RL78/G23

Method of Setting Flash Read Protection

Introduction

This application note describes the flash read protection function of the RL78/G23.

Target Device

RL78/G23

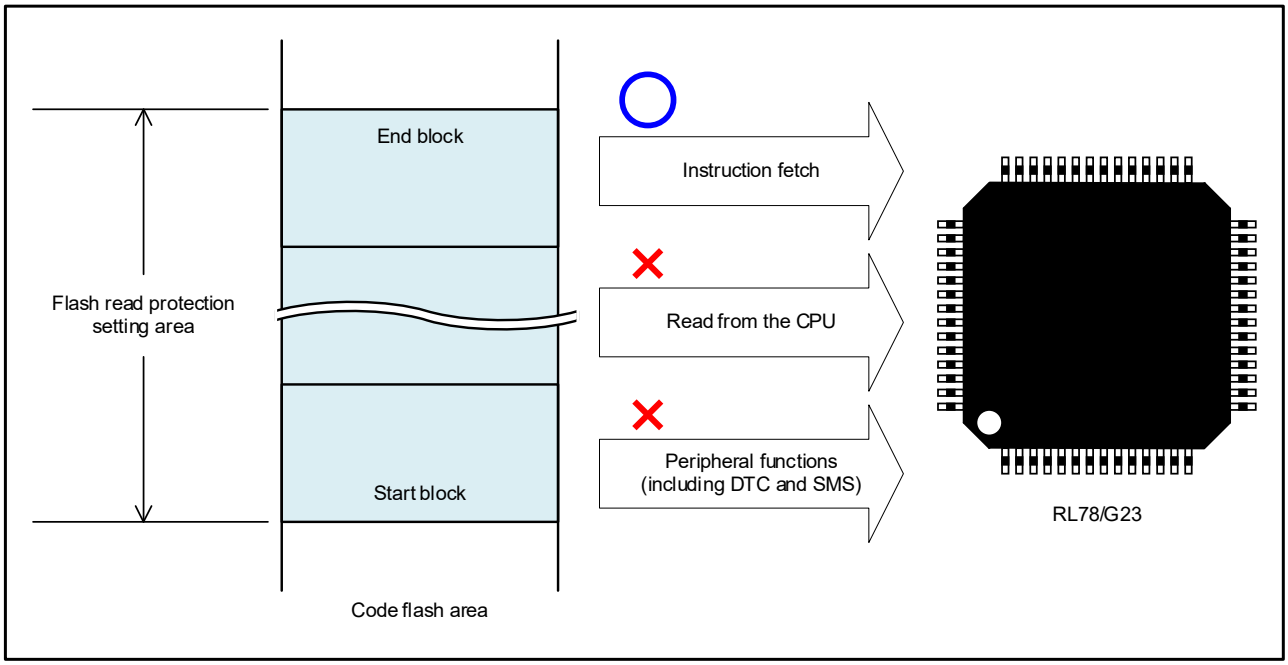
When applying the sample program covered in this application note to another microcomputer, modify the program according to the specifications for the target microcomputer and conduct an extensive evaluation of the modified program.

Contents

1. Overview

This application note describes flash read protection in regard to functions, usage, and other items.
The flash read protection function disables read accesses to a specified area in the code flash area. However, it enables instruction fetch by the CPU.

Figure 1-1 Overview of Flash Read Protection



2. Description of Functions

2.1 Setting of Flash Read Protection

To protect the code flash area by the flash read protection function, set the area to be protected in the extra area by using serial programming (by the flash memory programmer) or by using self-programming. Code flash areas within the ranges specified by the settings for the flash read protection start block and the flash read protection end block cannot be read. If a read-access disabled area is read, all values are read as FFH.

Figure 2-1 Start Block Setting

Item	Description
Content	Specify the start block number of the read-access disabled area. The specified block number is included in the read-access disabled area.
Setting range	From block 001H to the block number at the upper-limit address of flash memory
Restriction	Setting block 000H is prohibited.
Initial state	The initial setting is outside the specifiable range.
Setting method	Using the flash memory programmer or self-programming.

Figure 2-2 End Block Setting

Item	Description
Content	Specify the end block number of the read-access disabled area. The specified block number is included in the read-access disabled area.
Setting range	From start block number to the block number at the upper-limit address of code flash memory
Initial state	The initial setting is outside the specifiable range.
Setting method	Using the flash memory programmer or self-programming.

Remark For details on the relationship between the addresses and block numbers, refer to **Correspondence between Addresses and Block Numbers in Flash Memory** in the RL78/G23 User's Manual: Hardware.

2.2 Checking the Flash Read Protection Setting

The set value of flash read protection in the code flash area set in the extra area cannot be read. To check that flash read protection is set, read the read-access disabled area and confirm that FFH is read.

2.3 Releasing the Flash Read Protection Setting

To release the setting of the flash read protection function, change the settings for the flash read protection start block and the flash read protection end block (by using the flash memory programmer, or by self-programming).
The flash read protection setting set in the extra area cannot be released by erasing the code flash area.

2.4 Fixing the Flash Read Protection Setting and Releasing It

The flash read protection setting can be fixed by the flash memory programmer or by self-programming. The fixed flash read protection setting can be released only by the flash memory programmer. The fixed setting can be released only when the code flash area and the data flash area are blank with no setting in “Disabling Block Erase” and “Disabling Rewriting Boot Cluster 0”.

Figure 2-3 Fixing the Flash Read Protection Setting and Releasing It

Item	Description
Content	The settings for the flash read protection start block and the flash read protection end block are fixed or released. When the fixed settings are released, the settings for the flash read protection start block and the flash read protection end block are initialized.
Fixing method	Fix the settings using the flash memory programmer or self-programming.
Releasing method	Release the settings using the flash memory programmer.
Releasing conditions	Only the flash memory programmer can release the fixed settings only when the code flash area and the data flash area are blank with no setting in “Disabling Block Erase” and “Disabling Rewriting Boot Cluster 0”.

