Renesas RA Family

RA Arm® TrustZone® Example Project QSG

Introduction

This Quick Start Guide (QSG) provides basic steps to import and run example projects for RA Arm® TrustZone® (TZ) for the RA Family of microcontrollers with e2studio. It also highlights methods to handle MCU pins and guard functions in a TZ project. A background knowledge of e² studio, RA device hardware, and Arm® TrustZone® Tooling Primer is expected.

Target Device

RA Arm® Cortex®-M33 devices with TrustZone security extension.

Contents

1. Where To Find TZ Example Projects

You can find TZ example projects in the "/example_projects/board_name/trustzone" folder, in the ra-fsp-examples-master.zip file.

This ra-fsp-examples-master.zip can be downloaded from https://github.com/renesas/ra-fsp-examples.

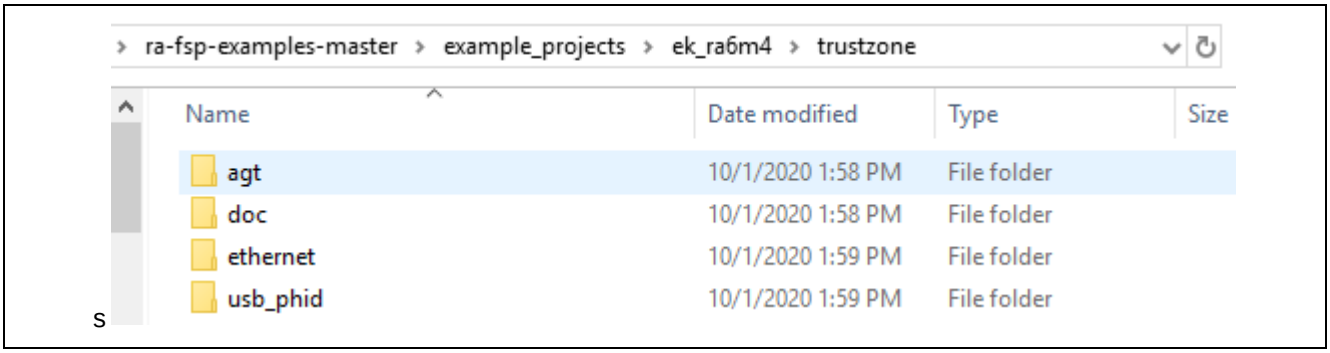

Figure 1. TZ Example Projects for EK-RA6M4 Kit in ra-fsp-examples-master.zip

Refer to Renesas Arm® TrustZone® Tooling Primer (r20an0577eg0101) and Security Design with Arm TrustZone - IP Protection App Note (r11an0467eu0100) for background knowledge of TZ project development.

2. Import and Build a TZ Project

A TZ example project consists of two projects within a workspace, a Secure project that is named with a prefix _s_ before the board name, and a Non-Secure project that is named with a prefix _ns_ before the board name. Follow the section "Importing an Existing Project into e2 studio" in FSP User's Manual to import a TZ example project. Browse to project folder, then import both import both secure and Non-Secure projects to your workspace at once, as shown in Figure 2.

