

[Notification]

R20TS0438EJ0100

Rev.1.00

Jun. 16, 2019

Prevent Illicit Indirect Function Calls and Improve the Quality of Your Program!

Renesas Compiler Professional Edition

Detection of Illicit Indirect Function Calls

Outline

This tool news introduces one of the features of Renesas compiler (CC-RL/CC-RX/CC-RH) professional edition; "Detection of illicit indirect function calls".

This feature enables a compiler to check whether the addresses of indirect function calls can be trusted at runtime. The program may enter runaway execution or malfunction when a modified function pointer is used in an indirect function call. This feature can prevent such a situation and protect the system against bugs and security attacks, thus, improving the quality and safety of user programs.

1. Features

1.1 Improve Quality and Safety of User Programs

"Detection of illicit indirect function calls" is a feature that prevents indirect function calls to illicit addresses at runtime.

When this feature is enabled, the compiler automatically generates (a) to (c) below.

- Automatically extracts the functions that may be indirectly called and register them to a "list of safe function addresses".
- Generates code for the checking function that searches the "list of safe function addresses" for the address of each function immediately before the function is indirectly called.
- If, in (b), the address of the called function is not found in the "list of safe function addresses", the compiler generates code to branch to the error-handling process.

By calling the function to "check the destination address of an indirect function call" and to "branch to the error-handling process," this feature can improve the quality and security of user programs.

Process flows with and without the use of "detection of illicit indirect function calls" are shown below.

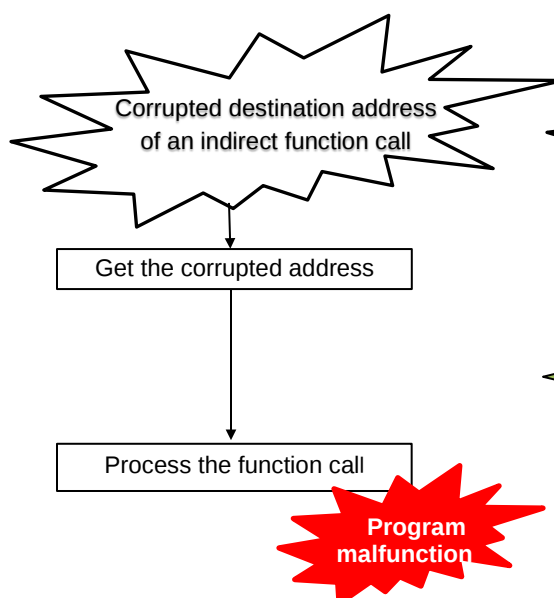


Figure 1-1 Standard processing

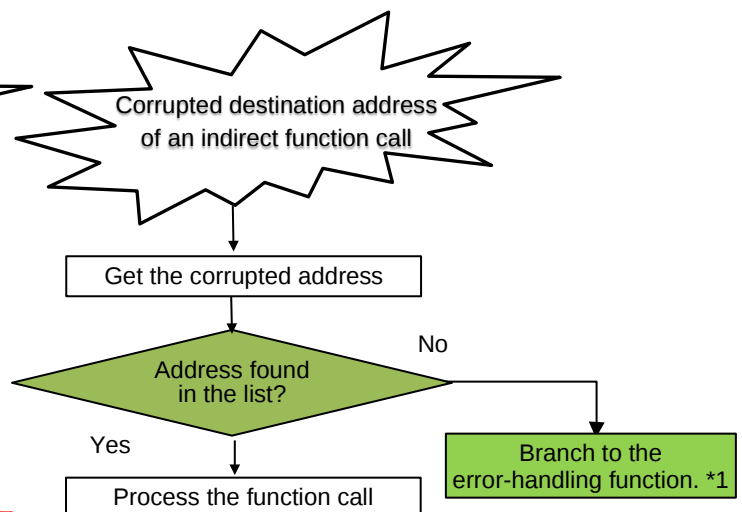


Figure 1-2 Process when "detection of illegal indirect function calls" is enabled

*1: The error-handling function can be defined by users.

1.2 Using This Feature

You can easily activate “detection of illicit indirect function calls” in integrated development environment GUI (CS+ or e² studio).

[For CS+]

- (1) From the menu bar, click [Display] > [Project tree] and select [Build tools].
- (2) On the [Property] tab > [Compile Options] > [Quality Improvement] category, click on the [Detect invalid indirect function call] property and select [Yes(-control_flow_integrity)].

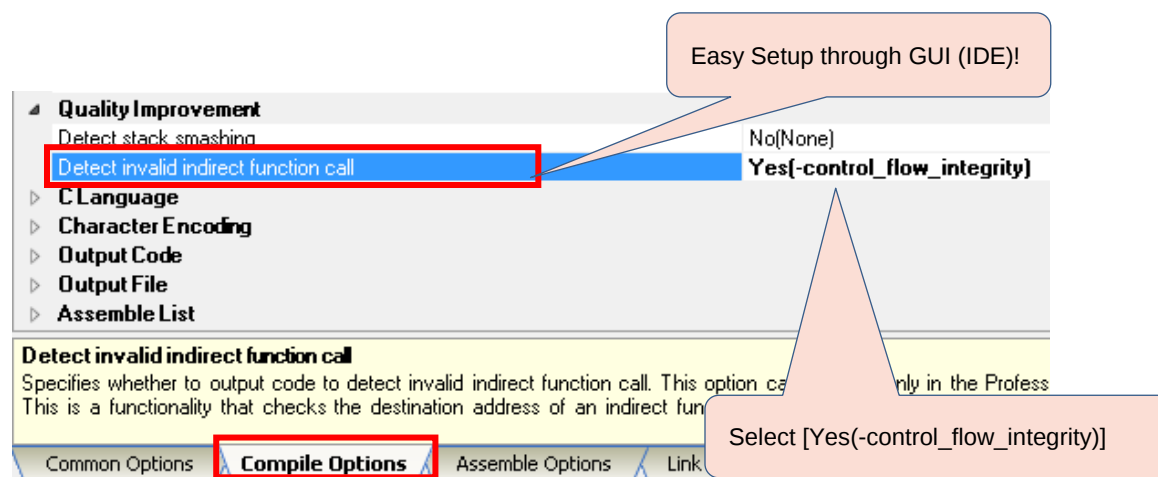


Figure 1-3 Settings for CS+

[For e² studio]