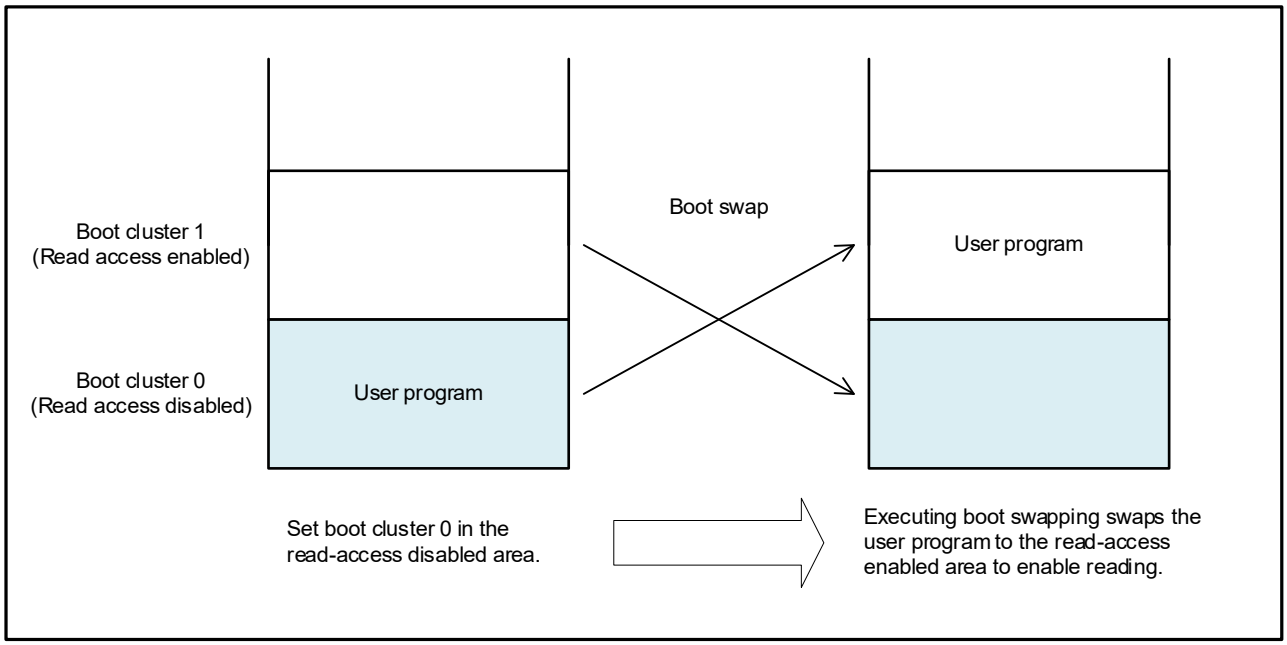
2.5 Notes on Debugging

The area specified as a read-access disabled area by the flash read protection setting cannot be read even by the on-chip debugger. Therefore, programs placed in read-access disabled areas cannot be debugged by the on-chip debugger. For this reason, when using the flash read protection function, set the flash read protection after program debugging is completed.

2.6 Notes on Boot Swapping

When a part of boot cluster 0 or boot cluster 1 is to be set as a part of the read-access disabled area, boot swapping may cause data in the read-access disabled area to be swapped with data in the read access-enabled area. To prevent this, when setting a part of boot cluster 0 or boot cluster 1 as part of the read-access disabled area, make the setting for prohibiting the rewriting of boot cluster 0 so as to prohibit boot swapping itself.

Figure 2-4 Boot Swap Operation



3. Software Settings

3.1 Placing a Program or Data in the Specific Area

Use section specification to place a program in the specific code flash area. Set the address so that the .text section and the .textf section (program code sections) are placed in a read-access disabled area.

- An example of section setting when an area (00004000H to 00006000) is set as a read-access disabled area

```
.text,.textf/04000
```

If constants used in the program are placed in a read-access disabled area, all of them are read as FFH. To avoid this problem, it is necessary to place the constants in an area that is not set as a read-access disabled area by the flash read protection.

In addition to the method of specifying the constant allocation area by the above-mentioned section specification, place constants by specifying the absolute address with the #pragma instruction, or by specifying the memory allocation area by using __near and __far in the source code.

- An example of C source whose absolute address is specified by the #pragma instruction

```
#pragma address X=0x7000
const int X;
```

In this example, constant X is placed at address 00007000H by the compiler.

- An example of C source whose memory allocation area is specified by __near and __far

```
const int __near A;
const int __far B;
```

In this example, constant A is placed in the near area and constant B is placed in the far area.