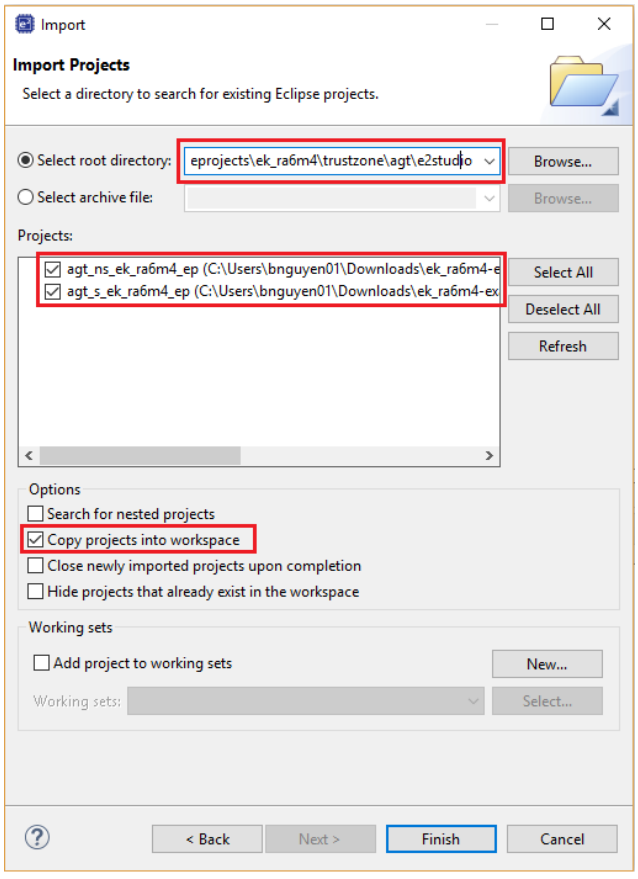

Figure 2. Import a TZ Example Project into e2stdio Workspace

After the TZ project is imported, follow the below steps to build a TZ project:

1. Double-click the Configuration.xml in the Secure project, then click “Generate Project Content” and build the Secure project. It is important to build the secure project every time the source code of the secure project is updated.
2. Double-click the Configuration.xml in the Non-Secure project, then click “Generate Project Content” and build the Non-Secure project.

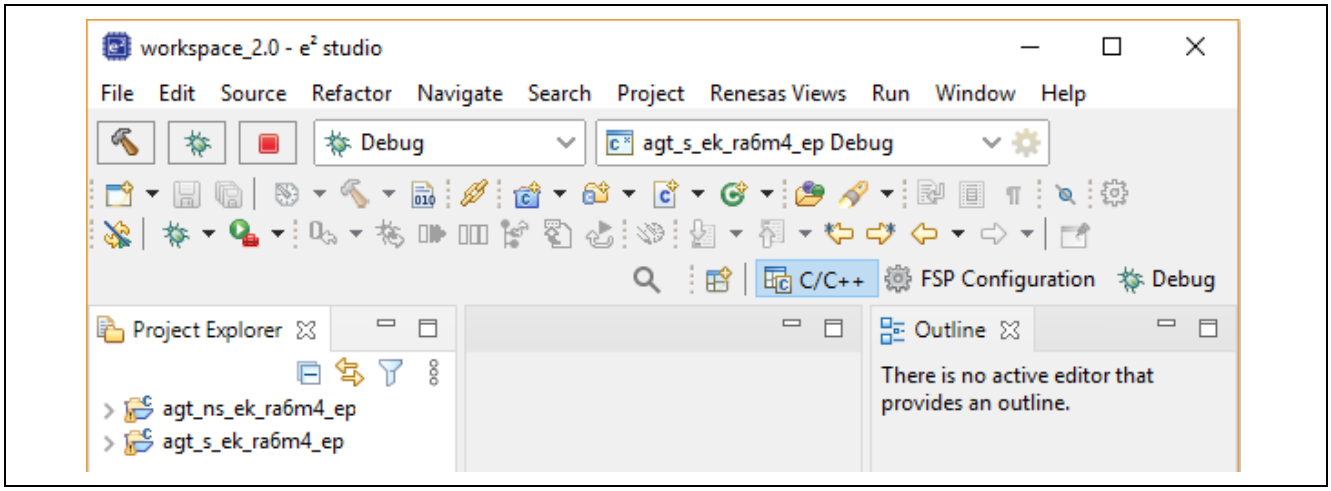

Figure 3. The TZ Example Project in e2Studio Workspace

Tip: You can use Project References setting in your Non-Secure project to ensure the Secure project is built every time the NS project is built, as shown in Figure 4. Note that this is not a default setting in the TZ example projects.

