RL78/G24

FAA AES Library Introduction Guide

Introduction

This document presents information on introduction of the RL78/G24 FAA AES library (abbreviated below as “AES library”). The AES library is a software library that implements AES cryptographic processing on the RL78 MCU. The AES library is designed to enable efficient processing on the RL78 MCU.

The Flexible Application Accelerator (FAA) is an application accelerator employing a Harvard architecture that was developed by Renesas Electronics Corporation. Using the FAA for cryptographic processing boosts the processing speed of the AES library. The library supports generating code using Smart Configurator by selecting encryption or decryption. For details, refer to 2.2, AES Library Code Generation.

For details of API functions, refer to RL78/G24 FAA AES Library: User’s Manual (R20UW0176).

Operation Confirmation Device

RL78/G24

For the memory usage of the software, refer to 3.2, ROM, RAM, and Stack Sizes and Processing Times.

Contents

1. Product Components

The files included in the product are listed in Table 1.1.

Table 1.1 AES Library Product Components

Component	Description
Sample program (r20an0691xx0100-rl78g24-aes-faa) <DIR>	
workspace <DIR>	
doc (document) <DIR>	
en (English version) <DIR>	
r20uw0176ej0100-rl78g24-aes-faa.pdf	User's manual
r20an0691ej0100-rl78g24-aes-faa.pdf	Introduction Guide
ja (Japanese version) <DIR>	
r20uw0176jj0100-rl78g24-aes-faa.pdf	User's manual
r20an0691jj0100-rl78g24-aes-faa.pdf	Introduction Guide (this document)
CS+ <DIR>	CS+ project folder
sample_aes_rl78_faa <DIR>	G24 sample project storage folder
src <DIR>	Program storage folder
main.c	Sample program source code
main.h	
r_sample_aes128.c	
r_sample_aes256.c	
r_test_data.c	
r_test_data.h	
smc_gen <DIR>	Folders automatically generated by Smart Configurator
Config_FAA	FAA-related source file storage folder
general	Common header file source file storage folder
r_bsp	Storage folder for initialization code, register definitions, etc.
r_config	Driver initialization configuration header storage folder
r_pincfg	Symbolic name setting header storage folder for ports
e^2 studio <DIR>	e^2 studio project folder
sample_aes_rl78_faa <DIR> Below omitted.	G24 sample project storage folder Below omitted.

2. Product Specifications

2.1 API Functions

The AES library supports the API functions listed below.

For details of API functions, refer to RL78/G24 FAA AES Library: User's Manual (R20UW0176).

Table 2.1 AES Library API Functions

API Function Name*1	Description
R_"XXX"_Aes_128_Keysch	AES 128-bit expanded key generation function
R_"XXX"_Aes_128_Ecbenc	AES 128-bit encryption function (ECB mode)
R_"XXX"_Aes_128_Ecbdec	AES 128-bit decryption function (ECB mode)
R_"XXX"_Aes_128_Cbcenc	AES 128-bit encryption function (CBC mode)
R_"XXX"_Aes_128_Cbcdec	AES 128-bit decryption function (CBC mode)
R_"XXX"_Aes_256_Keysch	AES 256-bit expanded key generation function
R_"XXX"_Aes_256_Ecbenc	AES 256-bit encryption function (ECB mode)
R_"XXX"_Aes_256_Ecbdec	AES 256-bit decryption function (ECB mode)
R_"XXX"_Aes_256_Cbcenc	AES 256-bit encryption function (CBC mode)
R_"XXX"_Aes_256_Cbcdec	AES 256-bit decryption function (CBC mode)

Note: 1. "XXX" in the function name represents the configuration name. The configuration name is specified in Smart Configurator when adding the FAA component. For details, refer to 2.2.1, Code Generation Procedure.

2.2 AES Library Code Generation

The AES library supports generating code using Smart Configurator. The code generation procedure and settings related to code generation are described below.

Note: For details of Smart Configurator operations, refer to the following documents.
- RL78 Smart Configurator User's Guide: e² studio (R20AN0579)
- RL78 Smart Configurator User's Guide: CS+ (R20AN0580)

2.2.1 Code Generation Procedure

1. Add the **Flexible Application Accelerator** component (referred to below as the FAA component). The character string specified for **Configuration name:** when adding the component will be reflected in the API function names. The initial value of the configuration name is **Config_FAA**. For details of API function names, refer to 2.1, API Functions.

