program or data in the block that is not subject to address translation is accessed while the program is being updated. Therefore, when accessing the block that is not subject to address translation during program update, suspend erase write and enter ROM Read Mode.

Also, read access from the ICU-M is not subject to address translation. The programing that is considering the execution area is required.

1.2 Write Operation by Boot Bank

Store the next booting bank information in data flash. If the booted bank is Bank A, the address is not translated. If the booted bank is Bank B, the address is translated. The following shows the operation by the boot bank.

1.2.1 Program A Starting

No address translation (Physical address = Logical address). Write target is Bank B.

Figure 1-3 shows the write operation by the program A starting.

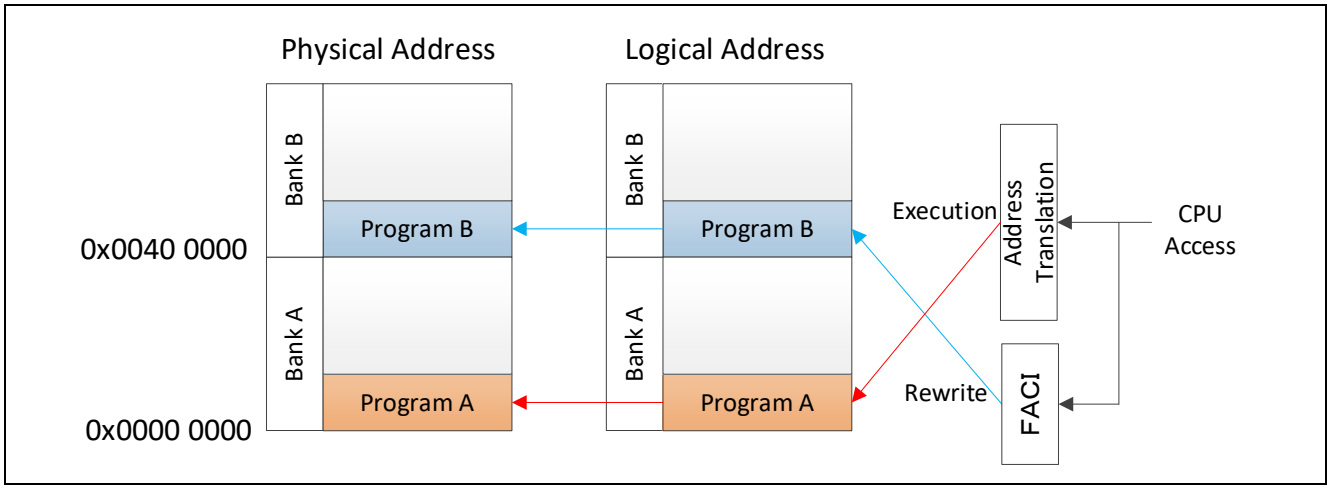

Figure 1-3 Write Operation by Program A Starting

1.2.2 Program B Starting

Address translation (Physical address ≠ Logical address). Write target is Bank A.

Figure 1-4 shows the write operation by the program B starting.

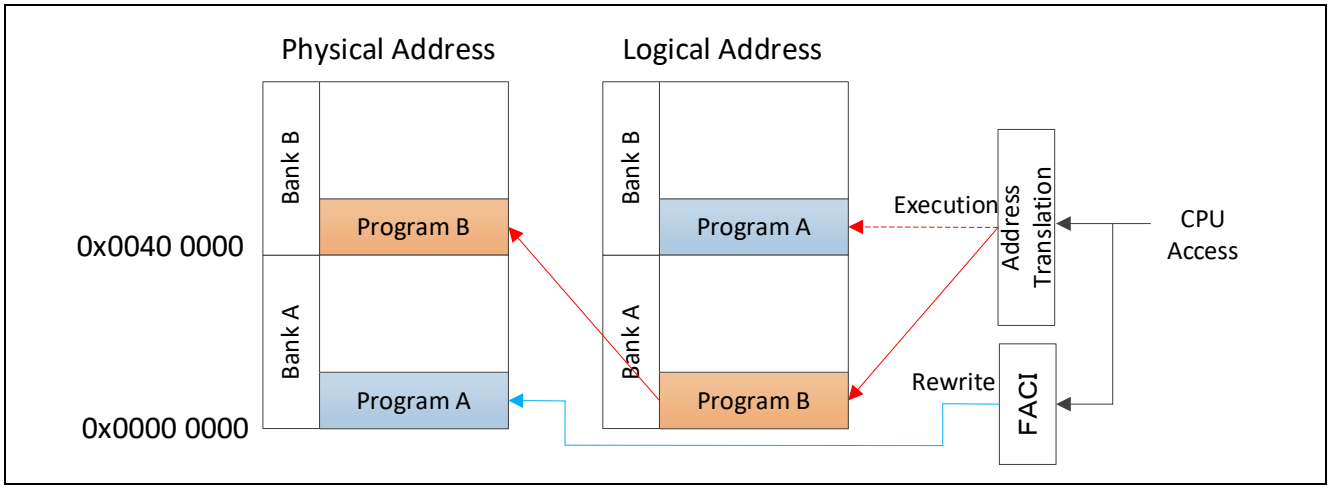

Figure 1-4 Write Operation by Program B Starting

1.3 BGO Function

1.3.1 Concurrent Prog/Erase Function

As the BGO (Background operation) function, support additionally the data flash reading during programming/erasing of code flash. In addition, if it is between different banks, program/erase suspend can be performed by all program/erase combinations. In this operation example, for realizing the concurrent programing/erasing that preferentially executes data flash erasing while erasing the code flash, program/erase suspend function is used. Figure 1-5 shows the flash memory related module configuration diagram.

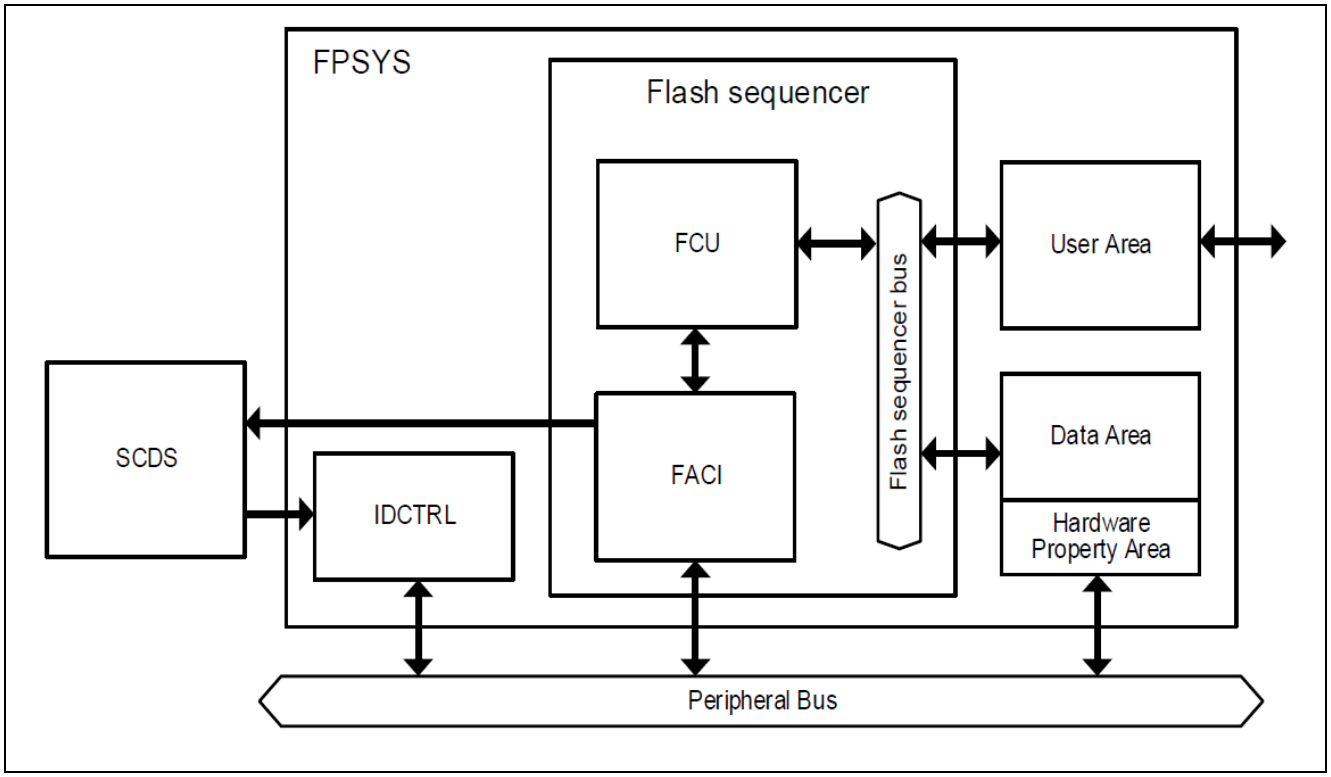

Figure 1-5 Flash Memory Related Module Configuration Diagram

2. Specification

2.1 Entire Specification

- In this application note, the user mat is rewritten with OTA 2Bank configuration by single map mode. Figure 2-1 shows the memory allocation.
- Using GCFU (Global Calibration Function Unit) function, when Bank A is started, set Bank A to operate as logical address 0x00000000 to 0x0017FFFF. When Bank B is started, set Bank B to operate as logical address 0x00000000 to 0x0017FFFF. The boot bank information is stored to the data flash. The starting bank is determined, and the address conversion is performed by the GCFU function.
- Rewrite area is performed for the bank different from the bank in which the program operates.
- Code flash memory mapping mode is single map mode. Operation mode is normal operation mode. Boot mat is user boot mode.
- RS-CANFD(ch1) is used as the data used for code flash writing, and stored to the internal RAM.
- The code flash rewrite target device uses RS-CANFD from the external device, and corresponding code flash rewrite processing is performed when receiving the specific ID and data. These combination of specific ID and data is called “CANFD Command” in this application note.

