

PG-FP6 V1.05 Flash Memory Programmer

User's Manual

All information contained in these materials, including products and product specifications, represents information on the product at the time of publication and is subject to change by Renesas Electronics Corporation without notice. Please review the latest information published by Renesas Electronics Corporation through various means, including the Renesas Electronics Corporation website (http://www.renesas.com).

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.
- 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.
- 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.
- 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/.

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.

PG-FP6 V1.05 Preface

Preface

Thank you for purchasing the PG-FP6. The PG-FP6 is a flash memory programmer for MCUs from Renesas Electronics.

If you have any questions about the PG-FP6, contact your local distributor.

You can download the latest manuals from the Renesas Tools homepage (https://www.renesas.com/pg-fp6).

PG-FP6 V1.05 Important

Important

Before using this product, be sure to read this user's manual carefully.

Keep this user's manual, and refer to it when you have questions about this product.

Purpose of use of the product:

This product is a device to support the development of systems that uses MCUs from Renesas Electronics. This product is a tool that erases, writes and verifies programs on a Renesas Electronics on-chip flash memory MCU on the target system.

Be sure to use this product correctly according to said purpose of use. Please avoid using this product other than for its intended purpose of use.

For those who use this product:

This product can only be used by those who have carefully read the user's manual and know how to use it.

Use of this product requires basic knowledge of electric circuits, logical circuits, and MCUs.

When using this product:

- (1) This product is a development-support unit for use in your program development and evaluation stages. When a program you have finished developing is to be incorporated in a mass-produced product, the judgment as to whether it can be put to practical use is entirely your own responsibility, and should be based on evaluation of the device on which it is installed and other experiments.
- (2) In no event shall Renesas Electronics Corporation be liable for any consequence arising from the use of this product.
- (3) Renesas Electronics Corporation strives to provide workarounds for and correct trouble with products malfunctions, with some free and some incurring charges. However, this does not necessarily mean that Renesas Electronics Corporation guarantees the provision of a workaround or correction under any circumstances.
- (4) Renesas Electronics Corporation cannot predict all possible situations and possible cases of misuse that carry a potential for danger. Therefore, the warnings in this user's manual and the warning labels attached to this product do not necessarily cover all such possible situations and cases. The customer is responsible for correctly and safely using this product.
- (5) The power adapter that comes with the product covered by this document conforms to the regionspecific standard. This fact must be taken into account when the product is to be used in some other country.
- (6) Renesas Electronics Corporation will not assume responsibility of direct or indirect damage caused by an accidental failure or malfunction in this product.

When disposing of this product:

Penalties may be applicable for incorrect disposal of this waste, in accordance with your national legislation.



PG-FP6 V1.05

Usage restrictions:

This product has been developed as a means of supporting system development by users. Therefore, do not use it as an embedded device in other equipment.

About product changes:

We are constantly making efforts to improve the design and performance of our product. Therefore, the specification or design of the product, or this user's manual, may be changed without prior notice.

About rights:

- (1) We assume no responsibility for any damage or infringement on patent rights or any other rights arising from the use of any information, products or circuits presented in this user's manual.
- (2) The information or data in this user's manual does not implicitly or otherwise grant a license to patent rights or any other rights belonging to Renesas or to a third party.
- (3) This user's manual and this product are copyrighted, with all rights reserved by Renesas. This user's manual may not be copied, duplicated or reproduced, in whole or part, without prior written consent from Renesas.

About diagrams:

Some diagrams in this user's manual may differ from the objects they represent.



Precautions for Safety

This chapter describes the precautions which should be taken in order to use this product safely and properly. Be sure to read and understand this chapter before using this product.

Contact us if you have any questions about the precautions described here.



WARNING indicates a potentially dangerous situation that will cause death or heavy wound unless it is avoided.



CAUTION indicates a potentially dangerous situation that will cause a slight injury or a medium-degree injury or property damage unless it is avoided.

In addition to the two above, the following are also used as appropriate.

△ means WARNING or CAUTION.

Example:



Example:



means A FORCIBLE ACTION.

Example:





Warnings for Power Supply:



If the power cable of the power adapter that comes with the product does not fit the receptacle, do not alter the power cable and do not plug it forcibly. Failure to comply may cause electric shock and/or fire.

Use a power cable which complies with the safety standard of the country.

Do not touch the plug of the power cable when your hands are wet. This may cause electric shock.

This product is connected signal ground with frame ground. If yours developing product is transform-less (not having isolation transformer of power), this may cause electric shock. Also, this may give an unrepairable damage to this product and your developing product.

While developing, connect power of the product to commercial power through isolation transformer in order to avoid these dangers.

To eliminate differences in potential between the grounds of this product and of the user system, only connect the plug of the power cable to the outlet after connecting this product and the user system.

If other equipment is connected to the same branch circuit, care should be taken not to overload the



If you smell a strange odor, hear an unusual sound, or see smoke coming from this product, then disconnect power immediately by unplugging the power cable from the outlet.

Do not use this as it is because of the danger of electric shock and/or fire. In this case, contact your local distributor.

Before setting up this product and connecting it to other devices, turn off power or remove a power cable to prevent injury or product damage.

Warnings to Be Taken for Handling:



Do not modify this product. Personal injury due to electric shock may occur if this product is modified. Modifying the product will void your warranty.

Warning for Installation:



Do not set this product in water or areas of high humidity. Spilling water or some other liquid into the product may cause un-repairable damage.

Warning for Use Temperature:



The maximum allowable ambient temperature for using this product is 35 °C. Care should be taken that a maximum ambient temperature is not exceeded when this product is to be used.



⚠ CAUTION

Caution on the Power Adapter:



Use only the supplied dedicated power adapter for this product.

Do not use the power adapter for other equipment.

Caution on Turning on the Power:



Observe the following specified order for the power-on and power-off procedures of the user system and this product. Doing otherwise may cause the user system or this product to fail.

Power ON: (1) This product ON, (2) User system ON

Power OFF: (1) User system OFF, (2) This product OFF

Caution on Handling This Product:



Exercise caution when handling the product. Be careful not to apply a mechanical shock.

Do not touch the connector pins of this product and the target MCU connector pins directly. Static electricity may damage the internal circuits.

When attaching and removing the cable, hold the plug of the cable and do not touch the cable. Do not pull this product by the communications interface cable or the flexible cable. Excessive flexing or force may break conductors.





Caution on System Malfunctions:



If this product malfunctions because of interference like external noise, do the following to remedy the

Exit the FP6 Terminal, and shut OFF this product and the user system.

After a lapse of 10 seconds, turn ON the power of this product and the user system again, and then launch the FP6 Terminal.

Caution on Disposal:



Penalties may be applicable for incorrect disposal of this waste, in accordance with your national legislation.

European Union regulatory notices:



The WEEE (Waste Electrical and Electronic Equipment) regulations put responsibilities on producers for the collection and recycling or disposal of electrical and electronic waste. Return of WEEE under these regulations is applicable in the European Union only. This equipment (including all accessories) is not intended for household use. After use the equipment cannot be disposed of as household waste, and the WEEE must be treated, recycled and disposed of in an environmentally sound manner.



Renesas Electronics Europe GmbH can take back end of life equipment, register for this service at "http://www.renesas.eu/weee".



Contents

Preface	4
Important	
Precautions for Safety	7
Contents	11
Terminology	16
Replacing Terms	18
1. Overview	10
• •	20
, ,	21
•	21
1 0	21
	21
•	
9	
	23
	23
	24
o , ,	24
	24
3. Software Installation	30
	30
3	30
	31
4. Usage of the FP6 Terminal	
	33
T T	35
4.2.1 [Create New Setting] dialog box	35
- '-	36
	37
	38
	41
	42
	46
. ,	50
4.4 Menu Bar	
	52
	55
	61
	64
	65
4.6 Example of Operation Using the FP6 Terminal	66

4.6.1	Installing the FP6 Terminal and USB driver	
4.6.2	Connecting the FP6 to the host PC	
4.6.3	Connecting the target system	
4.6.4	Starting up the FP6 Terminal	
4.6.5	Setting up a programming environment	
4.6.6	Executing the [Start] command	
4.6.7	System shutdown	72
5. Usage	e in Standalone Mode	73
5.1 Det	ails of Buttons, Message Display, and Status LEDs	73
5.2 Sta	ndalone Operation Menu	75
5.2.1	[Commands] menu	75
5.2.2	[Project] menu	76
5.2.3	[Utility] menu	76
6. Usage	e of the Remote Connector	77
6.1 Rer	mote Interface Mode	77
7. Usage	e of Communications Commands	78
7.1 Sta	rting the Communications Software	78
7.1.1	Connecting the system	78
7.1.2	Starting the FP6	78
7.1.3	Starting communications software	78
7.2 Con	nmand Lists	79
7.3 Des	scription of Commands	81
7.4 Des	scription of FP6 Control Commands	82
7.4.1	autocon command	82
7.4.2	brt command	83
7.4.3	conf command	84
7.4.4	downprm command	
7.4.5	downset command	86
7.4.6	fcks command	
7.4.7	files command	
7.4.8	hex command	
7.4.9	hlp command	
7.4.10	lod command	
7.4.11	prm command	
7.4.12	progarea command	
7.4.13	res command	
7.4.14	selftest command	
7.4.15	serno command	
7.4.16	set_auth command	
7.4.17	sound command	
7.4.18	speed_mode command	
7.4.19	srec command	
7.4.20	trc command	
7.4.21	upprm command	
7.4.22	upset command	
7.4.23	ver command	
	scription of FP6 Device Commands	
7.5.1	bln command	
7.5.2	clr command	
7.5.3	con command	
7.5.4	dcon command	
7.5.5	dlm command	107



7.5.6	ep command	108
7.5.7	ers command	109
7.5.8	ers_chip command	109
7.5.9	gdi command	110
7.5.10	ged command	111
7.5.11	gid command	111
7.5.12	glb command	112
7.5.13	gob command	112
7.5.14	gof command	113
7.5.15	gos command	113
7.5.16	got command	114
7.5.17	gsc command	114
7.5.18	gtm command	115
7.5.19	idc command	115
7.5.20	opb command	116
7.5.21	otp command	116
7.5.22	pfo command	117
7.5.23	prg command	118
7.5.24	read command	119
7.5.25	rsc command	120
7.5.26	scf command	
7.5.27	sed command	
7.5.28	sid command	
7.5.29	sig command	
7.5.30	slb command	
7.5.31	spd command	
7.5.32	stm command	
7.5.33	sum command	
7.5.34	vrf command	
	e Here B	405
	ption Utility Program	
	t Code	
	mmand-line Syntax	
8.3 Sta	rt Options	125
٥. ٥	EL LD LIEB D	100
	sas Flash Programmer Utility Program	
	t Code	
	mmand-line Syntax	
	of Commands	
9.4 Sta	rt Options	127
10 Con	nectors and Cables	120
	ver-Supply Connector	
	ial Connector	
10.2.1	Serial cable connected to the 9-pin D-sub serial connector	
	B Connector	
10.3.1	USB cable	
	get Connector	
10.4.1	Target cable (14-pin type)	
10.4.2	14-pin to 16-pin conversion adapter for the E1 emulator	
10.4.3	20-pin conversion adapter for the PG-FP6	
	D Connector	
10.5.1	GND cable	
10.6 Rer	mote Connector	137

11. E	Examples of Connections with Microcontrollers	139
11.1	78K and V850 (UART communications)	139
11.2	78K and V850 (CSI communications)	
11.3	78K and V850 (CSI-H/S communications)	
11.4	78K0S (Single-wire UART communications)	142
11.5	78K0R (Single-wire UART communications)	142
11.6	78K0 (TOOLCx and TOOLDx communications)	143
11.7	V850E2 (Single-wire UART communications)	143
11.8	V850E2 (CSI communications)	
11.9	RL78 (Single-wire UART communications, VDD = EVDD)	145
11.10	RL78 (Single-wire UART communications, VDD ≠ EVDD)	145
	RX and SuperH (SCI communications)	
	R8C	
11.13	RX100, RX200, RX65x, and RX66T (FINE communications)	147
	RH850 type 1 (1-wire UART communications)	
11.15	RH850 type 1 (2-wire UART or CSI communications)	149
	RH850 type 2 (2-wire UART or CSI communications)	
	Renesas Synergy™ (UART communications)	
11.18	RE (UART communications)	151
11.19	RA (UART communications)	152
12. T	Froubleshooting	
12.1	-	
12.2	Problems during Operation	
	2.2.1 When an error produces the message 'ERROR: 004 No response'	
12	2.2.2 When an error produces the message '023 Inv. Sig. addr.'	
12	2.2.3 When an error produces the message 'Communication failure or timeout'	154
12 🗆	Points for Caution	156
13.1	Checking before Connection	
13.1	Manipulating the User Boot Mat	
13.2	Erasing a Chip	
13.4	Auto-Padding with 0xFF	
13.5	Wide Voltage Mode	
13.6	Switching to Dual Mode	
13.7	RPI Files	
	RPE Files	
	Verification after Protecting the MCU	
	Changing the Speed of Communications with the FP6	
13.10	Changing the Speed of Communications with the FP6	150
14. N	Maintenance and Warranty	159
14.1	Maintenance	
14.2	Warranty	
14.3	Repair Provisions	
14.4	How to Make Request for Repair	
Appe	endix A. Messages	161
A.1	Messages Defined in the FP6 Terminal	161
A.2	Error Messages Produced by the FP6 Main Unit	163
A.3	Error Messages Produced by the FP6 Main Unit that are Only Displayed in the Terminal	171
A.4	List of Security and Safety Functions of the Target Device that May Affect the Operation of the	
Progr	ammer	172
_		
	endix B. Supplementary Information	
B.1	32-Bit CRC Method	173



PG-FP6 V1.05

B.2	Divi	sion Method	174
B.3		Bit CRC Method	
Арр	endi	C. Equivalent Circuits of the Target Interface	177
App	endi	CD. Electrical Specifications of the Remote Interface	178
D.1		olute Maximum Ratings (TA=0 to 40°C)	
D.2		Characteristics (T _A =0 to 40°C, C=0pF (Unloaded Condition))	
D.3	AC	Characteristics (T _A =0 to 40°C, C=0pF (Unloaded Condition))	179
D	.3.1	Standard mode	
D	.3.2	Bank mode	181
D	.3.3	Simple mode	
aaA	endi	κ Ε. Electrical Specifications of the Target Interface	186
		olute Maximum Ratings (TA=0 to 40°C)	
		Characteristics (T _A =0 to 40°C)	

PG-FP6 V1.05 Terminology

Terminology

The meanings of the terms used in this document are as follows.

Term	Meaning	
FP6	Abbreviation of the flash memory programmer PG-FP6	
FP6 Terminal	Windows® application for setting up the PG-FP6 main unit and handling commands	
MCU	Abbreviation of "microcontroller unit"	
Target device	On-chip flash memory microcontroller from Renesas Electronics	
Target system	User-designed board on which the target device is mounted	
Setting file	FP6's setting file (file extension: *.esf or .es6). This file contains settings regarding the programming environment such as the target device and options.	
Program file	Program to be written to the MCU. For the FP6, the following file formats are supported. <rl78, 78k,="" and="" v850=""> a. Intel HEX format HEX file b. Intel HEX format HCUHEX file c. Motorola S-record format HEX file d. Motorola S-record format HCUHEX file e. RPI file (only supported for RL78 products) f. RPE file <rx and="" family="" superh=""> a. Intel HEX format HEX file b. Motorola S-record format HEX file c. DDI file (only supported for SuperH products) d. RPI file e. RPE file <rh850 and="" family="" family,="" r8c="" ra="" re="" renesas="" synergy™=""> a. Intel HEX format HEX file b. Motorola S-record format HEX file c. RPI file (not supported for R8C products) d. RPE file</rh850></rx></rl78,>	
	Note Only the ASCII character code (1 byte) is supported. Unicode is not supported.	
Flash-option data	General term for MCU operation settings such as security settings	
HEX file	HEX file of Intel HEX format type or Motorola S-record format type that does not include flash-option data	
HCUHEX file	For details, refer to the following Web page.	
	https://www.renesas.com/us/en/hcu	
DDI file	File that contains data in multiple flash areas generated by the Flash Development Toolkit	
RPI file	Image file generated by the RFP that combine usable HEX files and flash-option data	
RPE file	An encrypted program file that has been generated by the encryption utility program	
Flash Development Toolkit	Software for programming the on-chip flash memory of Renesas MCUs. For details, refer to the following Web page. https://www.renesas.com/fdt	
RFP	Abbreviation of "Renesas Flash Programmer", software for programming the on-chip flash memory of Renesas MCUs. For details, refer to the following Web page. https://www.renesas.com/rfp	
Parameter file	Information file specific to the target device (file extension: *.pr5 or .pr6). This file is generated by the PG-FP6. Each parameter file holds parameter information required for programming of the flash memory in the target device.	



PG-FP6 V1.05 Terminology

Term	Meaning	
FINE	Single- or dual-line communications interface operating through the FINE pins of an MCU. Some of our MCUs support programming via single-line FINE.	
ID authentication mode	One of the security features of the MCU. Connection of the flash programmer is protected by ID authentication.	
	For details, refer to the user's manual of the MCU.	
Command protection mode	One of the security features of the MCU. Execution of individual commands (e.g., the erase command) can be restricted.	
	For details on operations while the security feature is enabled, refer to the user's manual of the MCU.	
TSIP	Dedicated hardware secure IP (Trusted Secure IP) for managing encryption keys. For details, contact a Renesas Electronics sales office.	
ID Tag	Data for programming in the data flash memory of some V850 target devices. For details, refer to the user's manual of the target device.	

PG-FP6 V1.05 Replacing Terms

Replacing Terms

Some terms used in this application should be replaced as shown in the tables below, depending on the MCU to be used.

• When an RL78 MCU is to be used:

Term in This Application	To be Replaced with
Access window (AW)	Flash shield window

• When an RH850 with an extended user area is to be used:

Term in This Application	To be Replaced with
User Boot Area	Extended user area

1.Overview

The FP6 is a tool that is used to erase, write, and verify programs on a Renesas Electronics on-chip flash memory MCU on the target system.

1.1 Features

- Standalone programming
- Programming through a dedicated GUI under PC control
- Up to eight instances of programming environment available
- Specialized for use on production lines (command control via serial communication and remote control of signals from external devices)
 - Compatibility with the PG-FP5 interface allows utilization of resources developed with the PG-FP5.
- Programming of a unique code to a designated area of flash memory
- The FP6 Manager allows the customization required in development and mass-production, such as prevention of a programming operator from modifying the programming settings.
- · Self-testing function
- Support for high-volume programming by gang programming with the use of multiple PG-FP6 units*1
- Enhancement of the FP6 Manager and the encryption of program files to improve security against theft*2

Notes: 1. FP6 Terminal V1.03.00 or a later version

2. FP6 Terminal V1.04.00 or a later version

1.2 Supported MCUs

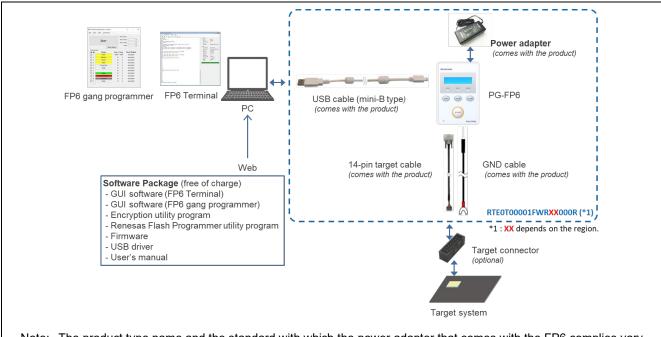
MCUs supported by the FP6 are listed on the Web page at the following link:

https://www.renesas.com/pg-fp6

PG-FP6 V1.05

1.3 FP6 System Configuration

The system configuration of the FP6 is shown below.



Note: The product type name and the standard with which the power adapter that comes with the FP6 complies vary with the region where it is to be used. Be sure to use the power adapter that is appropriate for your region.

Figure 1.1 Image of FP6 Connection

Table 1.1 Product Type Names for Ordering

Target Region	Product Type Name		Plug Shape			Voltage Range ^{*1}
Japan	RTE0T00001FWRJP000R	A				AC: 100-240 V
Europe and USA	RTE0T00001FWREA000R	SE	C	BF	A A	
China, Hong Kong, Chinese Taipei, South Korea, Singapore	RTE0T00001FWRAS000R	Bo o	0 0		0 0	
		SE	С	BF	Α	

Note: This voltage range is for the power adapter. For the voltage intended for the power cable, check the indication around the plug.

Cautions:

- 1. Since regulations that apply to the FP6 vary with the region, we cannot ship a product to a region other than that from which the order was made. For example, if you place an order in Japan, you cannot purchase a product intended for Europe and the USA.
 - Please purchase the product from a Renesas Electronics Corporation representative (responsible for sales) or distributor in the region where it is to be used.
- 2. If you wish to know which model is available in a region not included in the above table, please contact either a Renesas Electronics Corporation representative (responsible for sales) or distributor.
- 3. The power adapter that comes with the FP6 complies with the regulations that are applicable in the target region. Its plug is also in the shape that is usable in that region.

1.4 Optional Products

We provide useful optional products (separately sold) for use with the FP6.

- 14-pin to 16-pin conversion adapter for the E1 emulator (type name: QB-F14T16-01)
- 20-pin conversion adapter for the PG-FP6 (type name: RTE0T00001FWRB0000R)
- User system interface cable (20-pin to 20-pin) for the E2 emulator (type name: RTE0T00020KCAC0000J)
- User system interface cable (20-pin to 10-pin) for the E2 emulator (type name: RTE0T00020KCAC1000J)

For details on the optional products, refer to the following Web page in the Development Tools section of the Renesas site.

https://www.renesas.com/pg-fp6

The optional products are also available for purchase from Naito Densei Machida Mfg. Co., Ltd. Contact the company through the following site for details.

• Web site for Naito Densei Machida Mfg Co., Ltd:

https://www.ndk-m.co.jp

1.5 Operating Environments

1.5.1 Hardware environment

Host PC

— Processor: At least 1 GHz

Main memory: We recommend at least 2 GB.

At least 1 GB (or at least 2 GB for 64-bit editions of Windows OS) is required.

Display: Resolution should be at least 1024 x 768.