- (1) From the menu bar, select [Project] > [Properties] to open the property dialog box.
- (2) Click on [C/C++ Build] > [Settings] > [Tool Settings] tab, and select [Compiler] > [Miscellaneous] and activate [Generate an incorrect indirect function call detection code].

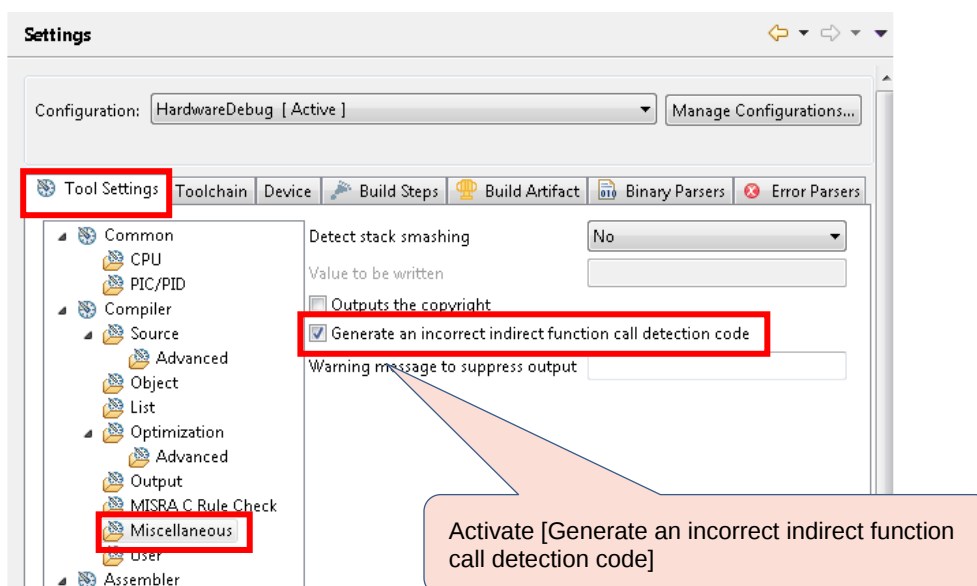


Figure 1-4 Settings for e² studio

2. More Features of Professional Edition

- Checking of source code against MISRA-C rules

Learn more about this feature in the tool news below.

<https://www.renesas.com/search/keyword-search.html#genre=document&q=r20ts0342>

[Notification] Perform MISRA-C Rule Check During Compilation to Reduce Man-hours and Improve Quality for Program Development!

Introducing MISRA-C Rule Checking Feature of Renesas Compiler Professional Edition

- Synchronization Features in the Updating of Control Registers

Learn more about this feature in the tool news below.

<https://www.renesas.com/search/keyword-search.html#genre=document&q=r20ts0347>

[Notification] Automatic Insertion of Synchronization Processing to Reduce Man-hours for Development of RH850 Family!

Synchronization Features in the Updating of Control Registers of Renesas Compiler Professional Edition

- Detection of Stack Smashing

Learn more about this feature in the tool news below.

<https://www.renesas.com/search/keyword-search.html#genre=document&q=r20ts0378>

[Notification] Dynamic Checking for Corruption in Stack Area for Quality and Security Enhancement!

Introducing Detection of Stack Smashing Feature of Renesas Compiler Professional Edition

- Other Useful Features

Renesas compiler professional edition provides more additional features*.

*: Enhanced security for dynamic memory management functions, half-precision floating point, etc.

For details, see the following leaflet.

<https://www.renesas.com/search/keyword-search.html#genre=document&q=r20pf0024>

For details about the features of the Renesas compiler professional edition, refer to the following application note. It describes the features that can improve the quality of your programs and accelerate product development period.

We also provide examples of C source which you can try immediately by copy/pasting.

<https://www.renesas.com/search/keyword-search.html#genre=document&q=r20out4026>

Renesas compiler professional edition

3. Purchasing the Product

To order a product, contact your local Renesas Electronics sales office or distributor.

If you own the standard edition node-locked license, you can upgrade the compiler from standard edition to professional edition by additionally purchasing the upgrade (edition) license. For orderable part numbers, see the following web pages for the compiler package.

CC-RL: https://www.renesas.com/rl78_c

CC-RX: https://www.renesas.com/rx_c

CC-RH: https://www.renesas.com/rh850_c

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Jun.16.19	-	First edition issued

Renesas Electronics has used reasonable care in preparing the information included in this document, but Renesas Electronics does not warrant that such information is error free. Renesas Electronics assumes no liability whatsoever for any damages incurred by you resulting from errors in or omissions from the information included herein.

The past news contents have been based on information at the time of publication. Now changed or invalid information may be included.

URLs in Tool News also may be subject to change or become invalid without prior notice.

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.