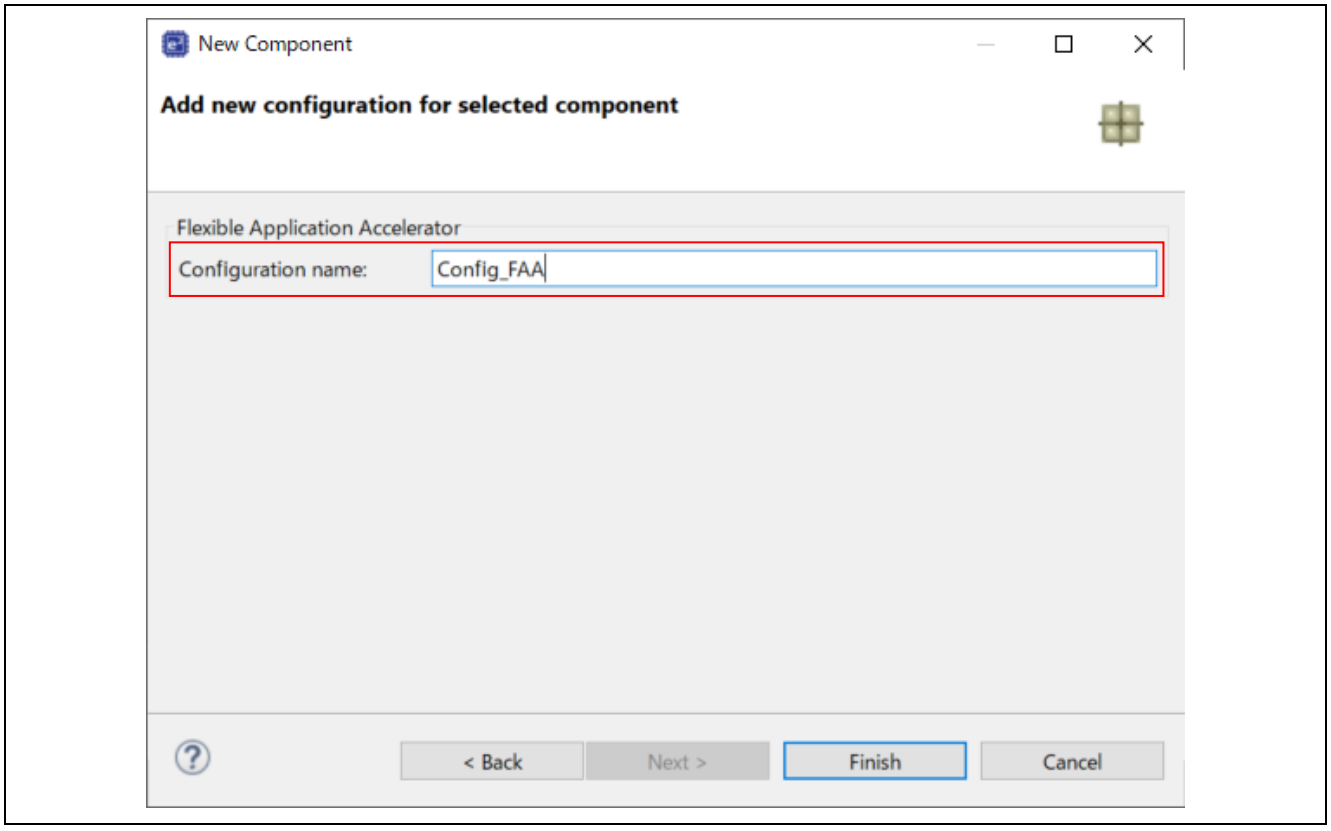

Figure 2.1 Adding a Component

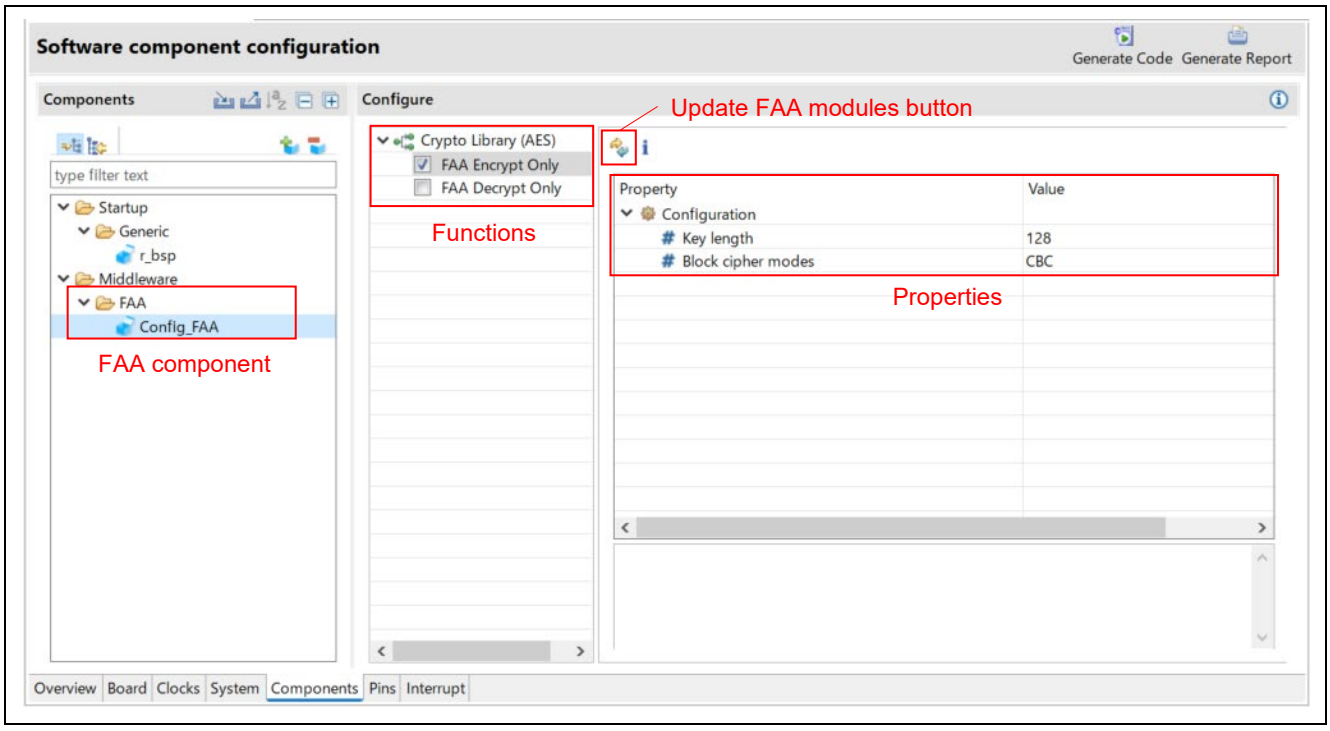

Figure 2.2 Software component configuration Window

2. Download the AES library.
   Click the **Update FAA Modules** button to display the FAA module download window. Select the AES library and download it.

3. Add a function
   Select one of the functions. Selecting both will cause the data capacity of the FAA to be exceeded during code generation, making the library unusable. For details of the functions, refer to 2.2.2, Functions.

4. When you select a function, its properties become configurable.
   Under **Property**, enter settings for **Key length** and **Block cipher modes**, then generate code. For details of the properties, refer to 2.2.3, Properties.

5. Code is generated according to the selected function and properties and stored in **\src\smc_gen\Config_FAA**.
   For details of the generated code, refer to 2.2.4, Details of Generated Code.

2.2.2 Functions

The functions are described below.

Table 2.2 Functions

Function*1	Description
FAA Encrypt Only	AES encryption using FAA
FAA Decrypt Only	AES decryption using FAA

Note: 1. It is not possible to select both functions at the same time because the data capacity of the FAA is insufficient.

2.2.3 Properties

The properties are described below.

Table 2.3 Properties

Property	Description
Key length	Selects the ley length to be used for encryption or description (128 or 256 bits).
Block cipher modes	Selects the block cypher mode (ECB, CBC, or ECB+CBC).