— Interface: USB2.0 or serial interface (RS-232C)

1.5.2 Software environment

- Operating System
 - Windows 7 (32-bit edition, 64-bit edition)
 - Windows 8.1 (32-bit edition, 64-bit edition)
 - Windows 10 (32-bit edition, 64-bit edition)
 - Microsoft .NET Framework 4.5.2 or later

1.6 Hardware Specifications

Table 1.2 Hardware Specifications

Hardware	Items	Specifications
FP6 main	Operating power	Supplied via the power adapter (5 V, 2 A): recommended
unit	supply	USB-bus power supply (VBUS 4.5 V min./500 mA max.)
	Operating environment condition	Temperature: 5°C to 35°C (no condensation)
	Storage environment condition	Temperature: –15°C to 55°C (no condensation)
	Package size	$140 \times 90 \times 30$ mm (not including projections)
	Weight	Approximately 245 g
	Operation mode	FP6 Terminal operation, standalone operation, remote operation, and communication command operation
Power adapter	Specifications	Power adapter for each region*1
Host PC	Target host PC	PC/AT compatible
interface	USB connector	Type mini-B, USB 2.0
	USB cable	Approximately 2 m
	Serial port	9-pin D-Sub male port for RS-232C*2
Target	Target connector	15-pin D-Sub female connector
interface	Target cable	14-pin type Cable length: Approximately 42 cm
	Power supply	1.8 V to 5.5 V, 500 mA max.*3
	Power supply detection	Available
	GND cable	Approximately 1 m
Remote interface	Remote connector	15-pin D-sub female connector

Notes: 1. The power adapter that comes with the FP6 varies with the region where it is to be used. For the product type names, see Table 1.1, Product Type Names for Ordering.

- 2. Connecting to the host PC has to use a cross cable.
- 3. The maximum power-supply current is 100 mA when USB bus power is being supplied; however, this depends on the performance of the USB host in terms of the supply of power.

1.7 Formats of Program Files

For a HEX file to be readable by the FP6, it must have the correct format and satisfy the following conditions. If a program file with a non-supported format is read, an error will occur.

1.7.1 Intel HEX format

- The format file ends with the end record.
- All lines consist solely of record types 00 to 05.

1.7.2 Motorola S format

- The format file ends with the end record (S7, S8, or S9).
- All lines consist solely of record types S0 to S9 (excluding S4).



1.7.3 RPI files

An RPI file is an image file which combines a program file and flash option data and is generated by using the RFP. For details on the RFP, refer to the following Web page.

https://www.renesas.com/rfp

1.7.4 RPE files

An RPE file is a file in which a program file is encrypted and can be generated by the encryption utility program that comes with this product. For how to generate such files, refer to chapter 8, Encryption Utility Program.

PG-FP6 V1.05

1.8 Regulatory Compliance Notices

1.8.1 European Union regulatory notices

This product complies with the following EU Directives. (These directives are only valid in the European Union.)

CE Certifications:

Electromagnetic Compatibility (EMC) Directive 2014/30/EU

EN 55032 Class A

WARNING:

This is a Class A product. This equipment can cause radio frequency noise when used in the residential area. In such cases, the user/operator of the equipment may be required to take appropriate countermeasures under his responsibility.

EN 55024

- Information for traceability
 - Authorized representative & Manufacturer

Name: Renesas Electronics Corporation

Address: TOYOSU FORESIA, 3-2-24, Toyosu, Koto-ku, Tokyo 135-0061, Japan

Person responsible for placing on the market

Name: Renesas Electronics Europe GmbH

Address: Arcadiastrasse 10, 40472 Dusseldorf, Germany

Trademark and type names

Trademark: Renesas
Product name: PG-FP6

Type names: RTE0T00001FWRJP000R

RTE0T00001FWREA000R RTE0T00001FWRAS000R

Environmental Compliance and Certifications:

Waste Electrical and Electronic Equipment (WEEE) Directive 2012/19/EU

1.8.2 United States regulatory notices

This product complies with the following EMC regulation. (This is only valid in the United States.)

FCC Certifications:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CAUTION: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

2.FP6 Main Unit: Names and Functions of Parts

This chapter gives the names and functions of the parts on the FP6 main unit.

2.1 FP6 Control Panel

Indicators and buttons are placed on the top of the FP6.

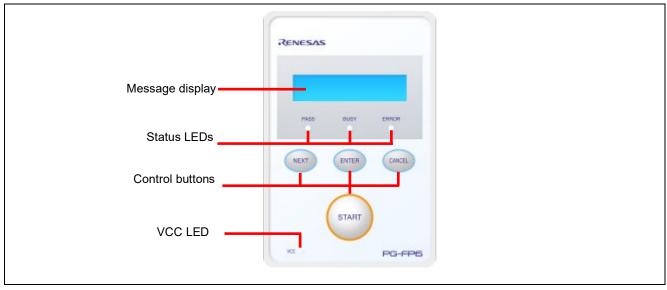


Figure 2.1 FP6 Top View <Control Panel>

(1)	Indicators
•	Message display

An LCD display of 16 $\times\,2$ characters that indicates the operating mode or

menus.

It is mainly used when the FP6 is in standalone mode.

• Status LEDs These LEDs show the operating state of the FP6.

PASS (blue) indicates a normal end, BUSY (orange) indicates processing in

progress, and ERROR (red) indicates an abnormal end.

VCC LED This LED is illuminated (green) when power is being supplied to the user

system.

(2) Buttons

[NEXT] button Proceeds to the next menu item.

• [ENTER] button Selects the item shown in the message display.

[CANCEL] button
 Cancels the current selection and returns to the previous menu item. The

currently running command cannot be stopped, except for the [Read] command.

• [START] button Executes the [Start] command with the current active-programming-area setting.

2.2 FP6 Connectors

The power-supply connector, serial port, and USB connector are placed on the host interface side of the FP6

The target connector, GND connector, and remote connector are placed on the target connector side of the FP6.

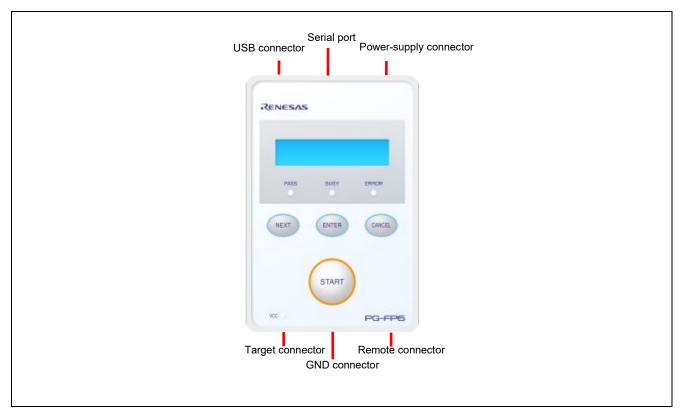


Figure 2.2 FP6 Top View <Connectors>

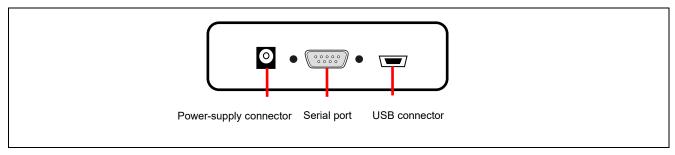


Figure 2.3 FP6 Host Interface Side

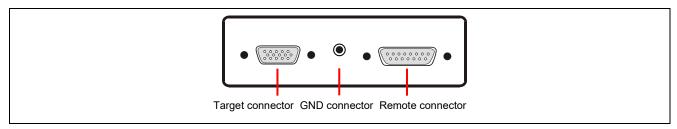


Figure 2.4 FP6 Target Connector Side

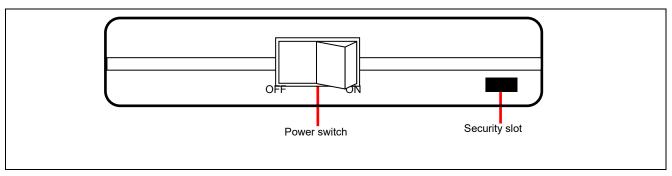


Figure 2.5 Power Switch

(1) Power-supply connector

Connect the power-supply connector to the power adapter for your region. For details on the power-supply connector specifications, refer to chapter 10, Connectors and Cables.

Note: Do not use a power adapter other than that included with the PG-FP6.

(2) Serial port

Communication is established by connecting the host PC serial port and the FP6 serial port via a serial cable (RS-232C crossover cable). The data transfer conditions are as follows.

- Data transfer speed: 9,600 bps, 19,200 bps, 38,400 bps, 57,600 bps, or 115,200 bps
- Data bit: 8 bits
- Parity: none
- Stop bit: 1 bit
- Flow control: hardware

The transfer speed can be changed although it is set to 9,600 bps by default. For details on the serial connector specifications, refer to chapter 10, Connectors and Cables.

(3) USB connector

Communication is established by connecting the FP6 USB connector (mini-B type) and the host PC USB port via a USB cable. This connector conforms to USB 2.0 standards. For details on the USB connector specifications, refer to chapter 10, Connectors and Cables.

(4) Target connector

Connect the target connector to the target system via the target cable. For details on the target connector specifications, refer to chapter 10, Connectors and Cables.

(5) GND connector

To reinforce the GND, connect the GND connector of the FP6 and the GND of the target system via the GND cable. For details on the GND connector specifications, refer to chapter 10, Connectors and Cables.

Note: The FP6 and target system may be damaged if there are differences in potential between the grounds of the FP6 and of the target system. Use the GND cable to eliminate differences in potential before connecting the target cable.

(6) Remote connector

The FP6 can be remote controlled by connecting the remote connector and an external control device. For details on remote operation, refer to chapter 6, Usage of the Remote Connector, and chapter 10, Connectors and Cables.

(7) Power switch

The power switch turns on/off the FP6.

(8) Security slot

This is a security slot for the Kensington lock.

PG-FP6 V1.05 3. Software Installation

3. Software Installation

This chapter explains how to install software.

3.1 Obtaining Software

Download the PG-FP6 software from the following Web page.

https://www.renesas.com/pg-fp6

Note: We recommend the use of the latest version of software to assure the correct operation of the FP6.

3.2 Installation

This section explains the installation procedure for the PG-FP6 software.

Table 3.1 Installation

Item	Method	
	Execute the downloaded executable file (PG-FP6_Package_Vxxx.exe) and follow the directions on the	
software	installer screen. After installation, the USB driver detects the FP6 by plug-and-play.	

PG-FP6 V1.05 3. Software Installation

3.2.1 Notes on installation

- (1) Basically we recommend using the latest version.
- (2) You might be asked to reboot your computer after installing the FP6. Be sure to close all other applications before rebooting your computer.
- (3) You must have administrator privileges to install the FP6.
- (4) The FP6 can only be installed in a folder that is named using ASCII characters (excluding the 11 characters / * : < > ? | " \ ; , and character strings that begin and end with a space). The FP6 might not operate correctly if installed in a folder that is named using other characters.
- (5) The FP6 cannot be installed from a network drive or on a network drive.
- (6) The installer does not specify environment variable paths. If these paths are required, add them after installation.
- (7) The Microsoft .NET Framework and the Microsoft Visual C++ runtime libraries are required to run the installer. If the Microsoft .NET Framework and the Microsoft Visual C++ runtime libraries are not installed, the FP6 Terminal will install them.
- (8) Make sure that your host PC is connected to the network before installing the program. If you wish to install the program on a host PC that is not connected to the network, first go to the Microsoft Download Center and install the Microsoft .NET Framework 4.5.2 or later before installing the FP6 Terminal.
- (9) If the installer is started on a non-Japanese version of Windows and the path contains multi-byte characters, it will cause an error, and the installer will not start.
- (10) The following folders created after installation (including the files under the folders) contain files required for the tools to operate. Do not delete them.
 - (Windows is the 32-bit edition and the system drive is C:)
 - C:\Program Files\Renesas Electronics\Programming Tools\
 - (Windows is the 64-bit edition and the system drive is C:)
 - C:\Program Files (x86)\Renesas Electronics\Programming Tools\
- (11) To change the folder of the installed tools, uninstall all software related to CS+ (integrated development environment from Renesas), the FP6 Terminal, and the USB driver, and install them again.
- (12) In the environment where CS+, the FP6 Terminal, and the USB driver for the FP6 are installed, the FP6 Terminal and the USB driver for the FP6 are included in the target software of the CS+ integrated uninstaller. If you do not wish to delete them, exclude them from the uninstallation targets.
- (13) If a CS+ instance launched via Rapid Start is in the notification area (system tray) during installation, the following error message will appear. Exit the application, and run the installer again.

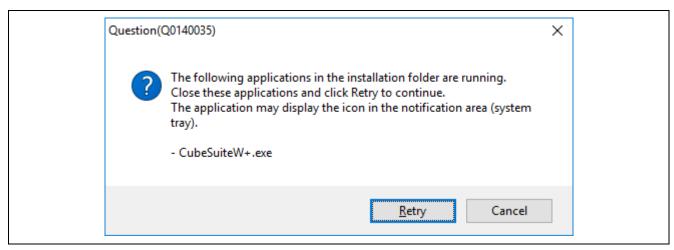


Figure 3.1 Message Dialog Box (Question (Q0140035))

PG-FP6 V1.05 3. Software Installation

3.3 Uninstallation

This section explains how to uninstall the PG-FP6 software. The uninstallation order is not prescribed.

Table 3.2 Uninstallation

Item	Method
PG-FP6 software	Use [Add or Remove Programs] on the Control Panel to uninstall the FP6 Terminal and the USB driver. The names are [PG-FP6] and [Renesas USB Driver x86 for PG-FP6] (or [Renesas USB Driver x64 for PG-FP6]), respectively.

4. Usage of the FP6 Terminal

4.1 Main Window

The main window of the FP6 Terminal that has been started up is shown below.

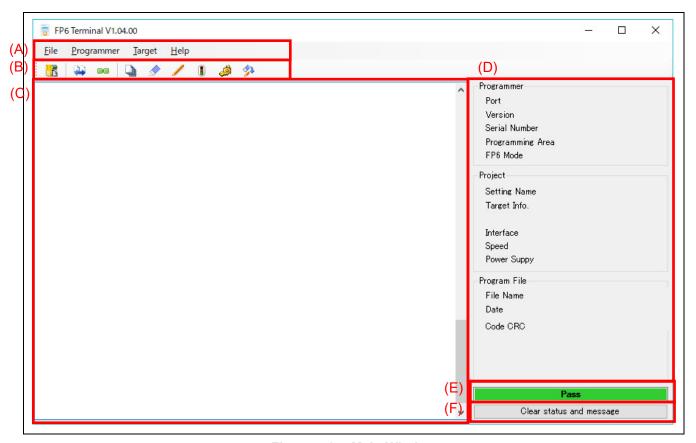


Figure 4.1 Main Window

Table 4.1 Main Window

Name		Description	Refer to
(A)	Menu bar	Commands executable through the FP6 Terminal	4.4
(B)	Toolbar	Frequently used commands (provided as buttons)	4.5
(C)	Console window	Execution result and log of commands	-
(D)	Parameter window	Programming parameter settings	-
(E)	Status bar	State of command execution indicated by colors and messages	-
(F)	[Clear status and message] button	Clears state information and messages.	-

(A) Menu bar

This is the menu for operating the programmer. For details on the menu bar, see section 4.4, Menu Bar.

(B) Toolbar

The frequently used menu items can be executed by clicking on the buttons. For details on the toolbar, see section 4.5, Toolbar.

(C) Console window

This window shows the execution result and log of commands.

Note that log entries older than the 3000th line are automatically deleted.

(D) Parameter window

This window shows the settings of the FP6 when a setting file or a program file is downloaded, the FP6 is connected, or the programming area is changed. However, the information on connection with the target device is not displayed when "Restrict Upload from FP6" is selected in the [FP6 Manager] dialog box (see Figure 4.21).

(E) Status bar

The current state of the FP6 and the result of command execution are displayed. This facility is effective only when a command is executed from the menu bar. The state shown on this bar is not updated when a command is executed through the console window.

Table 4.2 Status Information

Status	Description
Busy	Command execution is in progress.
Pass	Command execution ended normally.
Error	Command execution failed.

(F) [Clear status and messages] button

The displays in the console window and status bar are cleared and the states of the LEDs of the FP6 are cleared.

4.2 Creating a New Setting

4.2.1 [Create New Setting] dialog box

Selecting [File]-[New Setting File...] from the menu bar opens the [Create New Setting] dialog box, as shown below.

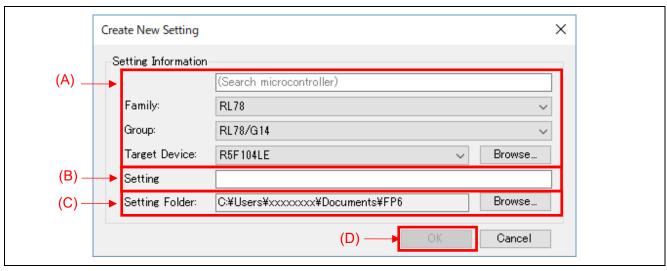


Figure 4.2 [Create New Setting] Dialog Box

(A) Target device

Select the family, group, and type name of the MCU of the target device.

Entering the group or type name of the MCU in [(Search microcontroller)] initiates a search for the target device and displays the details of the first target device to have matched.

Remark: Using the [Browse] button is not generally necessary.

(B) Setting name

Specify the name of a setting to be created.

Remarks: 1. Since the setting name is used for a setting File name, only use characters that are allowed for file names.

2. Up to 46 alphanumeric characters can be used for each setting name.

(C) Folder

Specify the path to the folder in which a setting File will be created.

(D) OK

Click on the [OK] button to create a setting File in the specified folder and open the [Setup] dialog box.

4.3 [Setup] Dialog Box

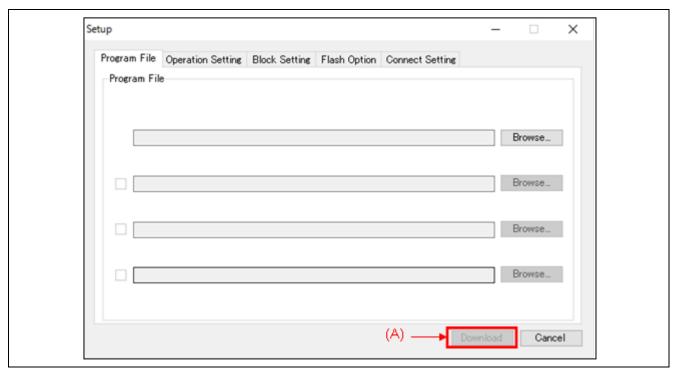


Figure 4.3 [Setup] Dialog Box

(A) [Download]/[OK] button

[Download] is displayed when the FP6 is connected and [OK] is displayed when it is not connected. Clicking on this button applies the changes made in the [Setup] dialog box to the setting file, and closes the [Setup] dialog box. When the FP6 is connected, the setting file, parameter file, and program file are downloaded to the FP6.

4.3.1 [Program File] tabbed page

The [Program File] tabbed page allows you to select the files to be written to the target device.



Figure 4.4 [Program File] Tabbed Page

(A) Endian

Select the endian according to the data of the program file. This item is not displayed when the target device does not support switching of the endian.

(B) Program file

Use the [Browse] button to select the program file to be written to the flash memory of the target device.

Caution: When selecting an RPE file, set the password for the RPE file in the [FP6 Manager] dialog box.

(C) Check boxes for selecting multiple files

When a check box is selected, the corresponding [Browse] button becomes selectable. You can select multiple program files in this way.

Remark: Multiple DDI, HCUHEX, RPI, or RPE files cannot be selected.

(D) CRC-32

The checksum (CRC-32) of the selected file is displayed.

Caution: This checksum is calculated from the entire file including a linefeed code. Therefore, it does not match the checksum acquired from the target device.

4.3.2 [Operation Setting] tabbed page

The [Operation Setting] tabbed page allows you to change settings related to the operation of flash memory.

Remark: Some items may not be displayed or the values of some items may not be changeable depending on the selected target device or program file.

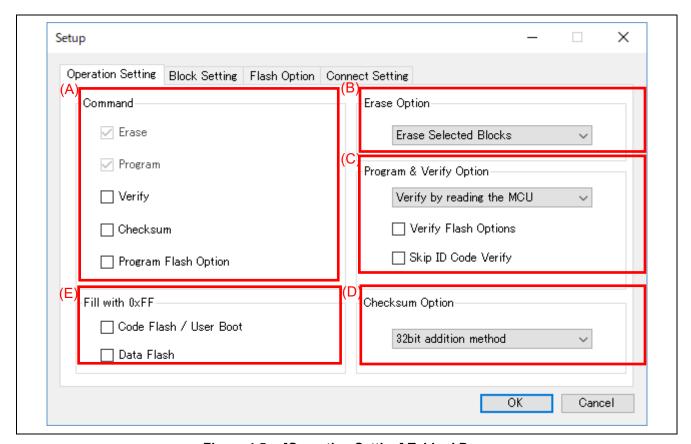


Figure 4.5 [Operation Setting] Tabbed Page

(A) Command

Select the command(s) to be executed in response to pressing the [START] button on the FP6 or clicking on the [Start] button on the FP6 Terminal. When multiple commands are selected, they are executed in order from the top. The five processes listed below can be selected as commands. Note that some commands may not be available depending on the selected target device.

Remark: If you wish to execute any of these commands individually, select it from the [Target] menu.

- Erase
 - This command erases flash memory data in the range selected for "(B) Erase Option".
- Program

This command programs data in the range selected for "(C) Program & Verify Option".

- Verify
 - This command verifies data in the range selected for "(C) Program & Verify Option".
- Checksum

This command acquires the checksum of flash memory. The method selected for "(D) Checksum Option" is used for calculating the checksum.

· Program Flash Option

This command applies the flash-option data, including "lock bits", "OTP", "flash access window", "option bytes", and "security", which have been configured on the [Block Setting] and [Flash Option] tabbed pages.

Caution: If the contents of the [Flash Option] tabbed page have been modified, programming of the flash options must be enabled to execute the command since the settings will not be made in the target device.

(B) Erase Option

Select an option for "Erase" under "Command".

Erase Selected Blocks

Only the blocks selected on the [Block Setting] tabbed page will be erased. For the [Block Setting] tabbed page, see section 4.3.3, [Block Setting] tabbed page.

Erase All Blocks

All blocks will be erased.

Caution: Security features of some MCUs may prevent erasure of certain blocks.

Erase Chip

All blocks will be erased with flash options cleared.

Cautions:

- 1. This option does not restore the default state (at shipment) of the MCU. The MCU may not operate unless the correct flash options are written after the chip has been erased.
- 2. When "Chip Mode" is selected on the [Block Setting] tabbed page, "Erase Chip" is automatically selected as the erase option and cannot be changed on the [Operation Setting] tabbed page.
- 3. When "Erase Chip" is executed, the chip erasure command or the configuration clear command will be executed after all blocks are erased. For details of these commands, refer to the user's manual of the MCU.

(C) Program & Verify Option

Select an option for "Program" or "Verify" under "Command".