3.2 Referencing Functions or Subroutines Placed in Read-Access Disabled Areas

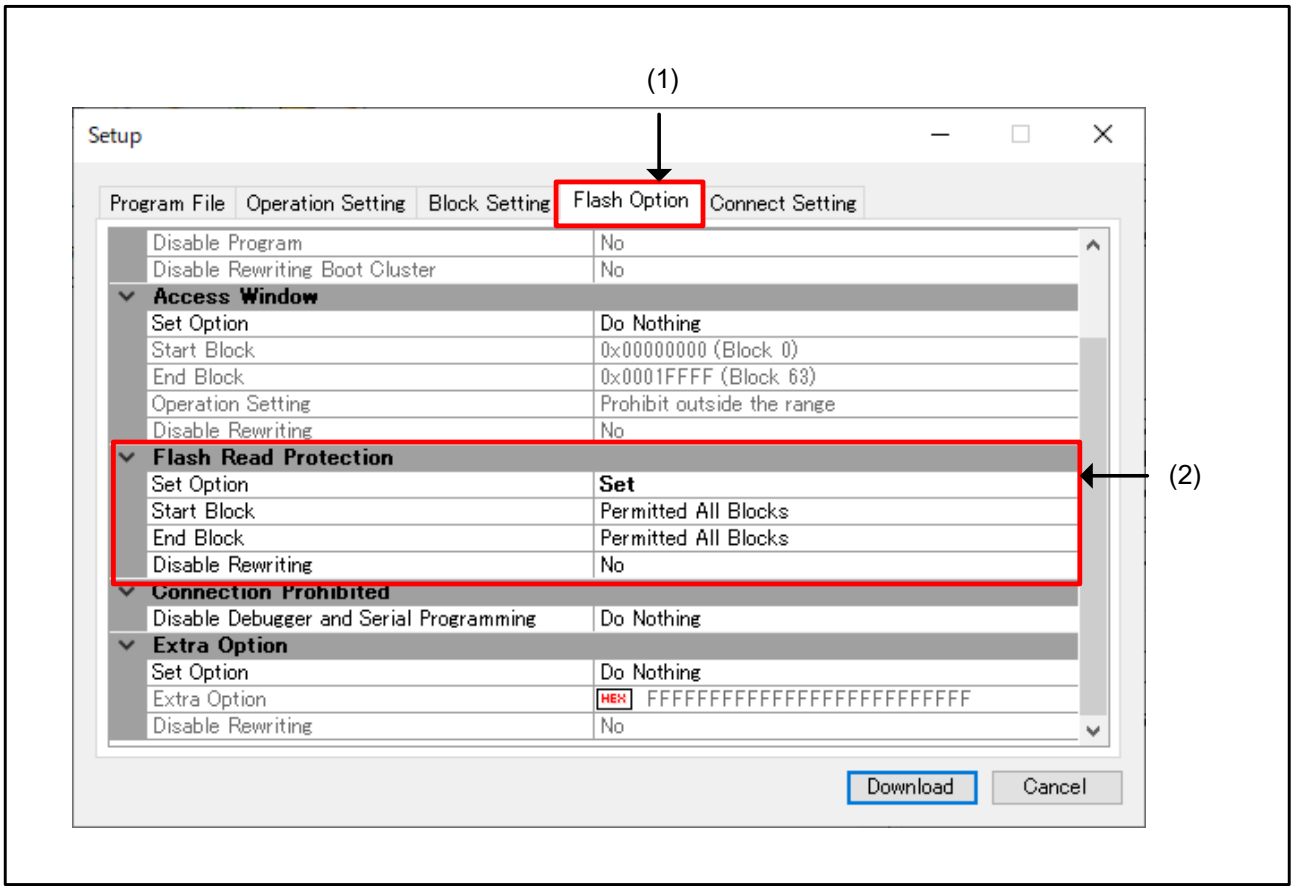
Functions or subroutines placed in read-access disabled areas can be called as usual.

4. Setting Procedures

4.1 Flash Memory Programmer FP6

Perform the following procedure to set flash read protection using FP6.

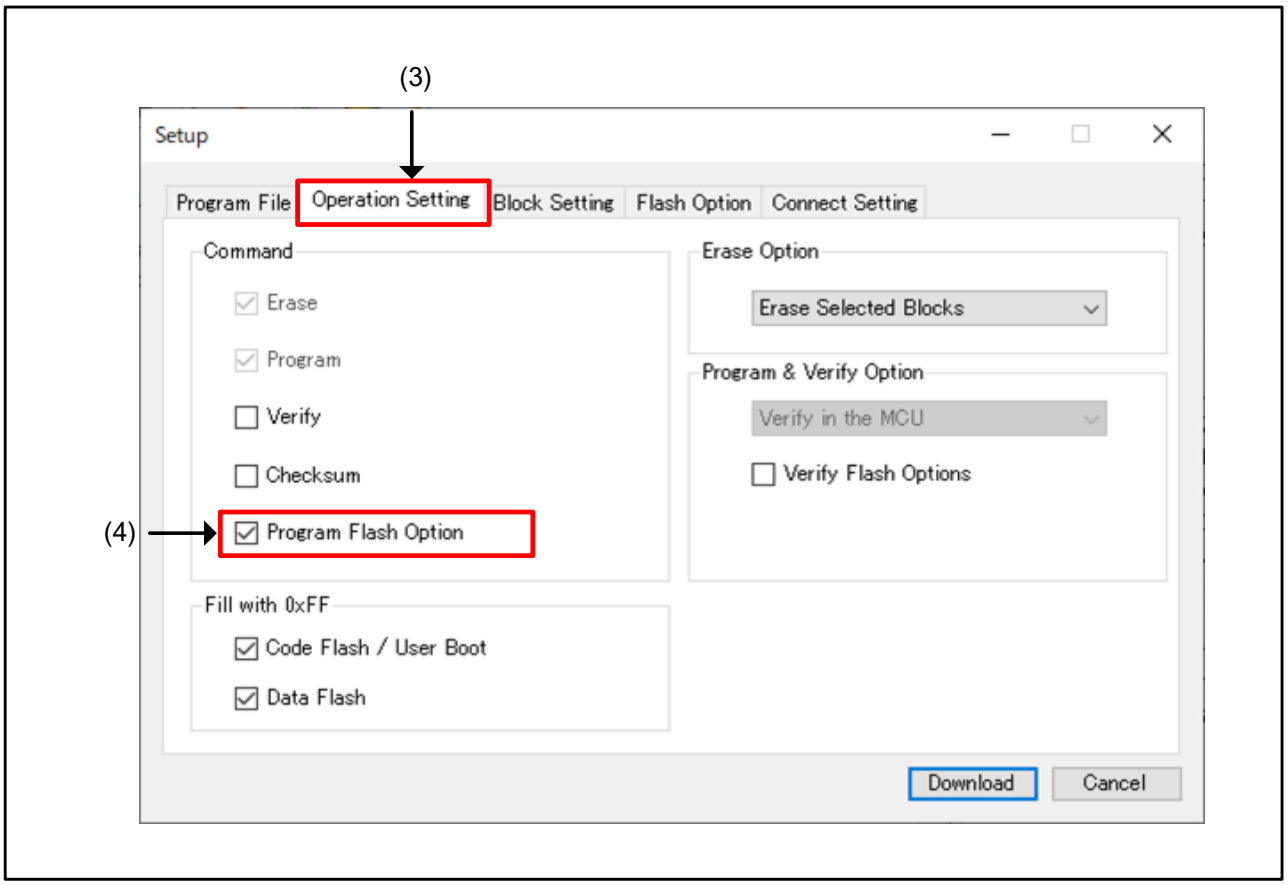
Figure 4-1 FP6 Flash Read Protection Setting Procedure (1/3)



(1) From the [Setup] dialog box of FP6, select the [Flash Option] tab.
(2) Set each item in Flash Read Protection.

