RZ/G,RZ/V SECURITY SOLUTION OVERVIEW

RENESAS ELECTRONICS CORPORATION

Disclaimer

1. Renesas Electronics & its affiliates do not make any warranty of accuracy, usefulness, certainty or any other kind, relating to the contents & any other information in this presentation (hereinafter "Contents").The Contents including but not limited to physical & electrical specifications/characteristics of products, block diagrams, etc. are subject to change without any notice. In no event shall Renesas Electronics & its affiliates be liable for any loss, expense or damage arising out of or in connection with the use of or reliance upon the Contents. Please refer to the product datasheet & user manual for the most accurate information for the purpose of planning & developing your product.
2. All product & company names & logos are trademarks™ or registered® trademarks of their respective holders

RENESAS

PURPOSE OF THIS DOCUMENT

This document describes what security solutions are available and prepared for RZ/G and RZ/V. For more information, please download the manual from the web page below.

RZ MPU Security Package

This document covers the following RZ/G and RZ/V devices with security features.

<Target device>

RZ/G2L, RZ/G2LC, RZ/G2UL

RZ/G2H, RZ/G2M, RZ/G2N, RZ/G2E

RZ/G3S

RZ/V2L

RZ SECURITY SOLUTION CONCEPT

RZ security solutions protect IoT products from cyber attacks.

Cyber Security Solutions

- Protect your IoT products from cyber attacks using Trustzone (Trusted Execution Environment) and Secure Boot.

IEC62443 Ready Solutions

- RZ security features with Secure IP are effective for obtaining IEC62443-4-2.

CYBER SECURITY SOLUTIONS

SECURITY FEATURES

This table shows the list of security features.

Download the Security Package for the relevant device from the web page below and incorporate it into the VLP* to enable the security functions. For details, please refer to the manual included in the Security Package.

*VLP : Verified Linux Package

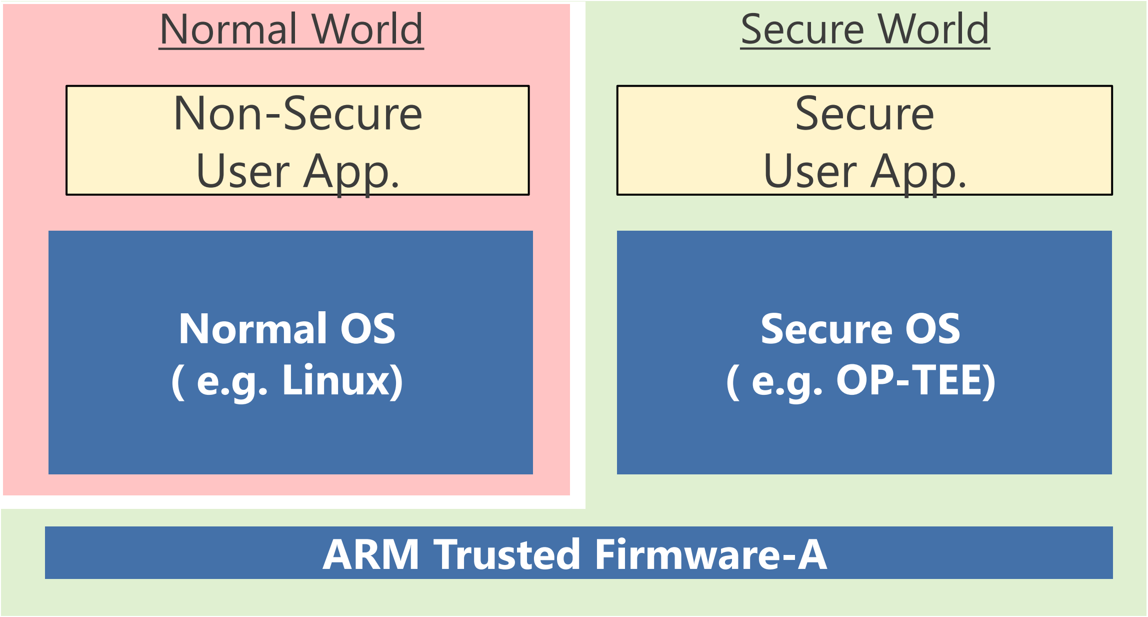
RZ MPU Security Package

Features	Descriptions	Functions and tools			
		Mask ROM	Secure IP	Trust Zone	Signature Tool
Trusted Execution Environment (TEE)	Isolated execution environment with ARM Trust Zone			✓	
Secure Boot	Detect falsification in programs loaded at startup	✓	✓	✓	
Signature addition for secure boot	Adding signatures to F/W for falsification detection		✓	✓	✓
Secure Debug	JTAG authentication connection （No authentication / JTAG authentication / Prohibit connection）	✓	✓	✓	

