M16C/5LD, 56D, 5L, 56, 5M, and 57 Groups

Flash Memory Security System

R01AN0837EJ0100
Rev. 1.00
Jan. 31, 2012

Abstract

This document describes the flash memory security system for the M16C/5LD, 56D, 5L, 56, 5M, and 57 Groups. This document describes setting methods to restrict accesses for program, read, and erase operations in standard serial I/O mode and parallel I/O mode of flash memory rewrite mode.
In this document, the internal flash memory is referred to simply as flash memory.

Products

M16C/5LD, 56D, 5L, 56, 5M, and 57 Groups

When using this application note with other Renesas MCUs, careful evaluation is recommended after making modifications to comply with the alternate MCU.

Contents

1. Specifications

Access to the flash memory can be restricted according to use. Table 1.1 lists Adding Security During Software Development and Table 1.2 lists Adding Security During Mass Production.
Refer to 3.4 “Security when Using User Boot Mode” for details on using the user boot.

Table 1.1 Adding Security During Software Development (1, 2)

Security Level	Purpose	Serial Programmer		Parallel Programmer		Reference
		Read	Program	Read	Program	
None	Development has priority. Anyone can access the flash memory.	✓	✓	✓	✓	3.1.1 “No Security”
Low	Simple security is required. If the ID code is lost, all data in the flash memory can be erased with a serial programmer.	◆	◆	✓	✓	3.1.2 “Security Level 1”

Notes:
1. ✓: Available, ◆: Available when the ID code is ready.
2. The user boot can be started even if the ID code is “Protect”.

Table 1.2 Adding Security During Mass Production (1, 2)

Security Level	Purpose	Serial Programmer		Parallel Programmer		Reference
		Read	Program	Read	Program	
Low ↕ High	Only those who know the ID can access the flash memory.	◆	◆	×	×	3.1.3 “Security Level 2”
	No one can read the flash memory. The flash memory can be updated.	×	◆	×	×	3.1.4 “Security Level 3”
	All accesses to the flash memory by programmers are disabled.	×	×	×	×	3.1.5 “Security Level 4”

Notes:
1. ◆: Available when the ID code is ready., ×: Not available
2. The user boot can be started even if the ID code is “Protect”.

2. Reference Application Notes

Application notes associated with this application note are listed below. Refer to these application notes for additional information.

- M16C/5LD Group High-performance Embedded Workshop Start-up Program in C (R01AN0048EJ)
- M16C/5L Group High-performance Embedded Workshop Start-up Program in C (R01AN0049EJ)
- M16C/5M Group High-performance Embedded Workshop Start-up Program in C (R01AN0050EJ)

3. Peripheral Functions

3.1 Flash Memory Security

This section describes the settings for each security level, and their advantages and disadvantages. Refer to 3.2 “ID Code Setting” and 3.3 “ROM Code Protect Setting” for details on setting the ID code and ROM code protect.

3.1.1 No Security

No restrictions are placed on accessing the flash memory with a serial or parallel programmers. Table 3.1 lists the Settings and Table 3.2 lists the Advantage and Disadvantage.

Table 3.1 Settings

ID Code	ROM Code Protect
FFFFFFFFFFFFFFh (default value)	No setting required

Table 3.2 Advantage and Disadvantage

Advantage	Disadvantage
The ID code does not need to be managed.	Anyone can access to the flash memory with a serial or a parallel programmer. Therefore the flash memory may be read, programmed, or erased anytime.

3.1.2 Security Level 1

Access to the flash memory with a serial programmer is restricted to those who know the ID code. Access to the flash memory with a parallel programmer is not restricted.
Table 3.3 lists the Settings and Table 3.4 lists the Advantages and Disadvantages.

Table 3.3 Settings

ID Code	ROM Code Protect
Arbitrary ID (except for “Protect” and “ALeRASE”)	No setting required

Table 3.4 Advantages and Disadvantages

Advantage	Disadvantage
• Only those who know the ID code can access the flash memory. • If the ID code is lost, all data in the flash memory can be erased using the forced erase function including the ID code area. • The flash memory can be accessed with a parallel programmer.	• After data in the flash memory is erased with the forced erase function, the flash memory may be programmed. • Anyone can access the flash memory with a parallel programmer. Therefore the flash memory may be read, programmed, or erased anytime.

