RISC-V

Third-Party Program Protection

Introduction

This application note describes the third-party program protection functionality of the RISC-V.

As used here, the term “third-party program” refers to valuable software IP supplied in formats such as libraries. The security functions of the RISC-V can be employed to prevent unauthorized usage of such software IP.

Third-party program protection makes use of the following functions of the RISC-V.

- Memory protection function (flash read protection)
- Unique ID
- User ID

Contents

1. Overview

1.1 About This Application Note

This application note describes the third-party program (software IP) protection that can be implemented using the functions of the RISC-V.

1.2 Background of Demand for Third-Party Program (software IP) Protection

software IP is subject to issues such as the following.

- Even when software IP is supplied in binary format, it can be duplicated and multiple copies can be used at the destination.
- Even when the software IP has been programmed to an MCU supplied as a finished product, it can be read from the flash memory and analyzed.

1.3 Possible Countermeasures

Some examples of countermeasures that can be implemented on the RISC-V to protect software IP are described below.

- Memory protection
  This approach prevents the software IP program code in the flash memory from being read.
  The memory protection function can be used to prohibit a specific area of the code flash from being read. By supplying MCUs with their software IP programmed in a read-prohibited area, strong protection is provided for the IP.
  ⇒ Refer to 2.1, MemoryMemory Protection (Flash Read Protection) .

- Startup control
  This approach checks an ID programmed in the flash memory when the software IP is launched.
  This approach is suitable for cases where the developer supplies the software IP in binary format.
  ⇒ Refer to 2.2.Startup Control (Link to Unique ID)
  ⇒ Refer to 2.3, Startup Startup Control (Link to User ID).

Purpose	Control	Function
software IP protection	Memory protection	Flash read protection
	Start control	Unique ID
		User ID

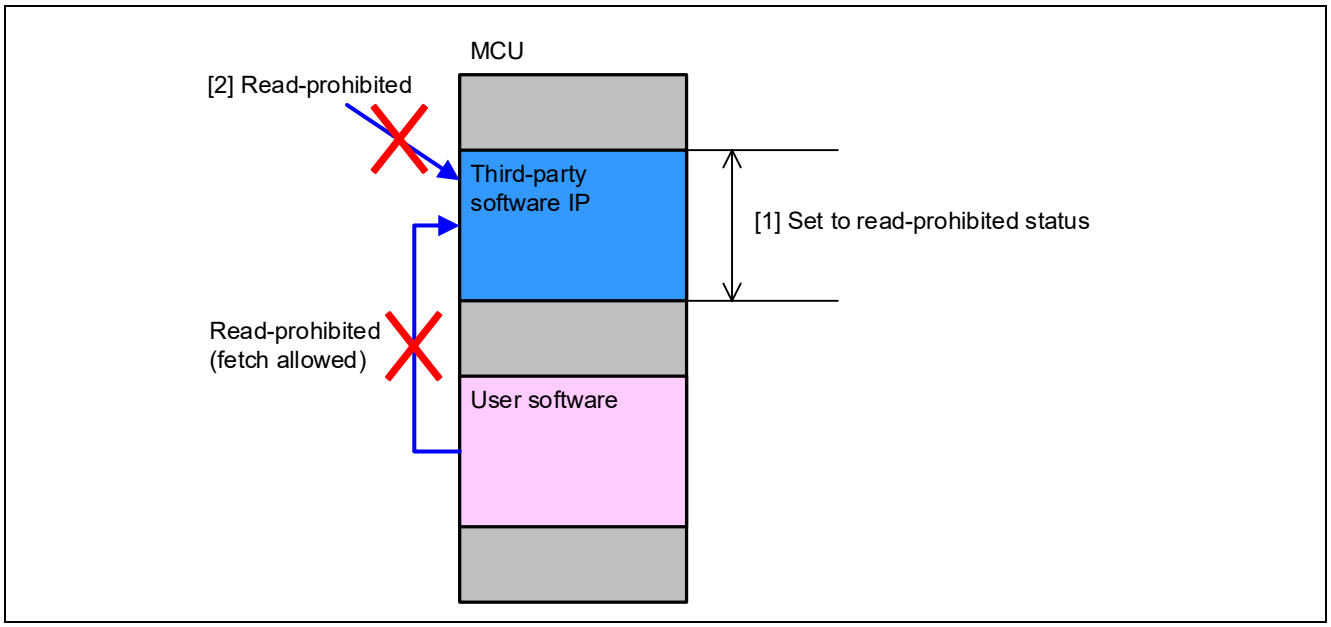
2. Security function of RISC-V

The RISC-V is provided with the security functions listed below. These functions can be used individually or in combination to protect software IP from unauthorized use.

