RA2E1 MCU Group

Security Manual

Introduction

The RA2E1 MCU Group incorporates many features that can be used to protect the content and operation of the MCU when it is integrated into an end-product. This document describes these features and provides general recommendations for their use. Associated Application Notes and other applicable documents that provide more details are listed for reference.

Since the RA2E1 is a general-purpose MCU, this Security Manual cannot offer specific guidance for all possible use cases, nor can it provide system-level security guidance. It is highly recommended that the application developer conducts a security analysis of the system into which the RA2E1 is integrated and create a threat model and security policy for the system and for the RA2E1, for example, using the ISO/SAE 21434 Threat Analysis and Risk Assessment (TARA) approach. It is the application developer's responsibility to decide what RA2E1 security features are necessary for the end-product and to implement them appropriately.

Although this Security Manual describes best secure practices for configuring the RA2E1 at the time of its release, the microcontroller threat landscape is constantly changing and evolving. Please refer to the Notice at the end of this document.

Contents

1. Introduction

1.1 Overview

This application note describes the security-related features of the RA2E1 MCU Group and offers guidance on how to use these features to create a product that has the appropriate level of cybersecurity based on the threat model for the intended application.

NOTE: Ultimately, it is up to the discretion of the application developer to determine how to design the security architecture of the end-product and what security features to employ. Critical items relating to the proper functioning of the MCU and possible security threats are noted in red sections.

1.2 Security Features

The RA2E1 MCU provides the following security-related features:

- MCU product and chip-unique identification
- Hardware-enforced isolation using a Security MPU
- Hardware-accelerated cryptography
- Immutable memory
- Various tamper detection features
- ID Code protection for debugger/programmer re-enablement

The RA Flexible Software Package (FSP) is the Renesas software platform available for use with the RA2E1 MCU Group. The FSP provides support for security solutions that are often required to secure an end-product, including:

- Secure boot
- Secure firmware updates

1.3 References

The following documents are referenced in this application note. These documents are available from the Renesas website, www.renesas.com.

Reference	Document Name	Document Number or URL
[RA2E1 User Manual]	RA2E1 Group User's Manual: Hardware	R01UH0852
[FSP User Manual]	RA Flexible Software Package Documentation	RA Flexible Software Package Documentation: Introduction (renesas.github.io)
[Boot Firmware]	Renesas RA Family System Specifications for Standard Boot Firmware	R01AN6347
[SP800-22 Test Report]	NIST SP800-22r1a Random Number Statistical Test Report for RA2E1	R01AN6212
[SP800-90B Test Report]	NIST SP800-90B Entropy Assessment Report for RA2E1	R01AN6860

1.4 Additional Guidance Documentation

The following additional guidance documents are referenced in this application note. Please note that due to documentation update cycles, the RA2E1 MCU Group may not be explicitly referenced in the latest version of these documents. These documents are available from the Renesas website, www.renesas.com.

Reference	Document Name	Document Number
[Bootloader Basic]	Secure Bootloader for RA2 MCU Series	R11AN0516

1.5 Abbreviations and Legend

The following abbreviations are used in this document.

Abbreviation	Meaning
AWS	Access Window Setting Register
BSP	Board Support Package
BTFLG	Access Window Setting Register bit, Startup Area Select Flag
CAC	Clock Frequency Accuracy Measurement Circuit
DTC	Data Transfer Controller
FAW	Flash Access Window
FAWE	Access Window Setting Register bits, Access Window End Block Address
FAWS	Access Window Setting Register bits, Access Window Start Block Address
FSP	Flexible Software Package
FSPR	Access Window Setting Register bit name, Protection of Access Window and Startup Area Select Function
HAL	Hardware Abstraction Layer
IDE	Interactive Development Environment
ISR	Interrupt Service Routine
LVD	Low Voltage Detection
MPU	Memory Protection Unit
PNRn	Part Numbering Registers
RASC	RA Smart Configurator
RFP	Renesas Flash Programmer
RTC	Realtime Clock
SMPU	Security MPU
TRNG	True Random Number Generator
TSN	Temperature Sensor
UIDRn	Unique ID Registers

1.6 Software Platform

The RA Flexible Software Package (FSP) is a software package provided by Renesas for developing applications on RA Family MCUs. The FSP provides Board Support Packages, HAL drivers, and middleware for RA Family MCUs.

The FSP Platform Installer includes the e^2 studio IDE, toolchain, and FSP packs. Alternately, the FSP Standalone Installer plus the RA Smart Configurator can be used with the IAR Embedded Workbench IDE or Arm Keil MDK.