3.1.3 Security Level 2

Access to the flash memory with a serial programmer is restricted to those who know the ID code. Access to the flash memory with a parallel programmer is disabled.
Table 3.5 lists the Settings and Table 3.6 lists the Advantages and Disadvantage.

Table 3.5 Settings

ID Code	ROM Code Protect
Arbitrary ID (except for “Protect” and “ALeRASE”)	Setting required

Table 3.6 Advantages and Disadvantage

Advantage	Disadvantage
• Access to the flash memory with a serial programmer is not permitted without the ID code. • The forced erase function is disabled.	If the ID code is lost, access to the flash memory is not permitted.

3.1.4 Security Level 3

When the ID code for accessing the flash memory with a serial programmer is validated, all data in the flash memory is erased and read access is disabled. Access with a parallel programer is also disabled.
Table 3.7 lists the Settings and Table 3.8 lists the Advantages and Disadvantages.

Table 3.7 Settings

ID Code	ROM Code Protect
“ALeRASE”	Setting required

Table 3.8 Advantages and Disadvantages

Advantage	Disadvantage
• When accessing the flash memory with a serial programmer, all data in the flash memory is erased. As a result, the flash memory cannot be read. • Management of the ID code is not required as it is predefined.	• Even the developer cannot read the flash memory as all data in the flash memory is erased when accessing it with a serial programmer. • The flash memory may be programmed after it is erased with the forced erase function.

3.1.5 Security Level 4

Access to the flash memory with serial and parallel programmers is disabled.
Table 3.9 lists the Settings and Table 3.10 lists the Advantages and Disadvantage.

Table 3.9 Settings

ID Code	ROM Code Protect
“Protect”	Setting required

Table 3.10 Advantages and Disadvantage

Advantage	Disadvantage
• Accessing the flash memory with a serial or a parallel programmer is disabled. As a result, the flash memory cannot be read, programmed, or erased. • The forced erase function is disabled.	The flash memory cannot be programmed at all.

3.2 ID Code Setting

The ID code is 7-byte data stored in 1-byte units, in the addresses, in the following order: 0FFFDFh, 0FFFE3h, 0FFFEBh, 0FFFEFh, 0FFFF3h, 0FFFF7h, and 0FFFFBh (ID code storage address). The ID code can be set by writing the program with the ID code setting in these addresses. Set arbitrary values in the ID code storage address. Select the C source startup Application in the High-performance Embedded Workshop (HEW), and create a new project workspace to generate a fvector.c file. fvector.c has setting codes for the ID code.

Figure 3.1 shows the Setting Code for the ID Code Created in fvector.c.

fvector.c uses the extended function directive command “.id”. The 7-byte ID code set in the ID code storage address can be described using the extended function directive command “.id”.

“FFFFFFFFFFFFFFh” is set as the default ID code value. Change the default value to change the ID code setting.

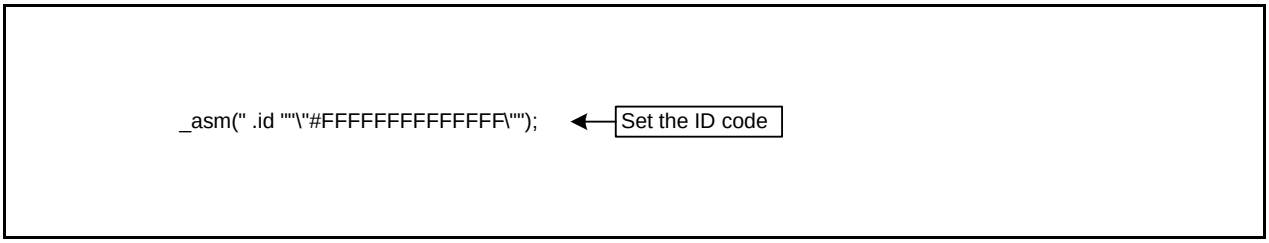

Figure 3.1 Setting Code for the ID Code Created in fvector.c

3.3 ROM Code Protect Setting

The ROM code protect can be set with bits ROMCP1 and ROMCR in the optional function select 1 address (OFS1). To enable the ROM code protect, set the ROMCP1 bit to 0 and the ROMCR bit to 1 in the OFS1 address. The OFS1 address is not a special function register (SFR), thus it cannot be rewritten by a program. Write appropriate values to the OFS1 address when writing a program to the flash memory. Select the C source startup Application in the HEW, and create a new project workspace to generate a fvector.c file. fvector.c has setting codes for the OFS1 address.