HARDWARE

ARM Trust Zone

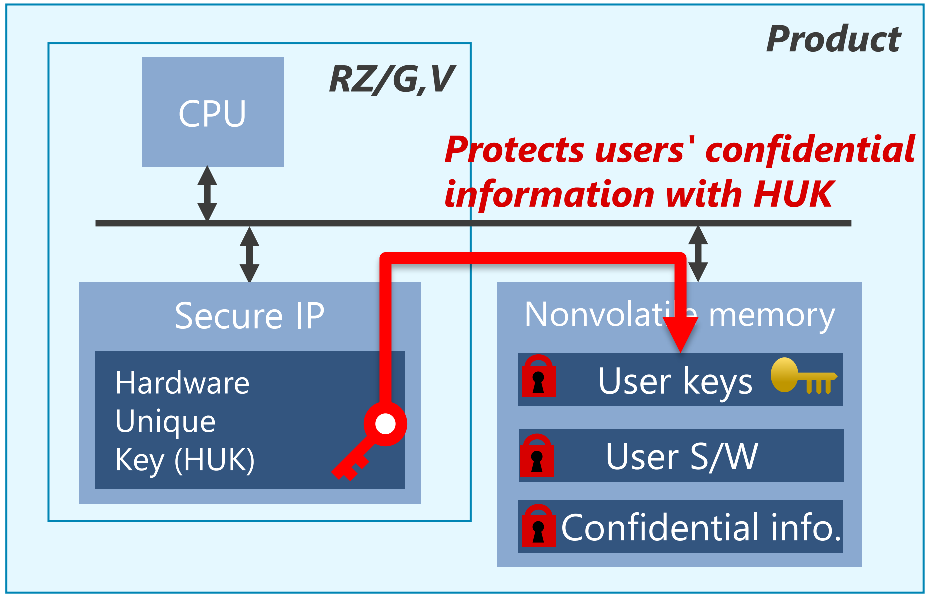
The software execution environment is separated into a normal world (non-secure area) and a secure world (secure area), and the secure area is isolated from external access to protect it from unauthorized access.