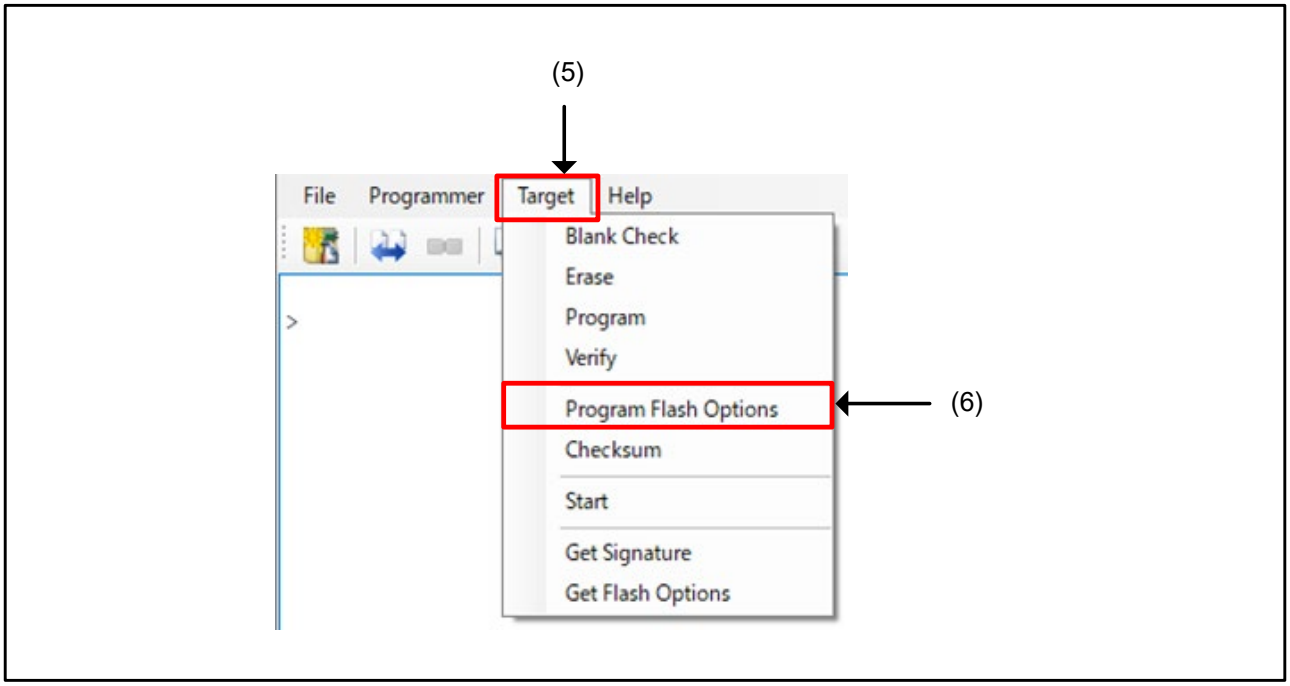
- Set Option
  - “Set”: Flash read protection is set.
  - “Do Nothing”: Flash read protection is not set.
- Start Block
  Set the flash read protection start block.
- End Block
  Set the flash read protection end block.
- Disable Rewriting
  - “Yes”: “Fixed” setting for flash read protection is made.
  - “No”: “Fixed” setting for flash read protection is not made.

Figure 4-2 FP6 Flash Read Protection Setting Procedure (2/3)



(3) From the [Setup] dialog box of FP6, select the [Operation Setting] tab.
(4) From Command, select “Program Flash Option”.

Figure 4-3 FP6 Flash Read Protection Setting Procedure (3/3)