Table 2-1 shows the system configuration diagram.

Table 2-1 Memory Allocation

Area	Physical Address	Block	Bank	Size	OTA Target
User boot mat	0x0800 0000 – 0x0800 FFFF	User boot area 0	BankA	64K bytes	Not target
User mat (Program A)	0x0000 0000 – 0x0001 7FFF	Block 0 to 5	BankA	96K bytes	Target
User mat (Program B)	0x0040 0000 – 0x0041 7FFF	Block 0 to 5	BankB	96K bytes	Target

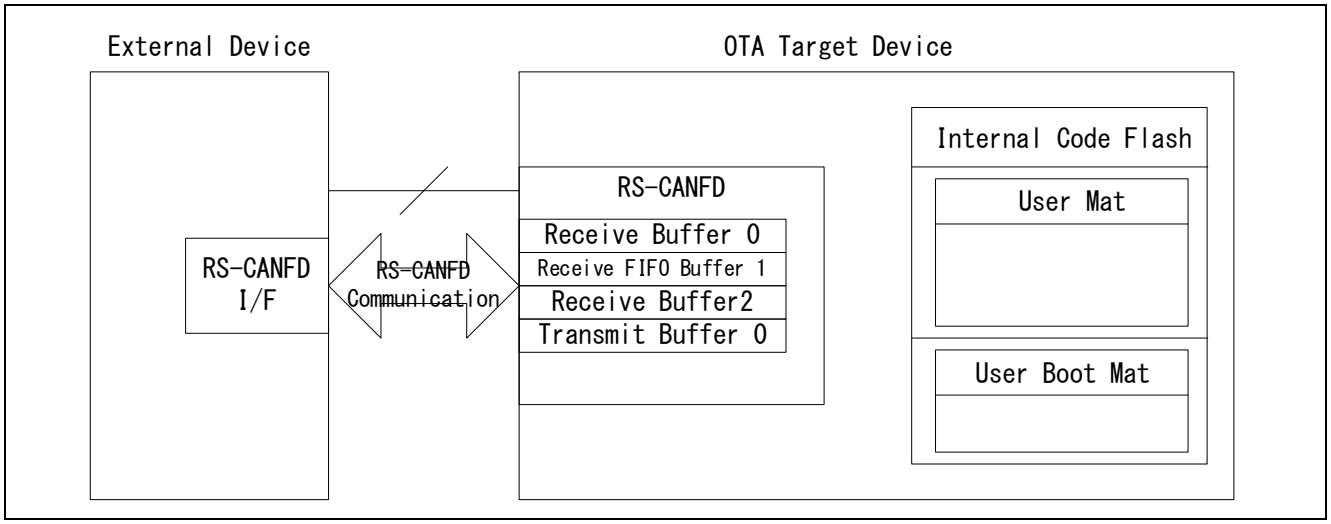

Figure 2-1 System Configuration Diagram

2.2 RS-CANFD Communication Specification

- Use channel 1.
- Set the communication speed the normal bit rate 1Mbps and the data bit rate 2Mbps.
- Set the communication frame to the CANFD frame.
- For storing each command transmitted from the external device, set the number of receive rules for channel 1 to “2”.

2.3 CANFD Command Specification

- Rewrite start command starts the code flash rewrite processing by transmitting the command from the external device to the code flash rewrite target device.
- Write data request command requests the write data by transmitting the command from the code flash rewrite target device to the external device.
- Write data download command transmits the write data from the external device to the code flash rewrite target device.
- Write end command completes the rewrite processing by transmitting the command from the code flash rewrite target device to the external device.

Table 2-2 shows the CANFD command specification.

Table 2-2 CANFD Command Specification

Buffer	Channel	Command Name	Transmission/Reception	Standard ID	Data Length	Data
0	1	Rewrite start command	Reception	H’100	1 Byte	H’00
1	1	Write data download	Reception	H’110	64 Bytes	Download code flash write data download 512 bytes (64Byte x 8)
1	1	Write data request command	Transmission	H’111	1Byte	H’11
2	1	Write end command	Transmission	H’121	1Byte	H’22

2.4 Entire Sequences

Figure 2-2 to Figure 2-3 show the entire sequences.

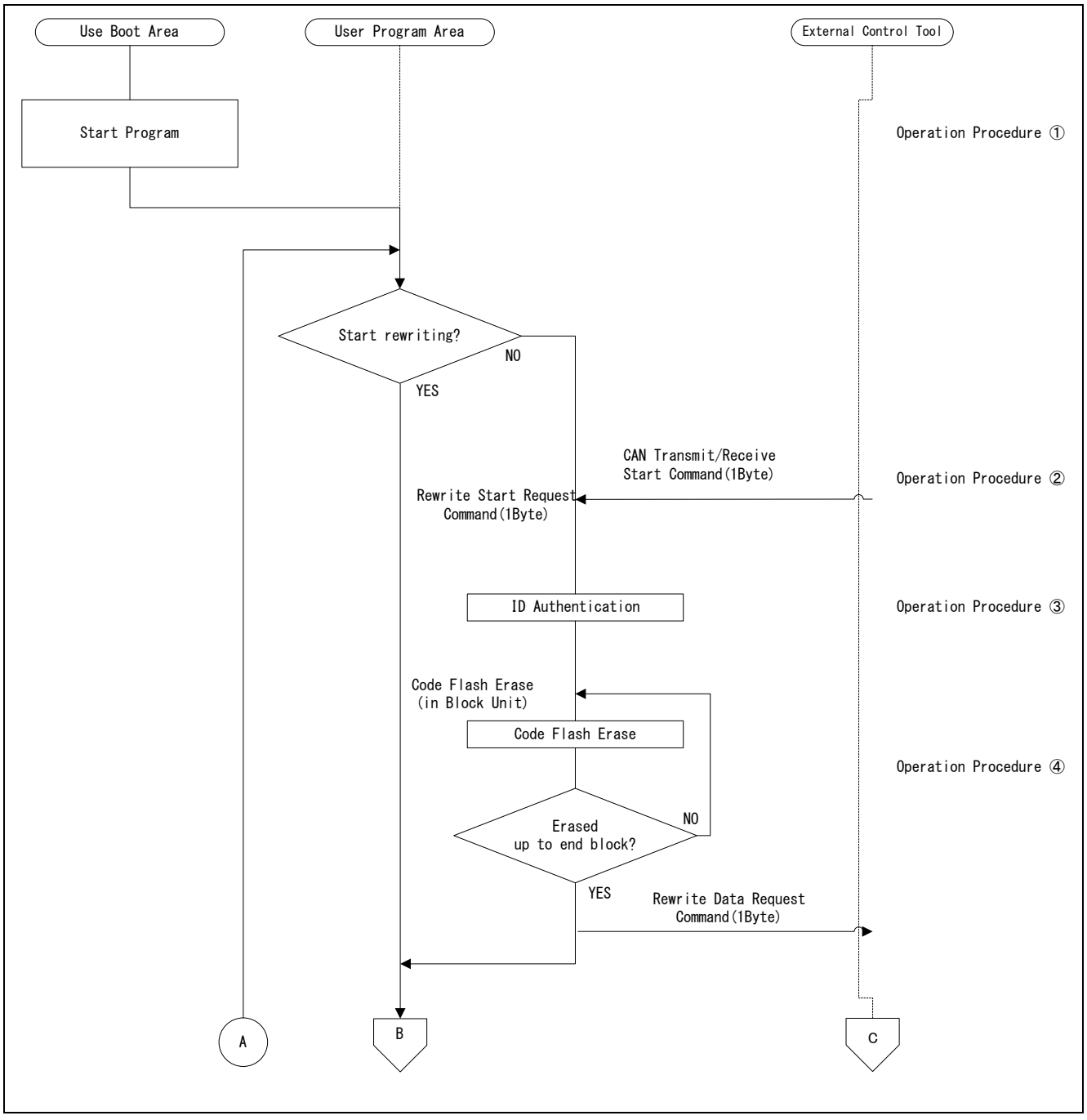

Figure 2-2 Entire Sequences Diagram (1)

