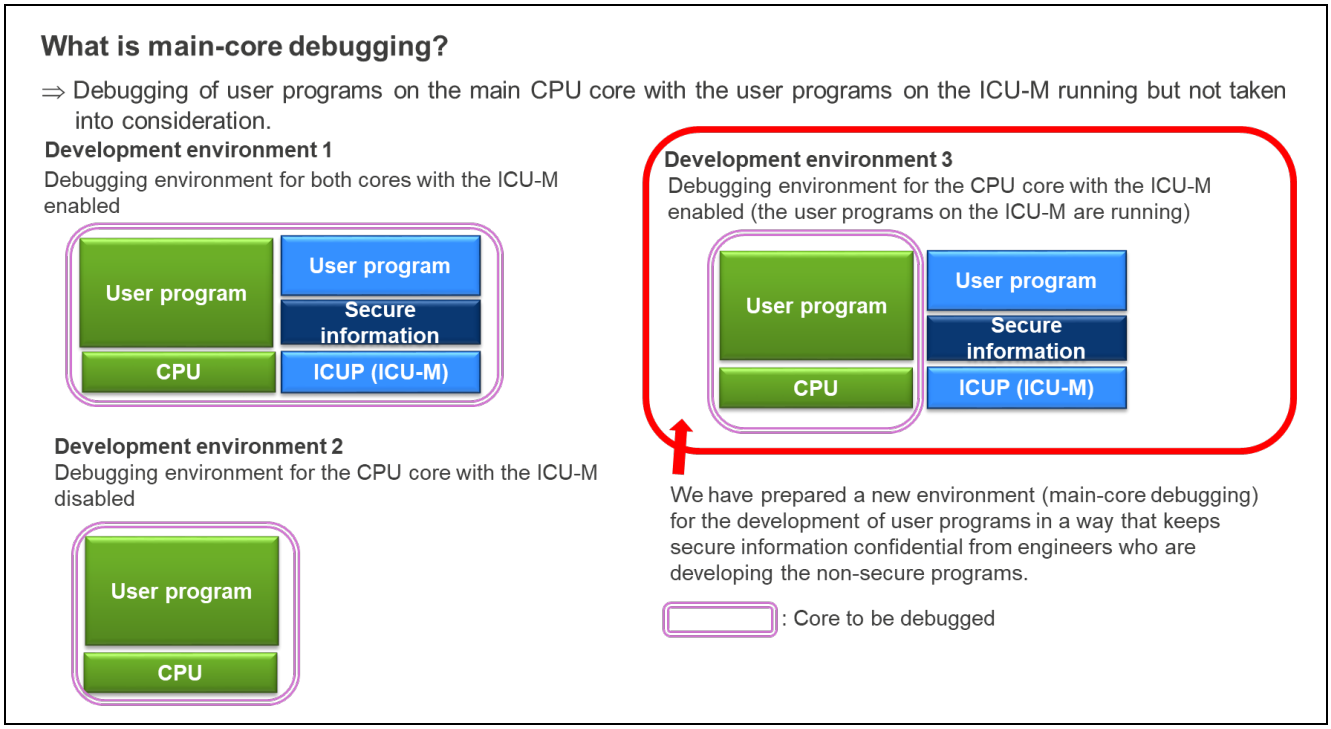
Security-Conscious Debugging Methods for RH850 Devices (Main-Core Debugging)

R20AN0511EJ0101
Rev.1.01
Mar.17.20

Introduction

In applications that use the Intelligent Cryptographic Unit Master (ICU-M), which is a hardware security module installed on the RH850, separately managing the secure user programs running on the ICU-M core and the non-secure user programs running on a main CPU core enables the development of user programs while keeping secure information confidential from engineers who are developing the non-secure programs. This application note describes the usage and gives notes on the debugging of the non-secure user programs running on a main CPU core (hereafter referred to as main-core debugging).



Target Devices

RH850/F1KH-D8, RH850/F1KM-S4

RH850/E2x, RH850/U2A

Contents

Terminology

Some specific words used in this user's manual are defined below.

Integrated development environment

This tool provides powerful support for the development of embedded applications for Renesas microcomputers. It has an emulator debugger function allowing the emulator to be controlled from the host machine via an interface. Furthermore, it permits a range of operations from editing a project to building and debugging it to be performed within the same application. In addition, it supports version management.