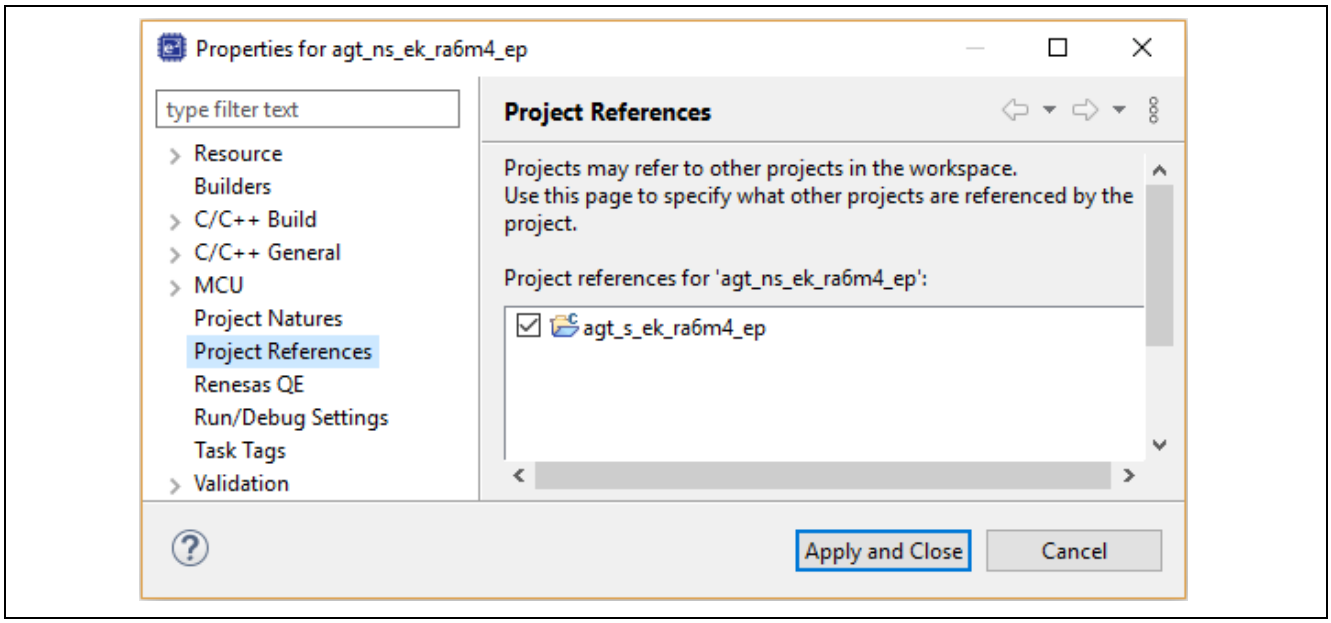

Figure 4. Project References in The Non-Secure Project

3. Debug a TZ Project

Right-click on the Non-Secure project, select “Debug As” then “Renesas GDB Hardware Debugging” to run the TZ example project.