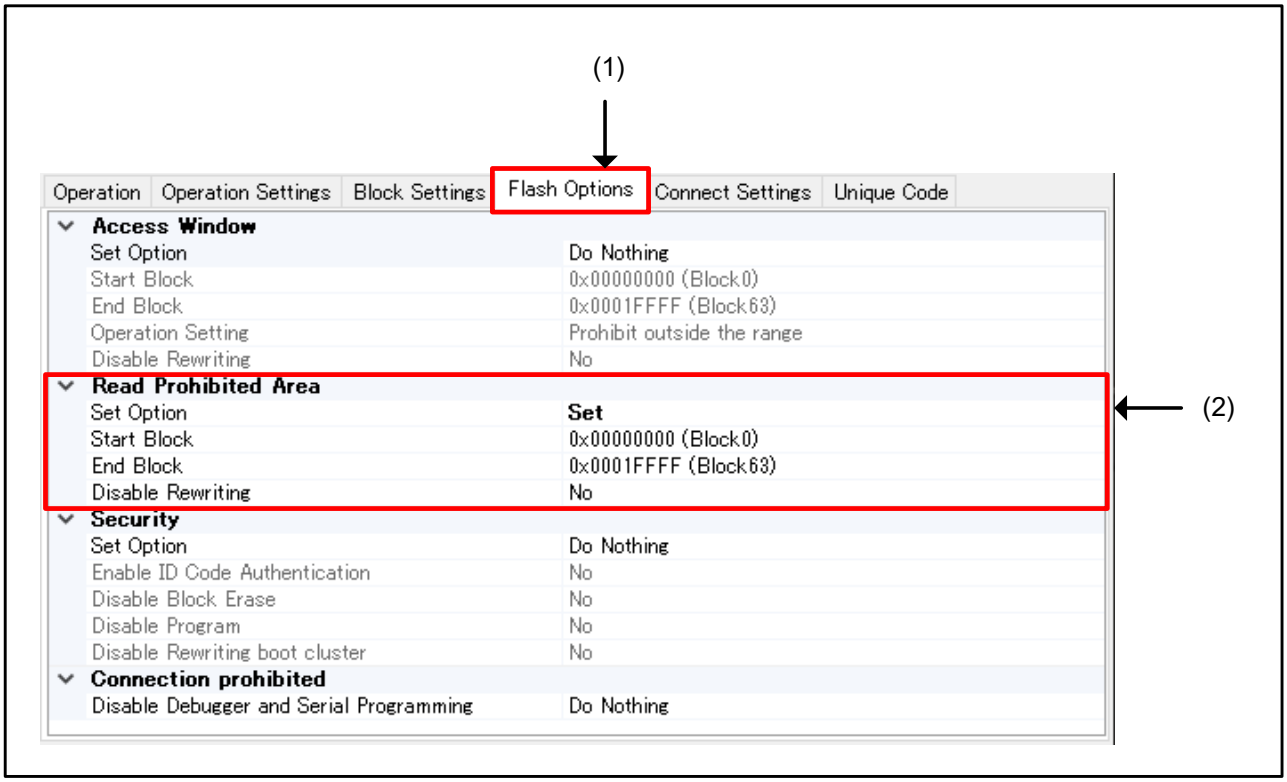


(5) Select [Target] in the menu bar of FP6.
(6) From the displayed drop-down menu, select [Program Flash Options] to start the flash read protection setting.

4.2 Flash Memory Programmer RFP

Perform the following procedure to set flash read protection using RFP.

Figure 4-4 RFP Flash Read Protection Setting Procedure (1/3)



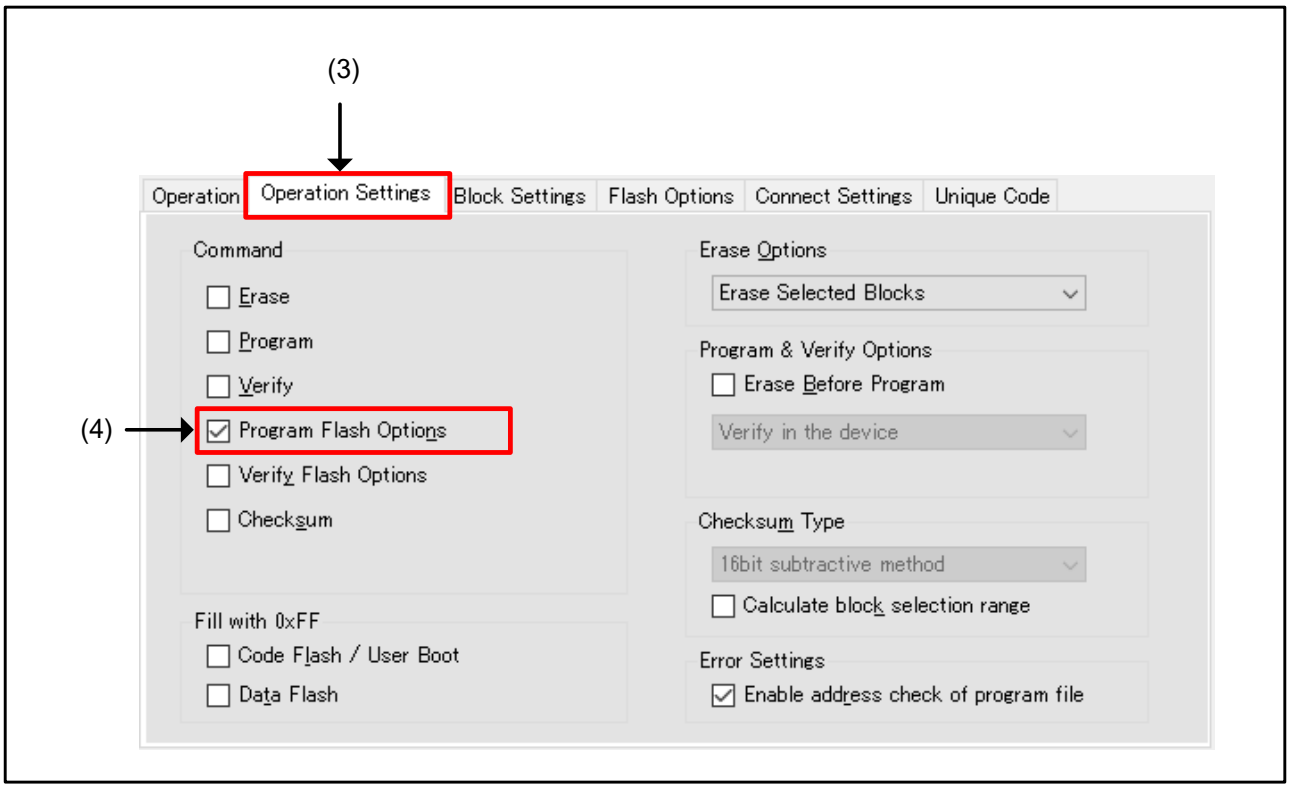
(1) From the [Tab window] on the [Main window] of RFP, select [Flash Options].
(2) Set each item in Read Prohibited Area.

- Set Option
  - “Set”: Flash read protection is set.
  - “Do Nothing”: Flash read protection is not set.
- Start Block