Emulator debugger

This means a software tool that is started up from the integrated development environment, and controls the emulator and enables debugging.

Host machine

This means a personal computer used to control the emulator.

Target device

This means the device to be debugged.

User system

This means a user's application system in which the MCU to be debugged is used.

User program

This means the application program to be debugged.

User system interface

This means the interface that the E1/E20/E2/IE850A emulator connects to a user's application system.

Configuration of E1/E20/E2/IE850A Manuals

When you debug RH850 family devices by using the E1/E20/E2/IE850A emulator, be sure to read the user's manuals stated in (1) and (2) below.

(1) E1/E20/E2/IE850A emulator user's manual

These user's manuals have the following contents:

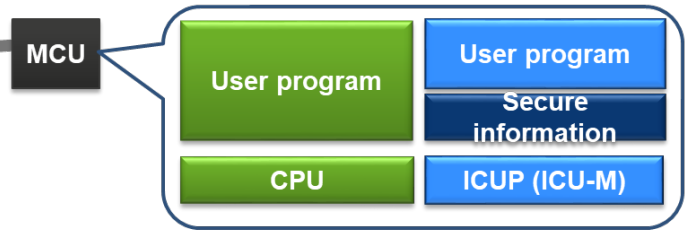
- Components of the emulator
- Hardware specification
- Connection to the emulator and the host machine and user system

(2) E1/E20/E2/IE850A Emulator Additional Documents for User's Manual

E1/E20/E2/IE850A Emulator Additional Documents for User's Manual describe the features of the debugger, items dependent on the given MCU, and give notes on usage.

1. Overview

The main-core debugging feature provided by the E1/E20/E2/IE850A emulator enables debugging of the user programs on a CPU while the ICU-M is operating.



■ Features of main-core debugging

Item	CPU	ICUP (ICU-M)
Operation of the user program	√	√
Features of debugging (downloading, control of execution, operating registers, viewing and setting memory, tracing, etc.)	√	×

√: Operation possible, ×: Operation not possible

Figure 1-1 Outline of Operations in Main-Core Debugging

1.1 Example of the Use of Main-Core Debugging

Since the engineers can develop software on the main-core side while keeping the operation of the ICU-M confidential, it is possible to establish development systems that suit the security levels of the software engineers.

(1) Assumed users involved in development

Figure 1-2 shows an example of the users for examples of the use of main-core debugging.