These installers, plus additional information, can be found at www.renesas.com/fsp.

1.7 Vulnerability Reporting

Renesas is committed to proactively addressing any potential security vulnerabilities within our products. To report a security vulnerability, please go to www.renesas.com/psirt and follow the instructions on the web page.

2. Identity

2.1 MCU Group Identity

The RA2E1 MCU Group chips contain a 16-byte read-only register that contains an immutable ASCII representation of the device part number. The PNRn Part Numbering Registers are documented in the [RA2E1 User Manual], including a part number listing.

The PNRn registers are located starting at address 0x0100_1C10. The ASCII digits of the PNRn register, in the format shown below, must read “R7FA2E1” to indicate that the device is an RA2E1 MCU. The other ASCII digits represent non-security related items such as package type, packing, operating temperature, and code flash memory size.

The contents of the PNRn are as follows (“x” is used to represent a “don’t care” value for security-related functionality, □ is used to represent a space (0x20 in ASCII)):

Table 1. Part Numbering Register Values

Address	ASCII Representation (Big Endian)
0x0100_1C10	xxxx
0x0100_1C14	E1xx
0x0100_1C18	7FA2
0x0100_1C1C	□□□R

For more details, refer to the following document:

- [RA2E1 User Manual]

2.2 Unique Identity

The RA2E1 MCU Group chips contain a 16-byte read-only register that contains an immutable 16-byte ID code (unique ID) for identifying the individual MCU. The UIDRn Unique ID Registers are documented in the [RA2E1 User Manual].

This value is guaranteed to be unique. It is serialised and, therefore, predictable, so it should not be used for identifying the end-product if a random or pseudorandom identifier is required.

This value can be obtained by using the FSP function `R_BSP_UniqueIdGet()`.

For more details, refer to the following document:

- [RA2E1 User Manual]

2.3 Cryptographic Identity

The RA2E1 MCU is not delivered with a provisioned cryptographic identity. Any cryptographic identity required by the application must be provisioned during production programming.

3. Isolation

3.1 Security MPU

The RA2E1 includes a security MPU that is designed to create a secure region that can be protected from non-secure program accesses.

The Security MPU can be configured to protect the following:

- Code flash (2 regions)
- SRAM (4 regions)
- Select peripherals (can include I/O registers, AES, TRNG, flash memory, data flash memory, TSN)

For best security design practices, external memory should always be considered non-secure.

Security MPU usage is not mandatory. The application developer is responsible for assessing the security risks of a monolithic architecture.

For more details, refer to the following documents:

- [RA2E1 User Manual]

3.2 Memory Protection Unit (MPU)

The RA2E1 MCU Group contains an Arm Cortex-M23 core with an Arm MPU, a Bus Master MPU, and a Bus Slave.

The Arm MPU can be used to protect memory regions by defining access permissions for different privilege states. See the Arm Developer documentation for more information about how to use the Arm MPU: Armv8-M Memory Model and Memory Protection User Guide

The Arm Bus Master MPU provides memory protection for bus masters other than the CPU, namely DMA/DTC. If access to a protected region is detected, the Bus Master and Bus Slave MPUs generate an internal reset or a non-maskable interrupt.

For more details, refer to the following documents:

- [RA2E1 User Manual]

4. Cryptographic Functions

The RA2E1 provides hardware acceleration for AES operations.

Table 2. RA2E1 Cryptographic Operations lists the cryptographic operations supported by the MCU.

The Application code should use cryptographic algorithms with sufficient strength as appropriate to the application's threat model.

Table 2. RA2E1 Cryptographic Operations

Algorithm	Operations	Specification	Key lengths	Modes
AES	Encryption, decryption	NIST FIPS PUB 197 NIST SP800-38A (ECB, CBC, CTR)	128 and 256 bits	ECB, CBC, CTR

The AES implementation in the RA2E1 does not provide countermeasures against electromagnetic side-channel attacks. It is a constant time implementation, and as such, it does provide countermeasures against timing attacks.

These cryptographic operations are intended to be used via one of the APIs provided in the FSP. The following APIs are currently provided:

- ocrypto: Ocrypto is a cryptography library that Renesas has licensed from Oberon Microsystems AG for use with the RA2E1. This is the recommended cryptographic library for RA2E1.
- PSA Certified Crypto APIs: For compatibility with RA4, RA6, and RA8 devices, the PSA Certified Crypto API implementation in Mbed TLS can be used. This library requires a larger memory footprint than ocrypto.
- TinyCrypt: An open-source cryptographic library.

The keys used for cryptographic operations will be in plain text. It is recommended to place these keys in a Secure region utilising the Security MPU.