- Memory protection function (flash read protection)
- Unique ID
- User ID

2.1 Memory Protection (Flash Read Protection)

The flash read protection function can be used to protect a specified range of the code flash memory area against read access by the CPU or DTC. Fetching of instructions in the specified range by the CPU is still possible. Note, however, that programs running from a read-prohibited area cannot themselves read read-prohibited data. It is therefore necessary that all data used by a program running from a read-prohibited area be located in an area that is not protected.



[1] The blocks in which the software IP is stored are designated as a read-prohibited area.
[2] The software IP can be run, but user software program cannot read the software IP program code. It also cannot be read using an external flash writer or the like.

Features: Prevents analysis or copying of software IP set to read-prohibited status. To prevent unauthorized use or re-use by the recipient of the software IP, it is necessary to supply MCUs with the software IP preprogrammed in a read-prohibited area of the flash memory.

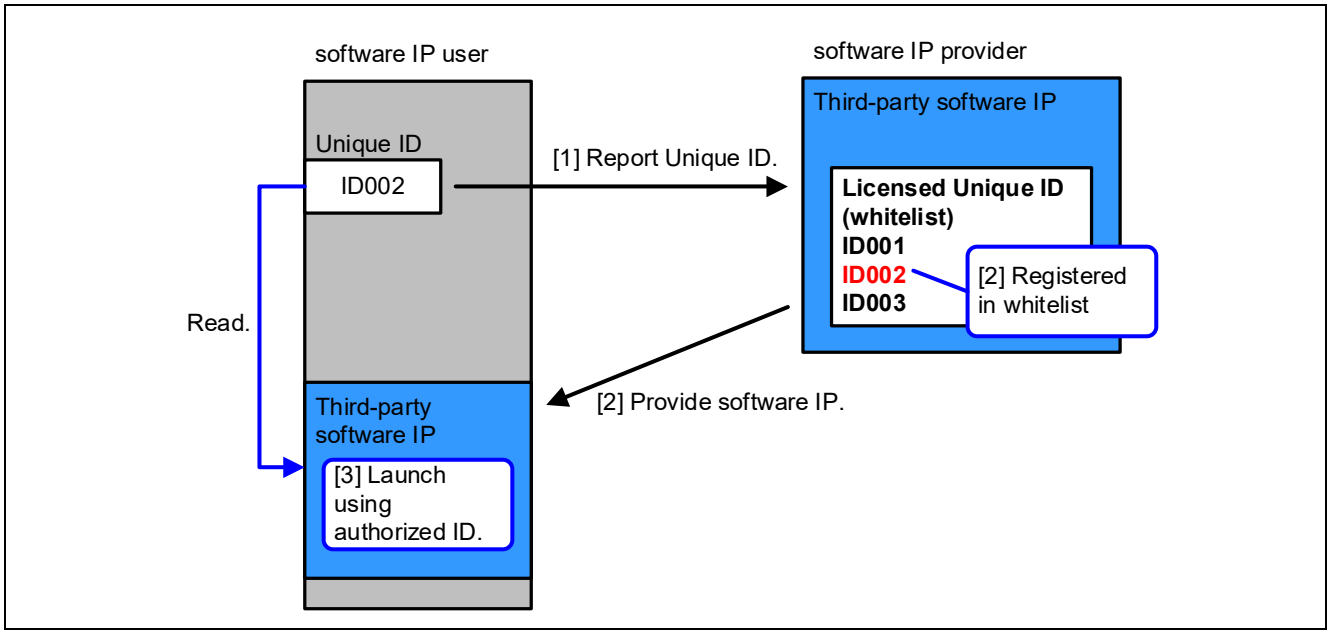
For information on how to set a memory area to read-prohibited status, refer to section 4, Memory Protection Setting Methods.