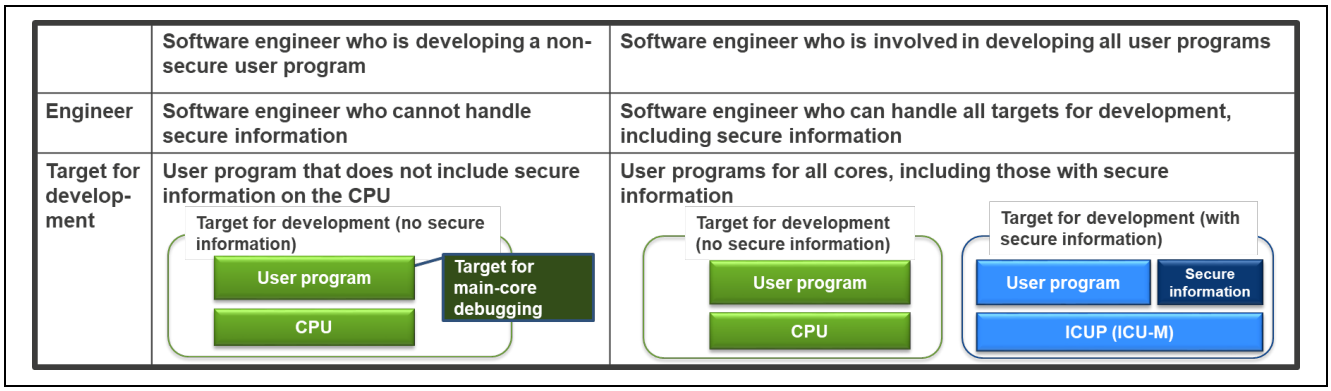
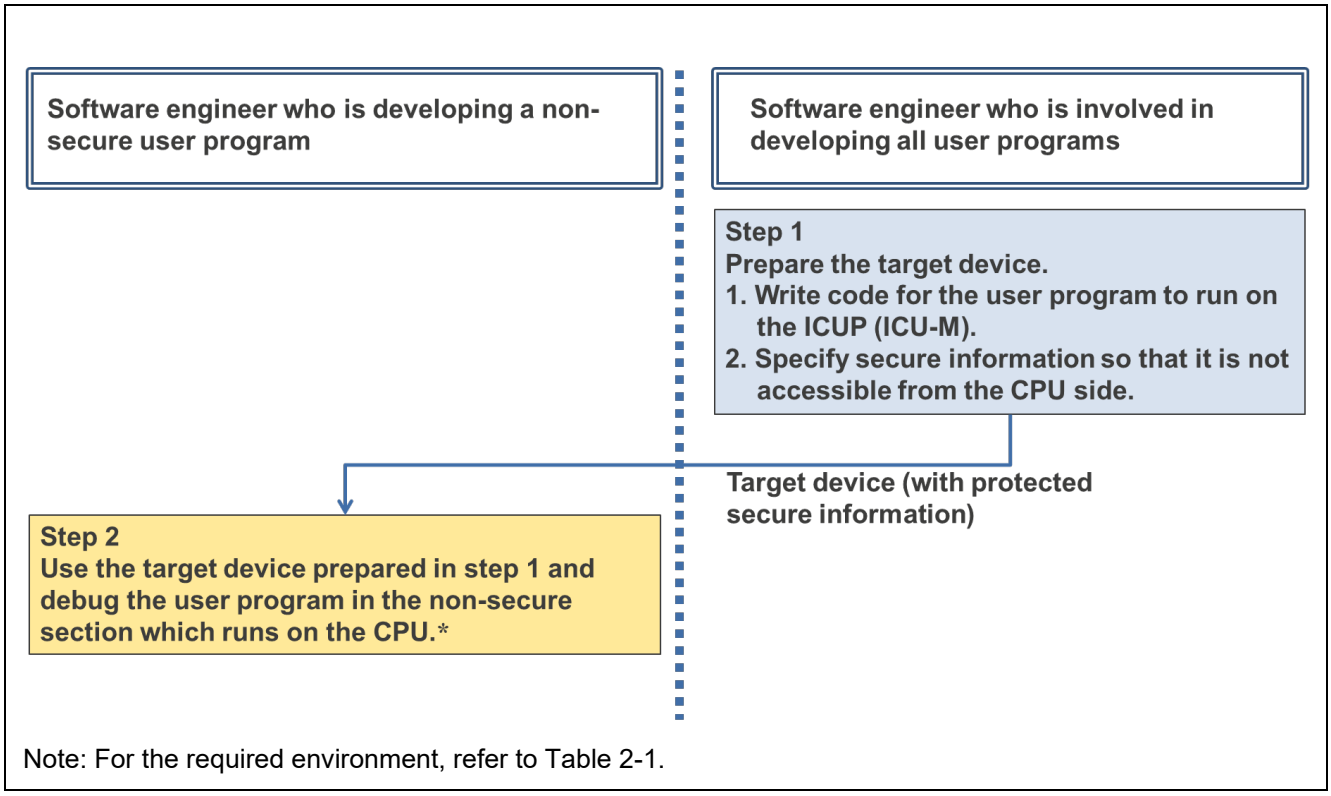


Figure 1-2 Example of the Use of Main-Core Debugging (Assumed Users Involved in Development)

(2) Example of operations

Figure 1-3 shows an example of operations.



Note: For the required environment, refer to Table 2-1.

Figure 1-3 Example of the Use of Main-Core Debugging (Example of Operations)

2. Required Environment

2.1 System Configuration and Required Environment

Figure 2-1 and Table 2-1 show the system configuration and required environment.