  Set the flash read protection start block.
- End Block

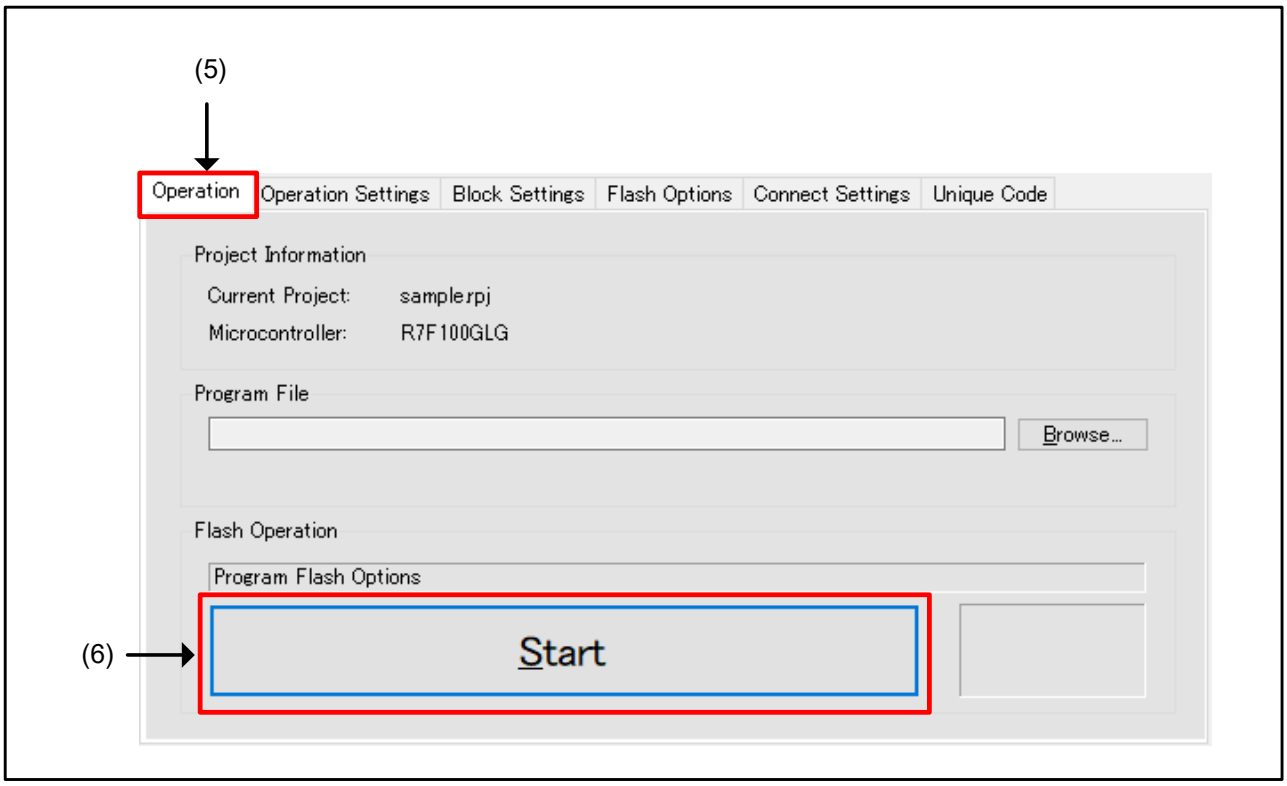
  Set the flash read protection end block.
- Disable Rewriting
  - “Yes”: “Fixed” setting for flash read protection is made.
  - “No”: “Fixed” setting for flash read protection is not made.

Figure 4-5 RFP Flash Read Protection Setting Procedure (2/3)



(3) From the [Tab window] on the [Main window] of RFP, select [Operation Settings].
(4) From Command, select “Program Flash Options”.

Figure 4-6 RFP Flash Read Protection Setting Procedure (3/3)



(5) From the [Tab window] on the [Main window] of RFP, select [Operation].
(6) Click “Start” to start the flash read protection setting.

4.3 Setting Change and Fixed Setting Release Procedures

4.3.1 Changing Unreadable Area Setting

To change the target protection area after the flash read protection setting, change the settings for the flash read protection start block and the flash read protection end block. Change areas using the flash read protection setting procedure.

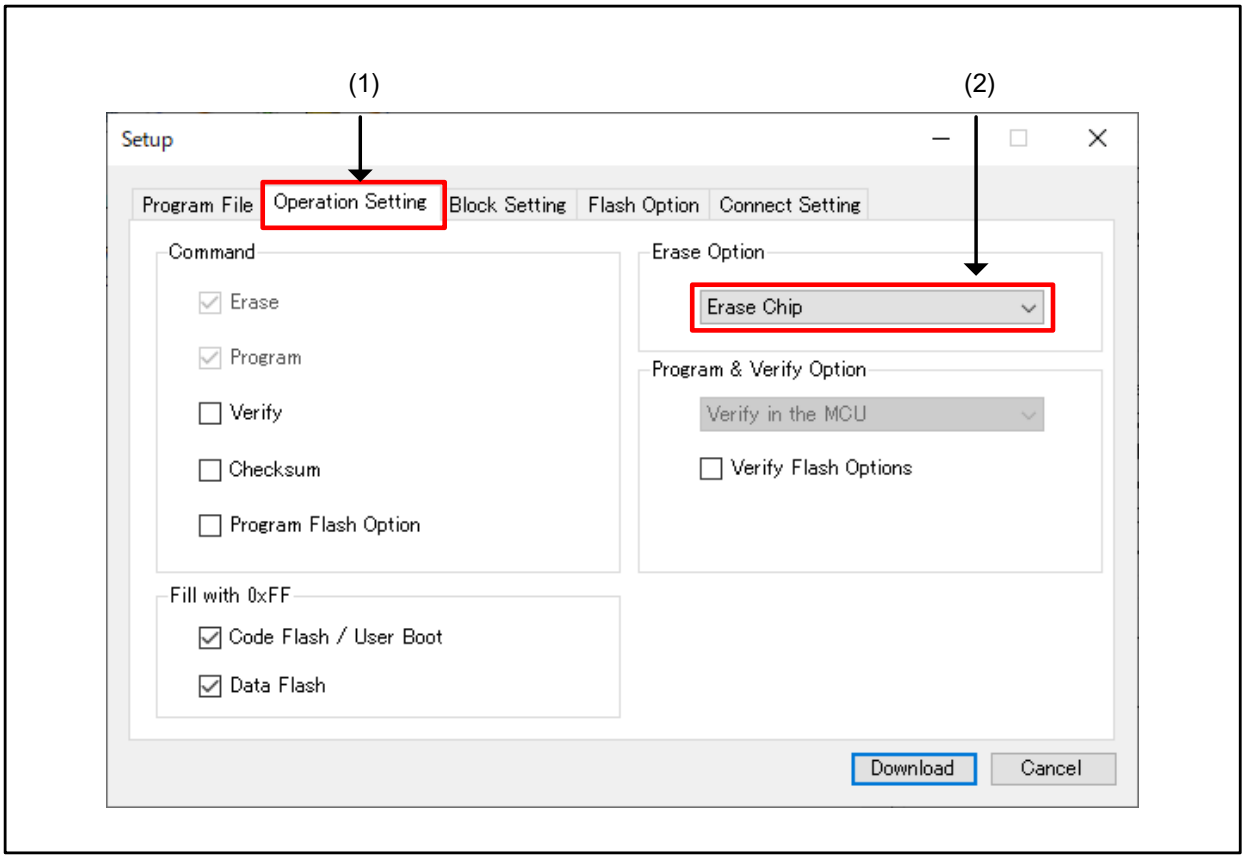
4.3.2 Releasing the Fixed Flash Read Protection Setting