For more details, refer to the following documents:

- [RA2E1 User Manual]
- [FSP User Manual]

5. Random Number Generation

The RA2E1 MCU Group provides True Random Number Generation. This feature has passed internal testing for both SP800-22 and SP800-90B compliance (see [SP800-22 Test Report] and [SP800-90B Test Report]).

The TRNG peripheral provides a seed, which is generated from an entropy source. Each TRNG request generates a 128-bit random number. This seed can either be used directly as a random number, or it can be used as a seed for a PRNG.

The TRNG is intended to be used via one of the APIs provided in the FSP. See 4. Cryptographic Functions for the list of APIs that are provided in the FSP.

The ocrypto library and TinyCrypt use the TRNG output directly; therefore, reseeding is inapplicable.

The PSA Certified Crypto API implementation in Mbed TLS uses the TRNG output as the seed for a counter DRBG. The reseeding interval is configured by defining the macro `MBEDTLS_CTR_DRBG_RESEED_INTERVAL` and setting it to the number of calls that can be made to `psa_generate_random()` before reseeding is required. The macro can be defined and set using either the e^2 studio IDE or the RA Smart Configurator (*MbedTLS (Crypto Only) module> RNG*). Reseeding will occur automatically if needed when `psa_generate_random()` is called.

For more details, refer to the following documents:

- [RA2E1 User Manual]
- [FSP User Manual]

6. Immutable Memory

A portion of the code flash of the MCU can be configured to be immutable. This property is commonly used to protect critical assets that define the identity of the device and control access to the device through a secure firmware update mechanism.

The RA2E1 supports a Flash Access Window, whereby all the code flash is configured as immutable except the code flash within a specified address range. The granularity of the specified range is one flash block. A flash block on the RA2E1 is 2 KB.

For example, consider the example shown in Figure 1. Flash Access Window Example

- The FAWS bits in the Access Window Setting (AWS) Register are set to 0x04.
- The FAWE bits in the Access Window Setting (AWS)Register are set to 0x07.

This configures the code flash as follows:

- Code flash at addresses 0x0000_0000 to 0x0000_1FFF is immutable (read-only).
- Code flash at addresses 0x0000_2000 to 0x0000_3FFF is mutable (read/write/erase).
- Code flash at addresses 0x0000_4000 to the top of memory is immutable (read-only).

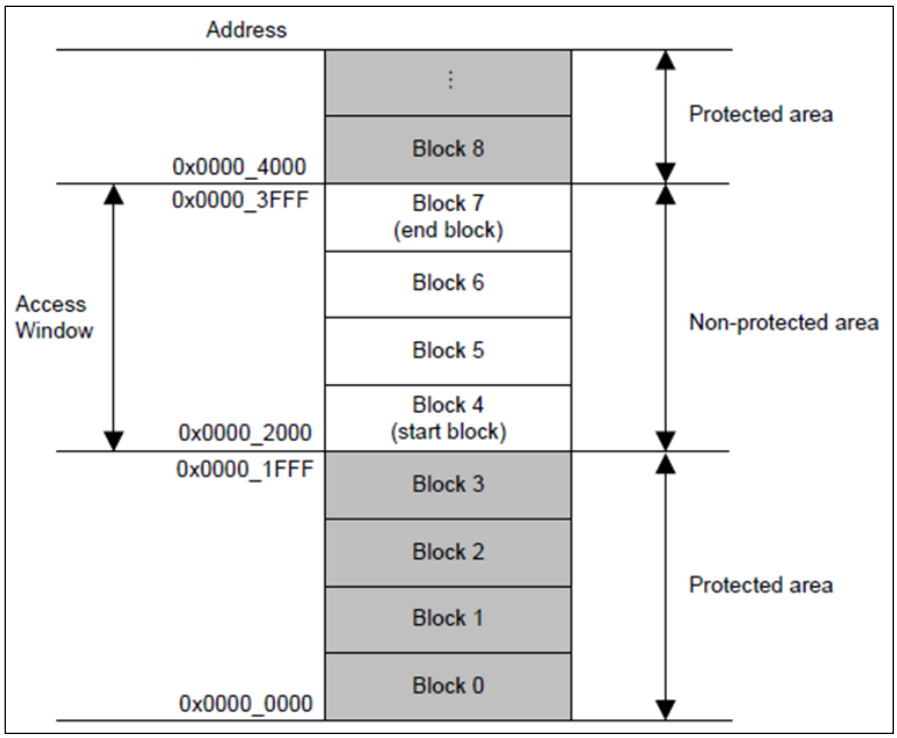

Figure 1. Flash Access Window Example

An application that intends to be configured with immutable flash blocks can be prototyped by leaving the FAW protection bit (FSPR) set to 1. This will allow the FAWS and FAWE registers to be erased using the boot firmware “Erase” command.