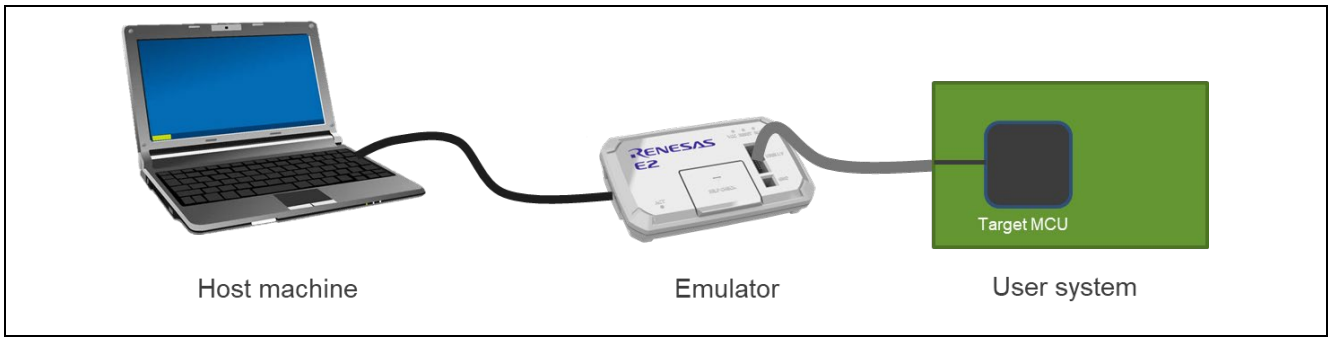


Figure 2-1 System Configuration

Table 2-1 Required Environment

Item	Target device	Detail
Emulator	RH850/F1KH-D8 RH850/F1KM-S4	RENESAS E1/E20/E2 emulator
	RH850/E2x RH850/U2A	RENESAS E2/IE850A emulator
Integrated development environment (version)	RH850/F1KH-D8 RH850/F1KM-S4	RENESAS CS+ (V6.01 or later versions)
		Green Hills Software MULTI (850eserv2 V2.047 or later versions)
	RH850/E2x RH850/U2A	RENESAS CS+ (V8.03 or later versions)
		Green Hills Software MULTI (850eserv2 V2.057 or later versions)

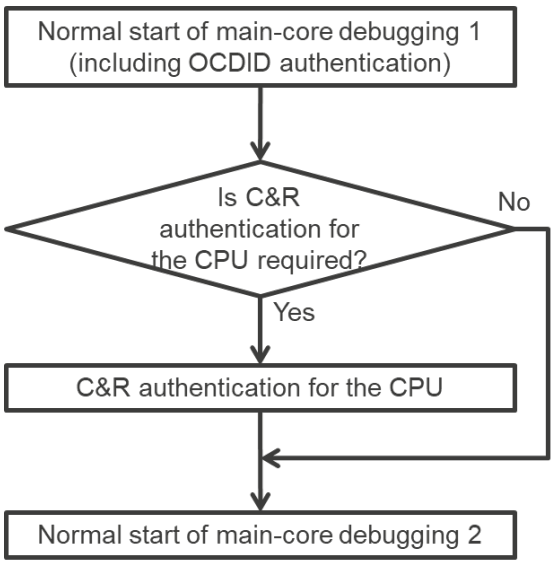
3. Using the Main-Core Debugging Feature

3.1 Starting Main-Core Debugging

Figure 3-1 shows how to start main-core debugging.

When C&R authentication is not required, main-core debugging is started in the same way as with the current debugger.

After main-core debugging is started, debugging features are used in the same way as with the current debugger.



Note: For C&R authentication for the CPU, refer to section 3.2.

Figure 3-1 Starting Main-Core Debugging

3.2 C&R Authentication with the Debugger

There are dialog and DLL methods for C&R authentication. In the dialog method, authentication is performed after the challenge data acquired from the ICU-M is displayed on the debugger and the user reads it, generates the response data, and enters the response data in the dialog box. In the DLL method, the user creates a DLL for generating the response data and registers it with the debugger in advance. After that, authentication is performed after the debugger passes the challenge data acquired from the ICU-M to the DLL and sends the response data generated by the DLL to the ICU-M.

3.2.1 DLL Method

(1) Creating an authentication DLL

Create a DLL that includes the following function.

```
int ConvertData(char target, unsigned int number, unsigned int* challenge,
unsigned int* response)
```

— Arguments

target: (Input) C&R for the CPU: 0, C&R for the ICU-M: 1
number: (Input) The number of elements in the array of challenge data
challenge: (Input) Array in which the challenge data have been stored
response: (Output) Array in which the response data have been stored

— Return values

0: Succeeded, 1: Failed

— Features

After the debugger passes the challenge data acquired from the ICU-M to the array `challenge`, generate the response data to be stored in array `response`. The debugger receives and sends the response data to the ICU-M and authentication proceeds.