2.2.4 Details of Generated Code

Table 2.4 and Table 2.5 list details of the code generated when each of the two functions is selected in Smart Configurator.

Table 2.4 Code Generated when FAA Encrypt Only Function Selected

File Name*1	Description
“XXX”_AesEnc.c	FAA encryption C source file
“XXX”_AesEnc.h	FAA encryption header file
“XXX”_common.c	FAA common function C source file
“XXX”_common.h	FAA common function header file
“XXX”_common.inc	FAA iodefine header file
“XXX”_r_aes_version.c	AES library version information definitions
“XXX”_r_aeskey.c	AES key generation C source file
“XXX”_r_mw_version.h	Version information header file
“XXX”_r_stdint.h	Type definition header file
“XXX”_src.dsp	FAA encryption assembler file

Note: 1. “XXX” in the function name represents the configuration name. The configuration name is specified in Smart Configurator when adding the FAA component. For details, refer to 2.2.1, Code Generation Procedure.

Table 2.5 Code Generated when FAA Decrypt Only Function Selected

File Name*1	Description
“XXX”_AesDec.c	FAA encryption C source file
“XXX”_AesDec.h	FAA encryption header file
“XXX”_common.c	FAA common function C source file
“XXX”_common.h	FAA common function header file
“XXX”_common.inc	FAA iodefine header file
“XXX”_r_aes_version.c	AES library version information definitions
“XXX”_r_aeskey.c	AES key generation C source file
“XXX”_r_mw_version.h	Version information header file
“XXX”_r_stdint.h	Type definition header file
“XXX”_src.dsp	FAA encryption assembler file

Note: 1. “XXX” in the function name represents the configuration name. The configuration name is specified in Smart Configurator when adding the FAA component. For details, refer to 2.2.1, Code Generation Procedure.

2.2.5 API Functions Usable with Each Smart Configurator Setting

Table 2.6 and Table 2.7 list the API functions that are usable with each function, key length, and block cipher mode setting available in Smart Configurator.

Table 2.6 Usable API Functions when FAA Encrypt Only Function Selected

API Function Name*1	Key Length					
	128-Bit			256-Bit		
	Block Cipher Mode					
	ECB	CBC	ECB+CBC	ECB	CBC	ECB+CBC
R_“XXX”_Aes_128_Keysch	○	○	○	×	×	×
R_“XXX”_Aes_128_Ecbenc	○	×	○	×	×	×
R_“XXX”_Aes_128_Ecbdec	×	×	×	×	×	×
R_“XXX”_Aes_128_Cbcenc	×	○	○	×	×	×
R_“XXX”_Aes_128_Cbcdec	×	×	×	×	×	×
R_“XXX”_Aes_256_Keysch	×	×	×	○	○	○
R_“XXX”_Aes_256_Ecbenc	×	×	×	○	×	○
R_“XXX”_Aes_256_Ecbdec	×	×	×	×	×	×
R_“XXX”_Aes_256_Cbcenc	×	×	×	×	○	○
R_“XXX”_Aes_256_Cbcdec	×	×	×	×	×	×

○ = Usable
× = Not usable

Note: 1. “XXX” in the function name represents the configuration name. The configuration name is specified in Smart Configurator when adding the FAA component. For details, refer to 2.2.1, Code Generation Procedure.

Table 2.7 Usable API Functions when FAA Decrypt Only Function Selected

API Function Name*1	Key Length					
	128-Bit			256-Bit		
	Block Cipher Mode					
	ECB	CBC	ECB+CBC	ECB	CBC	ECB+CBC
R_“XXX”_Aes_128_Keysch	○	○	○	×	×	×
R_“XXX”_Aes_128_Ecbenc	×	×	×	×	×	×
R_“XXX”_Aes_128_Ecbdec	○	×	○	×	×	×
R_“XXX”_Aes_128_Cbcenc	×	×	×	×	×	×
R_“XXX”_Aes_128_Cbcdec	×	○	○	×	×	×
R_“XXX”_Aes_256_Keysch	×	×	×	○	○	○
R_“XXX”_Aes_256_Ecbenc	×	×	×	×	×	×
R_“XXX”_Aes_256_Ecbdec	×	×	×	○	×	○
R_“XXX”_Aes_256_Cbcenc	×	×	×	×	×	×
R_“XXX”_Aes_256_Cbcdec	×	×	×	×	○	○

○ = Usable
× = Not usable

Note: 1. “XXX” in the function name represents the configuration name. The configuration name is specified in Smart Configurator when adding the FAA component. For details, refer to 2.2.1, Code Generation Procedure.