To release the fixed flash read protection setting, execute “Erase Chip” for devices.

4.3.2.1 Flash Memory Programmer FP6

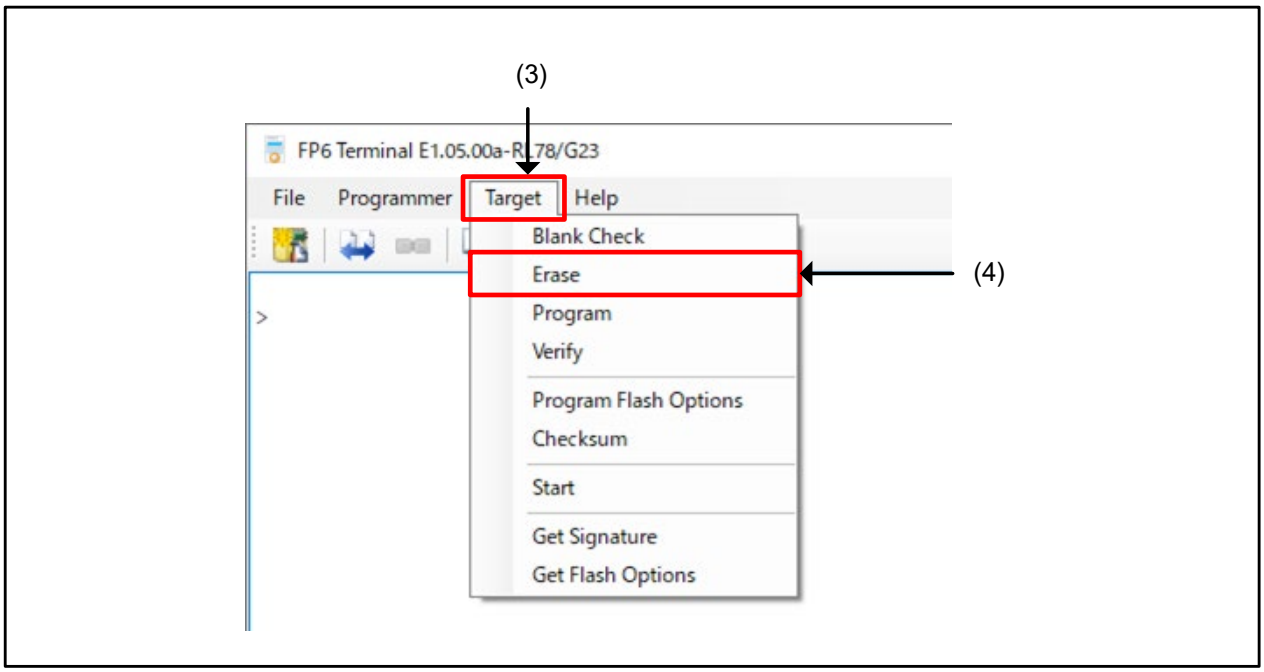
Perform the following procedure to release flash read protection using FP6.

Figure 4-7 FP6 Flash Read Protection Releasing Procedure (1/2)



(1) From the [Setup] dialog box of FP6, select the [Operation Setting] tab.
(2) In Erase Option, select “Erase Chip”.

Figure 4-8 FP6 Flash Read Protection Releasing Procedure (2/2)