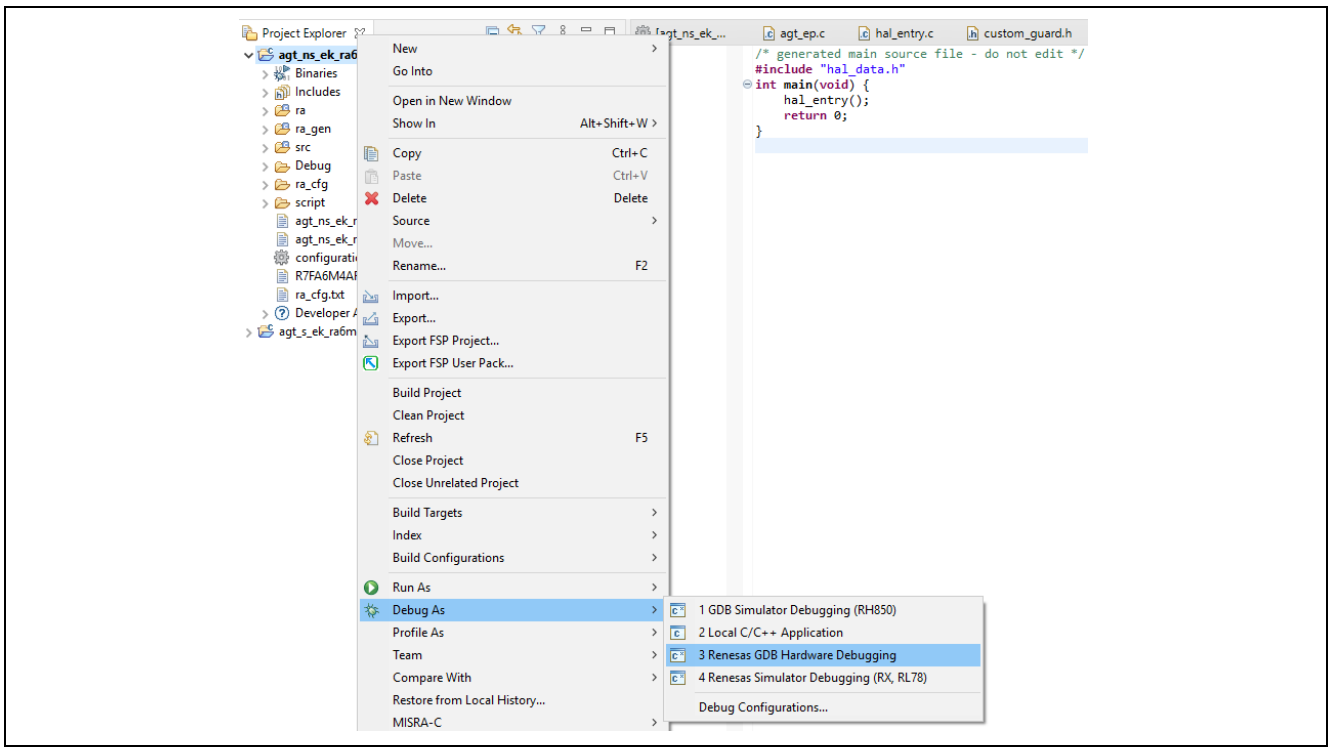

Figure 5. Debug a TZ Project

The Debug Configuration in the Non-Secure project is configured to allow downloading of both Secure and Non-Secure project at once, as shown in Figure 6.

Follow **readme.txt** in the example project folder to verify its functionalities.