2.2 Startup Control (Link to Unique ID)

The Unique ID is a unique value specific to the individual device that is stored in the flash memory when the MCU is manufactured.

By registering specific Unique IDs within a software program, it is possible to limit the individuals who can run it.

In cases where the software license is dependent on the number of copies of the product, it is possible to maintain a list of licensed Unique IDs within the software program and thereby ensure that it can only be run on user products with licensed Unique IDs.



[1] The software IP user reads the Unique ID and reports it to the software IP provider.
[2] The software IP provider records the reported Unique ID in a whitelist within the software IP and provides the software IP to the user.
[3] When the Unique ID matches, the software IP runs.

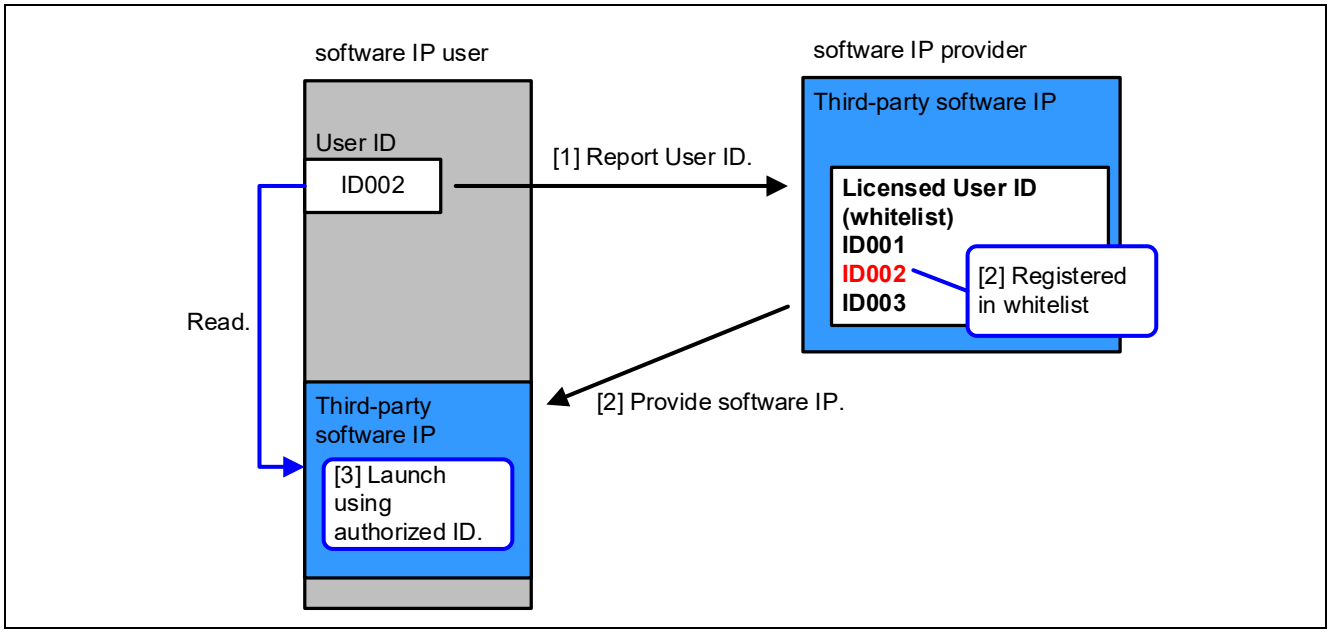
Features: Prevents unauthorized use in cases where it not possible to prohibit copying of the software IP. If the software IP is copied to another MCU with a different Unique ID, it will not run.

2.3 Startup Control (Link to User ID)

The User ID is a unique value that can be set by the microcomputer user.

By registering specific User IDs within a software program, it is possible to limit the individuals who can run it.