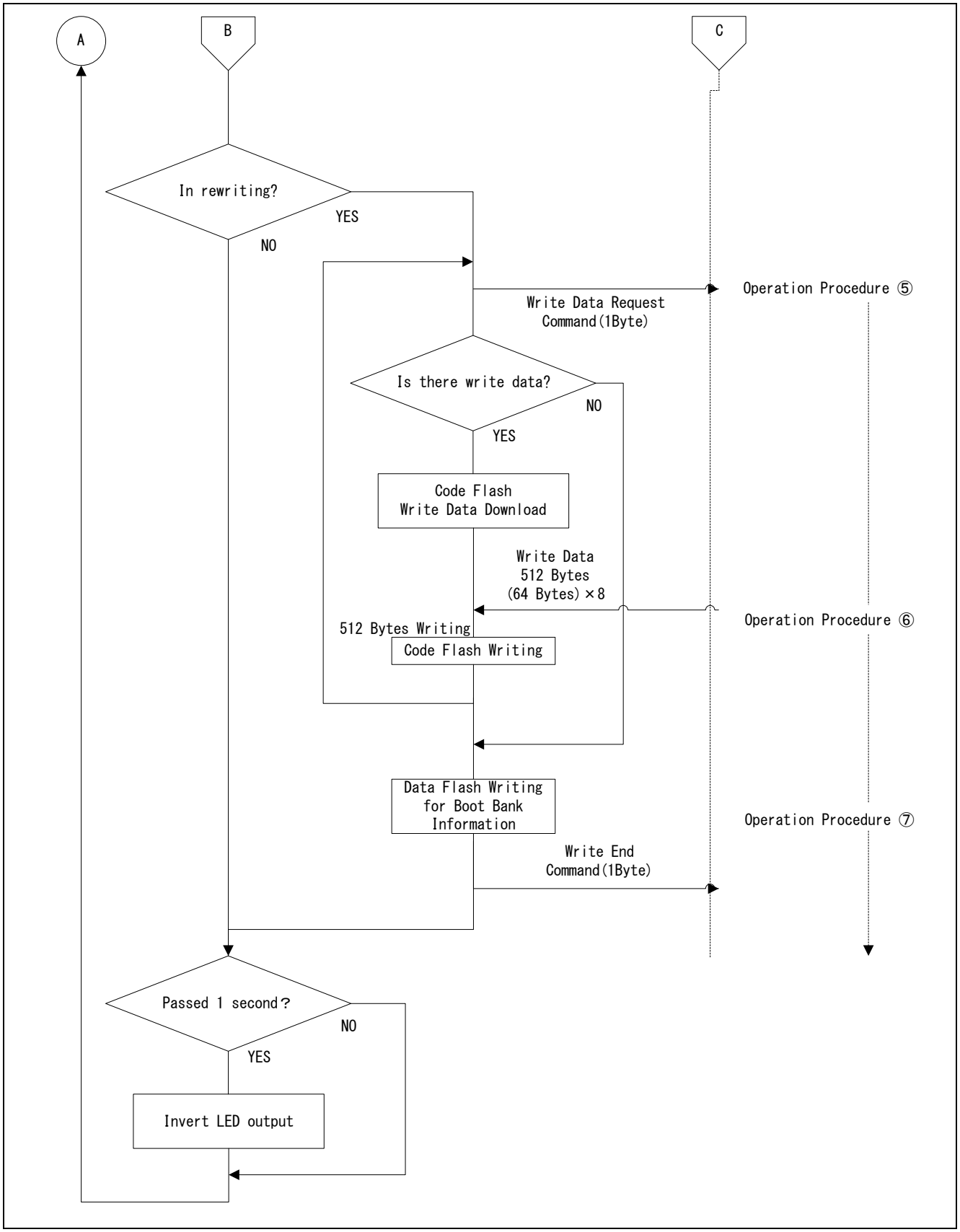

Figure 2-3 Entire Sequences Diagram (2)

2.5 Use Function

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

2.6 Operation Mode

In this application note, the operation mode for the microcomputer when rewriting code flash is performed on the user boot mode. In the user boot mode, the boot mat is the user boot mat.

Selection method for operation mode is set in the mode pin. Setting for the option byte is set by using Renesas Flash Programmer for RH850 family.

Table 2-3 shows the operation mode selection.

Table 2-3 Operation Mode Selection

Pin Setting Value			Option Byte Setting Value		Operation Mode	Boot Mat
MD1	MD0	TRST	STMSEL1	STMSEL0		
0	0	0	0	1	User boot mode	User boot mat

2.7 Memory Mapping

In this application note, the memory mapping when rewriting code flash is performed in single map mode. Table 2-4 shows the memory mapping selection.

Table 2-4 Memory Mapping Selection

Option Byte Setting Value		Memory Mapping
MAPMODE1	MAPMODE 0	
0	1	Single map mode

3. OTA Operation Example Using External Device

3.1 Operation Procedure

Operation procedure ① to ⑦ is corresponds to “2.4 Entire Sequence”.

3.1.1 ① Boot Bank Switching

After starting reset, the start program on the user boot mat reads the data flash, determinate the boot bank of user mat, and jumps to the user program by switching the suitable bank. Figure 3-1 shows the start program operation.

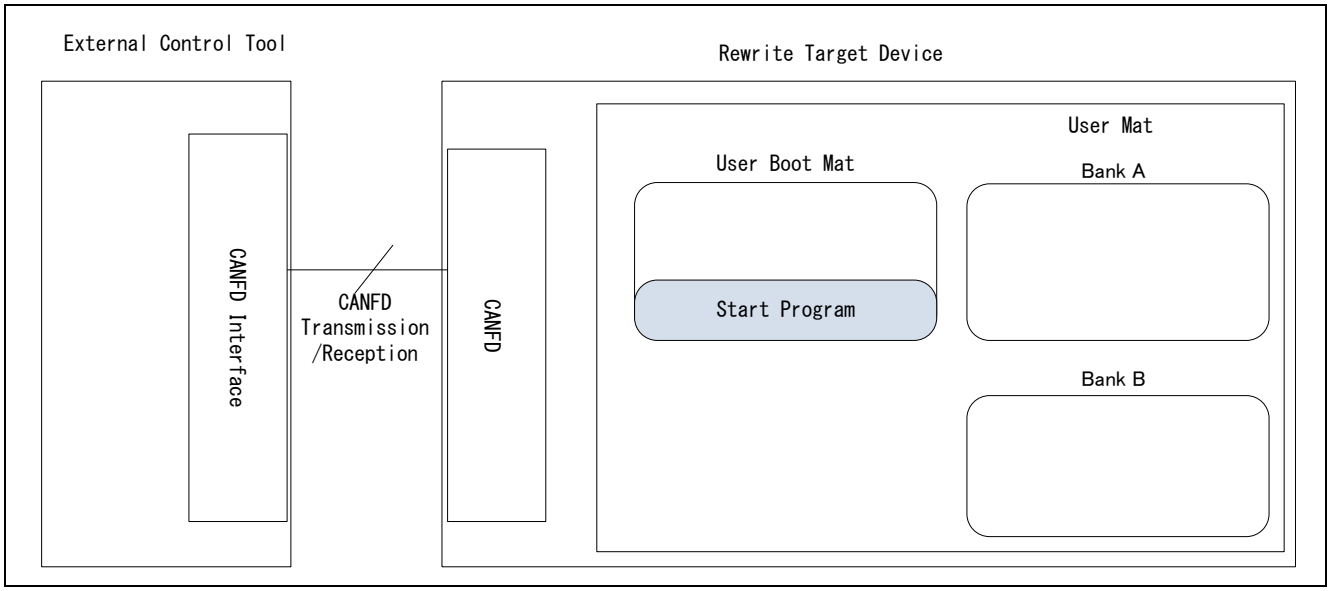

Figure 3-1 Start Up Program Operation

Table 3-1 “main_pe0() Function”

Function Name	Overview
main_pe0()	Program starting. After switching the boot bank of the user mat, jump to user program.

Figure 3-2 shows the “main_pe0() Function” flowchart.