Verification type

Select the type of verification from the items listed below. Note that the value is fixed for some target devices.

Verify by reading the MCU

Data will be acquired from the MCU with a read command, and the FP6 will perform verification. The comparison may not be executed in some cases, such as when execution of a read command is disabled by a setting for the MCU.

Verify in the MCU

Data will be sent to the MCU with a verify command, and the MCU will perform verification. Since the range of comparison may be extended depending on the specifications of the verify command, a verify error may occur if filling of 0xFF is not performed.

Verify Flash Options

Select whether or not to verify values in the flash option area.

To use this feature, select "Program Flash Option" under "Command".

Skip ID Code Verify

In general, do not select the check box when this feature is displayed as an option. However, use this feature in cases of the following type.



The security settings of the MCU may make reading of the ID code impossible since the ID code in the MCU is protected. This may lead to an error may occur in verification processing. To avoid errors of this type, select this check box to use the feature.

For details, refer to section 13.9, Verification after Protecting the MCU.

(D) Checksum Option

Select the method for calculation when "Checksum" is selected under "Command". Usable methods vary with the target device.

(E) Fill with 0xFF

Select this check box if you wish to fill the ranges that do not contain program file data with 0xFF. Target areas: Code flash and user-boot areas or data flash area

- When "Fill with 0xFF" is selected
 - Programming: 0xFF will be written to the ranges that do not contain program file data.
 - Verification: The ranges that do not contain program file data will be compared with 0xFF as the expected value.
- When "Fill with 0xFF" is not selected
 - Programming: No data will be written to the ranges that do not contain program file data.
 - Verification: The ranges that do not contain program file data will not be verified.

Remark: "Fill with 0xFF" cannot be deselected for some target devices.

Caution: Even if "Fill with 0xFF" is not used, filling of 0xFF is always performed in the minimum unit of programming by the MCU.

4.3.3 [Block Setting] tabbed page

The [Block Setting] tabbed page allows you to designate blocks in the target device to be handled.

Remark: Only the items supported by the target device are listed on this page.

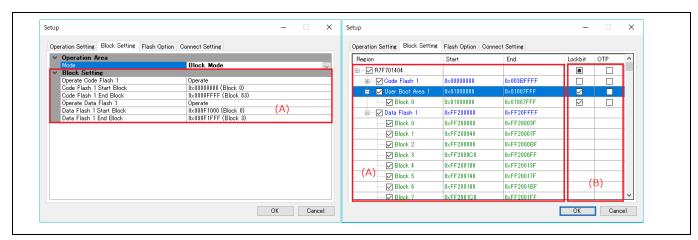


Figure 4.6 [Block Setting] Tabbed Page

(A) Operation area

Specify the target range for erase, program, and verify operations.

The flash memory can be handled as a whole (Chip Mode) or in block units (Block Mode).

Mode

Chip Mode

This mode is used to handle the entire chip.

Caution: When "Chip Mode" is selected, [Erase Option] on the [Operation Setting] tabbed page is fixed to "Erase Chip".

Block Mode

This mode is used to specify a range of blocks. Erasure, programming, and verification will not be executed for blocks outside the range.

Operation of code flash, data flash, and user boot flash
 Select whether the code flash, data flash, and user boot flash areas should be regarded as the target of operation.

Caution: When SuperH is selected as the target device, either code flash or user boot flash can be specified as the target of operation. When both areas need to be programmed simultaneously, you can select both areas by specifying a DDI-format file as the program file.

Start/end block of code/data/user boot flash
 Select the start and end addresses of the code flash, data flash, and user boot flash areas to be handled.

(B) Lock bits or OTP

To set the lock bits or OTP, select the target blocks on the [Block Setting] tabbed page and use communication commands. Alternatively, select "Set" for "Set Option" of each item on the [Flash Option] tabbed page and click [Program Flash Option] on the [Operation Setting] tabbed page and execute [Start].

Caution: When an HCUHEX or RPI file is selected, the lock bits or OTP cannot be changed.

4.3.4 [Flash Option] tabbed page

The [Flash Option] tabbed page allows you to specify flash options for the target device.

Remark: Only those items the target device supports are shown. For the meanings and details of the settings of the individual items, refer to the user's manual of the target device in use.

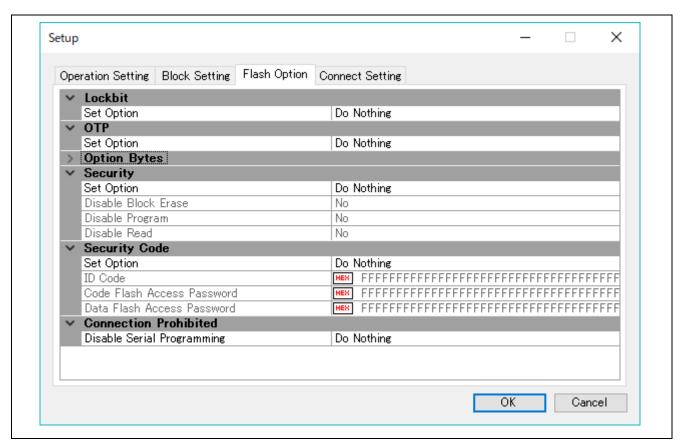


Figure 4.7 [Flash Option] Tabbed Page

(A) Lock bits

Select whether to set the lock bits. When "Set" is selected, the lock bits for the blocks selected on the [Block Setting] tabbed page will be set.

(B) OTP

Select whether to set the OTP. When "Set" is selected, the OTP for the blocks selected on the [Block Setting] tabbed page will be set.

(C) Access window

Select whether to set the access window.

- Set Option
 - "Do Nothing": Access window are not set.
 - "Set": The setting of access window is enabled.

Start Block/End Block

Select the start or end block from the pull-down menu.

- Operation Setting
 - "Prohibit outside the range": Programming or erasing of blocks outside the range from the start block to the end block is prohibited.

- "Prohibit inside the range": Programming or erasing of blocks within the range from the start block to the end block is prohibited.
- "Disable rewriting"
 - "No": Making changes within the access window is not disabled.
 - "Yes": Making changes within the access window is disabled.

(D) Option Bytes (OPBT)

You can change the settings of option bytes (OPBT).

· Enable Extended Option Bytes

Select "Enable" or "Disable", respectively, to enable or disable setting of extended option bytes (OPBT8 and above) and acquisition of their values.

Caution: Be careful when you rewrite the values of the extended option bytes since they may include important settings for the MCU.

OPBT0 to OPBT7

Enter the value of option bytes in 4-byte units in hexadecimal notation (bit 31 to bit 0).

OPBT8 and above

Enter the value of extended option bytes in 4-byte units in hexadecimal notation (bit 31 to bit 0).

(E) ICU-S

Enable or disable the ICU-S.

- "Set Option"
 - "Do Nothing": ICU-S is not set.
 - "Set": The ICU-S function is enabled.

Caution: For some target devices, the ICU-S cannot be disabled after it has been enabled. For details, refer to the user's manual of the target device.

(F) Security

Set security functions.

- "Set Option"
 - "Do Nothing": The security function is not set.
 - "Set": The security function is enabled.
- "Enable ID Code Authentication"
 - "No": The ID authentication function is disabled.
 - "Yes": The ID authentication function is enabled.
- "Disable Chip Erase / Disable Block Erase / Disable Program / Disable Read / Disable Rewriting boot cluster / Disable Initialize Command"
 - "No": The security function is not set for the target command.
 - "Yes": The use of the target command is prohibited.

Cautions:

- 1. Once any of the functions for disabling commands has been set for an MCU, the setting cannot be reversed.
- 2. Even if the security setting is "No", the security setting for the MCU is not reversed.



(G) Reset Vector

Enter the reset vector value of the target device in hexadecimal notation.

(H) Security Code

Set the ID code or the access password.

- "Set Option"
 - "Do Nothing": An ID code or access password is not set.
 - "Set": The setting of an ID code or access password is enabled.

ID Code

Enter the ID code in hexadecimal notation.

Code Flash Access Password

Enter the password for accessing code flash memory in hexadecimal notation.

Data Flash Access Password

Enter the password for accessing data flash memory in hexadecimal notation.

(I) Boot Area

Specify the end block of the boot area.

(J) Connection Prohibited

Make the setting for disabling connection in serial programming mode or both the debugger and serial programming mode.

- "Disable Serial Programming"
 - "Do Nothing": Serial programming is not disabled.
 - "Set": Connection in serial programming mode is disabled.
- "Disable Debugger and Serial Programming"
 - "Do Nothing": Debugger and serial programming are not disabled.
 - "Set": Connection in debugger and serial programming mode is disabled.

Caution: Once the Connection Prohibited function is set for an MCU, the setting cannot be reversed.

(K) DLM

Make the setting for DLM transitions.

- "Set Option"
 - "Do Nothing": A transition of the DLM state is not to be set.
 - "Set": The setting of DLM transitions is enabled.

"Target State"

Select the destination of the DLM transition from the pull-down menu.

(L) DLM Keys

Specify the DLM key file for use in DLM authentication which is to be set for the target device.

For details on how to generate DLM keys, refer to chapter 9, Renesas Flash Programmer Utility Program.

- "Set Option"
 - "Do Nothing": A DLM key is not to be set.
 - "Set": The setting of a DLM key is enabled.



DLM key file

Open the [Open] dialog box by clicking on ..., and specify a DLM key file.

Remark: If a DLM key file is not specified, programming of the flash memory will not proceed.

(M) Boundary

Set the size of the secure and non-secure areas of the target device.

- · "Set Option"
 - "Do Nothing": Boundaries are not to be set.
 - "Set": The setting of boundaries is enabled.
- "Secure [KB]"

Enter the size of the secure area in KB units.

"NSC [KB]"

Enter the size of the non-secure callable area in KB units.

Caution: Confirm the specifiable sizes in the user's manual of the target device since limits will apply.

(N) Flash Read Protection

Make the setting for flash read protection.

- "Set Option"
 - "Do Nothing": Flash read protection is not to be set.
 - "Set": The setting for flash read protection is enabled.
- "Start Block/End Block"

Select the start or end block from the pull-down menu.

Remark: To enable reading of all blocks, select "Permitted All Blocks".

- · "Disable rewriting"
 - "No": Rewriting of flash read protection is not disabled.
 - "Yes": Rewriting of flash read protection is disabled.

(O) Extra Option

Make the setting for the extra option.

- · "Set Option"
 - "Do Nothing": An extra option is not to be set.
 - "Set": The setting of an extra option is enabled.
- · "Disable rewriting"
 - "No": Rewriting of an extra option is not disabled.
 - "Yes": Rewriting of an extra option is disabled.

Caution: Once the Extra Option function is set for an MCU, the setting cannot be reversed.

4.3.5 [Connect Setting] tabbed page

The [Connect Setting] tabbed page allows you to fill the information necessary for connecting the MCU.

Remark: The items displayed on this page vary with the type of the target device.

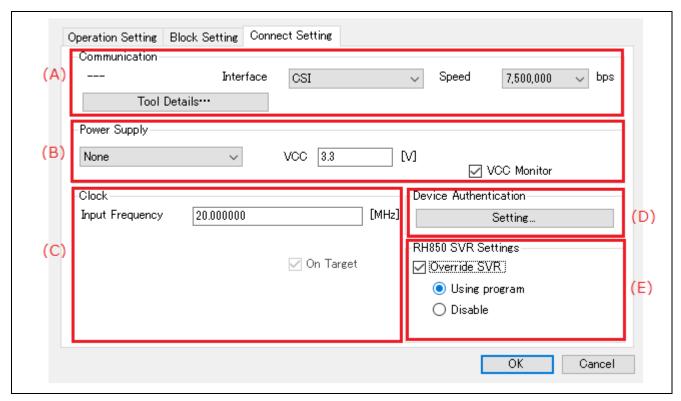


Figure 4.8 [Connect Setting] Dialog Box

(A) Communication

• Information on the programmer

The communication port and serial number of the currently connected FP6 are displayed.

Remark: You cannot select any other FP6 through this dialog box. To do so, select [Programmer]–[Setup PC Connection] in the main window.

- Interface
 - Select the method for communicating with the target device.
- Speed

Select the communication speed in the communication mode selected for "Interface".

Tool Details

Click on this button to open the [Tool Details] dialog box, which enables setting of the states of the mode pins at the time of connection and of the reset pin at the time of disconnection.

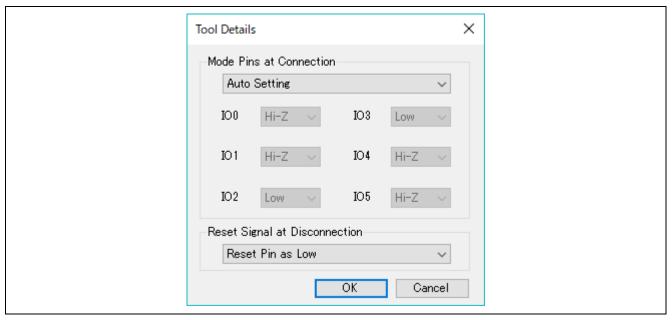


Figure 4.9 [Tool Details] Dialog Box

• [Mode Pins at Connection]

To modify the levels on the mode pins (I/O pins) at the time of connection, change "Auto Setting" to "Custom Setting". You can then change the pin settings to the high-impedance state or to the high or low output level.

Remark: Depending on the target device, certain selections may not be available.

For pin assignments, refer to Table 10.3, Pin Configuration of the Target Connector (14-Pin Type), and Table 10.4, Pin Configuration of the Target Connector (20-Pin Type).

• [Mode Pins at Disconnection]

Select the state of the reset pin at disconnection from the target device.

Reset Pin as Low

After disconnection, a low-level signal is continuously output from the RESET pin.

Reset Pin as Hi-Z

After disconnection, the RESET pin is held low for a short time and then placed in a Hi-Z state. This setting is used when making the target device operate after completion of the FP6 processing.

(B) Power Supply

Power Supply from FP6/None

Select whether power should be supplied from the FP6 or the target system during the process of connecting the target device.

Remark: We recommend supplying power from the target system to the MCU for on-board programming. Specify the voltage value within the range of 1.8 V to 5.5 V.

Caution: The voltage value should meet the operating conditions of the target device and target system.

Wide Voltage

Select this check box to perform programming in wide voltage mode. For details on wide voltage mode, refer to section 13.5, Wide Voltage Mode.

VCC Monitor

Select this check box to detect an error when there is a gap of approximately $\pm 5\%$ from the voltage value that was entered in [VCC].

Caution: The voltage value is measured on the FP6 side of the target cable. Accordingly, this facility does not quarantee that the voltage set for the target device on the target system is being supplied.

(C) Clock

Set the frequency of the input clock, the multiplication ratio of the main clock, and the multiplication ratio of the peripheral clock. Set the input clock frequency in MHz. If the value is smaller than 1 MHz, use a decimal. The display is switched depending on the type of the target device. You can check the clock settings for each target device in the Points for Caution stated in the Release Note, which can be obtained from the Renesas Tools homepage (https://www.renesas.com/pg-fp6).

In addition, specify whether a clock in the target system or that on the FP6 side is the source of the clock signal for supply to the target device. When the [On Target] check box is selected, a clock in the target system is used. When the [On Target] check box is not selected, the clock on the FP6 side is used.

(D) Device Authentication

· "Set Option"

Clicking on this button opens the [Authentication Code] dialog box. Use this button if you wish to change the authentication code required for connecting the target device in which the ID code or access password is set. Enter the ID code for authentication in hexadecimal notation (0 to 9 and A to F).

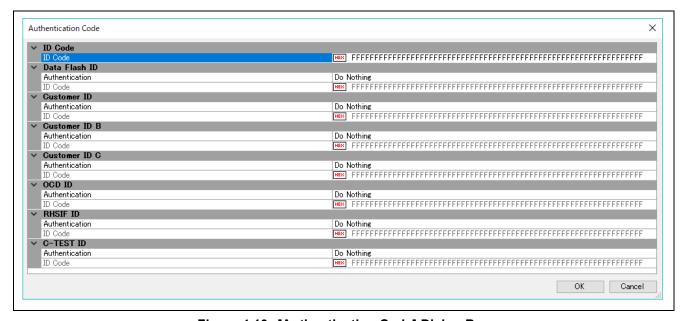


Figure 4.10 [Authentication Code] Dialog Box

Cautions:

- When an RX-family device is connected via the FP6, input the value in the order (control code) ID1, ID2, ..., ID16.

Example:

When the number of effective bytes = 16, control code = 0x45, ID code = ID1=0x01, ID2=0x02, ID3=0x03, ID4=0x04, ID5=0x05, ID6=0x06, ID7=0x07, ID8=0x08, ID9=0x09, ID10=0x0A, ID11=0x0B, ID12=0x0C, ID13=0x0D, ID14=0x0E and ID15=0x0F, the value will be '450102030405060708090A0B0C0D0E0F'.



- When RX72x, RX71x, RX66x, RX65x, or RX64x device is connected via a debug tool which has been specified with the CS+ or e2 studio, the order for input of the authentication code changes to that shown below.
 - ID4 ID3 ID2 ID1 ID8 ID7 ID6 ID5 ID12 ID11 ID10 ID9 ID16 ID15 ID14 ID13
- FP6 repeats it up to three times if ID code authentication fails.
- When an RA-family, Renesas Synergy™-family, or RE-family device is connected to the FP6, input values to be specified for registers of the target device in order of bits 127 to 0 in byte units. Since the input specification may also differ with the tool, confirm the input specification of the tool you will be using.

Remark: The default authentication code in some target devices at the time of shipment is all FFs. For details, refer to the user's manual of the target device.

(E) RH850 SVR Setting

Make the settings for the SVR parameters when the PG-FP6 is connected to the target device.

- "Override SVR parameters"
- "Using program files": The parameters from the program file are used.
- "Disable SVR": The SVR function is disabled.

4.3.6 [User Keys] tabbed page

The [User Keys] feature is for storing the encrypted user keys in the TSIP. For the type of user keys and the features, refer to the user's manual of the boot firmware.

Caution: The [User Keys] feature may be displayed for a target device that does not actually support user keys. Refer to the user's manual of the target device regarding whether or not the user key function is available.

Remark: The user key is written by the [Program] command.

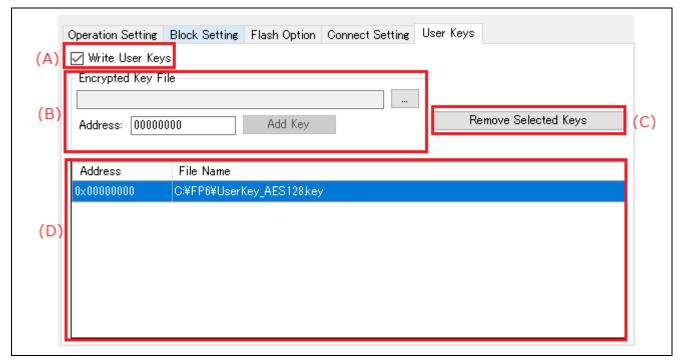


Figure 4-11 [User Keys] Tabbed Page

(A) Write User Keys

Usage or non-usage of the feature for writing the user key can be set in this checkbox.

Check the box to select the use of user keys.

(B) Encrypted Key File

Specify a user key file or the address to which the file is to be written.

For details on how to generate user key files, refer to chapter 9, Renesas Flash Programmer Utility Program.

"Encrypted Key File"

Open the [Open] dialog box by clicking on ..., and specify a user key file.

"Address"

Enter the address to which the user key file is to be written.

"Add Key"

Register the user key file in the list of key files by clicking on the Add Key button.

(C) Removing user key files

When a file to be removed is selected from a list of key files, clicking on the Remove Selected Keys button removes the file from the list.

(D) List of key files Information on key files is displayed in a list.

4.4 Menu Bar

4.4.1 [File] menu

4.4.1.1 [New Setting File...]

This menu item is used to select a new target device, create a new setting file, and download it to the FP6.

4.4.1.2 [Open Setting File...]

This menu item is used to open a setting file which has been created and download it to the FP6.

Caution: When a setting file created by using the FP5 is selected, the [Config Setting] check box on the [Block Setting] tabbed page of the [Setup] dialog box is not selected by default. If necessary, select the [Config Setting] check box before clicking on [Download] in the [Setup] dialog box after importing settings. This note is only applicable to the RX651 and RX65N groups.

4.4.1.3 [Upload Files]

This menu item is used to upload a program file and the setting file that are stored in the FP6 to the PC.

Remark: This menu item is not executable when [Disable Upload] is selected for the currently connected FP6.

[File Upload] dialog box
 Specify the file to be uploaded and the directory where the file is to be saved.

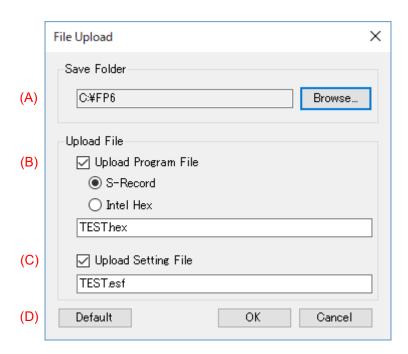


Figure 4.12 [File Upload] Dialog Box

(A) [Save Folder]

Specify the directory where the file is to be saved after it has been uploaded.

(B) [Upload Program File]

When a program file is to be uploaded, specify the file format (S-Record or Intel Hex) and select the check box. Although the text box initially shows a file name, the name can be changed.



(C) [Upload Setting File]

When a setting file is to be uploaded, select this check box. Although the text box initially shows a file name, the name can be changed.

(D) [Default] button

of the data.

Clicking on this button restores the dialog box to its initial values.

4.4.1.4 [File Checksum]

This menu item is used to calculate the checksum of the data in the program file, which is saved in the currently connected FP6, and display the value in the console window.

• [File Checksum] dialog box

Specify an area (or all areas) of the data saved in the FP6 and the method for calculating the checksum

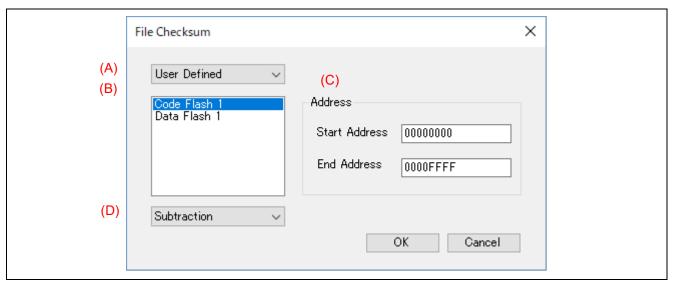


Figure 4.13 [File Checksum] Dialog Box

(A) Drop-down list box for specifying the area

Specify [All Areas] to calculate the checksum of the files in all areas.

Specify [User Defined] to calculate the checksum of the files in a particular area.