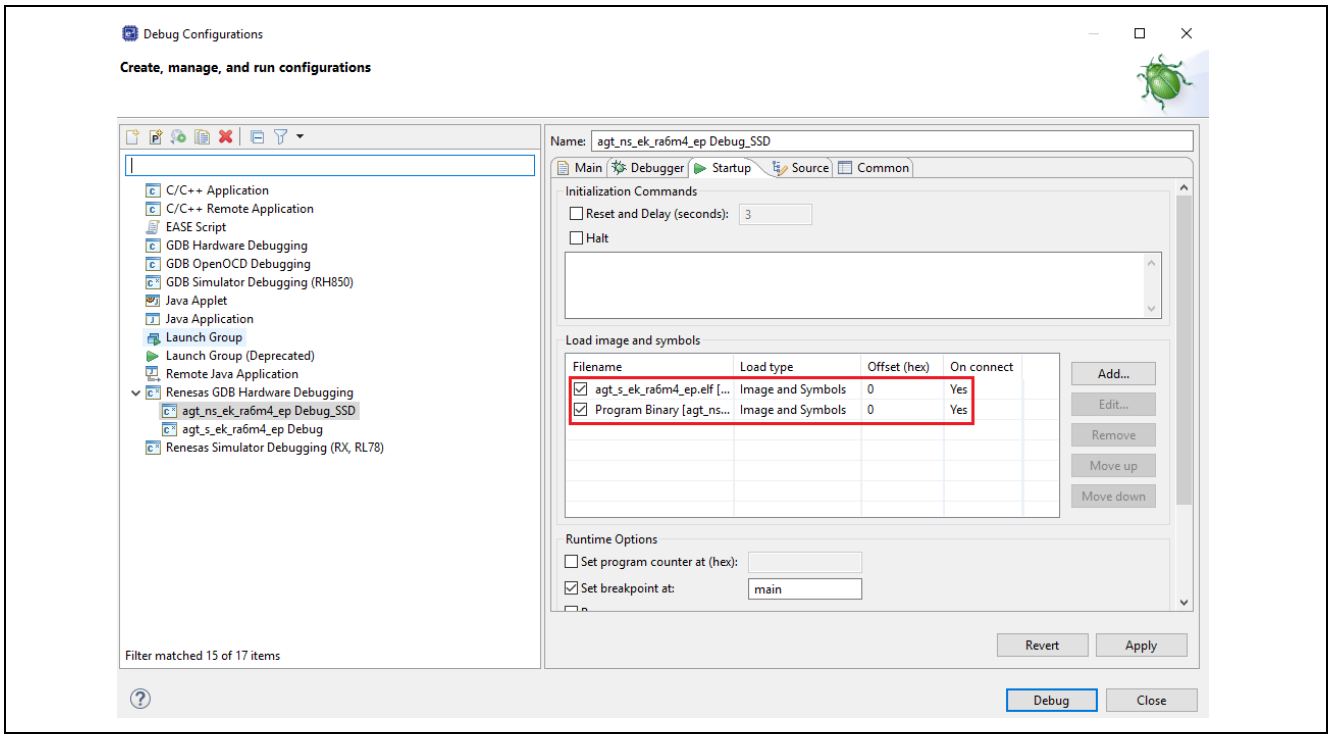

Figure 6. Startup Settings in the Non-Secure Project

4. Control Non-Secure Pin in The Non-Secure Project

A MCU pin is in Non-Secure mode when it is disabled in the Pin Configuration of the Secure project and is enabled in the Non-Secure project, as shown in Figure 7 and Figure 8.