In cases where the software license is dependent on the number of copies of the product, it is possible to maintain a list of licensed User IDs within the software program and thereby ensure that it can only be run on user products with licensed User IDs.



[1] The software IP user reads the user ID and reports it to the software IP provider.
[2] When the user ID matches, the software IP runs.

Functionally similar to a Unique ID, but with restrictions on reading the user ID, you can expect stronger protection than a Unique ID.

For more information on the user ID function, please contact a Renesas QA or retailer.

3. Use cases for third-party program (software IP) protection

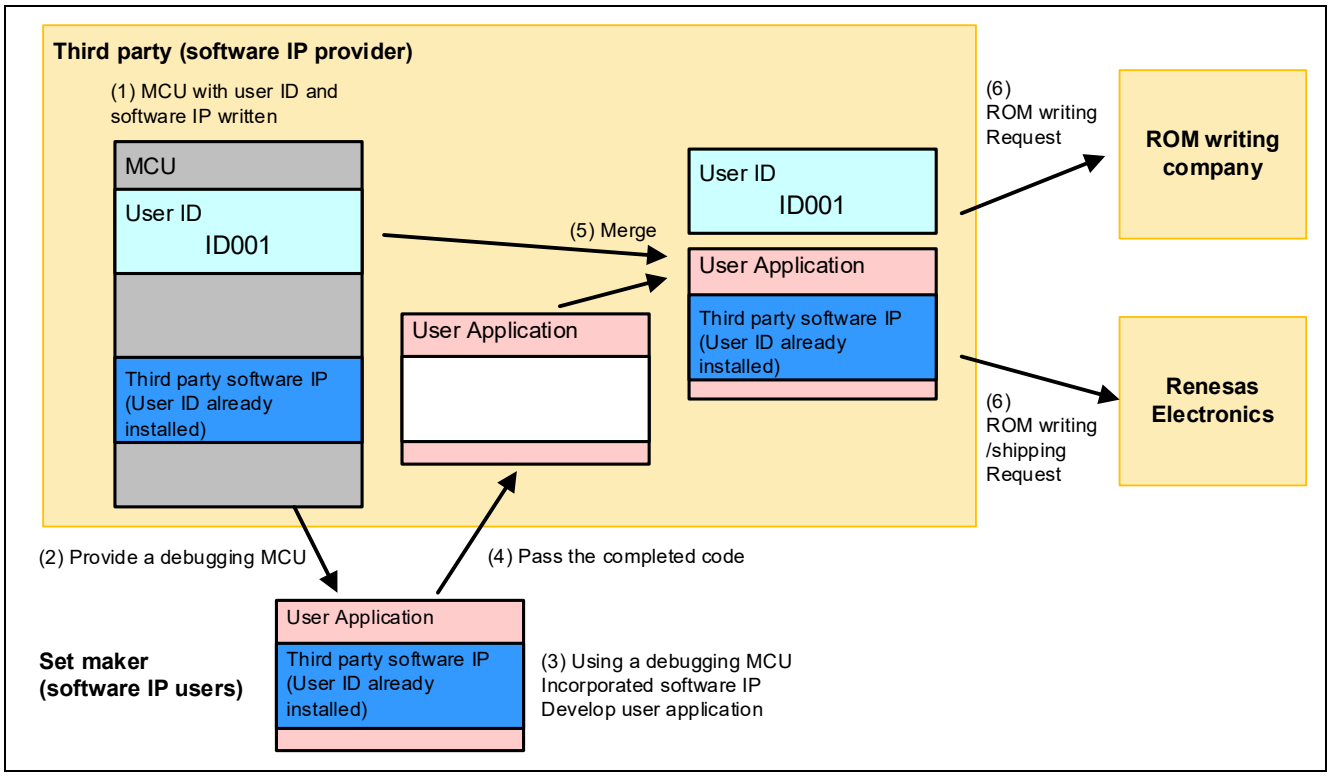
The user ID is used as an example to show a use case for third-party program (software IP) protection.

It also protects user application programs as well as third-party programs (software IP), so it also shows use cases.

3.1 Third-party program protection

Protects the third-party software IP in the case where the third party undertakes the entire software program development.