(B) Selection of an area

When [User Defined] is selected in (A) above, select the required area.

(C) [Start Address] and [End Address]

When [User Defined] is selected in (A) above, specify the start and end addresses for the range to be used in calculation.

(D) Method for calculating the checksum

Select the method for calculating the checksum.

4.4.1.5 [Recently used setting files]

This menu item is used to display the setting files that have most recently been created (up to eight filenames).

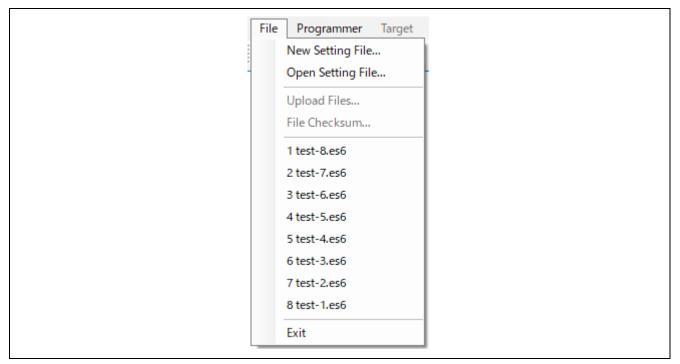


Figure 4.14 [Recently used setting files] Dialog Box

4.4.1.6 [Exit]

This menu item is used to close the FP6 Terminal.

4.4.2 [Programmer] menu

4.4.2.1 [Setup PC Connection]

This menu item is used to select the port and baud rate for communications between the FP6 Terminal and the FP6.

[PC Connection] dialog box

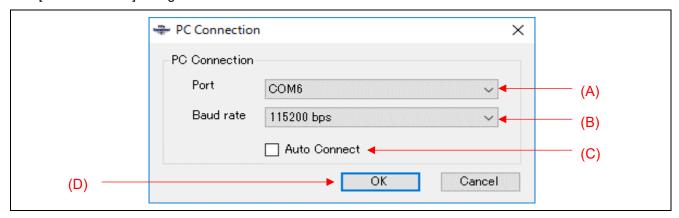


Figure 4.15 [PC Connection] Dialog Box

(A) [Port]

Select the communications port connected to the FP6. When a USB interface cable is used for connection, "COMx: FP6(S/N:xxxxxxxxx)" will be displayed.

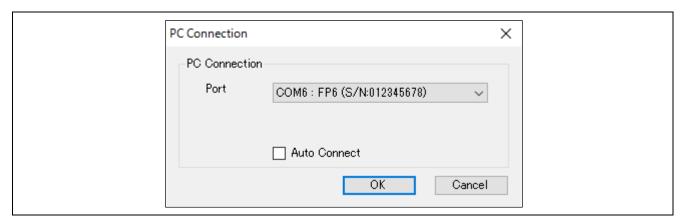


Figure 4.16 [PC Connection] Dialog Box (USB Connection)

(B) [Baud rate]

Select the baud rate for communications between the FP6 and the serial port of the PC.

Remarks:

- 1. [Baud rate] is hidden when a USB-connected port is selected for [Port].
- 2. Confirm the baud rate of the FP6 main unit from [Utility]-[RS232C Baudrate] on the LCD message display and set the same baud rate here.

(C) [Auto Connect]

When this check box is selected, the [PC Connection] dialog box will be skipped before the main window of the FP6 Terminal opens in cases where the FP6 is connected to the same COM port as in the previous connection or to any COM port via USB.

(D) [OK]

Clicking on this button starts connection to the FP6 with the current settings. When the PC is connected to the FP6, the firmware version of the FP6 will be checked. If the firmware version does not match that expected by the FP6 Terminal, the [Update Firmware] dialog box will appear. Select whether to update the firmware.

4.4.2.2 [Firmware Update]

This menu item is used to update the FP6 firmware.

4.4.2.3 [Logging]

This menu item is used to save the communication log for the results of command execution displayed on the console window. Selecting this menu item opens the [Save File] dialog box, in which you can specify the location where the file will be saved and the file name. While a log is being acquired, a check mark (\sqrt) is displayed next to the [Logging] menu item. When the menu item is selected again, the $\sqrt{}$ mark will disappear and the acquired log data will be saved in the file.

4.4.2.4 [Select Programming Area]

This menu item is used to change the active programming area for the currently connected FP6.

• [Select Programming Area] dialog box

Selecting the [Select Programming Area] menu item opens the [Select Programming Area] dialog box, in which you can change the programming area for the currently connected FP6. To change the programming area, select an area and click on [OK]. To cancel the change, click on [Cancel]. Data that have been saved in the programming area can be deleted by clicking on the [Delete] button for the selected area.

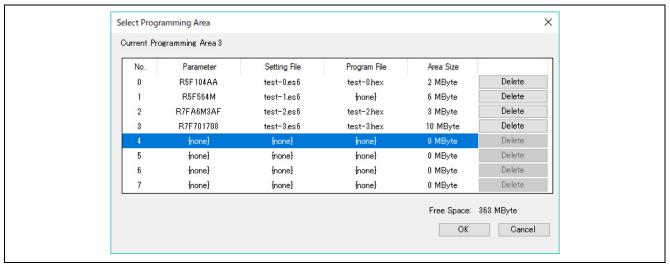


Figure 4.17 [Select Programming Area] Dialog Box

4.4.2.5 [Buzzer]

This menu item is used to make settings regarding the output from the buzzer included in the FP6. When the output of the buzzer sound is enabled, the FP6 makes a buzzer sound upon completion of the target device operation in response to pressing the [START] button on the FP6 or clicking on the [Start] button on the FP6 Terminal. While the output of the buzzer sound is enabled, a $\sqrt{}$ mark is displayed next to the [Buzzer] menu item.

4.4.2.6 [Self Test]

This menu item is used for self-testing of the FP6.

[Self Test] dialog box

After self-testing of the FP6 hardware has completed, the following dialog box will appear to show the result of self-testing of the FP6 hardware.

Cautions:

- 1. The MCU and equipment connected to the target connector and remote connector must be removed before the test.
- 2. Execute the test while power is being supplied from the power adapter to the FP6.

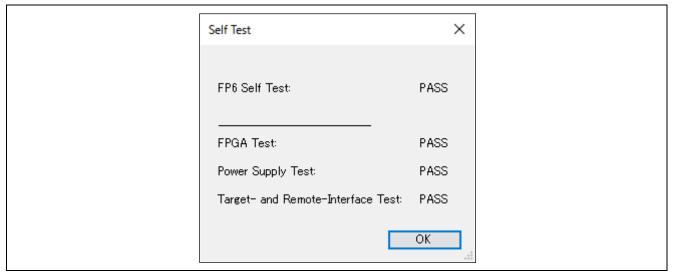


Figure 4.18 [Self Test] Dialog Box

4.4.2.7 [FP6 Manager]

This menu item is used to make security settings, such as disabling uploading or modification of FP6 settings, and change the operation mode of the FP6 main unit.

(1) Setting a password in the FP6

To execute [FP6 Manager], a password needs to be set in the FP6. If no password has been set in the currently connected FP6, the [Set Password] dialog box will appear.

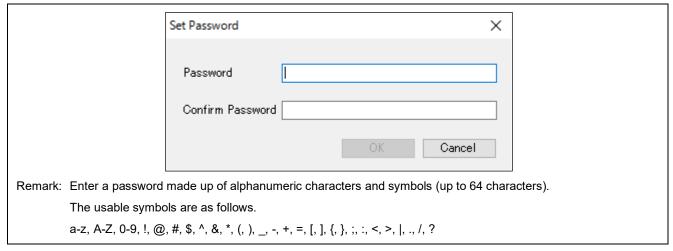


Figure 4.19 [Set Password] Dialog Box

(2) Login to FP6 Manager

If a password is already set in the FP6, the [Login to FP6 Manager] dialog box will appear. In this dialog box, enter the password and log in to the [FP6 Manager] menu.

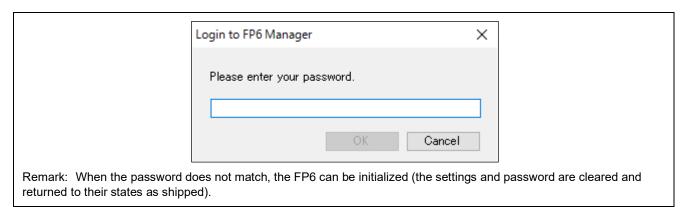


Figure 4.20 [Login to FP6 Manager] Dialog Box

[FP6 Manager] dialog box

This dialog box allows you to set security facilities or restrictions on the operation of the FP6 main unit, select the encryption of data, and provide other optional facilities. It also allows you to initialize the FP6 main unit.

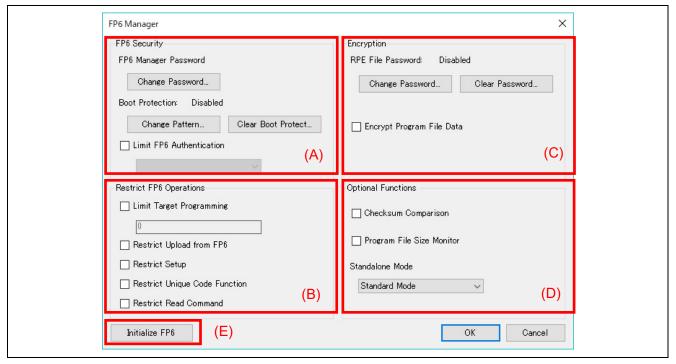


Figure 4.21 [FP6 Manager] Dialog Box

(A) FP6 Security

This area is for making the security settings (password or pattern) including a limit on the number of times authentication can be attempted on the FP6 main unit. Up to 32 patterns for authentication and a limit of three, five, or ten attempts at authentication can be specified.

FP6 Manager Password

Allows you to change the password for logging in to the [FP6 Manager] dialog box.

Boot Protection

Provides a facility for locking the FP6 main unit.

Pressing the [NEXT], [ENTER], and [CANCEL] buttons on the FP6 main unit sets and clears the authentication patterns. Pressing the [START] button specifies the pattern.

(B) Restrict FP6 Operations

This area is for restricting the operation of the FP6.

Limit Target Programming

The number of times the target device can be programmed is set (0 to 100000).

Once the set number has been reached, programming and verifying facilities are not available.

To enable the facilities again, set a larger number or disable this facility.

Restrict Upload from FP6

This box is for prohibiting the uploading of settings files included in program files from the FP6 main unit.

Restrict Setup

This box is for prohibiting the downloading of settings files and program files to the FP6 main unit.

Restrict Unique Code Function

This box is for prohibiting programming of the unique code and setting of the ID code.

For details on programming of the unique code, refer to section 7.4.15, serno command. For setting of the ID code, refer to section 7.5.28, sid command, and section 7.5.19, idc command.

Restrict Read Command

This box is for prohibiting execution of the following reading commands for the target device. gdi command, gid command, gos command, and read command

(C)Encryption

This area is for setting and clearing the passwords of RPE files.

For details on RPE files, refer to chapter 8, Encryption Utility Program.

Encrypt Program File Data

Program files to be stored in the FP6 main unit are always encrypted (AES; 128-bit block length). If this setting is enabled, programming the device and the verification time will be slightly lowered.

(D)Optional Functions

This area is for selecting optional functions and standalone operating modes that you may wish to use in command execution.

Checksum Comparison

When this function is enabled and the checksum (*sum*) command of the target device is executed, the checksum of the downloaded program file will be displayed. An error will be reported if there is a mismatch.

Program File Size Monitor

When this function is enabled and the programming (*prg*) or verify (*vrf*) command is executed, an error will be reported in cases where the selected program file has data that exceeds the programmable area of the target device.

Standalone Mode

Switch the operating mode of the FP6 main unit.

<Standard Mode>

The default mode at shipment.



<Bank Mode>

In this mode, the active programming area is switched by using bank signals instead of a standalone menu. For bank mode, refer to chapter 6, Usage of the Remote Connector.

<Simple Mode>

In this mode, the setting file is switched by using the [NEXT] and [CANCEL] buttons. For simple mode, refer to chapter 5, Usage in Standalone Mode.

(E)Initialize FP6

Click on this button to initialize the settings and password that were downloaded to the FP6.



4.4.3 [Target] menu

This menu is used to perform operations for the target device, such as erasure or programming. When the selected target device does not support a given function, the corresponding menu item will be hidden. This menu is invalid when the FP6 has not been connected.

4.4.3.1 Blank Check

This command checks if data has already been written to the target device.

4.4.3.2 Erase

This command erases flash memory in the target device.

4.4.3.3 Program

This command writes data that has been downloaded to the FP6 to the flash memory in the target device.

4.4.3.4 Verify

This command compares data written to the target device with data downloaded to the FP6.

4.4.3.5 Read

This command reads data from the flash memory in the target device.

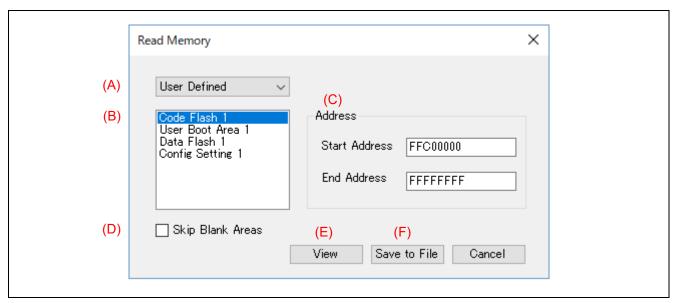


Figure 4.22 [Read Memory] Dialog Box

(A) Drop-down list box for specifying the area

Specify [All Areas] to read information in all areas of memory.

Specify [User Defined] to read information on any selected area of memory.

(B) Selection of an area

When [User Defined] is selected in (A) above, select the required area.

(C) [Start Address] and [End Address]

When [User Defined] is selected in (A) above, specify addresses where the range of information to be read starts and ends.

(D) [Skip Blank Areas]

Select this checkbox when blank areas are to be skipped in the reading of memory data.



(E) [View] button

Information that has been read from memory is displayed in the console window. Data from memory are displayed in units of 4 Kbytes. Clicking on any key continually repeats starting the output of the information in memory.

(F) [Save to File] button

Information that has been read from memory is saved to a file.

Remark: Select the format of the file for saving the memory data when specifying a file name in the [Save File] dialog box.

4.4.3.6 Program Flash Options

This command sets flash options, such as option bytes, security, flash access window, OTP, and lock bits, which have been set on the [Flash Option] tabbed page of the [Setup] dialog box, in the target device.

4.4.3.7 Initialize Device

This command initializes the settings for flash memory, boundaries and so on, and cause the DLM state to change to SSD.

4.4.3.8 DLM Transition

This command causes a transition to the DLM state. In the [DLM Transition] dialog box, selecting the target DLM state and clicking on Transition cause the required transition of the DLM state.

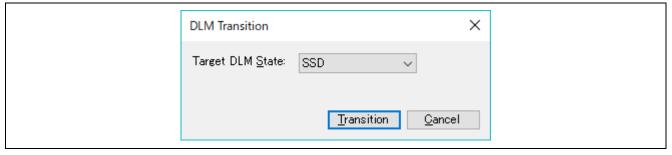


Figure 4.23 [DLM Transition] Dialog Box

(A) Target DLM State

The target DLM state is selected.

(B) Use Unique ID authentication

When this checkbox is selected, the unique ID authentication feature is used during transition to the RMA state.

4.4.3.9 Checksum

This command acquires the checksum of data of flash memory in the target device.

4.4.3.10 Start

This command executes the commands selected in the [Operation Setting] tabbed page of the [Setup] dialog box.

4.4.3.11 Connect

This command is used for connection or disconnection with the target device. This menu item can be selected only when automatic connection of the FP6 (see 7.4.1, autocon command) is disabled. Executing this command connects the target device, placing a tick against the menu item. Executing this command again disconnects the target device, removing the tick from the menu item.

4.4.3.12 Get Signature

This command establishes connection with the target device and displays MCU information in the console window.

4.4.3.13 Get Flash Options

This command acquires information on flash options from the target device and displays it in the console window and a popup dialog box. The acquired information can also be saved as a new setting file.

[Flash Options] dialog box
 The result of executing the Get Flash Options command will be displayed on the [Block Setting] and [Flash Option] tabbed pages of this dialog box.

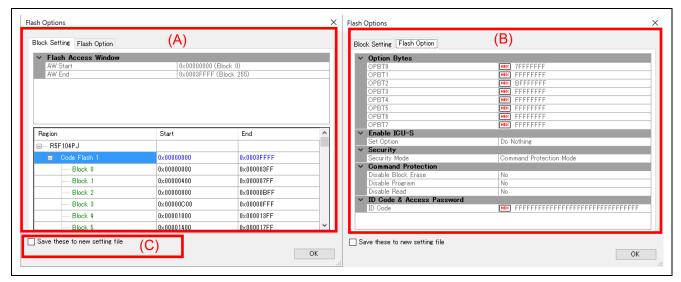


Figure 4.24 [Flash Options] Dialog Box

(A) [Block Setting] tabbed page

This page shows the settings made for [Lockbit & OTP], [Flash access window], and [End block of the boot area] on the [Block Setting] tabbed page of the [Setup] dialog box. For details, see section 4.3.3, [Block Setting] tabbed page.

(B)[Flash Option] tabbed page

This page shows the settings made on the [Flash Option] tabbed page of the [Setup] dialog box. For details, see section 4.3.4, [Flash Option] tabbed page.

Remark: Some data may not be acquired depending on the state of the MCU. Items for which no data have been acquired from the target device are left blank.

(C)[Save these to new setting file] checkbox

Select this checkbox if you wish to save the flash-option data that have been acquired as a new setting file.

Remark: Data will not be saved in a setting file if all data have not been acquired.



4.4.4 [Help] menu

4.4.4.1 [About FP6 Terminal]

This menu item shows the version information of the FP6 Terminal.

4.5 Toolbar

The menu items frequently used on the FP6 Terminal are displayed as buttons on the toolbar. Similar to the target menus on the menu bar, some buttons may be hidden depending on the selected operation or type of the target device.

Table 4.3 Toolbar Buttons

Icon	Description
	The same action as selecting [New Setting File] in the [File] menu.
	The same action as selecting [Select Programming Area…] in the [Programmer] menu.
	The same action as selecting [Connect] in the [Target] menu.
	Left side: Connect the FP6 when it is disconnected Right side: Disconnect the FP6 when it is connected
	The same action as selecting [Blank Check] in the [Target] menu.
	The same action as selecting [Erase] in the [Target] menu.
	The same action as selecting [Program] in the [Target] menu.
8	The same action as selecting [Verify] in the [Target] menu.
	The same action as selecting [Program Flash Options] in the [Target] menu.
***	The same action as selecting [Start] in the [Target] menu.

4.6 Example of Operation Using the FP6 Terminal

This chapter explains a series of basic FP6 operations using the FP6 Terminal, taking a case where the RL78/G14 is used as the target device as an example.

Series of operations described in this chapter:

The operation conditions for this chapter are as follows.

Host PC interface: USBProgramming area: Area 0

Target device: R5F104LE (RL78/G14)
 Power supply: 5 V supplied from the FP6
 Clock supply: 32 MHz (on-chip oscillator clock)

• Communications interface: Single-wire UART (1 Mbps)

Security setting: Disabled
 Operation mode: Chip mode
 Flash options: Not used

The operation steps described in this chapter are as follows.

- (1) Installing the FP6 Terminal and USB driver
- (2) Connecting the FP6 to the host PC
- (3) Connecting the target system
- (4) Starting up the FP6 Terminal
- (5) Setting up a programming environment
- (6) Executing the [Start] command
- (7) System shutdown

4.6.1 Installing the FP6 Terminal and USB driver

Refer to chapter 3, Software Installation, and install the FP6 Terminal and the USB driver on the host PC.

4.6.2 Connecting the FP6 to the host PC

- 1. Connect the USB connector of the FP6 to the USB port on the host PC via a USB cable.
- 2. Connect the power adapter (which comes with the FP6) to the FP6.
- 3. Turn on the power switch on the FP6. Do not connect the target device before turning on power.

4.6.3 Connecting the target system

Be sure to turn on the power of the FP6 before connecting the target system.

1. Connect the GND connector of the FP6 to the target system via the GND cable.

Note: The FP6 and target system may be damaged if there are differences in potential between the grounds of the FP6 and of the target system. Use the GND cable to eliminate differences in potential before connecting the target cable.



2. Connect the target connector of the FP6 to the target system via the target cable.

Note: Connect the target system before supplying V_{CC} power from the target system.

4.6.4 Starting up the FP6 Terminal

1. Click on the [Start] menu and select [PG-FP6] to start the FP6 Terminal.

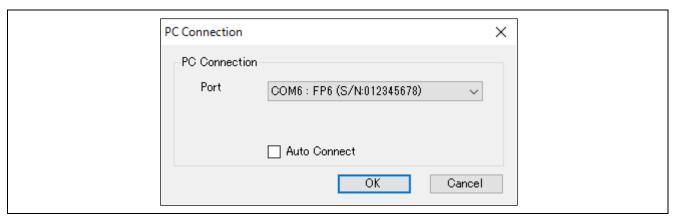


Figure 4.25 Connection between the FP6 Terminal and the FP6

- 2. Clicking on the [OK] button in the [PC Connection] dialog box connects the PC with the FP6 through the selected communication port.
- 3. When the FP6 Terminal is started correctly, the main window is opened.

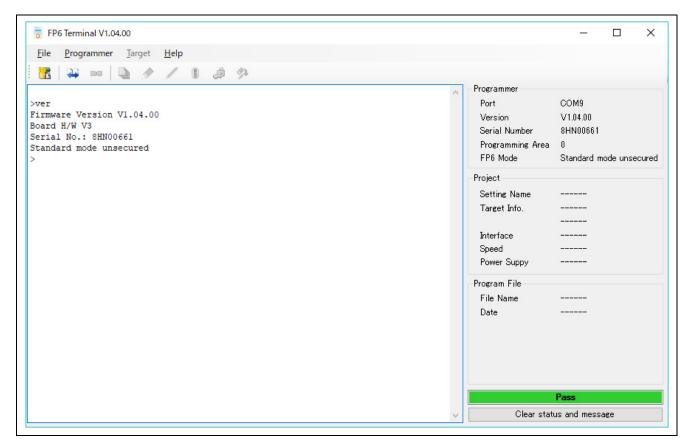


Figure 4.26 Main Window

4.6.5 Setting up a programming environment

1. When the main window is opened, select [New Setting File...].

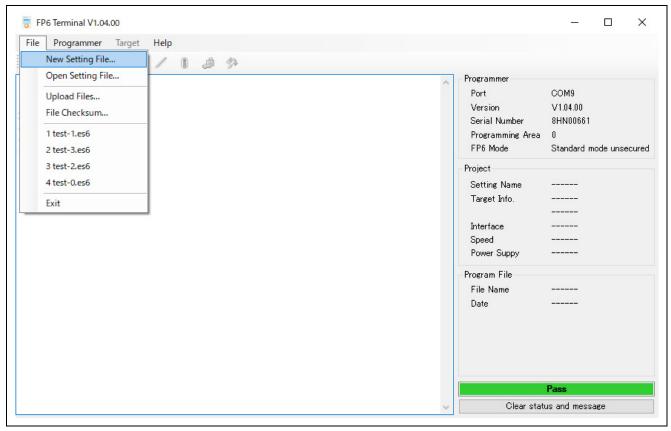


Figure 4.27 [Setup] Command

2. Create a new setting file. Select the family, group, and type name of the target device, and enter a setting name as shown in Figure 4.28, and click on the [OK] button.