Production programming of the end-product should configure the FAWS and FAWE registers appropriately and program the FSPR bit to 0. After the FSPR bit is programmed to 0, FAWS, FAWE, and the FSPR bit itself cannot be changed.

The code flash blocks that contain the Root of Trust should be made immutable. The immutable Root of Trust contains items such as a secure boot solution and root keys and certificates.

For more details, refer to the following documents:

- [RA2E1 User Manual]
- [FSP User Manual]

7. Tamper Protection

7.1 Operational Temperature Monitoring

Some attacks involve operating the MCU outside its specified temperature range to try to induce erroneous behavior. The on-chip Temperature Sensor (TSN) peripheral can be used to monitor the die temperature.

Refer to the detailed description of this peripheral and its associated electrical characteristics as stated in the [RA2E1 User Manual] for the requirements and limitations of this hardware feature.

The application code must periodically check the die temperature, compare it to the device’s operating range, and trigger a fault if the temperature is out of range.

If temperature attacks are in scope for the application’s threat model, this check should be performed at a rate that is consistent with the threat model of the application.

It is recommended to place the code that interacts with this peripheral in the Secure region if the application utilises the Security MPU.

For more details, refer to the following documents:

- [RA2E1 User Manual]
- [FSP User Manual]

7.2 Operational Voltage Monitoring

Some attacks involve operating the MCU outside its specified voltage range to try to induce erroneous behavior. The Low Voltage Detection (LVD) peripheral can be used to monitor the voltage level input to the VCC pin and alert if a selectable voltage threshold is crossed.

Refer to the detailed description of this peripheral and its associated electrical characteristics as stated in the [RA2E1 User Manual] for the requirements and limitations of this hardware feature.

There are three programmable voltage monitors on the MCU.

Voltage Monitor 0 can be configured to be active immediately upon reset using the voltage level selected in the Option-Setting Memory, resetting the MCU if the voltage drops below the selected value.

It is recommended to configure Voltage Monitor 0 to be active immediately upon reset at a level that is appropriate for the application to mitigate voltage fault injection attacks.

Voltage Monitor 1 and Voltage Monitor 2 can be configured for more advanced voltage detection scenarios.

It is recommended to place the code that interacts with the LVDs in the Secure region if the application utilises the Security MPU.

For more details, refer to the following documents:

- [RA2E1 User Manual]
- [FSP User Manual]

7.3 Clock Protection

Some attacks involve varying the frequency of the MCU clock to try to induce erroneous behaviour. The Clock Frequency Accuracy Measurement Circuit (CAC) peripheral counts pulses of the measurement target clock using a measurement reference clock. If the number of pulses is not within an allowable range, an interrupt is generated.

Refer to the detailed description of this peripheral and its associated electrical characteristics as stated in the [RA2E1 User Manual] for the requirements and limitations of this hardware feature.

If the application uses an external clock and clock attacks are in scope for the application’s threat model, the application should utilise the CAC.

It is recommended to place the code that interacts with this peripheral in the Secure region if the application utilises the Security MPU.

For more details, refer to the following documents:

- [RA2E1 User Manual]
- [FSP User Manual]

8. Internet Connectivity

The RA2E1 MCU Group does not include any hardware to facilitate internet connectivity. If the end-product includes additional hardware that provides internet connectivity, security best practices to support that connectivity in conjunction with the additional hardware should be implemented.

9. Secure Boot

To ensure secure initialization of the application, it is recommended to utilize and potentially customize the secure bootloader solution provided in the FSP.

For more details, refer to the following documents:

- [Bootloader Basic]

9.1 Second Stage Bootloader

The RA2E1 does not have a built-in (i.e., First Stage) secure bootloader; however, it is possible to implement an immutable bootloader using the secure bootloader solution provided in the FSP.

The FSP includes a port of the TrustedFirmware MCUboot project, an open-source secure boot and firmware update solution for 32-bit microcontrollers. Secure boot is usually very application-specific; therefore, Renesas provides multiple examples of how the secure boot solution can be used. Note that secure boot and secure firmware updates are provided as a unified solution.

Review the threat model and start-up time requirements of the application when implementing secure boot. Since all code flash on the RA2E1 is stored inside the chip, and the programmer and debugger interface should be locked upon deployment, it may be sufficient to implement only the secure firmware update portion of the secure bootloader solution.