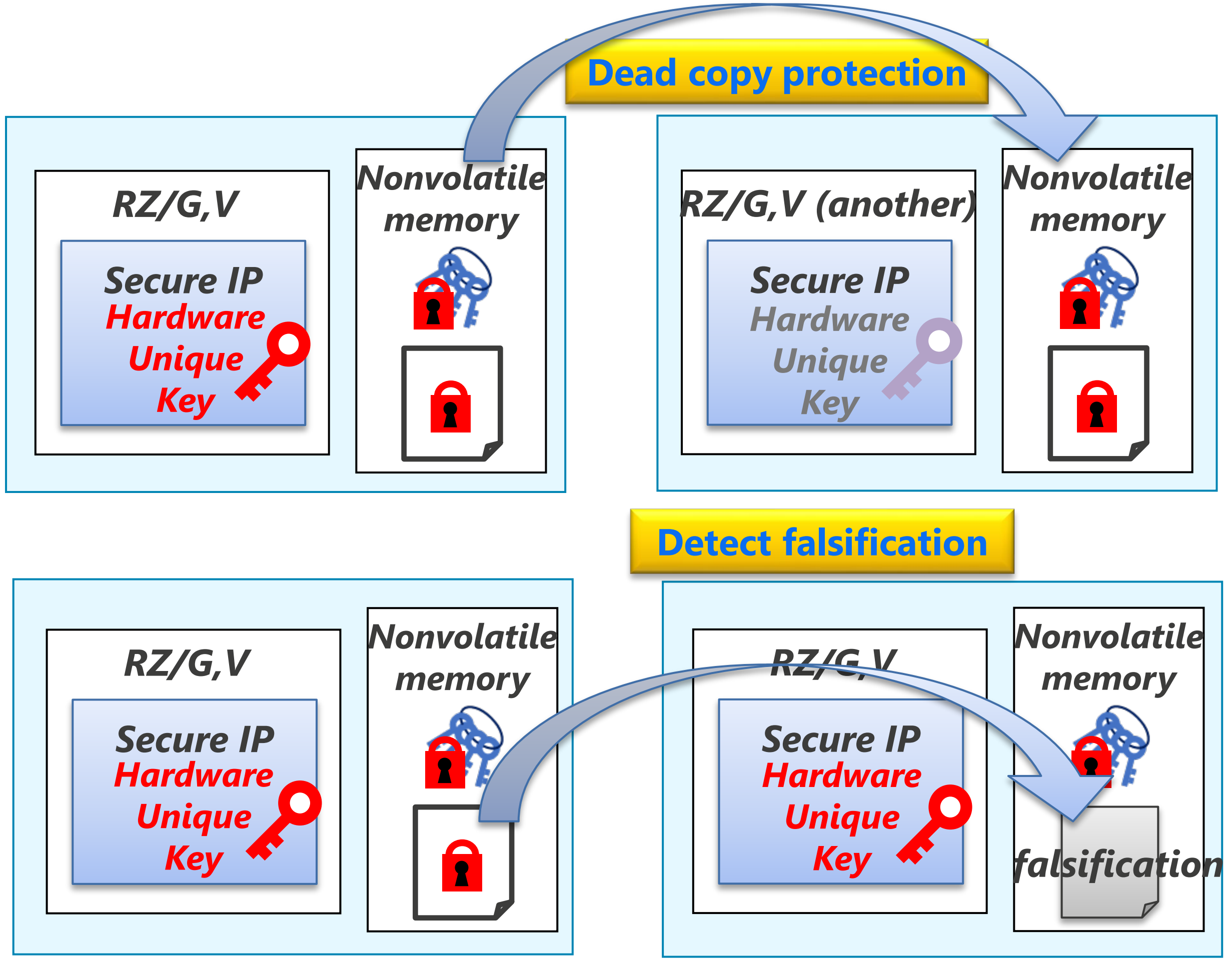


HARDWARE

Secure IP

Secure IP protects important data (user keys, user S/W, confidential information, etc.) by encrypting them with Hardware Unique Key(HUK) that is difficult to access from external.





How confidential information be protected?
Hardware Unique Key is based on unique values derived from the hardware mechanism, and this key is referenced only by Secure IP.

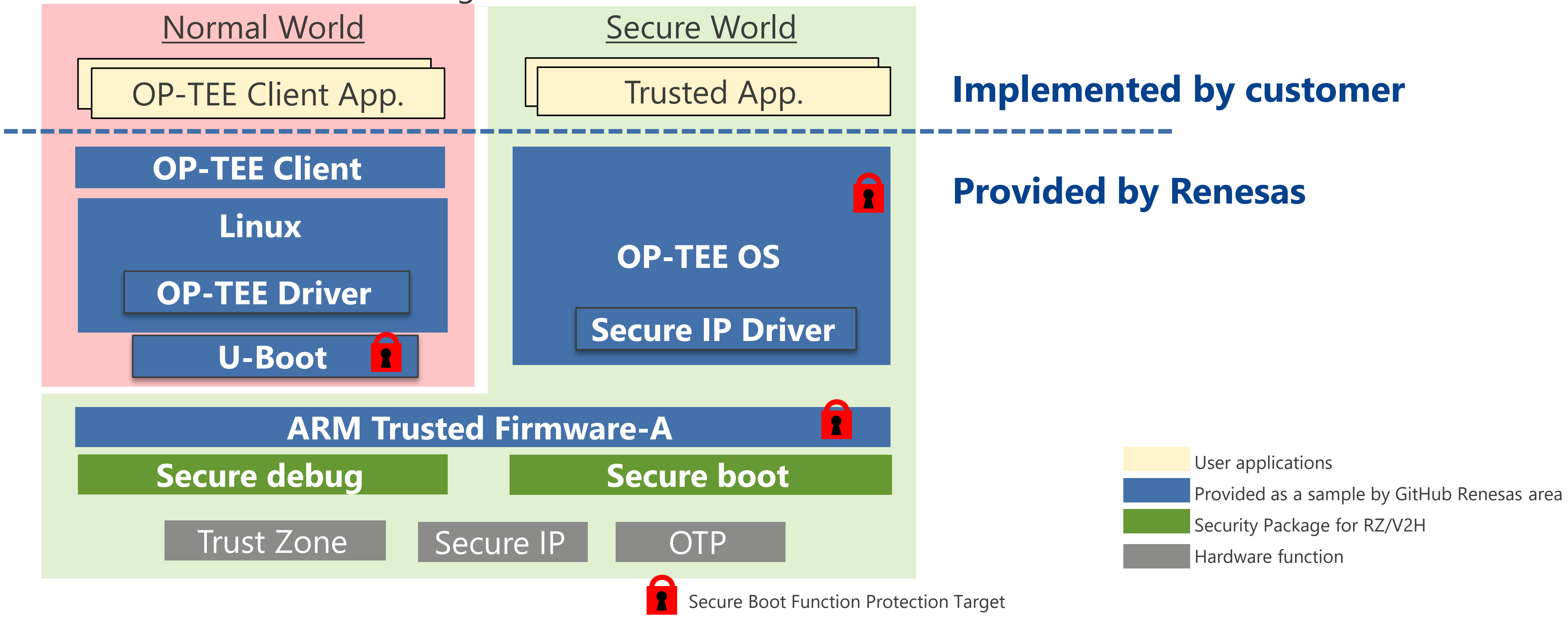
SOFTWARE

Security Package

A security package is provided for each OS provided for the RZ Family MPUs.