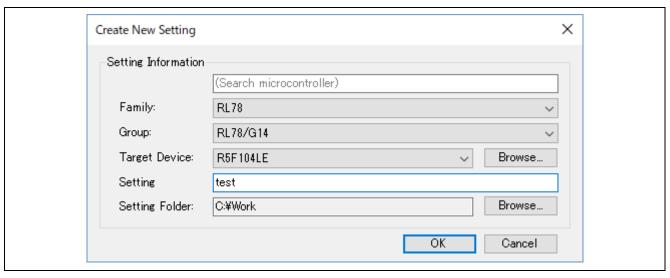


Figure 4.28 [Create New Setting] Dialog Box

3. The [Setup] dialog box will appear. Designate a program file on the [Program File] tabbed page. Click on the [Browse...] button to select a file.

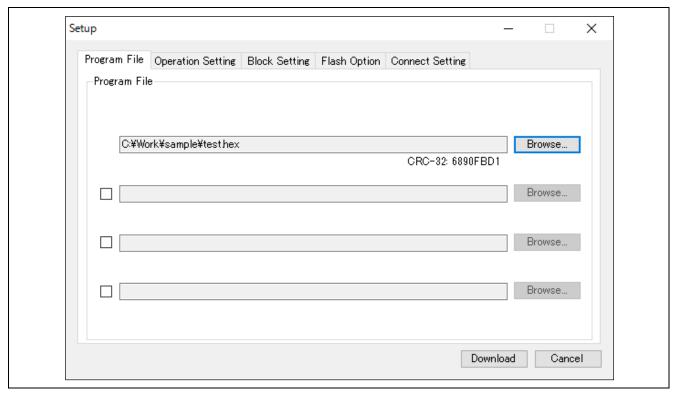


Figure 4.29 Selecting a Program File

4. Check that "chip mode" is selected as the operation mode on the [Block Setting] tabbed page.

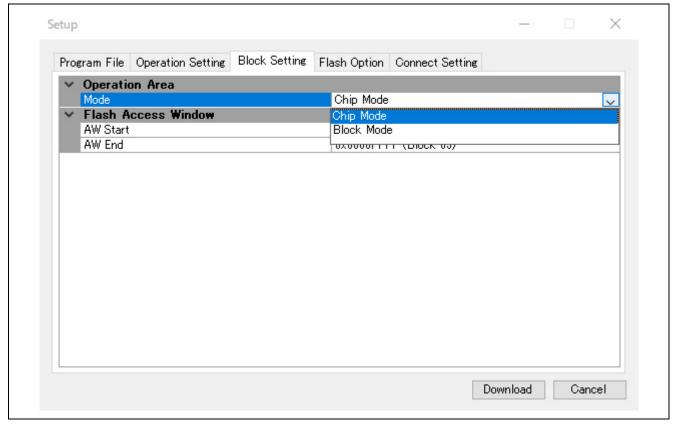


Figure 4.30 Changing the Block Setting

5. Click on the [Download] button to download parameter, setup, and program files to the FP6. When downloading is complete, the screen shown below will appear. This completes the setting of the programming environment.

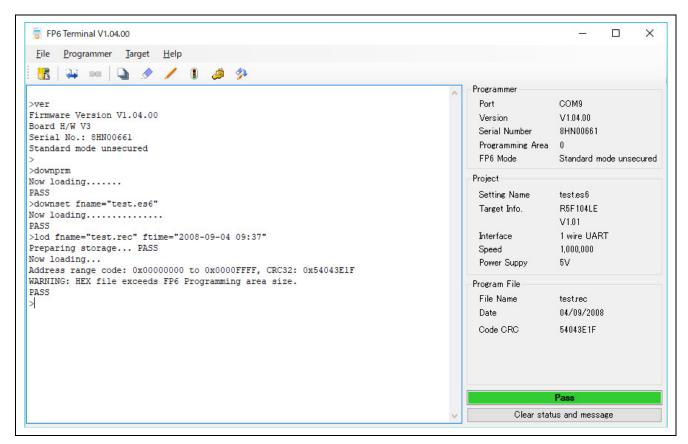


Figure 4.31 Downloading Parameter, Setup, and Program Files

4.6.6 Executing the [Start] command

Execute the [Start] command from the [Target] menu.

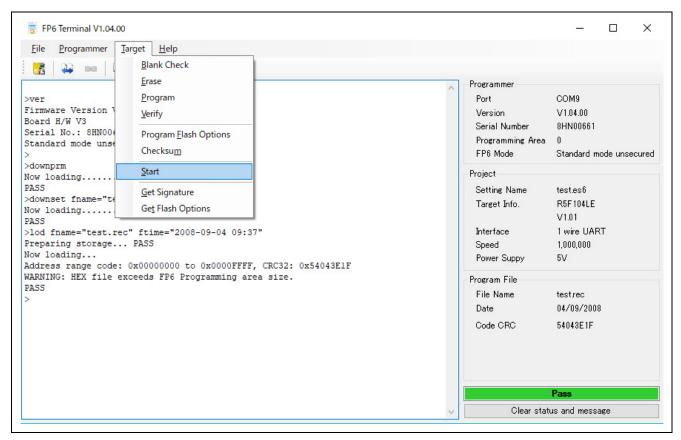


Figure 4.32 [Start] Command

When the [Start] command is executed, the [Erase] and [Program] commands are executed in that order for the R5F104LE.

Note: If you wish to write to another target system, turn the power off, connect the target system, and supply power before executing the [Start] command.

When execution of the [Start] command is completed, "Erase, Program operation finished" is displayed in the console window.

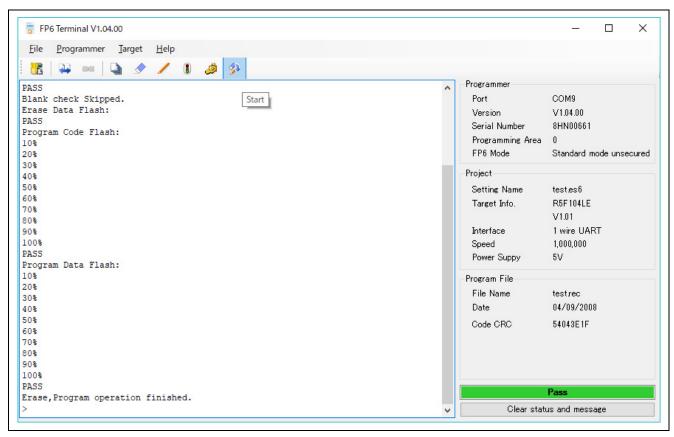


Figure 4.33 Result of Executing the [Start] Command

4.6.7 System shutdown

1. Remove the target system from the target cable.

Note: When Vcc is supplied from the target system, turn the power off before removing the target system.

- 2. If you do not intend to program any other target devices, execute the [Exit] command from the [File] menu to close the FP6 Terminal. All settings that have been made so far are saved in the setting file and can be restored when the FP6 Terminal is restarted. The parameter, setup, and program files are saved in the FP6 internal flash memory.
- 3. Turn off the power switch of the FP6.
- 4. Remove the power adapter and USB cable from the FP6.

Note: If an error has occurred in the above steps, refer to chapter 12, Troubleshooting, and appendix A, Messages. Also refer to 4.4.2.6, [Self Test], and perform self-testing. If this does not resolve the problem, see the FAQ (https://www.renesas.com/contact for inquiry.

5. Usage in Standalone Mode

The FP6 has a standalone mode in which the FP6 by itself can execute the [Erase], [Program], and [Start] commands without a host PC. This mode is useful for using the FP6 on the production line during mass production and for upgrading in the field.

Standard mode

Various functions on the LCD menu can be executed by operating buttons on the main unit or inputting the remote interface signal (NEXT, ENTER, CANCEL, START, VERIFY, or CLEAR).

Simple mode

This mode allows changing the programming areas by the NEXT button. In this mode, the functions on the LCD menu cannot be executed unlike in the standard mode. Table 5.1 shows assignments of remote interface signals in simple mode.

Table 5.1 Assignments of Remote Interface Signals in Simple Mode

Button on FP6 Main Unit	Pin Number Assigned to Remote Interface Signal	Function in Simple Mode		
CANCEL	5	CANCEL		
ENTER	6	Depends on the [Start] setting.		
NEXT	7	Changes programming areas. (Increments the number by 1. Returns to 0 after area 7.)		
START	9	Depends on the [Start] setting.		

Bank mode

Refer to chapter 6, Usage of the Remote Connector.

5.1 Details of Buttons, Message Display, and Status LEDs

In standalone mode, command menus are selected and executed using the control button ([NEXT], [ENTER], [CANCEL], or [START]) on the top of the FP6 main unit.

The selected command menu is shown in the message display, and the result of command execution is indicated by the message display and status LEDs.

The command menu consists of two levels of menus: a main menu and submenu.

[NEXT] button: Displays the next menu on the same level.

[ENTER] button: Selects or executes the menu item currently displayed.

Cancels the current selection and returns to the previous menu level. The command currently [CANCEL] button:

running cannot be stopped, except for the [Read] command.

Executes the [Start] command. It can be executed from any command menu, and the display [START] button:

returns to the same command menu after execution.



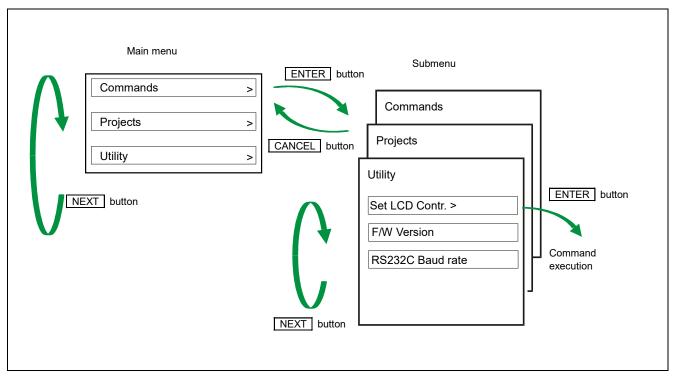


Figure 5.1 Transition of the States of Menus by Using Buttons

On the main menu level, the FP6 shows the selectable menu items. On the submenu level, the first line and the second line in the message display show the menu item and the response from the FP6, if any, respectively.

A command prompt '>' displayed at the end of a menu line indicates that it is selectable with the [ENTER] button, or that the menu (command) can be executed. If the command prompt '>' is not displayed at the end of a menu line, it means that the function is available only for display.

When power to the FP6 is turned on, 'Commands >' is displayed in the message display.

The status LEDs indicate the states of communications with the MCU and the result of execution, as shown below.

Table 5.2 Status LEDs

Status LED	Color	State
PASS	Blue	The selected command has been executed correctly. The command that has been correctly executed is displayed in the message display.
BUSY	Orange	The selected command is under execution. The detailed execution state is displayed in the message display.
ERROR	red	The selected command has been executed incorrectly. Details on errors are displayed in the message display.
VCC	green	Power is being supplied to the user system.

Note: For details on errors displayed in the message display, refer to appendix A.2, Error Messages Produced by the FP6 Main Unit.

5.2 Standalone Operation Menu

In standalone mode, the programming environment of the target device can be checked and then programs can be written by using the commands explained in this section.

5.2.1 [Commands] menu

The [Commands] menu provides various commands required for programming the target device. Select a command from this menu and press the [ENTER] button; the FP6 will then execute the command for the target device, based on the settings downloaded to the active programming area. For details on command execution, refer to section 4.4.3, [Target] menu.

Table 5.3 [Commands] Menu

Main Menu	Submenu		Description
[Commands >]	[E.P.	>]	Pressing the [ENTER] button executes the [Start] command.
	[Program	>]	Pressing the [ENTER] button executes the [Program] command.
	[Erase	>]	Pressing the [ENTER] button executes the [Erase] command.
	[Verify	>]	Pressing the [ENTER] button executes the [Verify] command.
[Program Flash >] Pressing the [E command.		>]	
	[Checksum	>]	Pressing the [ENTER] button executes the [Checksum] command. The checksum value read from the MCU is displayed in the message display. When there are multiple checksum values, pressing the [ENTER] button switches among the values.
1		Pressing the [ENTER] button executes the [Signature read] command. The MCU name is displayed in the message display.	
	[Erase Chip	>]	Pressing the [ENTER] button executes the [Initialize device] command.
	[Connect	>]	Pressing the [ENTER] button executes the [Connect] (con) command.
	[Disconnect	>]	Pressing the [ENTER] button executes the [Connect] (dcon) command.

5.2.2 [Project] menu

The [Project] menu is used to check information about switching the programming area and checking the setting file name, program file name, and CRC value.

Table 5.4 [Project] Menu

Main Menu	Submenu		Description
[Project >]	[Project Name	>]	Display the name of the setting file stored in the active programming area on the message display.*
	[PRM Name	>]	Display the name of the parameter file stored in the active programming area on the message display.*
		>]	Display the name of the program file stored in the active programming area on the message display.*
	[File Checksum	>]	Display the CRC-32 (the sum of the CRC-32 results for all areas which is displayed during downloading) of the entire file in the message display.*
	[Progarea	>]	Pressing the [ENTER] button causes a transition to the next programming area.

Note: If the file to be displayed has not been downloaded, [n.a.] is displayed. If the file name exceeds 16 characters, "~" is displayed as the 16th character.

5.2.3 [Utility] menu

The [Utility] menu is used to adjust the LCD contrast and check the firmware version of the FP6 main unit.

Table 5.5 [Utility] Menu

Main Menu	Submenu		Description
[Utility >]	[Set LCD Contr. >]		Adjust the contrast in the message display. After pressing the [ENTER] button, the contrast can be adjusted using the [NEXT] (darken) or [CANCEL] (lighten) button. To fix the contrast, click on the [ENTER] button.
	[F/W Version]	Pressing the [ENTER] button displays the FP6 firmware version.
	[RS232C Baud rate]	Pressing the [ENTER] button displays the current baud rate value set for the RS-232C host interface.

6. Usage of the Remote Connector

This chapter describes the usage of the remote connector.

The FP6 can be remotely controlled by connecting the remote connector and external control device. Remote control can be used to operate and check programming and the display of PASS, BUSY or ERROR from the external control device.

6.1 Remote Interface Mode

The remote interface has a standard mode and a bank mode.

The modes are switched by using [Operation Mode] of [FP6 Manager].

For details of the mode setting, refer to section 4.4.2.7, [FP6 Manager].

- Standard mode
 - The same signals as the control buttons (NEXT, ENTER, and CANCEL) on the command menu of the FP6 unit can be input.
- Bank mode

This mode allows inputting of the bank signals (BANK0 to BANK2) that indicate the programming area. The control buttons (NEXT, ENTER, and CANCEL) will change their functions to those inputting bank signals.



7. Usage of Communications Commands

This chapter describes how to use communications commands from a host PC to operate the FP6.

7.1 Starting the Communications Software

In order to use communications commands for operation, communications with the FP6 must be established with communications software. In this chapter, we shall describe how to use communications software to establish communications.

7.1.1 Connecting the system

For connection via the USB, connect a USB cable to the USB port on your host PC, and then connect the other end to the USB connector on the FP6. For connection via the RS-232C, connect an RS-232C cable to the RS-232C connector on your host PC and then connect the other end to the RS-232C connector on the FP6. Next, plug the power supply adapter into an outlet, then connect it to the FP6 power supply connector.

7.1.2 Starting the FP6

After the connections are made, turn on the FP6 power supply switch.

7.1.3 Starting communications software

Start communications software.

Check the COM port number with Device Manager.

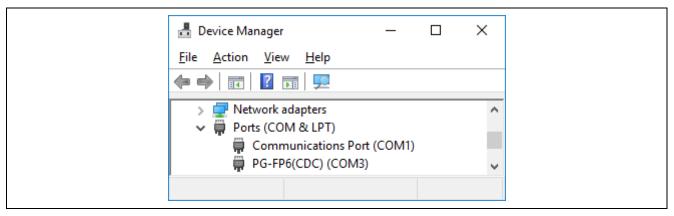


Figure 7.1 Checking the COM Port Number Settings

In the case of using the RS - 232C cable, select the data transfer conditions listed below.

Data transfer rate: 9600 bps, 19200 bps, 38400 bps, 57600 bps, or 115200 bps

Data bits: 8 bits Parity: None Stop bit: 1 bit

Flow control: Hardware

The default data transfer rate is 9600 bps, but it may be changed by the FP6 Terminal or terminal commands to another rate. In such cases, use [RS232C Baud rate] from [Utility] in the LCD panel of the FP6 main unit to check the transfer rate and make sure that it matches that of the host.

When communications software starts correctly, the main window will open. If communications are established, then a ">" will be displayed when the Enter key on the host PC is pressed. This completes the preparation for using communications commands.



Note: Press the Enter key once after FP6 has started. Alternatively, send a linefeed code once to FP6 by using communications software.

7.2 Command Lists

The following is a list of commands that control the FP6 main unit and the target device.

Table 7.1 List of FP6 Control Commands

Command Name	Description
autocon	This command is used to select whether to automatically or manually connect or disconnect the target device in the following processes, or to refer to the current setting.
	From entering flash memory programming mode to verifying the signature
	Leaving the flash memory programming mode
brt	Confirms and changes the data transfer rate during serial communications with the host PC.
conf	Displays a list of the information stored in the FP6.
dwnprm	Downloads the parameter file.
downset	Downloads the setting file.
fcks	Gets a checksum value of the program file that was downloaded to the active programing area of the FP6.
files	Displays the information concerning the program file, DLM key, and user key that were downloaded to the FP6.
hex	Uploads the program file in Intel HEX format.
hlp	Displays a list of available commands, with simple descriptions.
lod	Downloads the program file, DLM key, and user key to the active programming area of the FP6.
prm	Displays the information concerning the parameter file and setting file that were downloaded to the FP6.
progarea	Confirms, changes and deletes data in the active programming areas.
res	Resets the FP6.
selftest	Executes a self-test.
serno	Sets the unique code for embedding in the program file.
set_auth	Changes the authentication ID code to a desired value.
sound	Sets the buzzer.
speed_mode	Adjusts the waiting time and timeout time in communications with the target device.
srec	Uploads the program file in Motorola S format.
trc	Displays the communication information between the FP6 and target device.
upprm	Uploads the parameter file.
upset	Uploads the setting file.
ver	Displays the FP6 version.