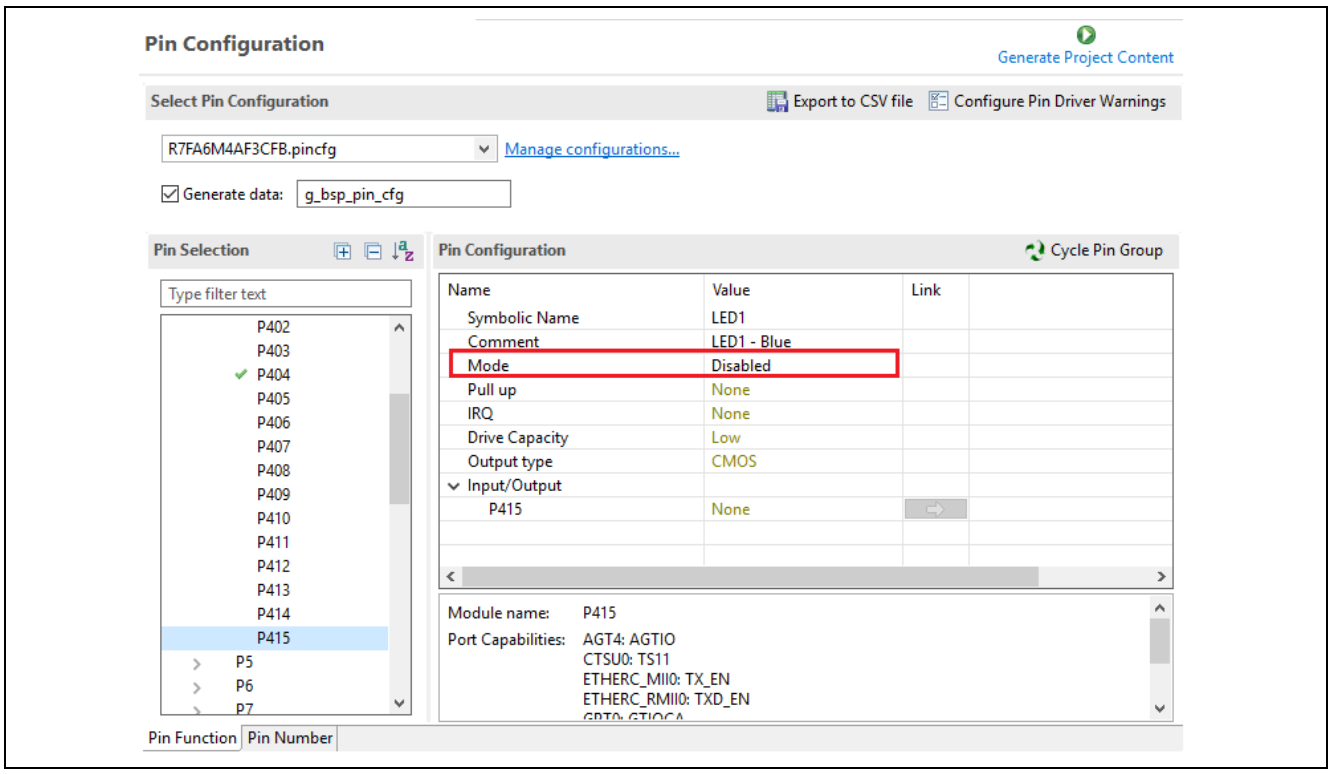

Figure 7. Disable Pin P415 (LED1) in The Secure Project

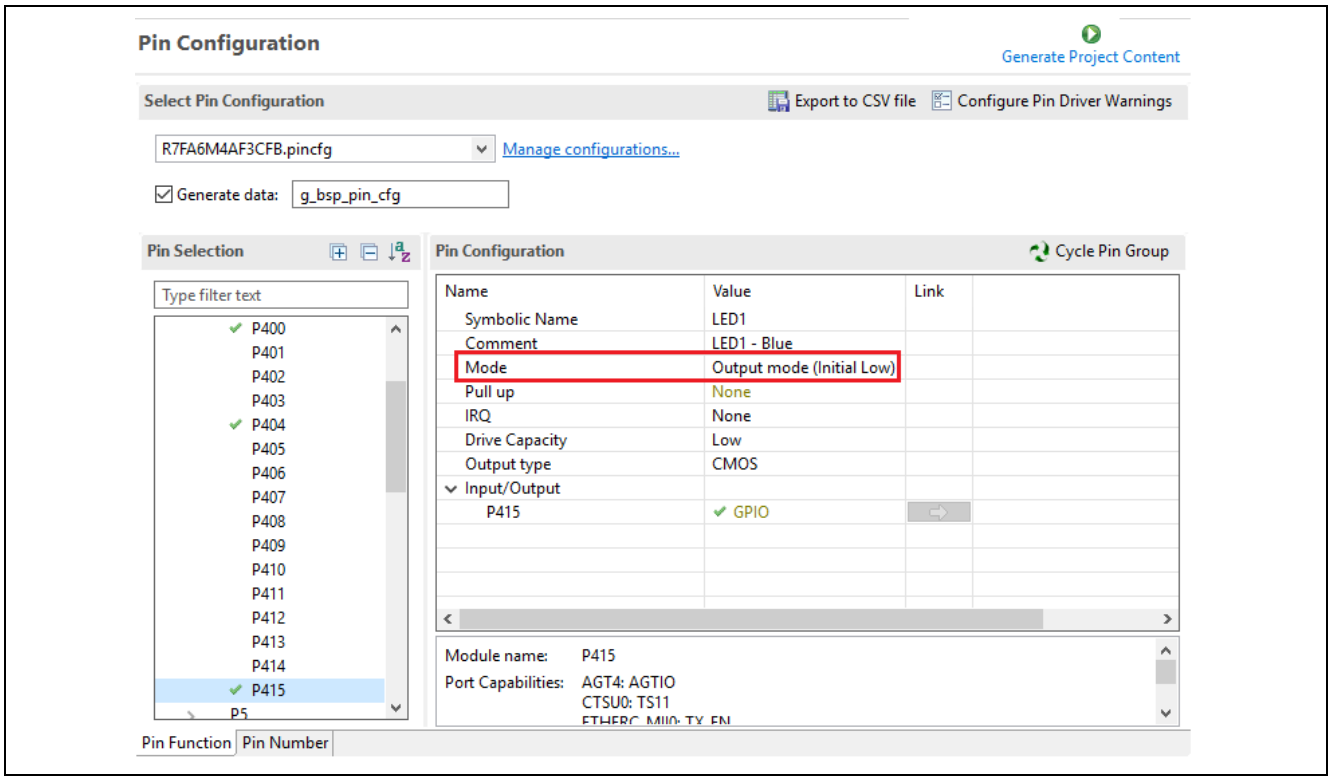

Figure 8. Enable Pin P415 (LED1) in The Non-Secure Project

You can control this Non-Secure pin by using driver APIs directly in the Non-Secure project.

```
/* Change LED state */
fsp_err_t err = R_IOPORT_PinWrite(&g_ioport_ctrl, (bsp_io_port_pin_t) g_bsp_leds.p_leds[RESET_FLAG], led_level);
```

Figure 9. Toggle LED1 in The Non-Secure Project

5. Control Secure Pin in The Non-Secure Project

A MCU pin is in Secure mode when it is enabled in the Pin Configuration in the Secure project, as shown in Figure 10.