Prevents unauthorized use of software IP by general users and set makers.

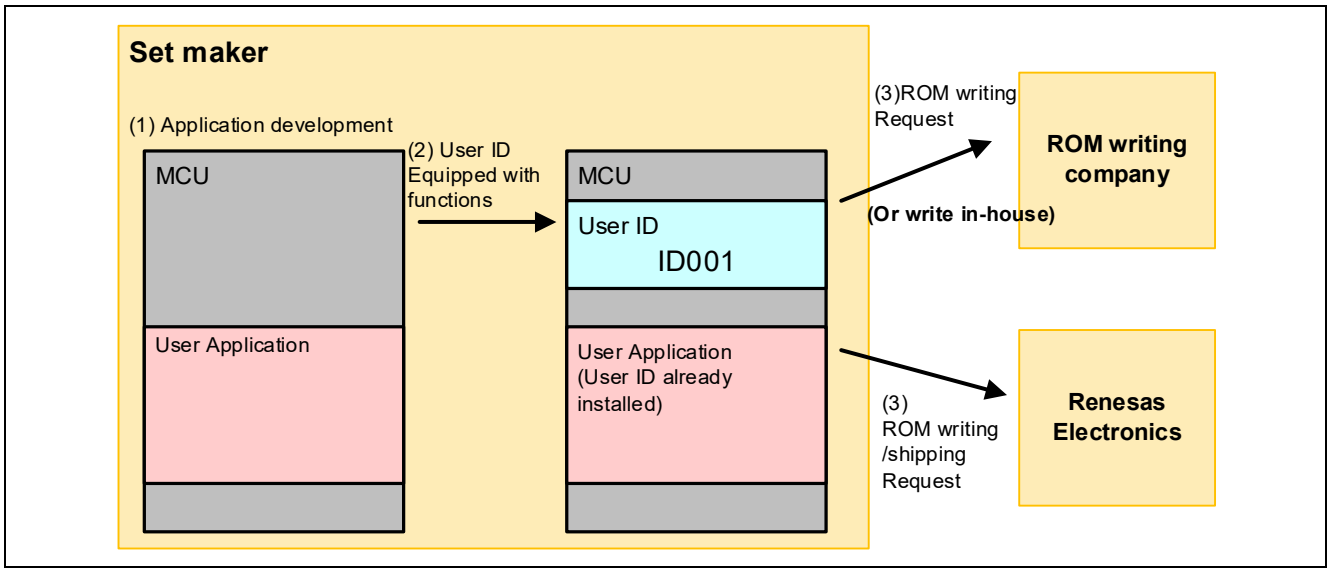


(1) Create an MCU with the user ID and software IP (user ID embedded) written in it
(2) Providing an MCU with a user ID and software IP written for debugging at the set maker
(3) Develop a user application that incorporates software IP using a debugging MCU
(4) Pass the completed user application code to a third party
(5) Merge with set maker application code at a third party
(6) Request ROM writing

3.2 User application protection (1/2)

In the case of software program development by the set maker, the user application of the set maker is protected.

Prevents unauthorized use of user applications by general users.