Table 7.2 List of FP6 Device Commands

cir Executes the Configuration clear. con Executes the processes from "transition to flash memory programming mode" to "signature verification". dcon Executes the termination of the flash memory programming mode. dlim Refers to the DLM state and causes a transition of the state. ep Executes erasure and then programming. ers Executes the Erase command. ers_chip Initializes the target device. gdi Gets the information of blank check and flash option. ged Gets the information of endian. gid Gets the information of lock bit. gob Gets the information of option byte. gof Gets the information of OFS. gos Gets the information of PS. gos Gets the information of ToP. gsc Gets the information of ToP. gsc Gets the information of Security. gtm Gets the information of Trusted Memory. idic Executes the ID code setting. opb Executes the OTP setting. pro Sets the flash options collectively. pro Executes the Security Release command. sed Executes the Security Release command. sed Executes the Security Release command. sed Executes the ISet Security] command. sed Executes the Signature read command. sig Executes the signature read command. sig Executes the Sexecute programming. stm Executes the Trusted Memory setting.	Command Name	Description
Executes the processes from "transition to flash memory programming mode" to "signature verification". doon	bln	Executes the blank check.
verification". decon Executes the termination of the flash memory programming mode. dlim Refers to the DLM state and causes a transition of the state. ep Executes erasure and then programming. ers Executes the Erase command. ers_chip Initializes the target device. gdi Gets the information of blank check and flash option. ged Gets the information of endian. gid Gets the information of lock bit. gob Gets the information of option byte. gof Gets the information of OFS. gos Gets the information of OFS. gos Gets the information of flash option. got Gets the information of of PP. gsc Gets the information of Security. gtm Gets the information of Security. gtm Gets the information of Trusted Memory. idc Executes the ID code setting. opb Executes the OTP setting. pro Sets the flash options collectively. prg Executes programming. read Reads the flash memory data from the target device. rsc Executes the Security Release command. sef Executes the Security Release command. sef Executes the Security I command. sed Executes the ID code and enables ID authentication in the serial programming mode. sig Executes the Serial programming. stm Executes the Secute Trusted Memory setting.	clr	Executes the Configuration clear.
dim Refers to the DLM state and causes a transition of the state. ep Executes erasure and then programming. ers Executes the Erase command. ers_chip Initializes the target device. gdi Gets the information of blank check and flash option. ged Gets the information of endian. gid Gets the information of lock bit. gob Gets the information of option byte. gof Gets the information of OFS. gos Gets the information of OFS. gos Gets the information of OTP. gsc Gets the information of Security. gtm Gets the information of Trusted Memory. idid Executes the ID code setting. opp Executes the OTP setting. pro Sets the flash options collectively. prg Executes the Security Release command. sef Executes the Security Command. sef Executes the ID code and enables ID authentication in the serial programming mode. sig Executes the Signature read command. structures the Colecksum command.	con	
ep Executes the Erase command. ers Executes the Erase command. ers_chip Initializes the target device. gdi Gets the information of blank check and flash option. ged Gets the information of endian. gid Gets the information of lock bit. ggb Gets the information of lock bit. ggb Gets the information of option byte. ggf Gets the information of OFS. ggs Gets the information of OFS. ggs Gets the information of OTP. ggs Gets the information of OTP. ggs Gets the information of Trusted Memory. idc Executes the ID code setting. opb Executes the OTP setting. opb Executes the OTP setting. pfo Sets the flash options collectively. prg Executes programming. read Reads the flash memory data from the target device. Executes the Security Release command. sed Executes the Set Security command. sed Executes the Signature read command. sid Sets the ID code and enables ID authentication in the serial programming mode. sig Executes the Securite Memory setting. spd Disables the serial programming.	dcon	Executes the termination of the flash memory programming mode.
Executes the Erase command. ers_chip Initializes the target device. gdi Gets the information of blank check and flash option. ged Gets the information of endian. gid Gets the information of lock bit. gob Gets the information of option byte. gof Gets the information of OFS. gos Gets the information of flash option. got Gets the information of OTP. gsc Gets the information of OTP. gsc Gets the information of Trusted Memory. idc Executes the ID code setting. otp Executes the OTP setting. pfo Sets the flash options collectively. prg Executes programming. read Reads the flash memory data from the target device. Executes the [Set Security] command. sed Executes the OEA Security ID authentication in the serial programming mode. sig Executes the Signature read command. sthe Executes the ID code and enables ID authentication in the serial programming mode. Executes the ID code and enables ID authentication in the serial programming mode. Executes the Signature read command. Executes the Signature read command. Executes the ID code and enables ID authentication in the serial programming mode. Executes the Signature read command.	dlm	Refers to the DLM state and causes a transition of the state.
ers_chip Initializes the target device. gdi Gets the information of blank check and flash option. ged Gets the information of endian. gid Gets the ID code. glb Gets the information of option byte. gob Gets the information of OFS. gos Gets the information of flash option. got Gets the information of OTP. gsc Gets the information of Trusted Memory. idc Executes the ID code setting. pth Executes the OTP setting. pth Executes the OTP setting. prig Executes the flash memory data from the target device. rsc Executes the Security Release command. sed Executes the ID code and enables ID authentication in the serial programming mode. sig Executes the lock bit setting. stm Executes the ISet Setsing. stm Executes the Serial programming. stm Executes the Serial programming.	ер	Executes erasure and then programming.
Gets the information of blank check and flash option. ged Gets the information of endian. gid Gets the ID code. glb Gets the information of lock bit. gob Gets the information of option byte. gof Gets the information of OFS. gos Gets the information of flash option. got Gets the information of OTP. gsc Gets the information of Security. gtm Gets the information of Trusted Memory. idc Executes the ID code setting. opb Executes the option byte setting. otp Executes the OTP setting. prof Sets the flash options collectively. prof Sets the flash memory data from the target device. rsc Executes the Security Release command. sed Executes the ID code and enables ID authentication in the serial programming mode. sig Executes the Signature read command. stm Executes the Irusted Memory setting.	ers	Executes the Erase command.
ged Gets the information of endian. gid Gets the ID code. glb Gets the information of lock bit. gob Gets the information of option byte. gof Gets the information of OFS. gos Gets the information of flash option. got Gets the information of OTP. gsc Gets the information of Trusted Memory. idc Executes the ID code setting. opb Executes the option byte setting. otp Executes the OTP setting. pfo Sets the flash options collectively. prg Executes programming. read Reads the flash memory data from the target device. rsc Executes the Security Release command. sed Executes the ID code and enables ID authentication in the serial programming mode. sig Executes the lock bit setting. spd Disables the serial programming. stm Executes the Trusted Memory setting.	ers_chip	Initializes the target device.
gid Gets the ID code. glb Gets the information of lock bit. gob Gets the information of option byte. gof Gets the information of OFS. gos Gets the information of OFS. gos Gets the information of OTP. gsc Gets the information of OTP. gsc Gets the information of Security. gtm Gets the information of Trusted Memory. idc Executes the ID code setting. opb Executes the option byte setting. otp Executes the OTP setting. pfo Sets the flash options collectively. prg Executes programming. read Reads the flash memory data from the target device. rsc Executes the Security Release command. sef Executes the ID code and enables ID authentication in the serial programming mode. sig Executes the Signature read command. slb Executes the Serial programming. stm Executes the Trusted Memory setting. sum Executes the Checksum command.	gdi	Gets the information of blank check and flash option.
Gets the information of lock bit. Gets the information of option byte. Gets the information of OPS. Gets the information of GPS. Gets the information of flash option. Gets the information of OTP. Gets the information of Security. gttm Gets the information of Trusted Memory. idid Executes the ID code setting. opb Executes the OTP setting. otp Executes the OTP setting. pro Sets the flash options collectively. Executes programming. read Reads the flash memory data from the target device. rsc Executes the Security Release command. scf Executes the Security I command. sed Executes the ID code and enables ID authentication in the serial programming mode. sig Executes the Signature read command. stb Executes the Signature read command. stb Executes the IS serial programming. stm Executes the Trusted Memory setting. sum Executes the Checksum command.	ged	Gets the information of endian.
Gets the information of option byte. Gets the information of OFS. Gets the information of Grant Of Dects of Gets the information of Grant Of Dects of Gets the information of OTP. Gets the information of OTP. Gets the information of Security. Gets the information of Trusted Memory. Gets the information of Trusted Memory. Gets the ID code setting. Opb Executes the OTP setting. Oth Executes the OTP setting. For Sets the flash options collectively. For Executes programming. Reads the flash memory data from the target device. For Executes the Security Release command. Set Executes the [Set Security] command. Set Executes the endian setting. Sid Sets the ID code and enables ID authentication in the serial programming mode. Sig Executes the Signature read command. Sib Executes the Serial programming. Stm Executes the Trusted Memory setting. Sum Executes the Checksum command.	gid	Gets the ID code.
Gets the information of OFS. Gets the information of flash option. Gets the information of OTP. Gets the information of Security. Gets the information of Security. Gets the information of Trusted Memory. idc Executes the ID code setting. opb Executes the option byte setting. otp Executes the OTP setting. pfo Sets the flash options collectively. prg Executes programming. read Reads the flash memory data from the target device. rsc Executes the Security Release command. sef Executes the [Set Security] command. sed Executes the ID code and enables ID authentication in the serial programming mode. sig Executes the ID code and enables ID authentication in the serial programming mode. sig Executes the lock bit setting. spd Disables the serial programming. stm Executes the Trusted Memory setting. sum Executes the Checksum command.	glb	Gets the information of lock bit.
Gets the information of flash option. Gets the information of OTP. Gets the information of security. Gets the information of Trusted Memory. idc	gob	Gets the information of option byte.
Gets the information of OTP. gsc Gets the information of Security. gtm Gets the information of Trusted Memory. idc Executes the ID code setting. opb Executes the option byte setting. otp Executes the OTP setting. pfo Sets the flash options collectively. prg Executes programming. read Reads the flash memory data from the target device. rsc Executes the Security Release command. scf Executes the [Set Security] command. sed Executes the endian setting. sid Sets the ID code and enables ID authentication in the serial programming mode. sig Executes the Signature read command. slb Executes the serial programming. stm Executes the Trusted Memory setting. sum Executes the Checksum command.	gof	Gets the information of OFS.
Gets the information of security. gtm Gets the information of Trusted Memory. idc Executes the ID code setting. opb Executes the option byte setting. otp Executes the OTP setting. pfo Sets the flash options collectively. prg Executes programming. read Reads the flash memory data from the target device. rsc Executes the Security Release command. scf Executes the [Set Security] command. sed Executes the endian setting. sid Sets the ID code and enables ID authentication in the serial programming mode. sig Executes the Signature read command. slb Executes the lock bit setting. spd Disables the serial programming. stm Executes the Checksum command.	gos	Gets the information of flash option.
gtm Gets the information of Trusted Memory. idc Executes the ID code setting. opb Executes the option byte setting. otp Executes the OTP setting. pfo Sets the flash options collectively. prg Executes programming. read Reads the flash memory data from the target device. rsc Executes the Security Release command. scf Executes the [Set Security] command. sed Executes the endian setting. sid Sets the ID code and enables ID authentication in the serial programming mode. sig Executes the Signature read command. slb Executes the serial programming. stm Executes the Trusted Memory setting. sum Executes the Checksum command.	got	Gets the information of OTP.
idc Executes the ID code setting. opb Executes the option byte setting. otp Executes the OTP setting. pfo Sets the flash options collectively. prg Executes programming. read Reads the flash memory data from the target device. rsc Executes the Security Release command. scf Executes the [Set Security] command. sed Executes the endian setting. sid Sets the ID code and enables ID authentication in the serial programming mode. sig Executes the Signature read command. slb Executes the serial programming. spd Disables the serial programming. stm Executes the Checksum command.	gsc	Gets the information of security.
Executes the option byte setting. otp	gtm	Gets the information of Trusted Memory.
otp Executes the OTP setting. pfo Sets the flash options collectively. prg Executes programming. read Reads the flash memory data from the target device. rsc Executes the Security Release command. scf Executes the [Set Security] command. sed Executes the endian setting. sid Sets the ID code and enables ID authentication in the serial programming mode. sig Executes the Signature read command. slb Executes the lock bit setting. spd Disables the serial programming. stm Executes the Trusted Memory setting. sum Executes the Checksum command.	idc	Executes the ID code setting.
pro Sets the flash options collectively. pro Executes programming. read Reads the flash memory data from the target device. rsc Executes the Security Release command. scf Executes the [Set Security] command. sed Executes the endian setting. sid Sets the ID code and enables ID authentication in the serial programming mode. sig Executes the Signature read command. slb Executes the lock bit setting. spd Disables the serial programming. stm Executes the Trusted Memory setting. sum Executes the Checksum command.	opb	Executes the option byte setting.
Prince and Programming. Reads the flash memory data from the target device. Reads t	otp	Executes the OTP setting.
Reads the flash memory data from the target device. Executes the Security Release command. Executes the [Set Security] command. Executes the endian setting. Sed Executes the endian setting. Sid Sets the ID code and enables ID authentication in the serial programming mode. Executes the Signature read command. SID Executes the lock bit setting. Spd Disables the serial programming. Stm Executes the Trusted Memory setting. Sum Executes the Checksum command.	pfo	Sets the flash options collectively.
Executes the Security Release command. Scf Executes the [Set Security] command. Sed Executes the endian setting. Sid Sets the ID code and enables ID authentication in the serial programming mode. Sig Executes the Signature read command. Slb Executes the lock bit setting. Spd Disables the serial programming. Stm Executes the Trusted Memory setting. Sum Executes the Checksum command.	prg	Executes programming.
Executes the [Set Security] command. sed Executes the endian setting. sid Sets the ID code and enables ID authentication in the serial programming mode. sig Executes the Signature read command. slb Executes the lock bit setting. spd Disables the serial programming. stm Executes the Trusted Memory setting. sum Executes the Checksum command.	read	Reads the flash memory data from the target device.
sed Executes the endian setting. sid Sets the ID code and enables ID authentication in the serial programming mode. sig Executes the Signature read command. slb Executes the lock bit setting. spd Disables the serial programming. stm Executes the Trusted Memory setting. sum Executes the Checksum command.	rsc	Executes the Security Release command.
Sets the ID code and enables ID authentication in the serial programming mode. Executes the Signature read command. Executes the lock bit setting. Disables the serial programming. Executes the Trusted Memory setting. Executes the Checksum command.	scf	Executes the [Set Security] command.
sig Executes the Signature read command. slb Executes the lock bit setting. spd Disables the serial programming. stm Executes the Trusted Memory setting. sum Executes the Checksum command.	sed	Executes the endian setting.
slb Executes the lock bit setting. spd Disables the serial programming. stm Executes the Trusted Memory setting. sum Executes the Checksum command.	sid	Sets the ID code and enables ID authentication in the serial programming mode.
spd Disables the serial programming. stm Executes the Trusted Memory setting. sum Executes the Checksum command.	sig	Executes the Signature read command.
stm Executes the Trusted Memory setting. sum Executes the Checksum command.	slb	Executes the lock bit setting.
sum Executes the Checksum command.	spd	Disables the serial programming.
	stm	Executes the Trusted Memory setting.
vrf Executes the Verify command.	sum	Executes the Checksum command.
,	vrf	Executes the Verify command.

7.3 Description of Commands

Each of the commands is described using the following format.

Command name

Presents an overview of the command.

Input format

Presents the input format for the command^{Note}.

Description of the function

Describes the function of the command.

Example of usage

Presents an example of using the command.

Note: The symbols used to describe the input format are defined below.

Notation	Description
Characters within single quotation marks ' '	Characters that must be input as displayed
Characters within angle brackets < >	Information that must be provided
Characters within parentheses ()	Optional items
Options separated by vertical bars	Options where only one option can be selected

7.4 Description of FP6 Control Commands

7.4.1 autocon command

This command is used to select whether to automatically or manually connect or disconnect the target device in the following processes, or to refer to the current setting.

- · From entering flash memory programming mode to verifying the signature
- · Leaving the flash memory programming mode

Input 1	format
---------	--------

'autocon' ('on | off')

Description of the function

Selects either automatic (on) or manual (off) execution, to be executed before and after the target command completion, of the processes from entering flash memory programming mode to verifying the signature (con command), and leaving the flash memory programming mode (dcon command). The initial value is automatic (on). If this command is executed without an option, the current setting is displayed (automatic (on) or manual (off)). The default setting is automatic (on).

on: The con command and dcon command are executed automatically.

off:

The con command and dcon command are executed manually. When set to manual (off), the con command is executed, the target command can be executed. Furthermore, various target commands can be executed multiple times. Execute the dcon command to terminate. Note that the ep command will automatically execute the con command and dcon command even if this is set to manual (off).

Example of Communication Software Terminal Display				
>autocon				
AutoCon is on / off				
>autocon on				
AutoCon is on				
>autocon off				
AutoCon is off				

7.4.2 brt command

Confirms and changes the data transfer rate for serial communications with the host PC.

Input format

'brt' ('9600' | '19200' | '38400' | '57600' | '115200')

Description of the function

This command can be used with its options to change the data transfer rate for serial communications with the host PC. When the data transfer rate is changed, it will be necessary to change the data transfer rate of the COM port setting with terminal software and reconnect.

If no options are used with this command, the current data transfer rate will be displayed.

If the serial connector is connected, the data transfer rate will be displayed.

If a USB connector is used, the USB version will be displayed.

- USB (HS) ... USB 2.0
- USB (FS) ... USB 1.1

The default data transfer rate is 9600 bps.

9600: Changes the data transfer rate to 9600 bps.

19200: Changes the data transfer rate to 19200 bps.

38400: Changes the data transfer rate to 38400 bps.

57600: Changes the data transfer rate to 57600 bps.

115200: Changes the data transfer rate to 115200 bps.

Example of usage

Example of Communication Software Terminal Display

>brt

[When the serial connector is connected at 115200 bps]

Current Baud rate is: 115200

>brt

[When the USB connector is connected at High speed]

Current Baud rate is: USB (HS)

>brt 19200

New Baud rate is: 19200



7.4.3 conf command

Displays a list of the information stored in the FP6.

Input format

'conf'

Description of the function

Displays information on data downloaded to the FP6 and the settings of the FP6.

		Example of Com	nuni	cation S	Software Terminal Di	splay
>conf						
Firmwa	are Version Vx.xx.xx					
Board	H/W Vx					
Seria	l No.: xxxxxxxxxx					
Standa	ard mode unsecured					
Active	e Program Area: O					
Numbe	r of Program areas: 8					
Max.	area size: 384 MByte					
Free	space: 363 MByte					
Area (0: 2 MByte					
	1: 6 MByte					
	2: 3 MByte					
	3: 10 MByte					
	4: O MByte					
	5: O MByte					
	6: O MByte					
Area	7: O MByte					
Area I	Filename	Dat	е	Time	Range	CRC
*0	test-0. hex	2019-1	0–17	17:35	00000000-00003FF	F 2673FC33
1	{unknown data}					
2	test-2. hex	2019-1	0–17	17:35	00000000-00003FF	F 2673FC33
3	test-3. hex	2019-1	0–17	17:35	00000000-00003FF	F 2673FC33
4	{unknown data}					
5	{unknown data}					
6	{unknown data}					
7	{unknown data}					
Area	File name				CRC Type	
*0	R5F104AA				25BDA75F PR5	
	test-0. es6				B6D40286 ESF	
1	R5F564M				1CC12600 PR5	
	test-1.es6				OFDBCF7A ESF	
2	R7FA6M3AF				DEC16EA8 PR5	
	test-2. es6				ABB4801E ESF	

3	R7F701708	92AC1CBE PR5
	test-3. es6	A43294EC ESF
4	{invalid}	PR5
	{invalid}	ESF
5	{invalid}	PR5
	{invalid}	ESF
6	{invalid}	PR5
	{invalid}	ESF
7	{invalid}	PR5
	{invalid}	ESF

AutoCon is on Sound is on EP mode: Standard speed mode is middle.

Security state is: Inactive Boot protection: disabled Max authentication number: 0

Current number of password authentication: 0
Current number of boot authentication: 0
Limit of ep/prg executions: disabled
Remain number of ep/prg executions: 0
Encrypt downloaded data: disabled
Encrypt file password: disabled

Manager flags: 0x00000100

HEX file Upload enabled

Device Setup enabled

Checksum comparison off

Error on 'HEX file exceeds flash range' disabled

Unique Code disabled
Read Command enabled
Manager option byte: 0x00
HEX file Upload enabled
Device Setup enabled
Checksum comparison off

Error on 'HEX file exceeds flash range' disabled

7.4.4 downprm command

Downloads the parameter file.

Input format

'downprm'

<Parameter file data>

Description of the function

Downloads the parameter file to the FP6 main unit. Before executing the downset command, be sure to execute the downprm command to download the parameter file.

7.4.5 downset command

Downloads the setting file.

Input format

'downset ('fname="filename"')'

<Setting file data>

Description of the function

Downloads the setting file to the FP6 main unit.

Be sure to execute the downprm command before the downset command.

Be sure to execute the lod command after the downset command.

File names without options are not stored.

fname="filename":

Specifies the name of the setting file to be downloaded. The maximum number of characters is 50.

If 51 or more characters are specified, the first 50 characters are used.



7.4.6 fcks command

Gets a checksum value of the program file that was downloaded to the active programing area of the FP6.

Input format

'fcks' (<type> (<start1> <end1> (<start2> <end2> (<start3> <end3> (<start4> <end4> (<start5> <end5>))))))

Description of the function

Gets a checksum value of the program file in the active programming area.

Specifies the calculation method, start address and number of bytes in the options.

If this command is specified without options, an appropriate calculation method for the target MCU is used for all the areas.

type: Specifies one of the following calculation methods.

crc: 32-bit CRC method crc16: 32-bit CRC method

ari: 16-bit subtraction calculation method (When a V850, RL78, or 78K is selected)

32-bit subtraction calculation method (When a RX, RH850, SuperH, or R8C is selected)

k0s sp: Division method (original)

startx: The start address is specified in hexadecimal. (A maximum of five ranges can be specified.)

endx: Specifies the end address in hexadecimal. (A maximum of five ranges can be specified.)

Example of usage

Example of Communication Software Terminal Display

> fcks crc 0 3fffff

Checksum Code Flash 1 : 000000-3FFFFF = 26218DD4

> fcks ari 0 3fffff 400000 41ffff

Checksum Code Flash 1 : 000000-3FFFFF = 61C0 Checksum Data Flash 1 : 400000-41FFFF = 0200

Checksum Total : 63C0

7.4.7 files command

Displays the information concerning the program file, DLM key, and user key that were downloaded to the FP6

Input format

'files' ('key') ('check')

Description of the function

If no options are used, the information (file name, creation date, size, and checksum) concerning the program file downloaded to the FP6 is displayed.

check: The checksum of all programming areas stored in the program file, from START to END, is recalculated with

the 32-bit CRC method, and cross-checked with the checksum stored in the FP6 during download.

key: Displays the data specified in key files without using a program file.

	Example of Communication Software Terminal Display							
Area	Filename	Date Time Ra	inge	CRC <cr+lf></cr+lf>				
*0	XXXXX. key	xxxx xxxx SE	CDBG <cr+< td=""><td>_F></td><td></td><td></td></cr+<>	_F>				
	XXXX. key	xxxx xxxx 00	000000 <c< td=""><td>R+LF></td><td></td><td></td></c<>	R+LF>				
1	1 {invalid} < CR+LF >							
2 X	2 XXXXXXXX.key xxxx xxxx 00002000 <cr+lf></cr+lf>							
3 X	XX. key	xxxx xxxx NONS	ECDBG <cr< td=""><td>+LF></td><td></td><td></td></cr<>	+LF>				
4 {	4 {invalid} <cr+lf></cr+lf>							
5 {	5 {invalid} <cr+lf></cr+lf>							
6 {	6 {invalid} <cr+lf></cr+lf>							
7 {	invalid} <cr+< td=""><td>·LF></td><td></td><td></td><td></td><td></td></cr+<>	·LF>						
>								

7.4.8 hex command

Uploads the program file to the host PC in Intel HEX format.

Input format

'hex' (<start1><length1>(<start2><length2>(<start3><length3>(<start4><length4>))))

Description of the function

If a program file has been downloaded to an active programming area, executing this command will upload the program file in Intel HEX format. If this command is executed without any options, the upload will be executed with the address size used during downloading. If a program has not been downloaded, "Invalid argument" will be displayed.

start address: The start address is designated as a hexadecimal number. (A maximum of four ranges can be specified.)

length: The number of bytes is designated as a hexadecimal number. (A maximum of four ranges can be specified.)

Example of usage

Example of Communication Software Terminal Display

> hex 0 3fff

Press any key to start/continue output.

.

:0000001FF

7.4.9 hlp command

Lists available commands with brief descriptions.

Input format

'hlp'

Description of the function

Lists available commands with brief descriptions.

Example of Communication Software Terminal Display								
>hlp								
(Control commands							
${\tt downprm/downset}$: Download parameter/customer settings							
upprm /upset	: Upload parameter/customer settings							
lod	: Download Intel Hex or Motorola S-record file							
hex/srec	: Upload Intel Hex / Motorola S-record file							
progarea	: Change Program area							
files	: Show downloaded HEX/SREC files in FP6 memory							
prm	: Show Parameter file (PRM/SET) information							
conf	: Show / Modify FP6 configuration							
brt	: Set Baud rate to host							
fcks	: Calculate file checksum (FP6 memory)							
ver	: Show firmware version							
res	: Reset FP6							
sound	: Enable / Disable sound generation							
trc	: Show Device communication trace							
selftest	: Perform a Selfcheck							
	Device commands							
bln	: Blankcheck							
ers	: Erase							
prg	: Program							
vrf	: Verify							
read	: Read							
ер	: Erase and Program							
sig	: Show device signature							
sum	: Get device checksum							
scf	: Set security information							

7.4.10 lod command

Downloads the program file, DLM key, and user key to the active programming area of the FP6.

Input format

key

'lod' ('add') ('key' <type> (<address>)) (fname="<filename>") ('ftime="<date and time>")

Description of the function

Downloads the program file, DLM key, and user key to an active programming area. After this command is executed, the program file must be downloaded to the FP6 in ASCII format using communications software. If using the terminal software, select [Transfer], and then select the program file. The options are to delete or not to delete the file before downloading, the file name, and the creation date. If this command is executed without any options, the file name and creation date will not be stored. Use the FP6 Terminal.