Figure 3.2 shows the Setting Code for the OFS1 Address Created in fvector.c.

fvector.c uses the extended function directive command “.ofsreg”. 1-byte code set in the OFS1 address can be described using the extended function directive command “.ofsreg”.

“FFh” is set as the default value. Change the default value to enable or disable the ROM code protect.

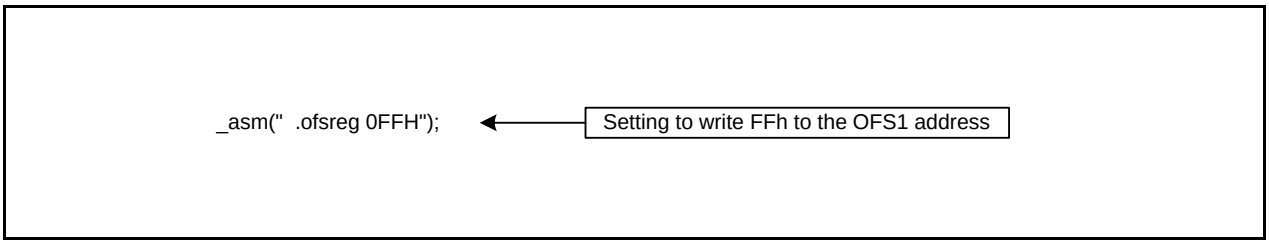

Figure 3.2 Setting Code for the OFS1 Address Created in fvector.c

3.4 Security when Using User Boot Mode

When using user boot mode, the ID code is not determined as shown in Figure 3.3 “Mode Determination”. Thus the security setting with the ID code or the ROM code protect is not valid, and the security described in 1. “Specifications” is not available, either.

Set security for user boot mode using the user boot program.

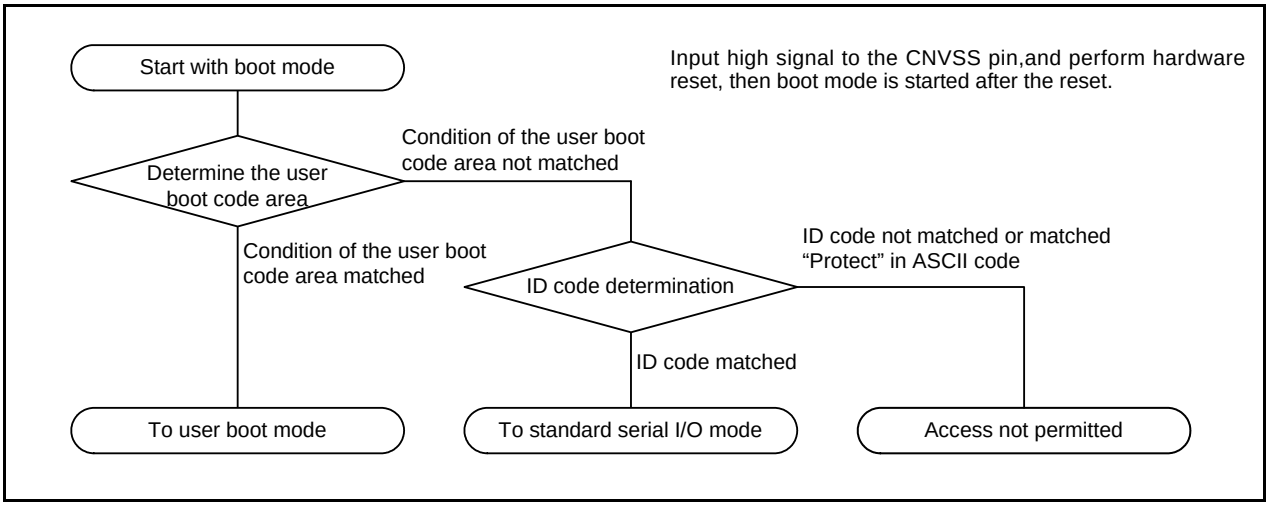

Figure 3.3 Mode Determination

4. Reference Documents

M16C/5LD Group, M16C/56D Group User's Manual: Hardware Rev.1.20
M16C/5L Group, M16C/56 Group User's Manual: Hardware Rev.1.10
M16C/5M Group, M16C/57 Group User's Manual: Hardware Rev.1.10
The latest versions can be downloaded from the Renesas Electronics website.