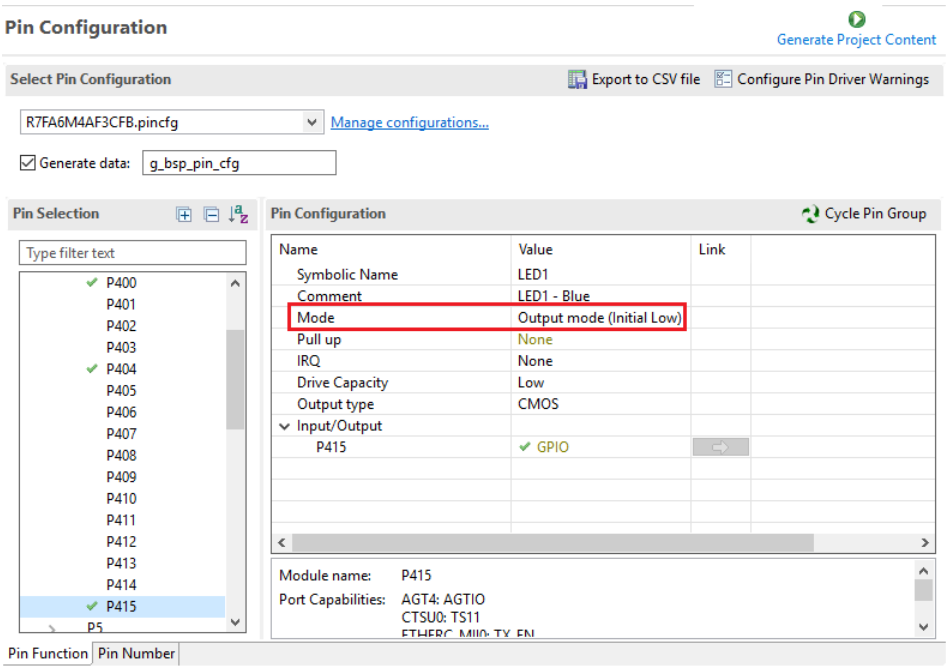

Figure 10. Enable Pin P415 in The Secure Project

If you want to control a secure pin, you need to create a guard function in the Secure project, as shown in Figure 11, then call this newly created guard function in the Non-Secure project.

```
/* Non secure callable function for LED1 */
BSP_CMSE_NONSECURE_ENTRY fsp_err_t led_set_guard (bsp_io_port_pin_t pin, bsp_io_level_t level)
{
    if(BSP_IO_PORT_04_PIN_15 == pin) //Only allowing access to LED1 (P415)
    {
        return R_IOPORT_PinWrite(&g_ioport_ctrl, pin, level);
    }
    else
    {
        return FSP_ERR_NOT_OPEN;
    }
}
```

Figure 11. Guard Function to Toggle LED1 in The Secure Project

Call the guard function to toggle LED1 in the Non-Secure project.

```
/* Turn ON LED to indicate callback triggered, along with output on RTT*/
led_set_guard(g_bsp_leds.p_leds[0], BSP_IO_LEVEL_HIGH);
```

Figure 12. Toggle LED1 in The Non-Secure Project

6. Remove Unused Guard Functions from TZ Project

FSP will automatically generate guard functions for stacks/drivers that are set as Non-Secure Callable in the "src" folder in the secure project. It is a good practice to remove guard functions when you don't use them. In the TZ example projects, it is handled by adding a macro to disable or enable un-used guard functions.

```
#include "guard.h"
#include "custom_guard.h"

#if UNUSED_GUARD_ON //Enable/disable unused guard functions

BSP_CMSE_NONSECURE_ENTRY fsp_err_t g_doc_status_get_guard(doc_ctrl_t *const p_api_ctrl, doc_status_t *p_status)
{
    /* Verify all pointers are in non-secure memory. */
    doc_status_t *p_status_checked = cmse_check_pointed_object (p_status, CMSE_AU_NONSECURE);
    FSP_ASSERT (p_status == p_status_checked);

    /* TODO: add your own security checks here */

    FSP_PARAMETER_NOT_USED (p_api_ctrl);

    return R_DOC_StatusGet (&g_doc_ctrl, p_status_checked);
}

BSP_CMSE_NONSECURE_ENTRY fsp_err_t g_doc_version_get_guard(fsp_version_t *const p_version)
{
    /* Verify all pointers are in non-secure memory. */
    fsp_version_t *const p_version_checked = cmse_check_pointed_object (p_version, CMSE_AU_NONSECURE);
    FSP_ASSERT (p_version == p_version_checked);

    /* TODO: add your own security checks here */

    return R_DOC_VersionGet (p_version_checked);
}

#endif

BSP_CMSE_NONSECURE_ENTRY fsp_err_t g_doc_open_guard(doc_ctrl_t *const p_api_ctrl, doc_cfg_t const *const p_cfg)
{
    /* TODO: add your own security checks here */

    FSP_PARAMETER_NOT_USED (p_api_ctrl);
    FSP_PARAMETER_NOT_USED (p_cfg);

    return R_DOC_Open (&g_doc_ctrl, &g_doc_cfg);
}

BSP_CMSE_NONSECURE_ENTRY fsp_err_t g_doc_close_guard(doc_ctrl_t *const p_api_ctrl)
{
    /* TODO: add your own security checks here */

    FSP_PARAMETER_NOT_USED (p_api_ctrl);

    return R_DOC_Close (&g_doc_ctrl);
}

BSP_CMSE_NONSECURE_ENTRY fsp_err_t g_doc_write_guard(doc_ctrl_t *const p_api_ctrl, uint16_t data)
```

Figure 13. Adding a Macro to Disable/Enable Un-Used Guard Functions

Website and Support

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

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

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Oct.01.20	—	First release document

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

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/.