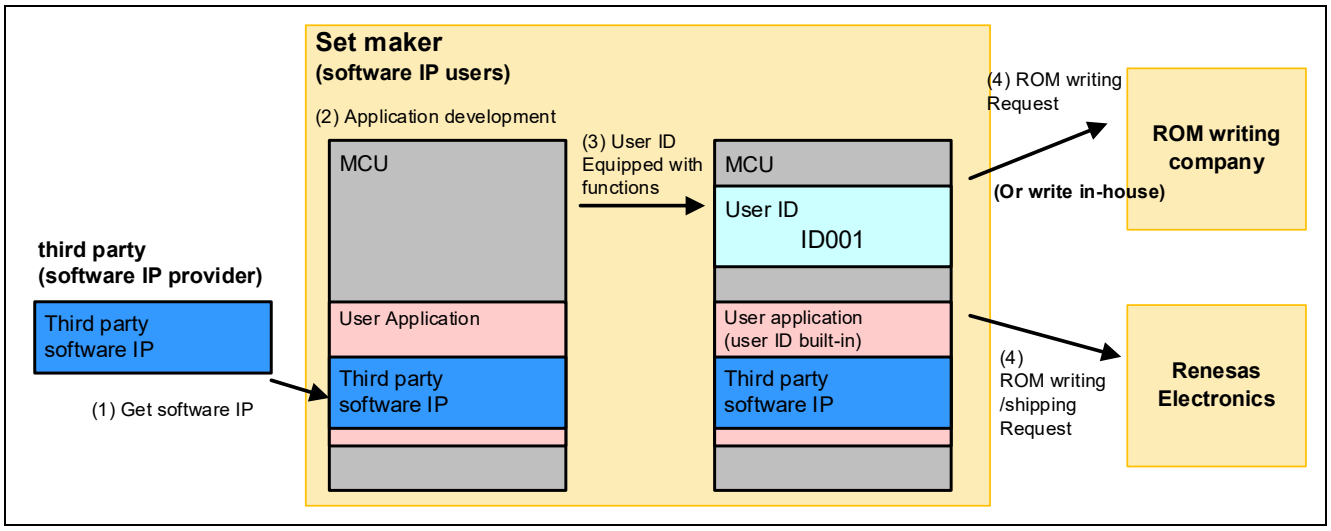


(1) Develop user applications with set makers
(2) Incorporate user ID function into microcomputer and user application
(3) Request ROM writing

3.3 User application protection (2/2)

In the case where software IP is provided by a third party and software program is developed by a set maker, the third party software IP and the user application of the set maker are protected.

Prevents unauthorized use of third-party software IPs and user applications by general users.



(1) Get a third-party software IP
(2) A set maker develops a user application that incorporates a third-party software IP
(3) Incorporate user ID function into microcomputer and user application
(4) Request ROM writing

4. Memory Protection Setting Methods

Memory protection is set via serial programming with self-programming of the option setting memory or using flash memory programmer, on-chip debugger.

4.1 Making Memory Protection Settings Using Renesas Flash Programmer

4.1.1 Setting up memory protection

As the flash writer for this microcontroller is currently under development, the following describes how to set the registers relevant of read protection.

To set up memory protection using the flash writer, perform the following steps.

(1) Set the Flash Read Protection Start Address to the FLRPROTS 23-0 bit of the Flash Read Protection Start Address Register (FLRPROTS).
   — The value range is from 0x0000_0000 to 0x000F_FFFC, excluding reserved areas.
   — The lower 2 bits are read as 0. When programming to the code flash, the lower 2 bits write value should be 0.

(2) Set the Flash Read Protection End Address to the FLRPROTE 23-0 bit of the Flash Read Protection End Address Register (FLRPROTE).
   — The value range is from 0x0000_0003 to 0x000F_FFFF, excluding reserved areas.
   — The lower 2 bits are read as 1. When programming to the code flash, the lower 2 bits write value should be 1.

(3) To enable Flash Read Protection, assign 0 to the DIS bit of the Flash Read Protection Access Control Register (FLRPROTAC).

(4) Read the data allocated in flash read protection registers in (1) to (3), from an object file or Motorola S-format file generated by the compiler and write the data to the MCU. If using the GUI interface of the tool, program the same data as allocated in (1) to (3).

4.1.2 Checking the memory protection settings

Read the memory protection settings from the following registers.

   — Memory Protection Start Address Register (FLRPROTS)
   — Memory Protection End Address Register (FLRPROTE)
   — Memory Protection Access Control Register (FLRPROTAC)

4.1.3 Removing Memory Protection

The memory protection setting can be released by erasing the code flash area.

4.1.4 Debugger Usage Notes

When the flash read protection function is enabled, programs placed in the read access prohibited area cannot be debugged. To debug a program, disable the memory protection function. On-chip debugging is enabled only when the flash read protection access control register (FLRPROTAC) is 0xFFFF_FFFF.

5. Reference Documents

RISC-V User's Manual: Hardware (R01UH1036EJ)

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	Mar.18.24	—	First edition issued

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/.