Caution: In V1.04.00 and later versions, the CRC of the program file in the range of the ROM space of the target device is calculated and displayed before the program file is downloaded. Data outside the range of the ROM space are not in the scope of CRC calculation.

add: Specifying the add option omits the erasure of data that have been stored in the FP6 before downloading of the file for programming.

Specifying the type of key.

<type> seckey: SECDBG key
nonseckey: NONSECDBG key

rmakey: RMA key

rmakey: RMA key userkey: User key

address Specifying the start address when the user key is specified. <type>

Notes: 1. The name of the file for programming and the date and time of its creation are specified as fname and ftime at the time of saving when the command is executed with the add option.

2. If the amount of data in the file from the target address for downloading overlaps earlier data, the later data to have been downloaded become valid.

fname = "filename":

Designates the file name of the program file that is downloaded. The maximum number of characters is 31. If 32 or more characters are specified, the first 31 characters are used.

ftime = "date and time":

Designates the creation date and time of the downloaded program file. The format is YYYY-MM-DD HH:MM.

YYYY: Year; MM: Month; DD: Date; HH: Hour; MM: Minute



Example of usage

Command	Status	Status LED	Message Display	Screen Output
lod	Display after execution of the command (before downloading)	BUSY	*** BUSY ***	Preparing storagePASS Now loading
	Display during downloading	BUSY	*** BUSY ***	
	Display after normal ending of the download	PASS	Returns to the display before executing the command.	PASS
	Display after error ending of the download	ERROR	Returns to the display before executing the command.	ERROR: <text></text>

Example of Communication Software Terminal Display

>lod

[When the MCU supports only the code flash area]

Address range: 0x00000000 to 0x00003FFF, CRC32: 0xC80EBAB6

PASS

>lod fname="sample.hex" ftime="2006-02-24 21:13"

[When the MCU also supports areas other than code flash]

Address range code: 0xFFF00000 to 0xFFFFFFFF, CRC32: 0xD253DA27 Address range data: 0x00100000 to 0x00107FF, CRC32: 0x0CA407F9 Address range boot: 0xFF7FC000 to 0xFF7FFFF, CRC32: 0xE39BE9B8

PASS

7.4.11 prm command

Displays the information concerning the parameter file and setting file that were downloaded to the FP6.

Input format

'prm'

Description of the function

Displays the information concerning the parameter file and setting file (parameter file name, parameter file checksum, setting file checksum, and setting file name) that were downloaded to all the programming areas of the FP6.

	Example of Communication Software Terminal Display					
>prm						
Area	File name	CRC	Туре			
*0	R5F571M	41F6142D	PR5			
	Test1	62189515	PRJ			
1	R5F571M	41F6142D	PR5			
	Test2	5AC4344E	PRJ			
2	78F1166	C8005840	PR5			
	{invalid}		PRJ			
3	{invalid}		PR5			
	{invalid}		PRJ			
4	{invalid}		PR5			
	{invalid}		PRJ			
5	{invalid}		PR5			
	{invalid}		PRJ			
6	{invalid}		PR5			
	{invalid}		PRJ			
7	{invalid}		PR5			
	{invalid}		PRJ			

7.4.12 progarea command

Confirms, changes and deletes data from active programming areas.

Input format

'progarea' ('clear' '0' | '1' | '2' | '3' | '4' | '5' | '6' | '7') | ('0' | '1' | '2' | '3' | '4' | '5' | '6' | '7')

Description of the function

The active programming area can be changed by designating a numerical option. Also, by designating the clear option, the data in the active programming area (parameter file, setting file, and program file) can be deleted. If there are no options, then the current active programming area is displayed.

clear: Clears the data in the active programming area (parameter file, setting file, and program file).

0: Changes the active programming area to 0.

1: Changes the active programming area to 1.

2: Changes the active programming area to 2.

3: Changes the active programming area to 3.

4: Changes the active programming area to 4.

5: Changes the active programming area to 5.

6: Changes the active programming area to 6.

7: Changes the active programming area to 7.

Example of usage

Example of Communication Software Terminal Display

>progarea

Active Program Area: 0

Max. code area size: 16 MByte Max. data area size: 4 MByte

Max. user boot area size: 4 Mbyte

>progarea clear 1

> progarea 0

Active Program Area: 0



7.4.13 res command

Resets FP6.

Input format

'res'

Description of the function

Resets and restarts the FP6 main unit.

Example of usage

Example of Communication Software Terminal Display

>res

Starting FP6...

Firmware Version Vx.xx.xx

Board H/W Vx

Serial No.:xxxxxxxxxx Standard mode unsecured

7.4.14 selftest command

Executes a diagnostic test.

Input format

'selftest'

Description of the function

Executes a self-test to diagnose hardware faults.

Example of usage

Example of Communication Software Terminal Display

>selftest

**** CAUTION ****

Remove any plugs from Target- and Remote-Connector before starting.

Any hardware attached to those connectors may be damaged by this test!

***** CAUTION ******

Target- and Remote-connector unplugged ? If yes, press 's' to start the test. Otherwise, press 'n' to cancel the test: s

FPGA Test: PASS

Power Supply Test: PASS

Target- and Remote-Interface Test: PASS

Selftest PASSED.

7.4.15 serno command

Sets the unique code for embedding in the program file.

Input format

'serno' <start address> <pattern>

Description of the function

Sets the unique code for embedding in the program file. This command becomes available when the unique code function is enabled by the FP6 Manager setting. A target command (such as ep, prg, and vrf) is executed with the specified address replaced by unique code in the program file. The setting of the unique code is cleared on completion of the target command.

Note: When filling with 0xFF is disabled and the area of data flash memory in the program file specified in the serno command is blank, embedding of the unique code in that area does not proceed.

start address: Specifies the start address in hexadecimal.

pattern: Specifies the unique code in hexadecimal notation. A maximum of 64 bytes can be specified.

Example of Communication Software Terminal Display						
>serno 8000 00010203						
ОК						

7.4.16 set_auth command

Changes the authentication ID code to a desired value.

Input format

'set_auth_id' <type> <id>

Description of the function

When the authentication ID code is changed from the value in the settings file (ESF), this command is used to specify the type of authentication ID code for which the value is to be set as the desired ID code.

The settings for ID code which have been made with this command are maintained unless the following operations proceed (the following operations disable the set ID).

- Executing the downprm or downset command
- Changing the programming area (executing [START] with the progarea command, the operation of the FP6 main unit, or in bank mode)
- Issuing a reset (with the res, version_up, or hwtest command)
- Turning off the power of the FP6 main unit

If the upset command is executed during retention of the settings of the ID code, the settings file is uploaded with the set ID.

<type>: Type of the authentication ID code

- id: Serial programming ID
- · cfpw: Password for code flash memory
- · dfpw: Password for data flash memory
- oid: OCD ID
- cid: Customer ID
- · dfid: Data flash ID
- · ctid: Customer Test ID
- · sifid: RHSIF ID

<id>

Specifies the authentication ID value.

Example of usage

Example of Communication Software Terminal Display

 $\verb|set_auth_id| | \verb|seri|| | 00112233445566778899 \verb|AABBCCDDEEFF||$



7.4.17 sound command

Sets the buzzer.

Input format

'sound' ('off' | 'on')

Description of the function

Sets the buzzer. "Enabled" or "disabled" is optionally designated. If no option is designated, the current setting is displayed.

off: Disables the buzzer.

on: Enables the buzzer.

Example of Communication Software Terminal Display				
>sound				
Sound is off				
>sound off				
Sound is off				
>sound on				
Sound is on				

7.4.18 speed_mode command

Adjusts the waiting time and timeout time for use in communications with the target device.

Input format

'wait_mode' ('middle' | 'low' | 'high')

Description of the function

With devices of the V850 (except for V850E2) and 78K (except for 78K0S) family as the targets, this command adjusts the waiting time and timeout time in communications with the target device according to the following options. When no option is specified, the command is output with the currently specified mode.

middle: Normal mode (default)

Communications with the target device continue with the default timing.

low: Safe mode

A wait is inserted in communications processing to improve the stability of the connection. An unstable connection may become stable in the safe mode; however, processing times will be delayed.

high: Fast mode

This mode accelerates communications processing relative to the default value. While fast mode accelerates processing in many cases, it may cause the connection to fail. This depends on the target device and the environment.

Example of usage

Example of Communication Software Terminal Display

>speed_mode

speed mode is middle.



7.4.19 srec command

Uploads the program file in Motorola S format.

Input format

'srec' (<start1><length1>(<start2><length2>(<start3><length3>(<start4><length4>))))

Description of the function

If a program file has been downloaded to an active programming area, executing this command will upload the program file in Motorola S format. If this command is executed without any options, the upload will be executed with the address size used during downloading. If a program has not been downloaded, "Invalid argument" will be displayed.

start address: The start address is designated as a hexadecimal number. (A maximum of four ranges can be specified.)

length: The number of bytes is designated as a hexadecimal number. (A maximum of four ranges can be specified.)

Example of usage

Example of Communication Software Terminal Display

> srec 0 3fff

Press any to start/continue output.

S0030000FC

:

S5030000FC

S70500000000FA

7.4.20 trc command

Displays the communication information between the FP6 and target device.

Input format

'trc'

Description of the function

Displays the communication information between the FP6 and target device. Up to 4096 lines can be stored.

If the communication information exceeds 4096 lines, old data is deleted.

Example of Communication Software Terminal Display							
>trc							
Debug Output							
Time us	Send	Rec.					
0008675924	17						
0008678930		02					
Total number of transmitted bytes : 266282							
Total number of received bytes : 006212							
	Time us 0008675924 0008678930 umber of tran	Time us Send 0008675924 17 0008678930 — umber of transmitte	utput Time us Send Rec. 0008675924 17 0008678930 02 umber of transmitted bytes				

7.4.21 upprm command

Uploads the parameter file.

Input format

'upprm'

Description of the function

If the parameter file has been downloaded to an active programming area, executing this command will upload the parameter file.

Example of usage

Example of Communication Software Terminal Display

>upprm

Press any key to start/continue output.

[FlashProParameterFile]

.

[CHECKSUM]

SUM=BA9F0491

[E0F]

7.4.22 upset command

Uploads the setting file.

Input format

'upset'

Description of the function

If the setting file has been downloaded to an active programming area, executing this command will upload the setting file.

Example of usage

Example of Communication Software Terminal Display

>upset

Press any key to start/continue output.

[FlashproCustomerSettingFile]

:

[CHECKSUM]

SUM=F7D4A9E7

[EOF]



7.4.23 ver command

Displays the FP6 version.

Input format

'ver'

Description of the function

Displays the FP6 version (firmware version, board hardware version, and serial number).

Example of usage

Example of Communication Software Terminal Display

>ver

Firmware Version Vx. xx. xx

Board H/W Vx

Serial No.:xxxxxxxxxx Standard mode unsecured

7.5 Description of FP6 Device Commands

7.5.1 bln command

Executes the blank check.

Input format

'bln'

Description of the function

Executes blank checking for the flash memory of the target device.

The area specified in operation mode is checked.

Example of usage

Example of Communication Software Terminal Display

>bIn

[When the area is blank]

Blank check Block 000:

Blank check Block 001:

Blank check Block 002:

Blank check Block 003:

PASS

Blank check operation finished.

>bIn

[When the area is not blank] Blank check Block 000: ERROR

ERROR(E051): Not Blank.

Blank check operation finished.

7.5.2 clr command

Executes "Configuration clear".

Input format

'clr'

Description of the function

Executes "Configuration clear".

Remark: For details of the "Configuration clear", refer to the user's manual of the MCU.

Example of usage

Example of Communication Software Terminal Display

>clr

Configuration clear :

PASS

Configuration clear operation finished.

7.5.3 con command

Executes the processes from "transition to the flash memory programming mode" to "signature verification".

Input format

'con'

Description of the function

Executes the processes from "transition to the flash memory programming mode" to "signature verification". In order to use this command, "manual" (off) must be set with the autocon command beforehand.

7.5.4 dcon command

Executes the process to end the flash memory programming mode.

Input format

'dcon'

Description of the function

Executes the process to end the flash memory programming mode. In order to use this command, "manual" (off) must be set with the autocon command beforehand.



7.5.5 dlm command

Refers to the DLM state and causes a transition of the state.

Input format

'dlm' (<type>) ('unique' <authentication code>)

Description of the function

Refers to the DLM state of the target device and causes a transition of the state.

dlm <type>: Specifies the DLM state.

SSD, NSECSD, DPL, LCK_DBG, LCK_BOOT, or RMA_REQ

unique Specifies this parameter when unique ID authentication is to proceed.

<authentication>:

Example of usage

Example of Communication Software Terminal Display

>dIm

Request DLM DLM state: SSD

PASS

DLM operation finished.

>dlm SSD Transit DLM DLM state: SSD

PASS

DLM operation finished.

7.5.6 ep command

Executes the [Start] command.

Input format

'ep' or 'epv'

Description of the function

Executes the [Start] command.

Command	Status	Status LED	Message Display	FP6 Response Message	
ер	Display while executing the command	BUSY	Display contents of the ers and prg commands	See the descriptions of the ers and prg commands.	
	Display after executing the command [When completed normally]	PASS	Returns to the display before executing the command.	PASS Erase, Program operation finished. or PASS EPV operation finished.	
	Display after executing the command [When terminated abnormally]	ERROR	ERROR: xxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	ERROR(Exxx): <text> Erase, Program operation finished.</text>	

Example of Communication Software Terminal Display				
>ep				
Blank check Skipped.				
Erase Chip:				
PASS				
Program Chip:				
10%				
20%				
30%				
40%				
50%				
60%				
70%				
80%				
90%				
100%				
PASS				
Erase, Program operation finished.				

7.5.7 ers command

Executes the Erase command.

Input format

'ers'

Description of the function

Erases the target flash memory.

The range specified in operation mode is to be erased.

If this command is executed with the "Erase Chip" specified, initialization of flash options is also executed.

Example of usage

Example of Communication Software Terminal Display

>ers

Blank check Skipped.

Erase Chip:

PASS

Erase operation finished.

7.5.8 ers_chip command

Initializes an MCU of the RA family.

Input format

'ers_chip'

Description of the function

Initializes an MCU of the RA family.

Example of usage

Example of Communication Software Terminal Display

>ers_chip

Erase Chip

PASS

Erase Chip operation finished.



7.5.9 gdi command

Gets the information of blank check and flash option.

Input format

'gdi'

Description of the function

Obtains the information of blank check and flash options.

Example of usage

Example of Communication Software Terminal Display

>gdi

Blank check

UB: FF

Trusted Memory:xx TMINF: xxxxxxxx

TM address: xxxxxxxx xxxxxxx

PASS

Get Device Info operation finished.

_	E 4	1	اء ۽ ء			
1.	5.1	ıv	aed	COII	ıma	пu

Gets the information of endian.

Input format

'ged'

Description of the function

Gets the information of endian.

Example of usage

Example of Communication Software Terminal Display

>ged

Get Endianness

Little Endian

PASS

Get Endianness operation finished.

7.5.11 gid command

Gets the ID code.

Input format

'gid'

Description of the function

Gets the ID code.

Example of usage

Example of Communication Software Terminal Display

>gid

PASS

OCD-ID operation finished.



7.5.12 glb command

Gets the lock bit.

Input format

'glb'

Description of the function

Gets the lock bit.

Example of usage

Example of Communication Software Terminal Display

>g1b

LockBits :

UB: FF PASS

LockBits operation finished.

7.5.13 gob command

Gets the information of option bytes.

Input format

'gob'

Description of the function

Obtains the information of option bytes.

Example of usage

Example of Communication Software Terminal Display

>gob

Extended Option Bytes : FFFFFFF

PASS

Option Bytes operation finished.



7.5.14 gof command

Gets the information of OFS.

Input format

'gof'

Description of the function

Gets the information of OFS.

Remark: For details of OFS, refer to the user's manual of the MCU.

Example of usage

Example of Communication Software Terminal Display

>gof

Get OFS

OFS: FFFFFFF FFFFFFF

PASS

Get OFS operation finished.

7.5.15 gos command

Gets the information of flash option.

Input format

'gos'

Description of the function

Reads and outputs the flash option information of the target device. When the read-disable setting is effective, unreadable data are not output.

Example of usage

Example of Communication Software Terminal Display

>gos

OFS: FFFFFFF FFFFFFF

PASS

Get Option Setting operation finished.



7.5.16 got command

Gets the information of OTP.

Input format

'got'

Description of the function

Gets the information of OTP.

Remark: For details of OTP, refer to the user's manual of the MCU.

Example of usage

Example of Communication Software Terminal Display

>got OTP flags :

PASS

OTP operation finished.

7.5.17 gsc command

Gets the information of security.

Input format

'gsc'

Description of the function

Gets the security information set on the MCU.

Example of usage

Example of Communication Software Terminal Display

>gsc

Command protection: FF

PASS

Security operation finished.



7.5.18 gtm command

Gets the information of Trusted Memory.

Input format

'gtm'

Description of the function

Gets the information of Trusted Memory.

Remark: For details of Trusted Memory, refer to the user's manual of the MCU.

Example of usage

Example of Communication Software Terminal Display

>gtm

Trusted Memory: FF TMINF: FFFFFFF

TM address: 00120060 00120064

PASS

Get Trusted Memory operation finished.

7.5.19 idc command

Executes the ID code setting.

Input format

'idc'

Description of the function

Executes the ID code setting.

Caution: Do not issue this command if you are using HCUHEX files.

Example of usage

Example of Communication Software Terminal Display

>idc

Set ID code

PASS

ID code operation finished.



7.5.20 opb command

Sets the option bytes.

Input format

'opb'

Description of the function

Sets the option bytes.

Example of usage

Example of Communication Software Terminal Display

>opb

Set Option Bytes

PASS

Option Bytes operation finished.

7.5.21 otp command

Executes the OTP setting.

Input format

'otp'

Description of the function

Executes the OTP setting.

Remark: For details of OTP, refer to the user's manual of the MCU. Caution: Do not issue this command if you are using HCUHEX files.

Example of usage

Example of Communication Software Terminal Display

>otp

Set OTP protection

PASS

OTP operation finished.



		-				
7.5.	.22	pfo	CO	mm	an	d

Sets the flash options collectively.

Input format

'pfo'

Description of the function

Sets the flash options collectively.

Example of usage

Example of Communication Software Terminal Display

>pfo

Set Flash Option

PASS

Program Flash Option operation finished.

7.5.23 prg command

Executes programming.

Input format

'prg'

Description of the function

Executes programming.

When filling with 0xFF is disabled, programming is performed to the locations where program file data exist. In this case, data is programmed with the minimum alignment unit of the MCU.

Caution: Do not issue this command if you are using HCUHEX files.

Example of usage

Example of Communication Software Terminal Display		
>prg		
Program Chip:		
10%		
20%		
100%		
PASS		
Program operation finished.		

7.5.24 read command

Reads data of the flash memory in the target device.

Input format

'read' ('skipblank') ('hex' | 'srec') ('all' | <start_address> <end_address>)

Description of the function

Reads data of the flash memory in the target device and outputs the data in the specified format.

If this command is executed without options, data in the range set in operation mode is read.

Caution: Do not issue this command if you are using HCUHEX files.

No option specified: Outputs data in the hexadecimal format.

skipblank: Reads data other than that in blank areas.

hex: Reads data with the Intel HEX format.

srec: Reads data with the Motorola HEX format.

all: Reads all readable areas in the target device.

start address: Designates the start address (in block units) with a hexadecimal number.

end_address: Designates the end address (in block units) with a hexadecimal number.

Example of usage

Example of Communication Software Terminal Display

>read FE000000 FE0000FF

Read FE000000 to FE0000FF:

Press any key to start/continue output.

FE000000: FB F9 F1 F9 F1 31 37 B1 E9 FF F9 FF 20 74 F5 F5 FE000010: F9 F9 FB ED FF B5 F7 F7 69 B9 FB F9 71 A9 36 75

:

FE0000F0: 3D FF BF 9F 7D 7F 6F 7D 77 1F DF FF FF FF FF FF

PASS

Read operation finished.



7.5.25 rsc command

Executes the Security Release command.

Input format

'rsc'

Description of the function

Executes the Security Release command.

Remark: For details of the Security Release command, refer to the user's manual of the MCU.

Example of usage

Example of Communication Software Terminal Display

>rsc

Release security

PASS

Release security operation finished.

7.5.26 scf command

Sets security information.

Input format

'scf'

Description of the function

Sets security information to the MCU.

Caution: Do not issue this command if you are using HCUHEX files.

Example of usage

Example of Communication Software Terminal Display

>scf

Set security Flags

PASS

Security operation finished.



7.5.27 sed command

Executes the endian setting.

Input format

'sed'

Description of the function

Executes the endian setting.

Example of usage

Example of Communication Software Terminal Display

>sed

Set Endianness

PASS

Set Endianness operation finished.

7.5.28 sid command

Sets the ID code and enables ID authentication in the serial programming mode.

Input format

'sid' (<ID Code>)

Description of the function

Sets the ID code and enables ID authentication in the serial programming mode.

ID Code: Specifies the ID code to be set by a hexadecimal number.

No option specified: Value of setting file downloaded is set.

Set the ID code with a size supported by the MCU.

If ID code with an unavailable size is specified, an error occurs.

Example of usage

Example of Communication Software Terminal Display

>sid 0123456789ABCDEF

Set Serial Programming ID

PASS

Set Progr. ID operation finished.



7.5.29 sig command

Executes the [Signature read] command.

Input format

'sig'

Description of the function

Executes the [Signature read] command.

Example of usage

Example of Communication Software Terminal Display

>sig

Device name: D70FXXXX
Device data: 10 DF 40
Device Version: 2.00
Firmware Version: 3.04

PASS

Signature operation finished.

7.5.30 slb command

Sets the Lock bit information.

Input format

'slb'

Description of the function

Sets the Lock bits on the MCU.

Example of usage

Example of Communication Software Terminal Display

>s lb

Set LockBits

PASS

 $LockBits\ operation\ finished.$



7.5.31 spd command

Disables the serial programming.

Input format

'spd'

Description of the function

Disables the serial programming for the MCU.

Example of usage

Example of Communication Software Terminal Display

>spd

Set Serial Programming Disable

PASS

Set SerProgDis operation finished.

7.5.32 stm command

Sets the Trusted Memory.

Input format

'stm'

Description of the function

Enables the Trusted Memory setting.

Remark: For details of the Trusted Memory, refer to the user's manual of the MCU.