Technical Update/Technical News
The latest information can be downloaded from the Renesas Electronics website.

C Compiler Manual
M16C Series, R8C Family C Compiler Package V.5.45
C Compiler User's Manual Rev.2.00
The latest version can be downloaded from the Renesas Electronics website.

Website and Support

Renesas Electronics website
http://www.renesas.com/

Inquiries
http://www.renesas.com/inquiry

Revision History	M16C/5LD, 56D, 5L, 56, 5M, and 57 Groups Flash Memory Security System

Rev.	Date	Description	
		Page	Summary
1.00	Jan. 31, 2012	—	First edition issued

General Precautions in the Handling of MPU/MCU Products

The following usage notes are applicable to all MPU/MCU products from Renesas. For detailed usage notes on the products covered by this manual, refer to the relevant sections of the manual. If the descriptions under General Precautions in the Handling of MPU/MCU Products and in the body of the manual differ from each other, the description in the body of the manual takes precedence.

1. Handling of Unused Pins
   Handle unused pins in accord 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 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. Unused pins should be handled as described under Handling of Unused Pins in the manual.
2. Processing at Power-on
   The state of the product is undefined at the moment 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 moment 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 moment 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 moment when power is supplied until the power reaches the level at which resetting has been specified.
3. Prohibition of Access to Reserved Addresses
   Access to reserved addresses is prohibited.
   — The reserved addresses are provided for the possible future expansion of functions. Do not access these addresses; the correct operation of LSI is not guaranteed if they are accessed.
4. Clock Signals
   After applying a reset, only release the reset line after the operating clock signal has become stable. When switching the clock signal during program execution, wait until the target clock signal has 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. Moreover, 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.
5. Differences between Products
   Before changing from one product to another, i.e. to one with a different part number, confirm that the change will not lead to problems.
   — The characteristics of MPU/MCU in the same group but having different part numbers may differ because of the differences in internal memory capacity and layout pattern. When changing to products of different part numbers, implement a system-evaluation test for each of the products.

Notice

1. All information included in this document is current as of the date this document is issued. Such information, however, is subject to change without any prior notice. Before purchasing or using any Renesas Electronics products listed herein, please confirm the latest product information with a Renesas Electronics sales office. Also, please pay regular and careful attention to additional and different information to be disclosed by Renesas Electronics such as that disclosed through our website.
2. Renesas Electronics does not assume any liability for infringement of 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. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
3. You should not alter, modify, copy, or otherwise misappropriate any Renesas Electronics product, whether in whole or in part.
4. 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 of these circuits, software, and information in the design of your equipment. Renesas Electronics assumes no responsibility for any losses incurred by you or third parties arising from the use of these circuits, software, or information.
5. When exporting the products or technology described in this document, you should comply with the applicable export control laws and regulations and follow the procedures required by such laws and regulations. You should not use Renesas Electronics products or the technology described in this document for any purpose relating to military applications or use by the military, including but not limited to the development of weapons of mass destruction. Renesas Electronics products and technology may 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.
6. Renesas Electronics has used reasonable care in preparing the information included in this document, but Renesas Electronics does not warrant that such information is error free. Renesas Electronics assumes no liability whatsoever for any damages incurred by you resulting from errors in or omissions from the information included herein.
7. Renesas Electronics products are classified according to the following three quality grades: "Standard", "High Quality", and "Specific". The recommended applications for each Renesas Electronics product depends on the product's quality grade, as indicated below. You must check the quality grade of each Renesas Electronics product before using it in a particular application. You may not use any Renesas Electronics product for any application categorized as "Specific" without the prior written consent of Renesas Electronics. Further, you may not use any Renesas Electronics product for any application for which it is not intended without the prior written consent of Renesas Electronics. Renesas Electronics shall not be in any way liable for any damages or losses incurred by you or third parties arising from the use of any Renesas Electronics product for an application categorized as "Specific" or for which the product is not intended where you have failed to obtain the prior written consent of Renesas Electronics. The quality grade of each Renesas Electronics product is "Standard" unless otherwise expressly specified in a Renesas Electronics data sheets or data books, etc.
   - "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; and industrial robots.
   - "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control systems; anti-disaster systems; anti-crime systems; safety equipment; and medical equipment not specifically designed for life support.
   - "Specific": Aircraft; aerospace equipment; submersible repeaters; nuclear reactor control systems; medical equipment or systems for life support (e.g. artificial life support devices or systems), surgical implantations, or healthcare intervention (e.g. excision, etc.), and any other applications or purposes that pose a direct threat to human life.
8. You should use the Renesas Electronics products described in this document within the range specified by Renesas Electronics, especially with respect to the maximum rating, operating supply voltage range, movement power voltage range, heat radiation characteristics, installation and other product characteristics. Renesas Electronics shall have no liability for malfunctions or damages arising out of the use of Renesas Electronics products beyond such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of its products, semiconductor products have specific characteristics such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Further, Renesas Electronics products are not subject to radiation resistance design. Please be sure to implement safety measures to guard them against the possibility of physical injury, and injury or damage caused by fire in the event of the failure of a Renesas Electronics product, 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, please evaluate the safety of the final products or system 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. Please use Renesas Electronics products in compliance with all applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive. Renesas Electronics assumes no liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. This document may not be reproduced or duplicated, in any form, in whole or in part, without prior written consent of Renesas Electronics.
12. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products, or if you have any other inquiries.