(2) Setting the authentication DLL

The created DLL must be registered in the debugger. According to the following example, register the authentication DLL with the debugger.

Example: For CS+

Right-click on [RH850 E1 (LPD) (Debug Tool)] and open [Property (P)].

Select “Yes” for [Use authentication dll] in [Security] on the [Connect Settings] tabbed page.

Specify the absolute path for the authentication DLL which is used for [Authentication dll] in [Security] on the [Connect Settings] tabbed page.

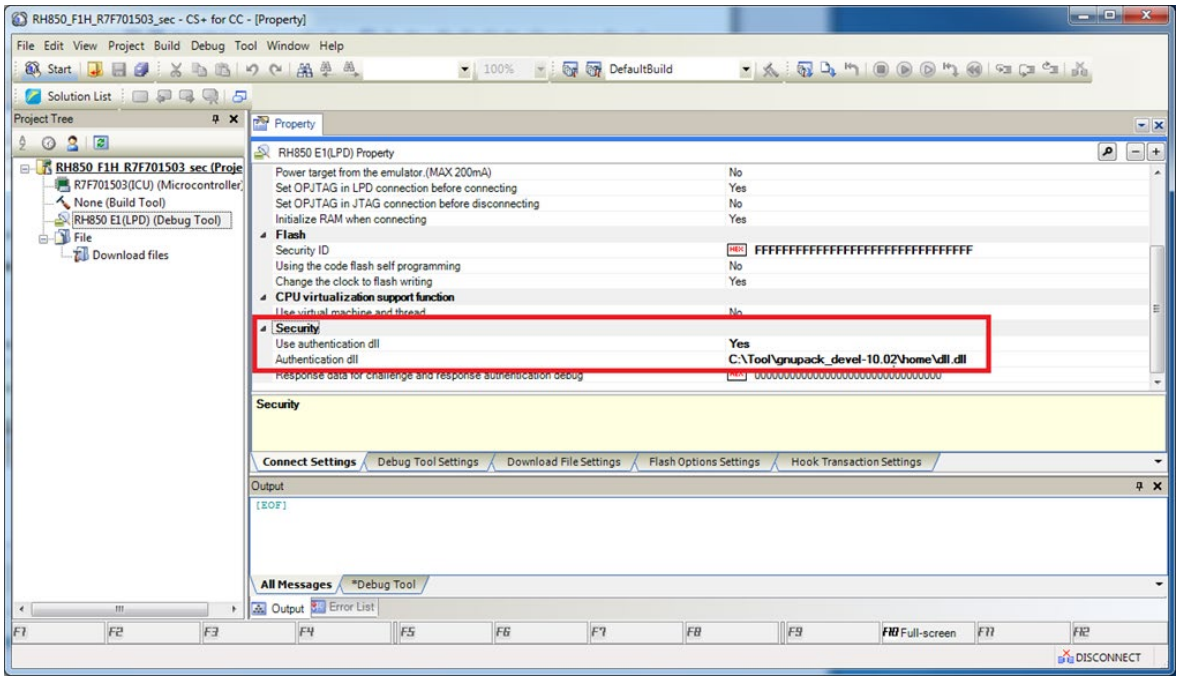


Figure 3-2 Setting the Authentication DLL

Example: For GHS MULTI

Specify the -cr_dll=<dll_path> option for the connect command when 850eserv2 is started.

Specify the full path to the authentication DLL as dll_path.

```
connect 850eserv2 -rh850 -e1lpd4=default … -
cr_dll=c:¥Tool¥Authentication¥CR_Auth.dll
```

3.2.2 Dialog Method

Example: For CS+

Right-click on [RH850 E1 (LPD) (Debug Tool)] and open [Property (P)].

Select “No” for [Use authentication dll] in [Security] on the [Connect Settings] tabbed page.

Select [Connect to Debug Tool (C)] under the [Debug (D)] menu. Once the debugger has normally acquired the challenge data, the dialog box shown in Figure 3-3 is displayed. Authentication proceeds through entry of the response data and clicking on [OK]. The data are aligned from the left in the order of bits 127 to 0.