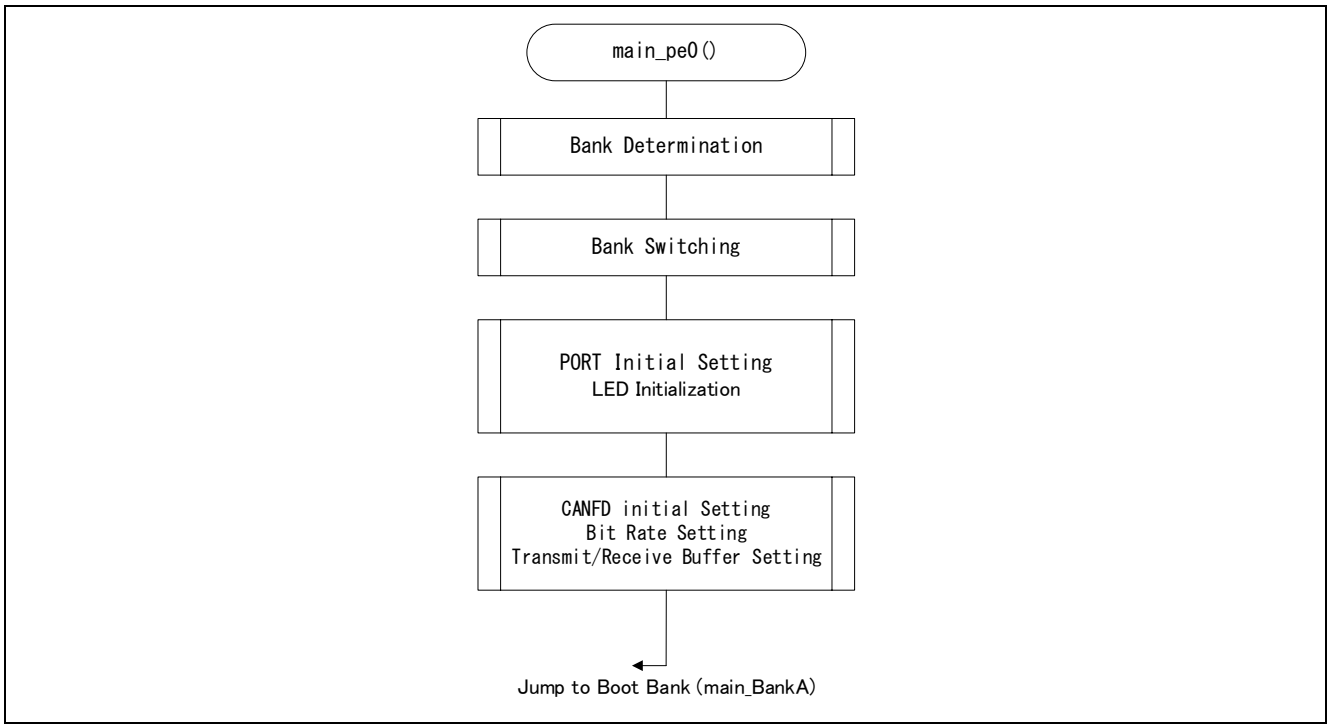

Figure 3-2 “main_pe0() Function” Flowchart

“Operation Procedure ①”

Figure 3-3 shows the “Bank Switching Function” flowchart.

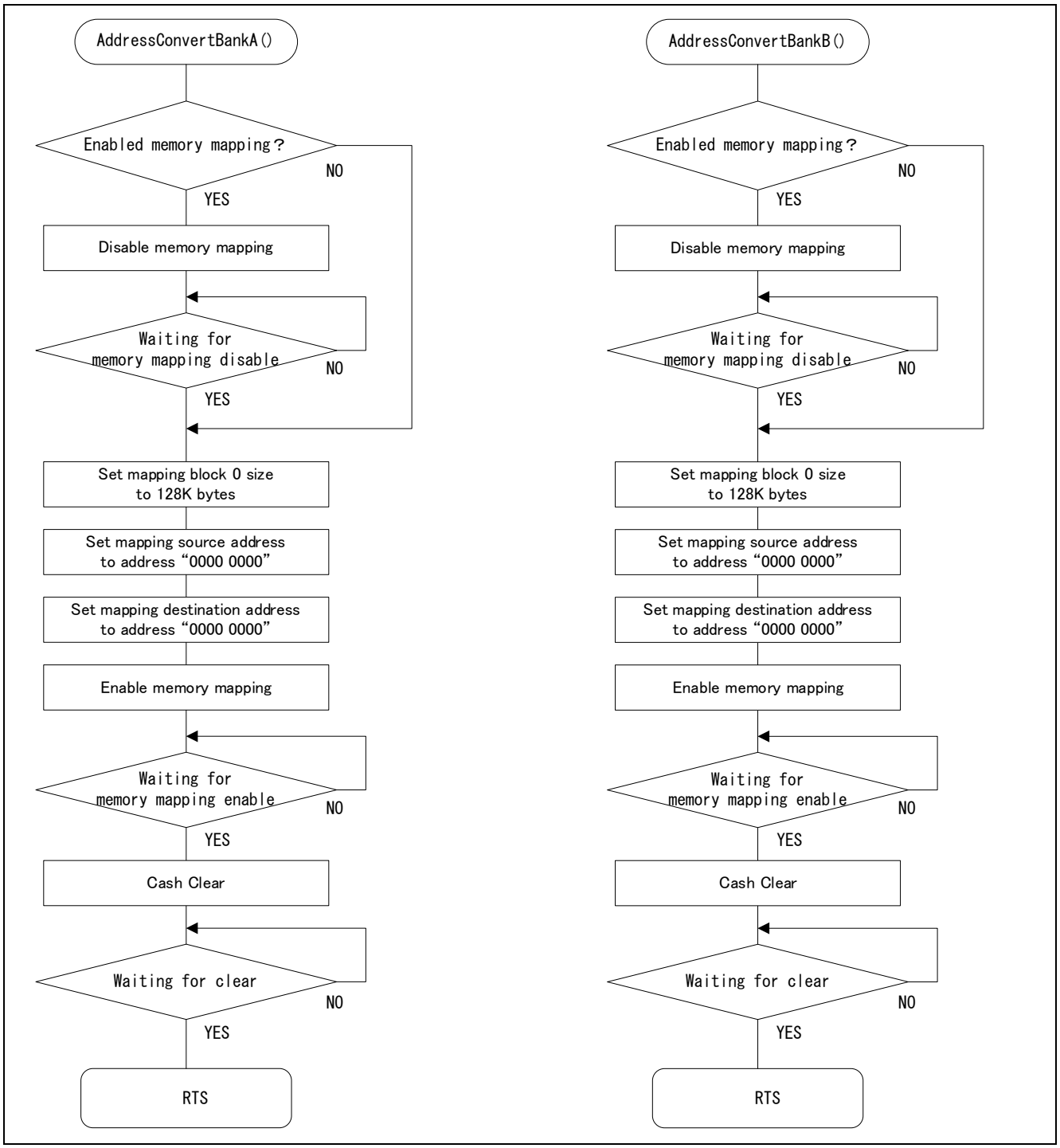

Figure 3-3 “Bank Switching Function” Flowchart

3.1.2 ② BGO Writing

By setting the Code Flash area to be written to a bank different from the startup bank, “Write Control Program” can be written to the code flash without transferring to RAM. When booting on Bank A, the code flash area of Bank B is rewritten by “Write Control Program” of Bank A.

In main routine, the user program constantly flickering LED is executed, and it executes OTA in parallel with the rewrite control program after receiving the rewrite start request command.

Figure 3-4 shows the code flash erase/write start operation.

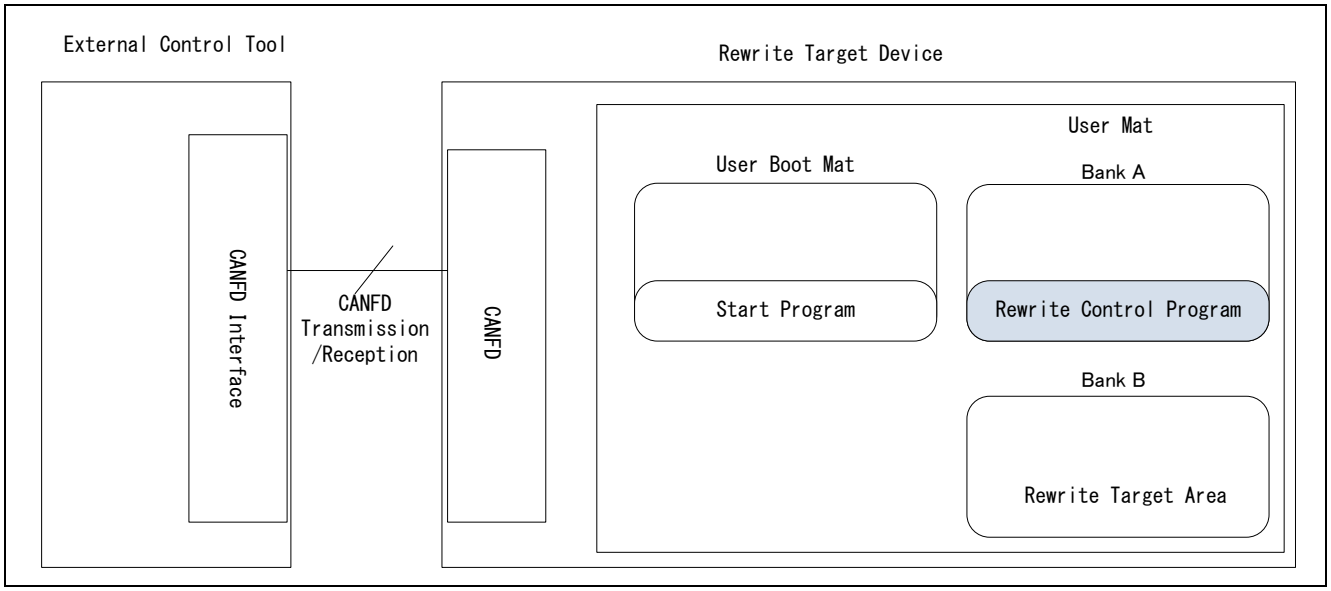

Figure 3-4 Code Flash Erase/Write Start Operation

Function Explanation

Table 3-2 “main_BankA () Function"

Function Name	Overview
main_BankA ()	Repeat LED flicking, and execute “Rewrite Control Program” after receiving rewrite start command.