The security package includes security IP drivers, secure boot functions, encryption/decryption APIs, ARM Trusted Firmware, and a reference environment using OP-TEE.

Reference environment using OP-TEE



SERVICE

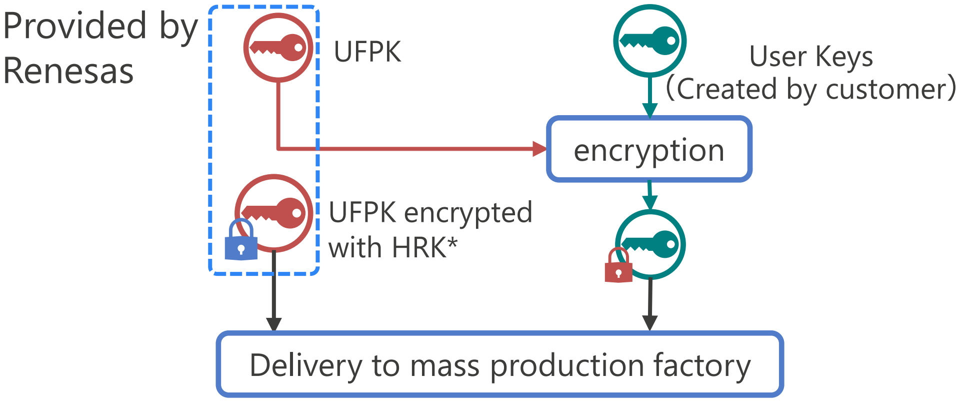
Renesas Key Wrap Service

This service is designed to make key writing more secure in the customer's mass production factory.
This service allows to use their own User Factory Programming Key(UFPK)*, further reducing the risk of user key leakage.

Customer Development Site

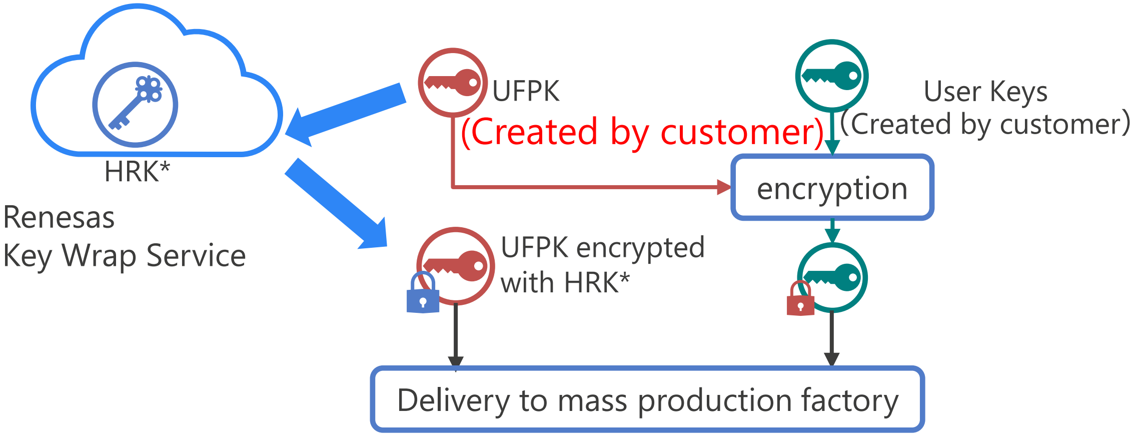
<Case of No Key Wrap Service>

UFPK is **common to all users**



<Case of Using Key Wrap Service>

UFPK is **different for each customer**



*User Factory Programming Key(UFPK) : Key to protect the user key until it is delivered from the customer development site to the mass production factory and written into the device.
*HRK (Hardware Root Key) : Key to protect factory write keys

IEC62443-4-2 READY SOLUTIONS

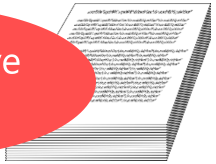
IEC62443-4-2 READY SOLUTIONS

DELIVERABLES

We offer three items that significantly reduce the time and cost of security development and certification for customers who use our RZ/G,V products to obtain IEC 62443-4-2.