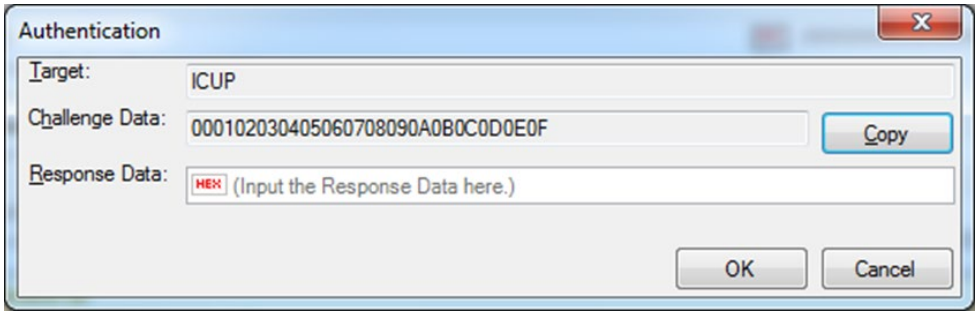


Figure 3-3 Example of Setting a Dialog Box (CS+)

Example: For GHS MULTI

Specify the -cr option for the connect command when 850eserv2 is started.

```
connect 850eserv2 -rh850 -e1lpd4=default … -cr
```

Once the debugger has normally acquired the challenge data, the dialog box shown in Figure 3-4 is displayed. Authentication proceeds through entry of the response data and clicking on [Authentication]. The data are aligned from the left in the order of bits 127 to 0.

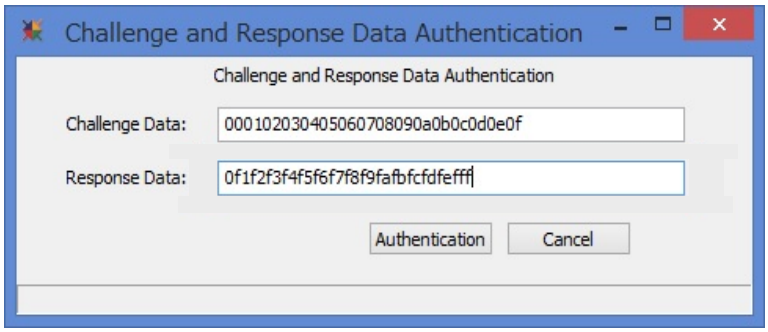


Figure 3-4 Example of Setting a Dialog Box (MULTI)

In case of success in authentication, "C&R security Authentication success" is displayed in the command pane and connection of the debugger is completed. In case of failure in authentication, "C&R security Authentication error" is displayed.

4. Notes

(1) When the following operations are done in the emulator debugger, operation of the ICU-M is temporarily stopped to avoid contention between the ICU-M and a core other than the ICU-M for access to shared resources.
- Reading from, writing to, or downloading to the code flash or data flash area
  Example 1: Downloading a user program
  Example 2: Executing a program while a software break is set in the code flash area
  Processing for rewriting the instruction to that for a break is performed when the program is executed.
- Reading from or writing to option bytes

(2) When the emulator debugger issues a reset, all cores including the ICU-M are reset.

(3) If a break in execution by the main core occurs, a reset will not be generated even if the ICU-M tries to issue a reset.

(4) When a peripheral break function is enabled during main-core debugging, the operation of the peripheral modules subject to the peripheral break function is stopped during breaks in execution by the main core. In case of access by a user program being executed on the ICU-M to a peripheral module which has stopped operating during this time, the program may not operate correctly. In such cases, disable the peripheral break function. For the peripheral modules subject to the peripheral break function, refer to the section on the on-chip debugging unit (OCD) in the user's manual for the target device.

Revision History

		Description	
Rev.	**Date**	**Page**	**Summary**
1.00	Sep.03.18	—	First edition issued
1.01	Mar.17.20	—	Added target devices.

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. 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 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 a product with a different part number, confirm that the change will not lead to problems.

   — The characteristics of Microprocessing unit or Microcontroller unit products in the same group but having a different part number may differ in terms of the 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 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. This document shall not be reprinted, 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.

(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.4.0-1 November 2017)

Corporate Headquarters

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

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/

Trademarks

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