Figure 3-5 shows “main_BankA () Function” flowchart.

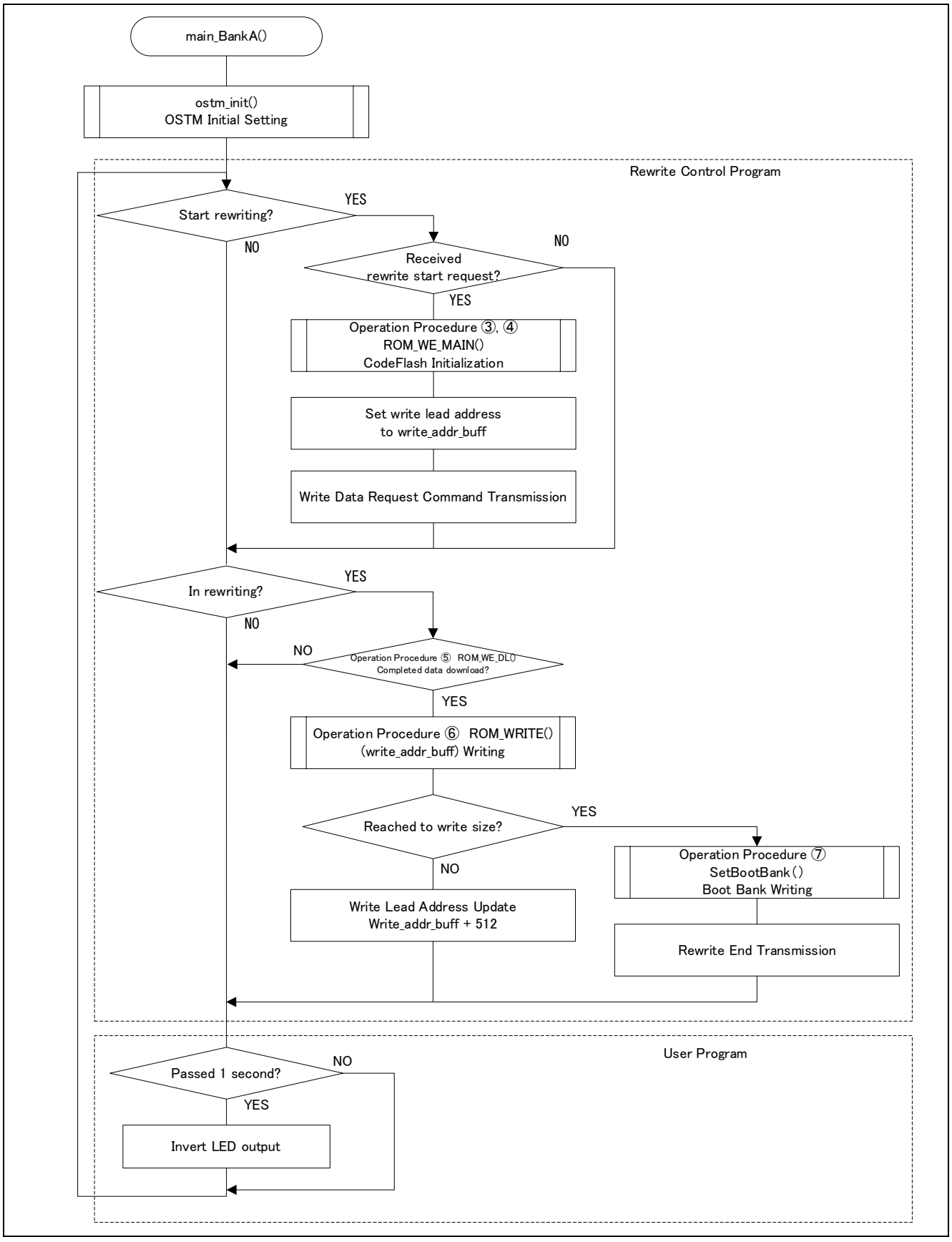

Figure 3-5 “main_BankA () Function” Flowchart

“Operation Procedure ②”

Function Explanation

Table 3-3 “Code Flash_WE_MAIN() Function”

Function Name	Overview
Code Flash_WE_MAIN()	Perform each function call of ID authentication, code flash erasing, code flash write data download, and code flash writing.

Figure 3-6 shows “Code Flash_WE_MAIN() Function” flowchart.

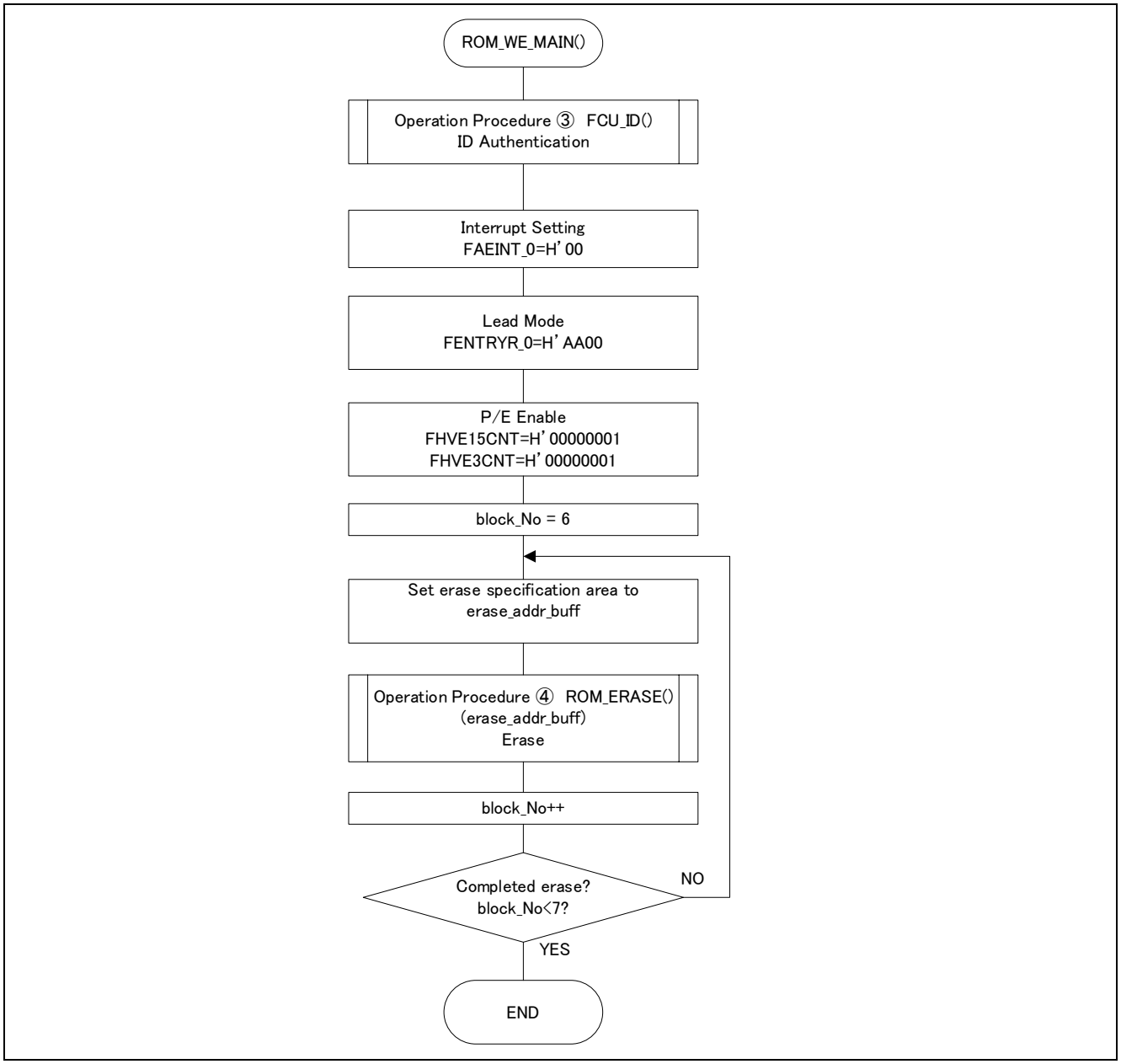

Figure 3-6 “Code Flash_WE_MAIN() Function” Flowchart

“Including Operation Procedure ③, ④”

3.1.3 ③ ID Authentication

Execute “ID Authentication Function” of “Rewrite Control Program”. ID authentication is executed by comparing the 256 bits ID preset in a special area of flash memory with the value of RHSIFIDIN 0 to 7.