2.3 Sample Project

The sample project performs encryption or decryption and then confirms if the result matches the expected value. The following Smart Configurator settings are used for code generation.

Function: FAA Encrypt Only

Key length: 128-bit

Block cipher mode: ECB+CBC

To change the function, key length, or block cipher mode settings, change the settings in Smart Configurator and then generate code. For the code generation method, refer to 2.2, AES Library Code Generation.

Using the sample program for reference, you can create your own programs utilizing API functions.

3. CC-RL (C Compiler)

3.1 Development Environment

The versions of the tools used to develop the product are listed below. When developing your own applications, use the latest versions of these tools.

- Integrated development environment
  e^2 studio 2023-07
  CS+ for CC V8.10.00
- C compiler
  CC-RL V1.12.01
- DSP assembler
  FAA Assembler V1.04.02

3.2 ROM, RAM, and Stack Sizes and Processing Times

The memory sizes and processing times for API functions when building a project using the following options are listed below for reference.

- Compiler options
  -cpu=S3 -memory_model=medium –Odefault
- Link options
  -NOOPtimize

The usable API functions vary depending on the Smart Configurator settings used for code generation. For details, refer to 2.2.5, API Functions Usable with Each Smart Configurator Setting.

Table 3.1 lists memory sizes for API functions. Sizes are listed for ROM, RAM, and stack on the CPU and for FAACODE and FAADATA on the FAA.

Table 3.1 ROM, RAM, Stack, FAACODE, and FAADATA Sizes [Bytes] for Each API Function

API Function Name*1	ROM*2	ROM*3	RAM	Stack	FAACODE*2	FAACODE*3	FAADATA
R_“XXX”_Aes_128_Keysch	2880		0	26	—*4		
R_“XXX”_Aes_128_Ecbenc	143	317		30	1056	1164	1972
R_“XXX”_Aes_128_Cbcenc	174			36	1100		
R_“XXX”_Aes_128_Ecbdec	143	317		58	1120	1228	1972
R_“XXX”_Aes_128_Cbcdec	174			64	1160		
R_“XXX”_Aes_256_Keysch	3325			28	—*4		
R_“XXX”_Aes_256_Ecbenc	143	317		30	1104	1212	1972
R_“XXX”_Aes_256_Cbcenc	174			36	1148		
R_“XXX”_Aes_256_Ecbdec	143	317		58	1168	1276	1972

Notes: 1. “XXX” in the function name represents the configuration name. The configuration name is specified in Smart Configurator when adding the FAA component. For details, refer to 2.2.1, Code Generation Procedure.
2. Values for ECB or CBC block cipher mode.
3. Values for ECB+CBC block cipher mode.
4. The expanded key generation function does not utilize the FAA.

Table 3.2 lists processing times for each API function.

Table 3.2 Processing Times for Each API Function

	time [us] @ system clock = 32 MHz	
API Function Name*1	1 block	3 blocks
R_“XXX”_Aes_128_Keysch	77	
R_“XXX”_Aes_128_Ecbenc	161	378
R_“XXX”_Aes_128_Ecbdec	331	583
R_“XXX”_Aes_128_Cbcenc	175	395
R_“XXX”_Aes_128_Cbcdec	346	600
R_“XXX”_Aes_256_Keysch	84	
R_“XXX”_Aes_256_Ecbenc	215	509
R_“XXX”_Aes_256_Ecbdec	455	785
R_“XXX”_Aes_256_Cbcenc	229	526
R_“XXX”_Aes_256_Cbcdec	470	801

Note: 1. “XXX” in the function name represents the configuration name. The configuration name is specified in Smart Configurator when adding the FAA component. For details, refer to 2.2.1, Code Generation Procedure

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Aug. 01, 2023	—	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/.