Security Package For Linux

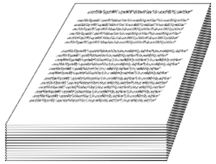
Renesas provides a security package for RZ/G, V products on our website. By using the driver software and libraries included in this package, you can achieve the security functions required for IEC62443-4-2 conformance evaluation.



Competitive point

Security Package Conformity Assessment Report

We provide IEC 62443-4-2 conformity assessment reports for security packages for Linux issued by **ISASecure** certification bodies. By using this, the security requirements to be met by the application can be clearly identified, and the man-hours required for the investigation and design process can be greatly reduced.



CIP Linux Package Conformance Assessment Report

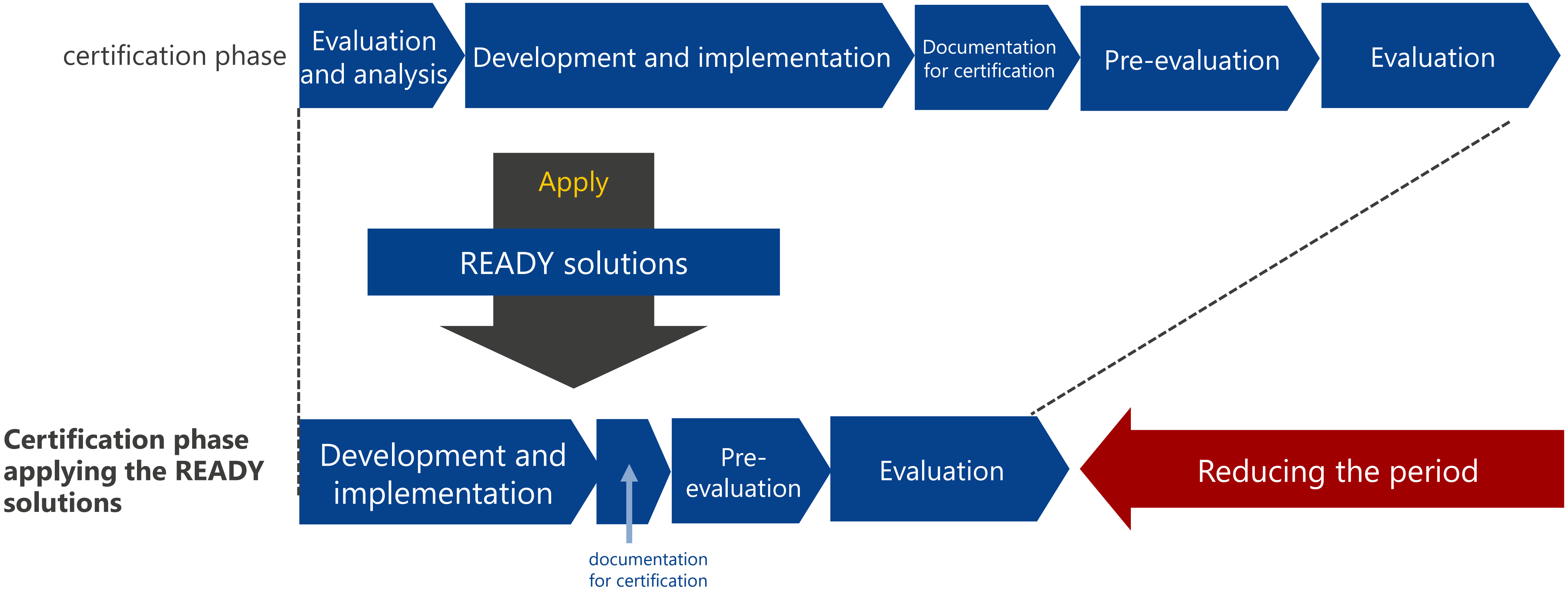
Many of the requirements of IEC 62443-4-2 must be realized by the device as well as by the software in general. By using the Linux package conformity assessment reports provided by CIP, customers can efficiently develop and implement IEC62443-4-2 compliant applications.

Please contact your distributor or Renesas sales representative to make a request.

IEC62443-4-2 READY SOLUTIONS

BENEFITS

Significantly reduced certification phase by applying Renesas solutions



certification phase
Evaluation and analysis
Development and implementation
Documentation for certification
Pre-evaluation
Evaluation
Apply
READY solutions
Certification phase applying the READY solutions
Development and implementation
Pre-evaluation
Evaluation
Reducing the period
documentation for certification

Renesas.com