In this application note, "0" for the first byte and "F" for other bytes are used as ID setting. Renesas Flash Programmer for RH850 family or the configuration setting command are used for changing ID setting.

Function Explanation

Table 3-4 “FCU_ID() Function”

Function Name	Overview
FCU_ID()	Execute comparison with ID set in the specific area of flash memory and ID authentication.

Figure 3-7 shows “FCU_ID() Function” flowchart.

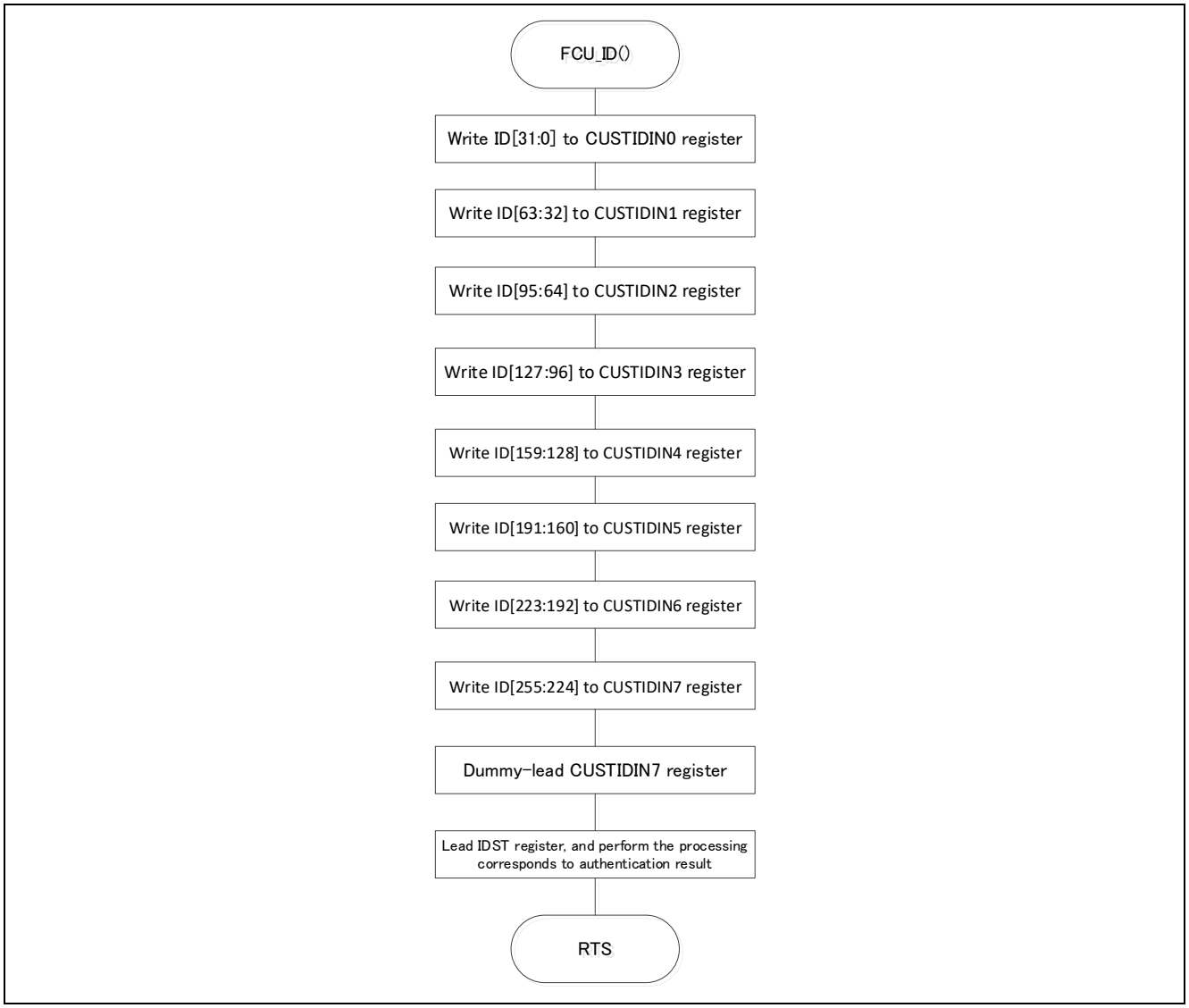

Figure 3-7 “FCU_ID() Function” Flowchart

“Operation Procedure ③”

3.1.4 ④ Code Flash Erase

After ID authentication, execute “Code Flash Erase Function” of “Rewrite Control Program”.

Issue block erase command to FACI command issue area, and erase the code flash rewrite specified area.

Function Example

Table 3-5 “Code Flash_ERASE() Function”

Function Name	Overview
Code Flash_ERASE()	Erase code flash rewrite specified area.

Figure 3-8 shows “Code Flash_ERASE() Function” flowchart.

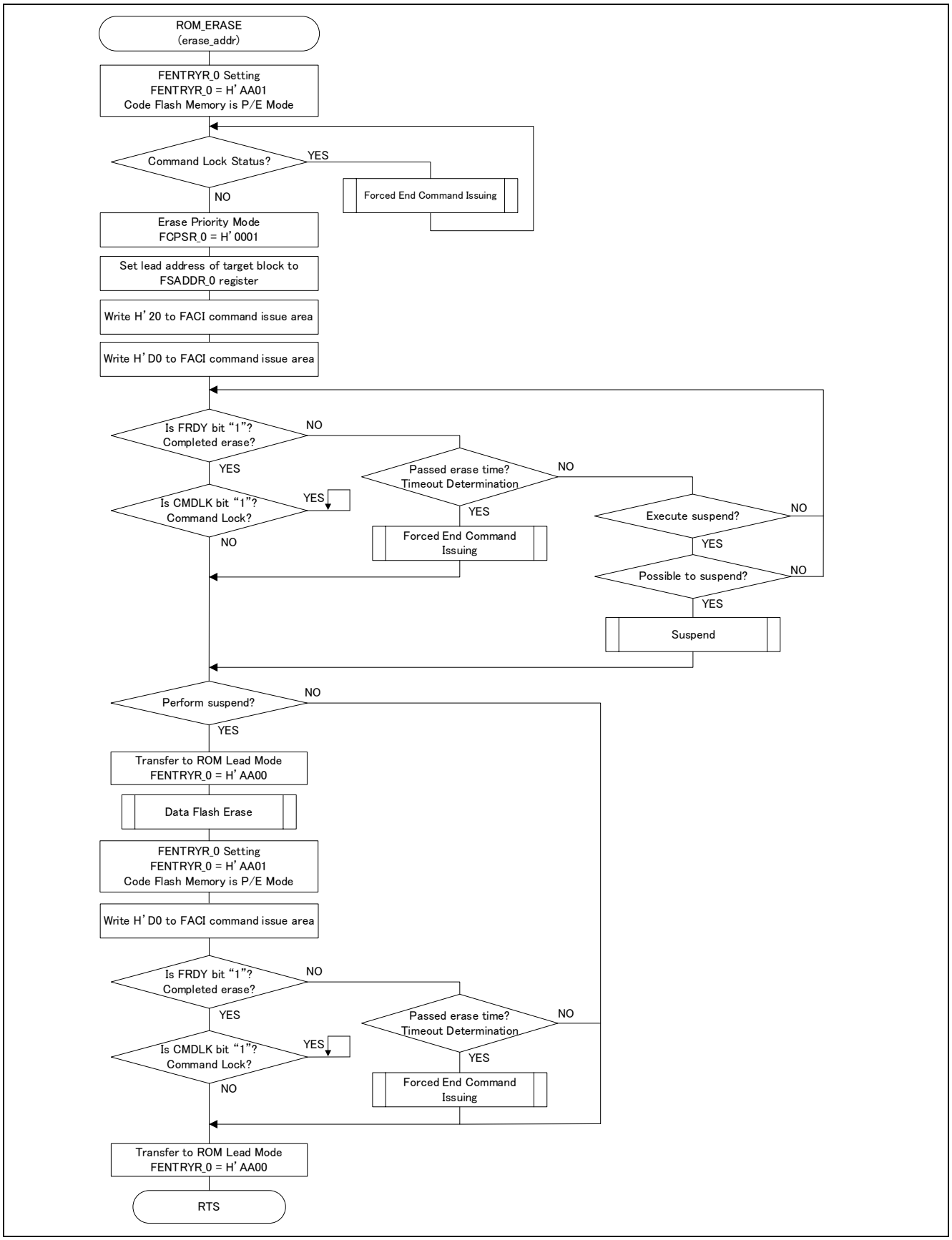

Figure 3-8 “Code Flash_ERASE() Function” Flowchart

“Operation Procedure ④”

Figure 3-9 shows “Code Flash_SUSP() Function”.