(Note 1) "Renesas Electronics" as used in this document means Renesas Electronics Corporation and also includes its majority-owned subsidiaries.

(Note 2) "Renesas Electronics product(s)" means any product developed or manufactured by or for Renesas Electronics.

RENESAS

SALES OFFICES Renesas Electronics Corporation http://www.renesas.com

Refer to "http://www.renesas.com/" for the latest and detailed information.

Renesas Electronics America Inc.
2880 Scott Boulevard Santa Clara, CA 95050-2554, U.S.A.
Tel: +1-408-588-6000, Fax: +1-408-588-6130

Renesas Electronics Canada Limited
1101 Nicholson Road, Newmarket, Ontario L3Y 9C3, Canada
Tel: +1-905-898-5441, Fax: +1-905-898-3220

Renesas Electronics Europe Limited
Dukes Meadow, Millboard Road, Bourne End, Buckinghamshire, SL8 5FH, U.K
Tel: +44-1628-585-100, Fax: +44-1628-585-900

Renesas Electronics Europe GmbH
Arcadiastrasse 10, 40472 Düsseldorf, Germany
Tel: +49-211-65030, Fax: +49-211-6503-1327

Renesas Electronics (China) Co., Ltd.
7th Floor, Quantum Plaza, No.27 ZhiChunLu Haidian District, Beijing 100083, P.R.China
Tel: +86-10-8235-1155, Fax: +86-10-8235-7679

Renesas Electronics (Shanghai) Co., Ltd.
Unit 204, 205, AZIA Center, No.1233 Lujiazui Ring Rd., Pudong District, Shanghai 200120, China
Tel: +86-21-5877-1818, Fax: +86-21-6887-7858 / -7898

Renesas Electronics Hong Kong Limited
Unit 1601-1613, 16/F., Tower 2, Grand Century Place, 193 Prince Edward Road West, Mongkok, Kowloon, Hong Kong
Tel: +852-2886-9318, Fax: +852 2886-9022/9044

Renesas Electronics Taiwan Co., Ltd.
13F, No. 363, Fu Shing North Road, Taipei, Taiwan
Tel: +886-2-8175-9600, Fax: +886 2-8175-9670

Renesas Electronics Singapore Pte. Ltd.
1 harbourFront Avenue, #06-10, keppel Bay Tower, Singapore 098632
Tel: +65-6213-0200, Fax: +65-6278-8001

Renesas Electronics Malaysia Sdn.Bhd.
Unit 906, Block B, Menara Amcorp, Amcorp Trade Centre, No. 18, Jln Persiaran Barat, 46050 Petaling Jaya, Selangor Darul Ehsan, Malaysia
Tel: +60-3-7955-9390, Fax: +60-3-7955-9510

Renesas Electronics Korea Co., Ltd.
11F., Samik Lavied' or Bldg., 720-2 Yeoksam-Dong, Kangnam-Ku, Seoul 135-080, Korea
Tel: +82-2-558-3737, Fax: +82-2-558-5141

Colophon 1.1