For more details, refer to the following documents:

- [Bootloader Basic]

10. Secure Firmware Update

The ability to update firmware in an end-product is becoming a standard requirement, especially if the product is connected to public infrastructure such as the internet. Any firmware update, whether through public infrastructure or a private connection, should be performed in a secure manner.

The FSP includes a port of the TrustedFirmware MCUboot project, an open-source secure boot and firmware update solution for 32-bit microcontrollers. Secure firmware update is usually very application-specific; therefore, Renesas provides multiple examples of how the secure firmware update solution can be used. Note that secure boot and secure firmware updates are provided as a unified solution.

There are many items to consider when devising a secure firmware update strategy, including:

How will the new image be received? Is it received over a secure channel, or does the image need to be encrypted for transfer to the product? A TLS connection can usually be considered a secure channel.

The authenticity of the image needs to be verified before it is programmed for execution. Therefore, the entire image must be received and stored locally. Will the new image be stored on-chip or in an external memory?

If the new image is stored externally prior to installation, does it need to be encrypted so an attacker cannot physically extract the plaintext binary?

Be sure to consider the threat model for the end-product when architecting a firmware update strategy.

For more details, refer to the following documents:

- [Bootloader Basic]

11. Provisioning

11.1 ID Code Protection

When the MCU is programmed for incorporation into an end-product, there are several available options. The most common ones are:

- If there is no desire to re-enable the debugging capability of the MCU or completely erase the flash contents, ID Code bit 127 should be programmed to 0, and either the FSPR bit should be programmed to 0 or the Security MPU should be enabled.
- To maintain the ability to re-enable debugging or completely erase the flash contents via the serial programmer interface, set the ID Code such that bits [127:126] are 0x03 and the remaining bits are a known value (not all 0xFF and not the value for the ALeRASE (“All Erase”) command).
- To maintain the ability to re-enable debugging but remove the ability to completely erase the flash contents via the serial programmer interface, set the ID Code such that bits [127:126] are 0x02 and the remaining bits are a known value.

For all cases where serial programmer access is enabled, the following limitations exist:

- If the Flash Access Window has been defined, then a block outside the FAW cannot be erased or programmed.
- If the FSPR bit is 0, then the Option-setting Memory (Config area) cannot be erased.
- If the FSPR bit is 0, then FAWS, FAWE, and BTFLG cannot be programmed.

The available configurations are summarised in the following table.

Table 3. ID Code Protection Options

ID Code	ID Code Sent	FSPR=0 or SMPU Enabled	Debugger Access	Serial Programmer Access
All 0xFF	N/A	No	Yes	Yes
	N/A	Yes	Yes	Block erase/program (1)
[127:126]=0x3, [125:0]=ID Code (not all 0xFF)	Match	No	Yes	Yes
	Match	Yes	Yes	Block erase/program (1)
	ALeRASE	No	No	All flash erased
	ALeRASE	Yes	No	No
[127:126]=0x2, [125:0]=ID Code	Match	No	Yes	Yes
	Match	Yes	Yes	Block erase/program (1)
[127]=0, [126:0]=X	Not ALeRASE	N/A	No	No
	ALeRASE	No	No	All flash erased
	ALeRASE	Yes	No	No

Note 1. Limitations:

- If the FAW is enabled and the target area is not entirely within the FAW, Erase and Write commands will fail.
- If FSPR=0, Option-setting memory (Config area) cannot be erased with the Erase command.
- If FSPR=0 and the target area contains FAWS, FAWE, FSPR, or BTFLG, a Write command will fail.

Do not use the value of the ALeRASE command (0x414C_6552_4153_45FF_FFFF_FFFF_FFFF_FFFF) as the ID code.

The most secure configuration is with the ID Code configured with bit 127 programmed to 0 and either the FSPR bit programmed to 0 or the Security MPU enabled; however, the application use case may require the ability to re-enable programming and/or debugging of the end-product. It is recommended to avoid using duplicate ID codes and, optimally, to use a unique ID Code for each chip.

For more details, refer to the following documents and sections of this document:

- [RA2E1 User Manual]
- [Boot Firmware]

12. Website and Support

Visit the following URLs to learn about key elements of the RA family, download components and related documentation, and get support:

RA Product Information	renesas.com/ra
RA2E1 Product Information	renesas.com/RA2E1
RA Product Support Forum	renesas.com/ra/forum
RA Flexible Software Package	renesas.com/FSP
Renesas Support	renesas.com/support
Renesas PSIRT	renesas.com/psirt

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Apr.03.25	—	Initial release

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/.