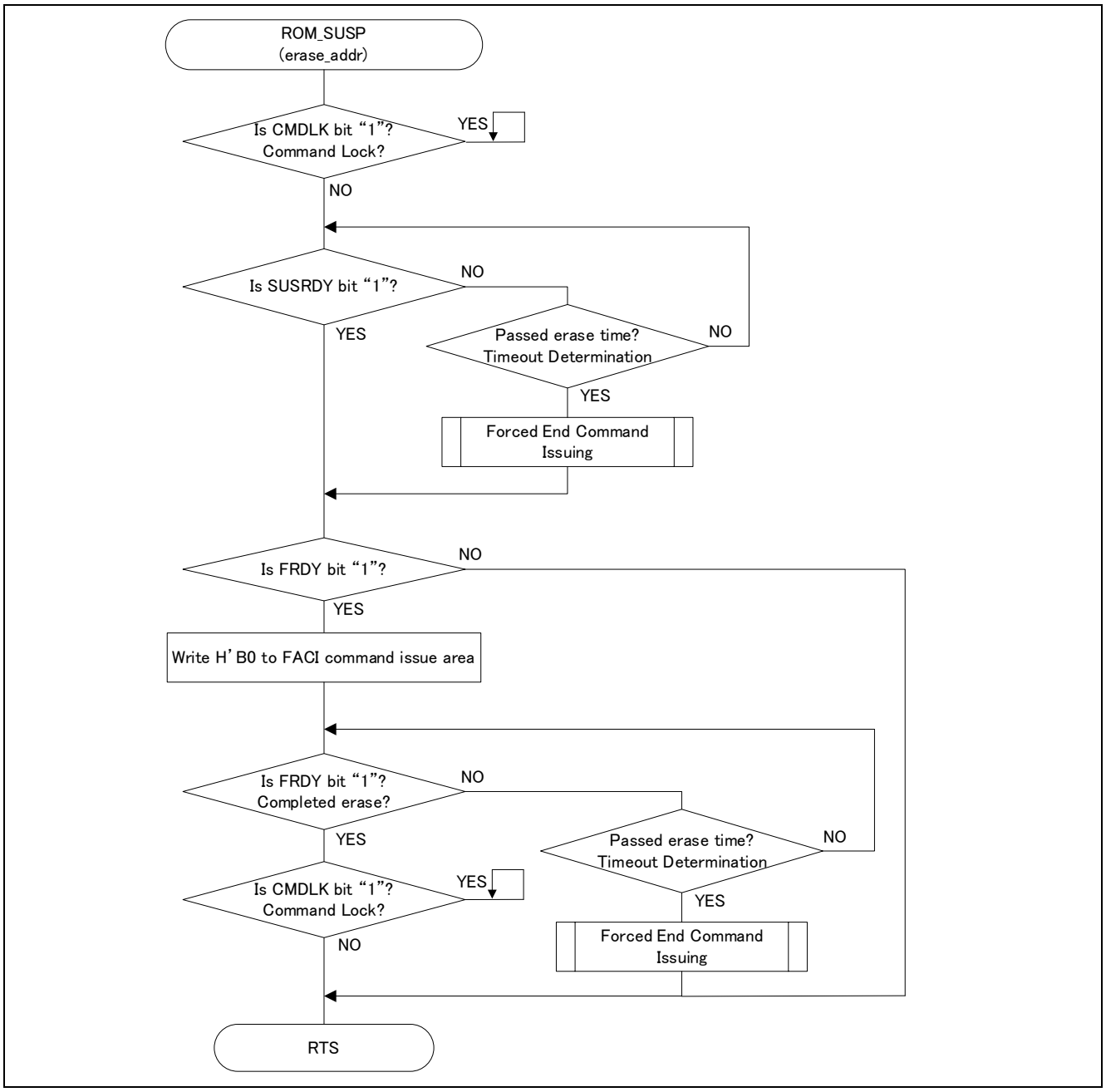

Figure 3-9 “Code Flash_SUSP() Function” Flowchart

3.1.5 ⑤ Code Flash Write Data Download

Execute “Code Flash Write Data Download Function”, and transmit the write data request command. The external device received the write data request command transmits the write data 512 bytes to the microcomputer by the write data download command. In “ Code Flash Write Data Download Function”, store the received write data to RAM.

Function Explanation

Table 3-6 “Code Flash_WE_DL() Function”

Function Name	Overview
Code Flash_WE_DL()	Download write data form external device.

Figure 3-10 shows “Code Flash_WE_DL() Function” flowchart.

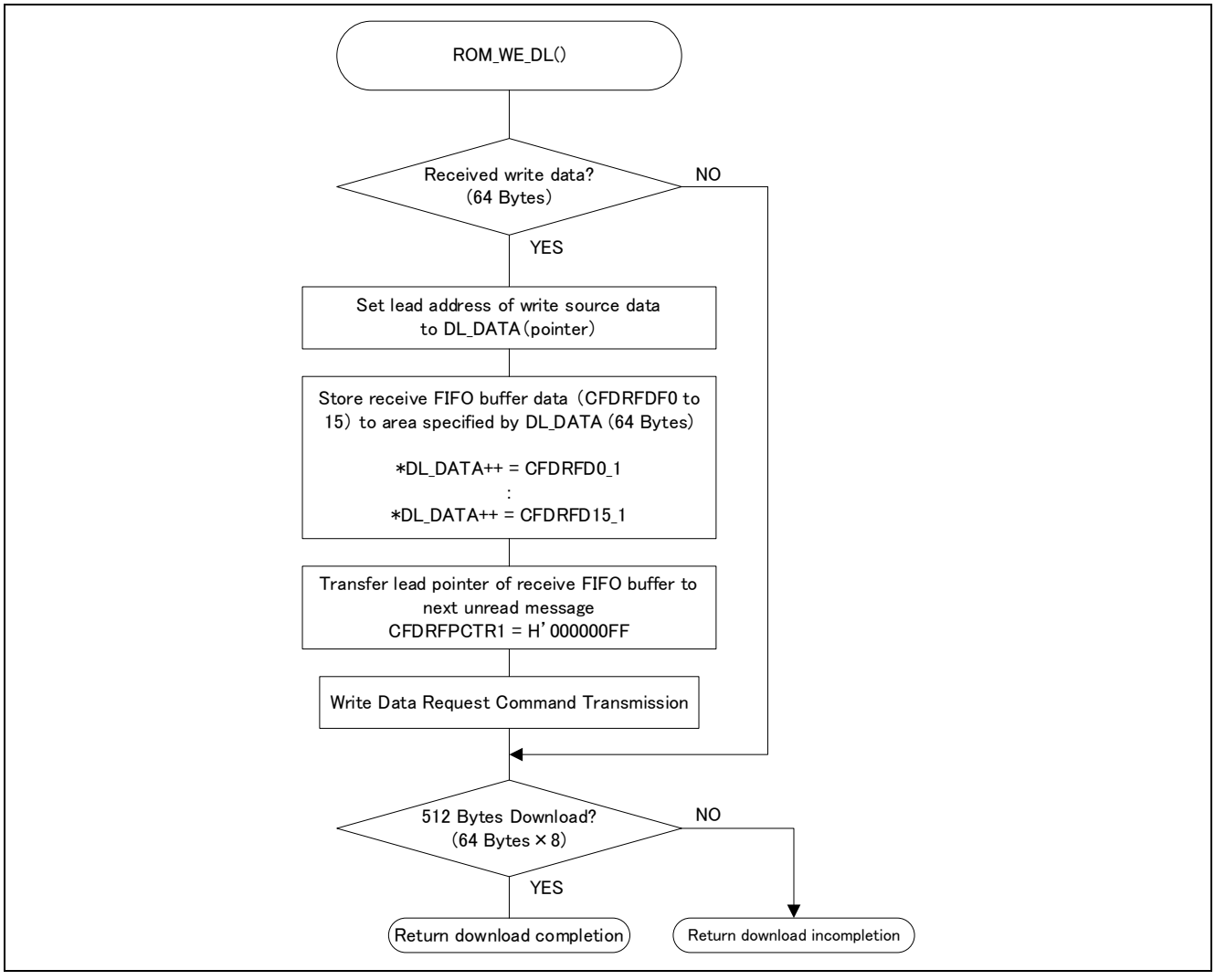

Figure 3-10 “Code Flash_WE_DL() Function “ Flowchart

“Function Procedure ⑤”

3.1.6 ⑥ Code Flash Writing

Write the write data received from the external device by CAN communication to code flash by using “Code Flash Write Function”.

Issue the program command to FACI command issue area, and write it to code flash rewrite specification area. When reaching the write size (96K bytes), terminate the flash rewriting.

Function Explanation

Table 3-7 “Code Flash_WRITE() Function”

Function Name	Overview
Code Flash_WRITE()	Write to code flash rewrite specified area (in 512 bytes unit).

Figure 3-11 shows “Code Flash_WRITE() Function” flowchart.