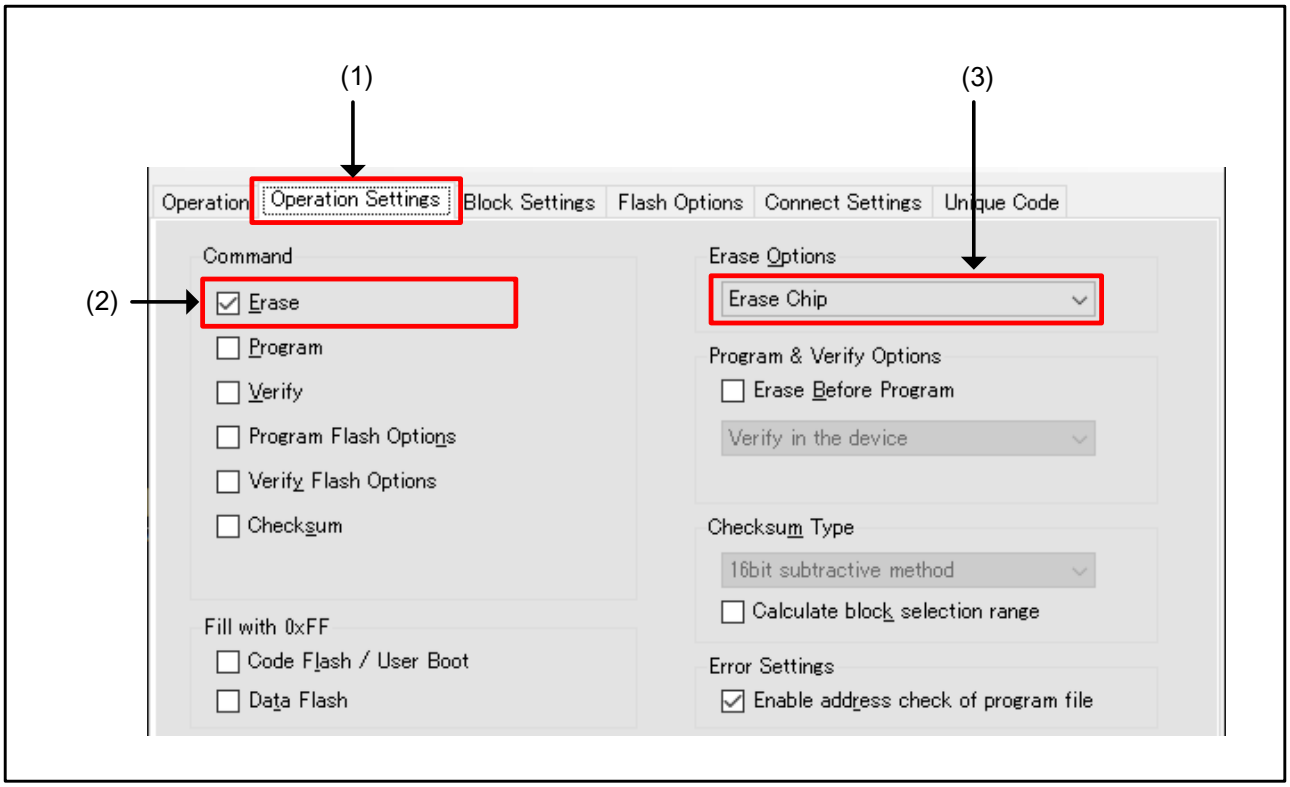


(3) Select [Target] in the menu bar of FP6.
(4) From the displayed drop-down menu, select [Erase] to erase the chip of the device and release the flash read protection setting.

4.3.2.2 Flash Memory Programmer RFP

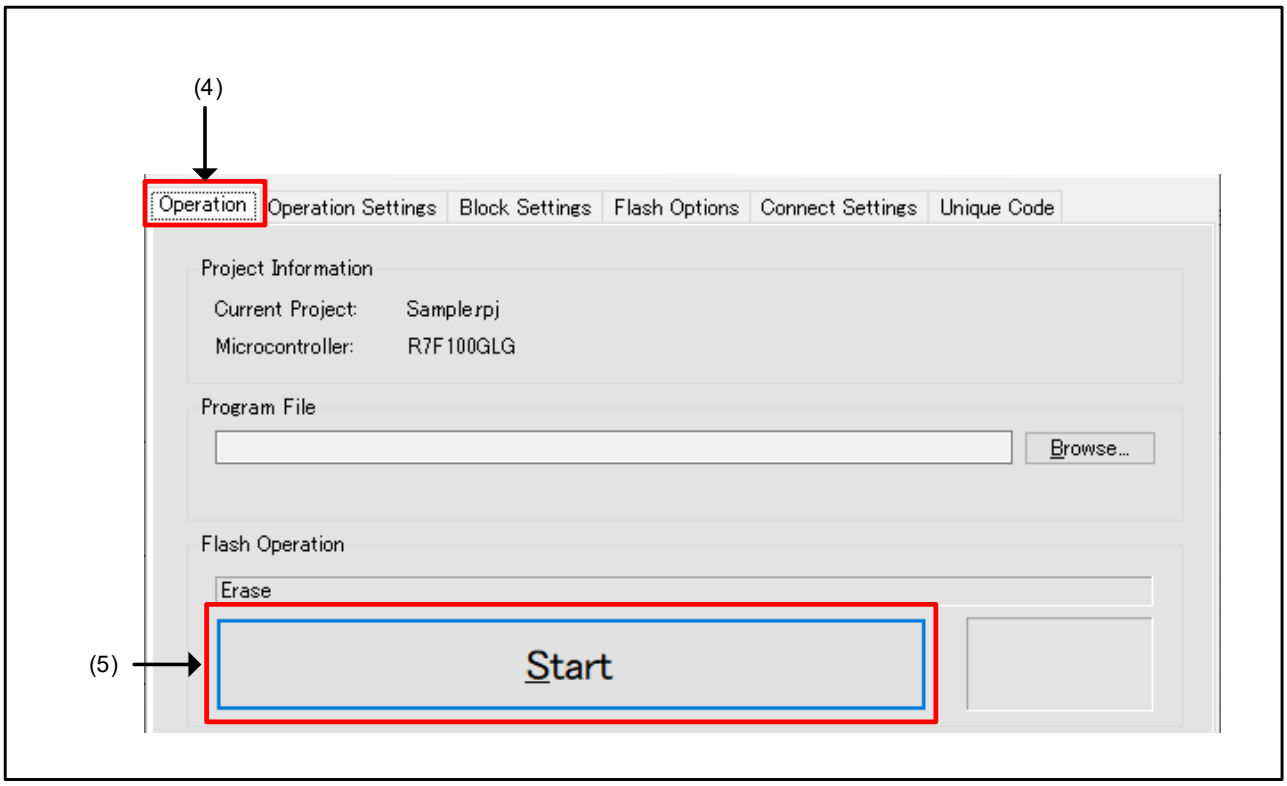
Perform the following procedure to set flash read protection using RFP.

Figure 4-9 RFP Flash Read Protection Setting Procedure (1/2)



(1) From the [Tab window] on the [Main window] of RFP, select [Operation Settings].
(2) From Command, select “Erase”.
(3) From Erase Options, select “Erase Chip”.

Figure 4-10 RFP Flash Read Protection Setting Procedure (2/2)



(4) From the [Tab window] on the [Main window] of RFP, select [Operation].
(5) Click “Start” to erase the chip of the device and release the flash read protection setting.

5. Reference Documents

RL78/G23 User’s Manual: Hardware (R01UH0896)
RL78 family user's manual software (R01US0015)
PG-FP6 Flash Memory Programmer User’s Manual (R20UT4469)
Renesas Flash Programmer Flash memory programming software User’s Manual (R20UT4540)
The latest versions can be downloaded from the Renesas Electronics website.

Technical update
The latest versions can be downloaded from the Renesas Electronics website.

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	2021.04.13	-	First Edition

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/.