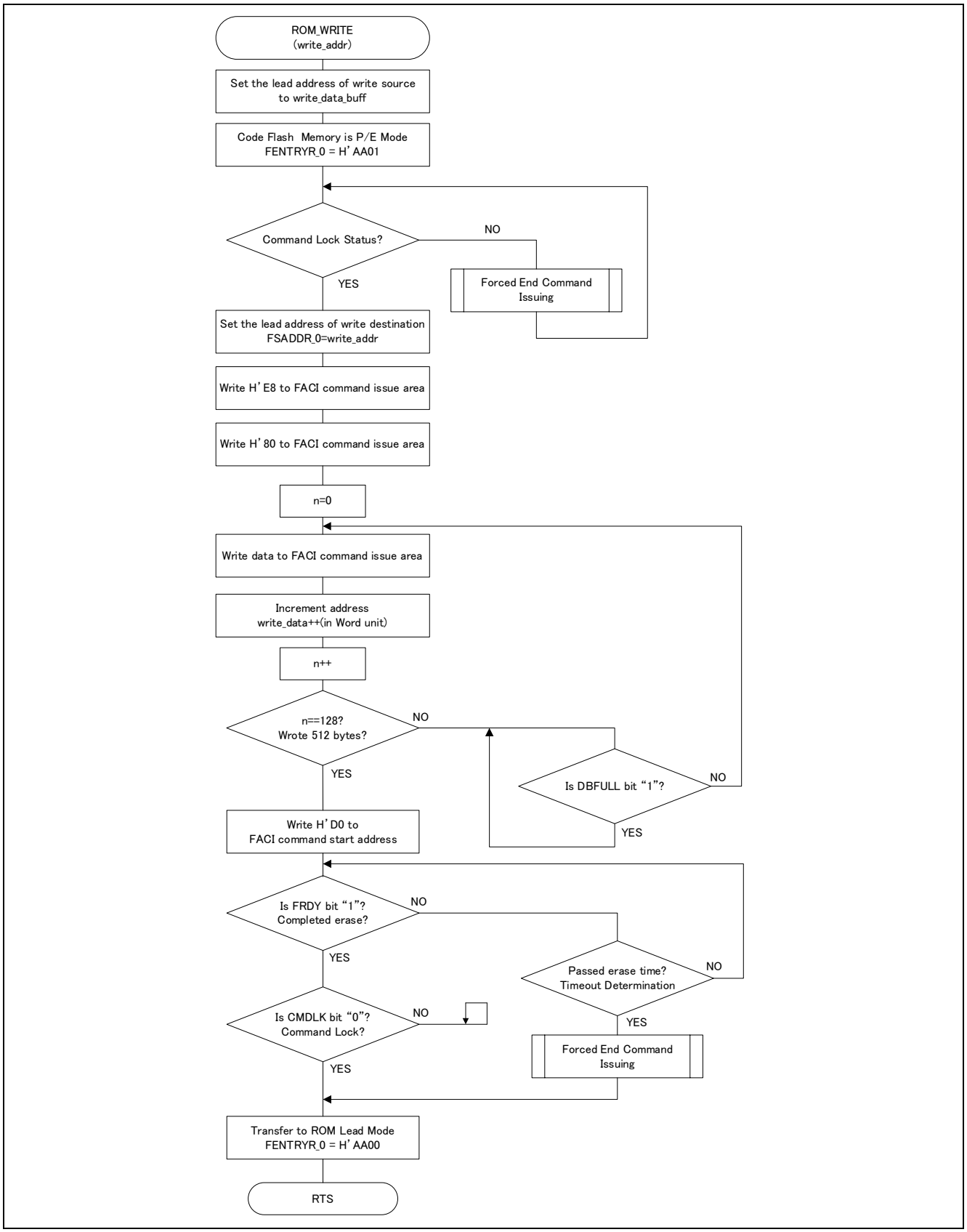

Figure 3-11 “Code Flash_WRITE() Function” Flowchart

”Operation Procedure ⑥”

3.1.7 ⑦ Boot Bank Information Write Function

After completing the rewriting, write next boot bank information to the data flash.

Function Explanation

Table 3-8 “SetBootBank () Function”

Function Name	Overview
SetBootBank ()	Determine the next boot bank information, and write it to the data flash.

Figure 3-12 shows “SetBootBank () Function” flowchart.

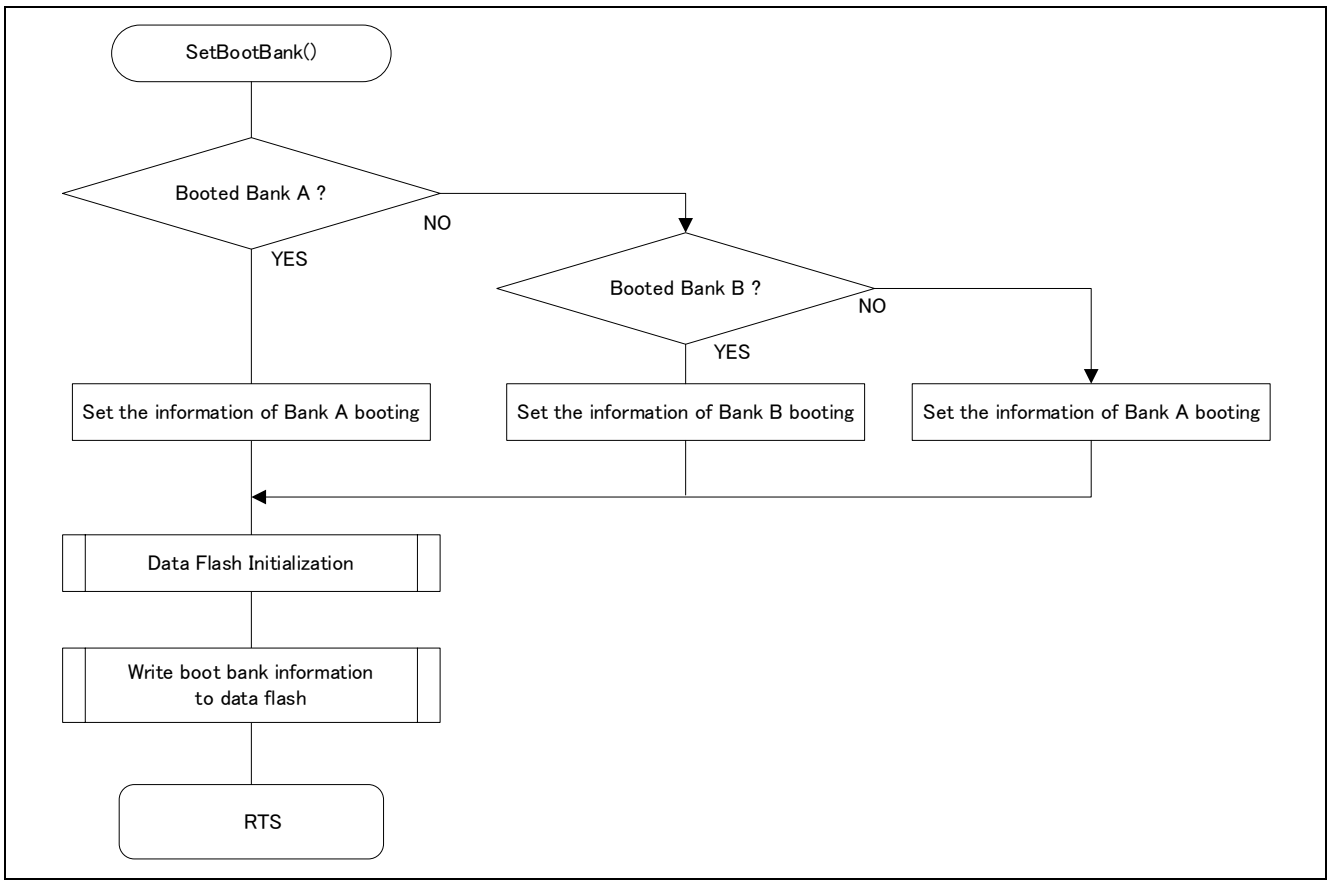

Figure 3-12 “SetBootBank () Function” Flowchart

“Operation Procedure ⑦”

4. Memory Allocation

4.1 Address Map

4.1.1 Address Allocation Diagram

Figure 4-1 shows the address allocation diagram.

Address	Section	
H'0000_0000	RESET	ROM(User Mat)
H'0000_0400	EIINTTBL	
	.rodata	
	.rosdata	
	.ROM.data	
	PE0.rodata	
	PE0.text	
	.secinfo	
	.syscall	
H'0001_4000	.Bank_textA	
	.Bank_text	
	.Bank_rosdata	
	.Bank_rodata	
H'0040_0000	PE1.rodata	
H'0800_0000	UBRESET	ROM(User Mat)
	.text	
H'FDA0_0000	PE1.bss	RAM
	PE1.stack.bss	
H'FDC0_0000	PE0.bss	
	PE0.stack.bss	
	.data	
	.bss	
H'FE00_0000	CRAM0.bss	
H'FE08_0000	CRAM1.bss	
H'FE0A_0000	RRAM.bss	

Address	FCU,FACI
H'FFA2_0000	FACI Command Issue Area

Figure 4-1 Address Allocation Diagram

Our Company's Website and Inquiry

Website
http://japan.renesas.com/

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

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/.