Example of usage

Example of Communication Software Terminal Display

>stm

Set Trusted Memory

PASS

Set Trusted Memory operation finished.



7.5.33 sum command

Executes the Checksum command.

Input format

'sum'

Description of the function

Executes the Checksum command and gets checksum values in the MCU.

Example of usage

Example of Communication Software Terminal Display

>sum

Checksum: 0x1234

PASS

Checksum operation finished.

7.5.34 vrf command

Executes the Verify command.

Input format

'vrf'

Description of the function

Executes the Verify command.

Example of usage

Example of Communication Software Terminal Display

>vrf

Verify Chip:

10%

20%

100%

PASS

Verify operation finished.



8. Encryption Utility Program

RPE.exe, which is bundled with this product, can be used to encrypt or decrypt program files.

Remark: RPE.exe is stored in the same location as that for FP6.exe in the folder where the FP6 Terminal has been installed.

8.1 Exit Code

When the operation was successful, exit code 0 is returned.

Otherwise, 1 is returned.

8.2 Command-line Syntax

The command-line syntax is as follows:

RPE <file> /password <password> [options...]

8.3 Start Options

The following lists start options for the PG-FP6.

Table 8.1 Start Options

Option	Description
file	Specifies the file to be input (this specification is mandatory).
	The file can be specified as a relative path from the working directory.
	Files to be encrypted: Intel Hex, S-Record, HCUHEX, and RPI
	Files to be decrypted: RPE
password	Specifies the password for use in encrypting or decrypting the file (this specification is mandatory).
	If the password includes symbols, enclose each in double-quotation marks (").
decrypt	Decrypts an encrypted file (RPE).
	If this option is not specified, the file is encrypted.
output	Specifies the destination for output of a file.
	If this option is not specified, the directory holding the input files is used.
	The file can be specified as a relative path from the working directory.
nooverwrite	Prohibits overwriting of output files.
?	Displays help information on the options.

Caution: Pathnames that include spaces must be enclosed in double-quotation marks (").

Remark: Enter a password made up of alphanumeric characters and symbols (up to 64 characters). The usable symbols are as follows.

Example:

- > RPE "out.hex" /password "0123456789"
- > RPE "out.hex" /password "0123456789" /output "out.rpe"
- > RPE "out.rpe" /decrypt /password "0123456789" /output "D:\outputdir\"



9. Renesas Flash Programmer Utility Program

rfp-util.exe, which is bundled with this product, can be used to run the following processing.

Remark: rfp-util.exe is stored in the same location as FP6.exe; that is, in the folder where the PG-FP6 has been installed.

- Encryption with the use of user factory programming keys (UFPKs) as DLM keys and user keys
- · Generation of random UFPKs and initialization vectors (IVs)
- Output of UFPK files for the Renesas Key Wrapping Service
- · Generation of Renesas key files
- Generation of RMA authentication codes with unique IDs

9.1 Exit Code

When the operation was successful, exit code 0 is returned.

Otherwise, 1 is returned.

9.2 Command-line Syntax

The command-line syntax is as follows:

rfp-util [command] [options...]

The following table gives descriptions of each item.

Table 9.1 Command-line Syntax

Item	Description
rfp-util.exe	A name of a file to be executed.
command	Command names prefixed by a slash (/) or a hyphen (-).
	command: genufpk, genkey, or calcresponse
options	Option names prefixed by a slash (/) or a hyphen (-).
	Specify parameters as required.
	Options and parameters are not case sensitive.
	Absolute or relative paths can be used for the name of the file.
?	Displays help information on the options.

Caution: Pathnames that include spaces must be enclosed in double-quotation marks (").

9.3 List of Commands

The following table gives descriptions of each command.

Table 9.2 List of Commands

Command	Description
genufpk	Generates a UFPK file.
	When generation was successful, the generated UFPK is displayed in the console.
genkey	Generates a Renesas key file.
	When generation was successful, a wrapped UFPK (W-UFPK), IV, and encrypted key (including a message authentication code, MAC) are displayed in the console.
calcresponse	Calculates a response value for use in challenge-and-response authentication and outputs it to the console.

9.4 Start Options

The following lists start options for the key encryption utility program.

Remark: A hexadecimal data or binary file can be specified for the parameters indicated as Hex data. To specify a file, use the path to the file with "file=" as a prefix.

Table 9.3 Common Options

Option	Parameter	Description	
output	File path	Specifies the name of a file to be output.	
		If this option is omitted, the execution result is output to the console.	
nooverwrite	None	If an output file already exists, an error will occur.	

Table 9.4 genufpk Command Option

Option	Parameter	Description	
ufpk	Hex data	x data Specifies the output of 32 bytes of binary data.	
		If this option is omitted, a random value is used for ufpk.	

Table 9.5 genkey Command Options

Option	Parameter	Description
iv	Hex data	Specifies an IV for use in encryption. The data size is 16 bytes.
		If this option is omitted, a random value is used for IV.
ufpk	File path	Specifies a UFPK file used in encryption.
wufpk	File path	Specifies a W-UFPK file obtained from the Renesas Key Wrapping Service.
key	Hex data	When the userkey option is not specified
		Specifies the DLM key data. The data size is 16 bytes.
		When the userkey option is specified
		Specifies the user key data. For the key data format and data size, refer to the user's manual of the TSIP.
		Note that this tool does not check the user key size.
userkey	XX	Generates a user key. Specify the type of user key as a one-byte hexadecimal parameter. For the values to be entered, refer to the user's manual of the TSIP.
		If this option is omitted, a DLM key is generated.

Table 9.6 calcresponse Command Options

Option	Parameter	Description
challenge	Hex data	Specifies a challenge value (the unique ID of the device is usually specified).
		The data size is 16 bytes.
key	Hex data	Specifies the DLM key data. The data size is 16 bytes.

Example:

(genufpk)

> rfp-util /genufpk /output "D:\example\ufpk.key"

(genkey)

> rfp-util /genkey /ufpk "D:\example\ufpk.key" /wufpk "D:\example\ufpk_enc.key" /key "000102030405060708090A0B0C0D0E0F" /output "D:\example\abc.rkey"

(calcresponse)

> rfp-util /calcresponse /challenge "ABCDEFGHIJKLMNOPQRSTUVWXYZ012345" /key "000102030405060708090A0B0C0D0E0F"

10. Connectors and Cables

10.1 Power-Supply Connector

The power-supply connector is laid out on the host interface side of the FP6.

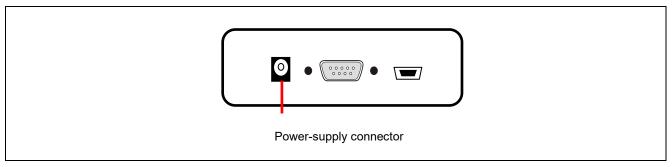


Figure 10.1 Power-Supply Connector

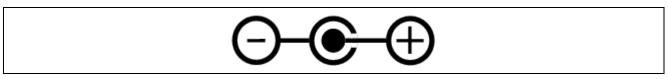


Figure 10.2 Pin Assignments of the Power-Supply Connector

Note: Do not connect a power adapter other than the one for the PG-FP6 to the power-supply connecter.

The following is the specification of the power-supply adapter.

Output: 5 V/2 A

Connector model No.: HEC0470-01-0630

10.2 **Serial Connector**

The serial connector (9-pin D-sub male connector) is laid out on the host interface side of the FP6.

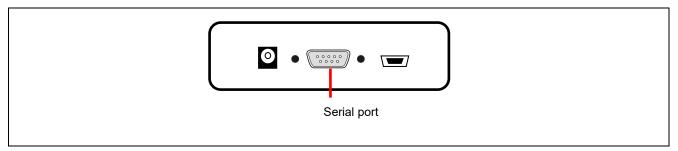


Figure 10.3 9-Pin D-Sub Serial Connector

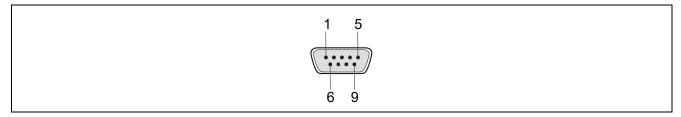


Figure 10.4 Pin Assignments of the Serial Connector

Table 10.1 List of Commands

Serial Connector	Signal Name
1	NC
2	RxD
3	TxD
4	NC
5	VSS
6	NC
7	RTS
8	CTS
9	NC

Note: Part number of the serial connector (9-pin D-sub male connector): DELC-J9PAF-20L9E (manufactured by Japan Aviation Electronics Industry, Limited)

10.2.1 Serial cable connected to the 9-pin D-sub serial connector

A serial cross cable is additionally required. The connectors on both sides are 9-pin D-sub female connectors. The following shows the connection.

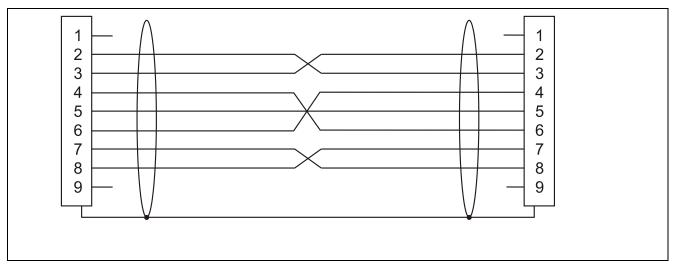


Figure 10.5 Connection of the Serial Cable

10.3 USB Connector

The mini-B type USB connector is laid out on the host interface side of the FP6.

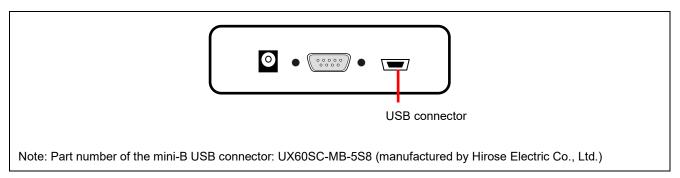


Figure 10.6 USB Connector (Host Interface Side of the FP6)

10.3.1 USB cable

The USB cable is approximately two meters long. The cable is equipped with a USB mini-B type connector and USB A type connector.

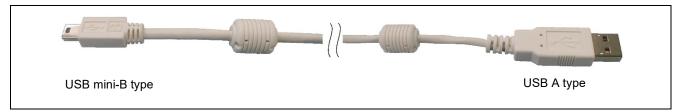


Figure 10.7 Appearance of the USB Cable

10.4 Target Connector

The target connector is laid out on the right side of the FP6.

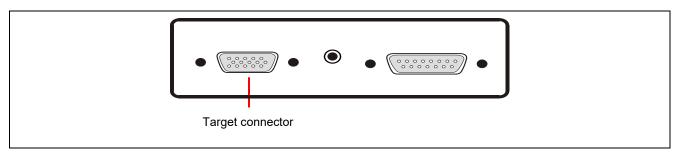
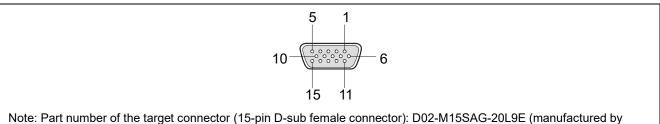


Figure 10.8 Target Connector (Target Connector Side of the FP6)



Japan Aviation Electronics Industry, Limited)

Figure 10.9 Pin Assignments of the Target Connector (15-Pin D-Sub Female Connector)

Table 10.2 Pin Configuration of the Target Connector

FP6 D-Sub 15	FP6 Signal Name
1	SO/TxD1/IO3
2	SI/RxD
3	SCK/IO4
4	RESET
5	NC*
6	FLMD1
7	TxD2/HS
8	VCC
9	VCC
10	IO1
11	NC*
12	FLMD0/IO0
13	102
14	CLK/IO5
15	GND

Note: Reserved pin. Leave this pin open.

Note: For the connection with the target device, refer to chapter 11, Examples of Connections with Microcontrollers.

10.4.1 Target cable (14-pin type)

The target cable (14-pin type) is a standard shielded cable and is approximately 42 centimeters long. The target cable is equipped with a 15-pin D-sub male connector and a 14-pin 2.54-mm pitch multipurpose female connector.

Note: The following are the recommended connectors to be connected to the 14-pin 2.54-mm pitch multipurpose female connectors.

- 7614-6002 (straight angle type manufactured by 3M Japan Limited)
- 2514-6002 (straight angle type manufactured by 3M Limited)

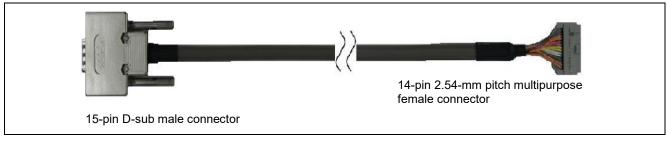


Figure 10.10 Appearance of the Target Cable (14-Pin Type)

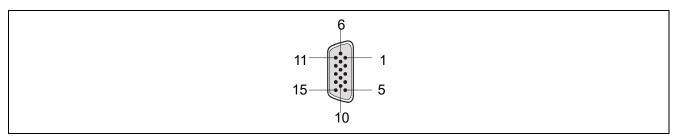


Figure 10.11 Pin Assignments of the 15-Pin D-Sub Male Connector of the Target Cable (14-Pin Type)

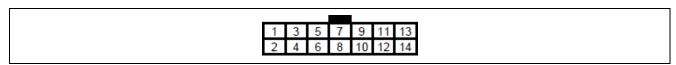


Figure 10.12 Appearance of the 14-Pin 2.54-mm Pitch Multipurpose Female Connector of the Target Cable (14-Pin Type) (View from the Socket Side)

Table 10.3 Pin Configuration of the Target Connector (14-Pin Type)

Signal Name (PG-FP6)	15-Pin D-Sub Male Connector	14-Pin 2.54-mm Pitch Multipurpose Female Connector
SCK/IO4	3	1
GND	15	2
CLK/IO5	14	3
FLMD0/IO0	12	4
SI/RxD	2	5
IO1	10	6
SO/TxD1/IO3	1	7
VCC	8	8
FLMD1	6	9
IO2	13	10
TxD2/HS	7	11
GND	15	12
RESET	4	13
Not used *	_	14

Note: Reserved pin. Leave this pin open.

Left open in the target cable. If you use the same 14-pin connector for debugging, please also refer to the user's manual of the emulator.

10.4.2 14-pin to 16-pin conversion adapter for the E1 emulator

When the 16-pin connector is used on the target system, use the 14-pin to 16-pin conversion adapter for the E1 emulator.

Caution: This conversion adapter is only usable with 78K and V850 target devices.

Remark: For the product information, refer to section 1.4, Optional Products.

10.4.3 20-pin conversion adapter for the PG-FP6

When the CoreSight 20-pin connector is used on the target system, use the 20-pin conversion adapter for the PG-FP6. When the 10-pin connector is used on the target system, use the 20-pin to 10-pin conversion cable to match it.

Remark: For the product information, refer to section 1.4, Optional Products.

Table 10.4 Pin Configuration of the Target Connector (20-Pin Type)

Signal Name (PG-FP6)	15-Pin D-Sub Male Connector	CoreSight 20-pin Connector	CoreSight 10-pin Connector	
Vcc	8,9	1	1	
FLMD1	6	2	2	
GND	15	3	3	
SCK/IO4	3	4	4	
GND	15	5	5	
SI/RxD	2	6	6	
Not used *1	_	7	7	
TxD2/HS	7	8	8	
Not used	_	9	9	
RESET	4	10	10	
Not used *1	_	11	_	
SO/TxD1/IO3	1	12	_	
Not used *1	_	13	_	
IO1	10	14	_	
GND	15	15	_	
CLK/IO5	14	16	_	
GND	15	17	_	
FLMD0/IO0	12	18	_	
GND	15	19	_	
102	13	20	_	

Note: Reserved pin. Leave this pin open.

10.5 **GND Connector**

The banana-jack GND connector is laid out on the target connector side of the FP6.

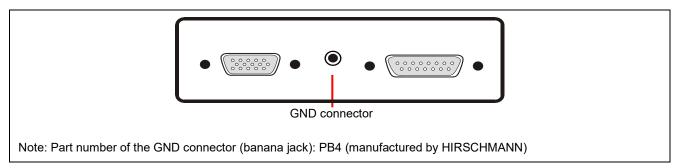


Figure 10.13 GND Connector (Target Connector Side of the FP6)

10.5.1 GND cable

The GND cable is approximately one meter long. The cable is equipped with a banana jack and a spade terminal.

Note: The FP6 and target system may be damaged if there are differences in potential between the grounds of the FP6 and of the target system. Use the GND cable to eliminate differences in potential before connecting the target cable.

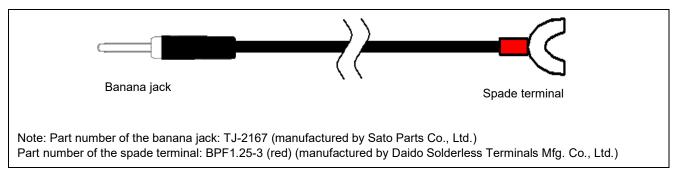


Figure 10.14 Appearance of the GND Cable

10.6 Remote Connector

The remote connector (a 15-pin D-sub female connector) is laid out on the target connector side of the FP6.

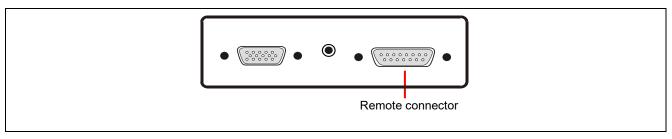
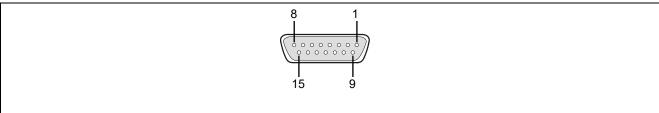


Figure 10.15 Remote Connector (Target Connector Side of the FP6)



Note: Part number of the remote connector (a 15-pin D-sub female connector): DALC-J15SAF-20L9E (manufactured by Japan Aviation Electronics Industry, Limited)

Figure 10.16 Pin Assignments of the Remote Connector (15-Pin D-Sub Female Connector)

The remote connector pins of the FP6 have the following functions. Table 10.5 shows the pin numbers on the remote connector of the FP6. Each input pin is pulled-up inside the FP6.

Table 10.5 Pin Functions of the Remote Interface

Pin Number	Input/ Output	Pin N	lame	Function	Active Level
1	Output	CONN		Indicates that the remote interface is connected. When the power of the FP6 is ON, the CONN is always valid.	High level
2	Output	BUSY		Outputs the status indicated by the status LED "BUSY".	High level
3	Output	PASS		Outputs the status indicated by the status LED "PASS".	High level
4	Output	ERROR		Outputs the status indicated by the status LED "ERROR".	High level
5	Input	Modes other than bank mode	CANCEL	Same as the function of the CANCEL button.	Low level
	Input	Bank mode	BANK0	Indicates the lowest 1 bit of the 3-bit programming area number.	Low level
6 Input Input	Input	Standard mode	ENTER	Same as the function of the ENTER button.	Low level
	Input	Bank mode	BANK1	Indicates the middle 1 bit of the 3-bit programming area number.	Low level
	Input	Standard mode	NEXT	Same as the function of the NEXT button.	Low level
	Input	Bank mode	BANK2	Indicates the highest 1 bit of the 3-bit programming area number.	Low level
8	Input	VRF		Executes verification.	Low level
9	Input	START		Inputs the "START" (Start command) signal.	Low level
10	Input	CLR		Clears the "PASS" and "ERROR" signals.	Low level
11 to 15		GND		GND pins	_

Note: Each input pin is pulled-up inside the FP6.

Table 10.6 Programming Areas and Banks

	BANK2	BANK1	BANK0
Programming area 0	0	0	0
Programming area 1	0	0	1
Programming area 2	0	1	0
Programming area 3	0	1	1
Programming area 4	1	0	0
Programming area 5	1	0	1
Programming area 6	1	1	0
Programming area 7	1	1	1

Remark: 0: Low level 1: High level

Note: Set BANK0, BANK1, and BANK2 to the low level in programming area 0. Set BANK0 and BANK1 to the high level and BANK2 to the low level in programming area 3.

11.Examples of Connections with Microcontrollers

The following shows examples of interface circuits. Refer to the recommended design for the connection of pins for the MCU. The pin names might differ depending on the target device. For details about the actual pin names, refer to the user's manual of each target device.

11.1 78K and V850 (UART communications)

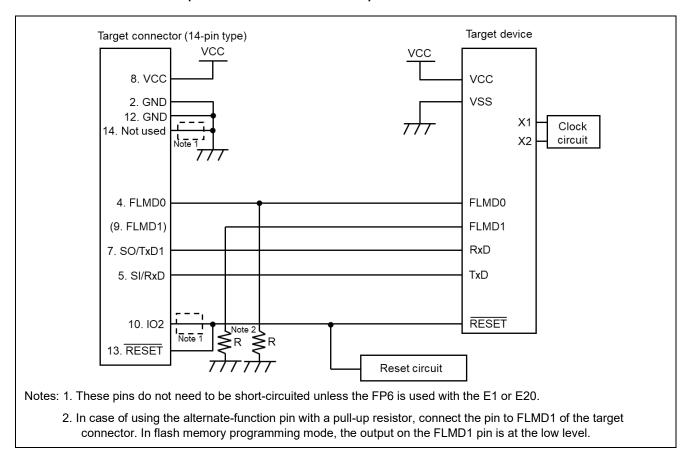


Figure 11.1 Example of a Circuit for 78K and V850 (UART – On-Chip Single-Power-Supply Flash Memory Microcontroller)

11.2 78K and V850 (CSI communications)

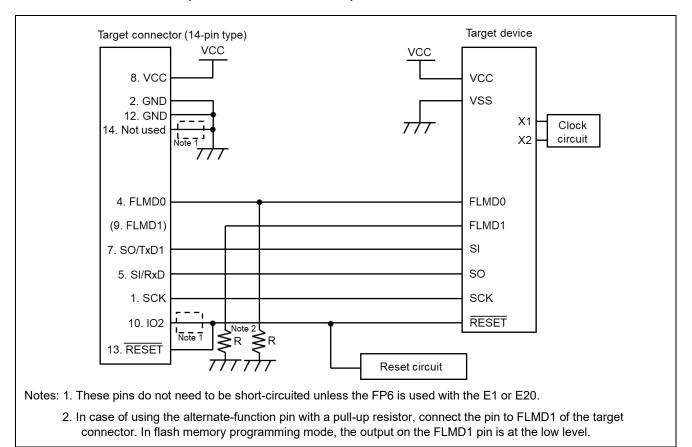


Figure 11.2 Example of a Circuit for 78K and V850 (CSI – On-Chip Single-Power-Supply Flash **Memory Microcontroller)**

11.3 78K and V850 (CSI-H/S communications)

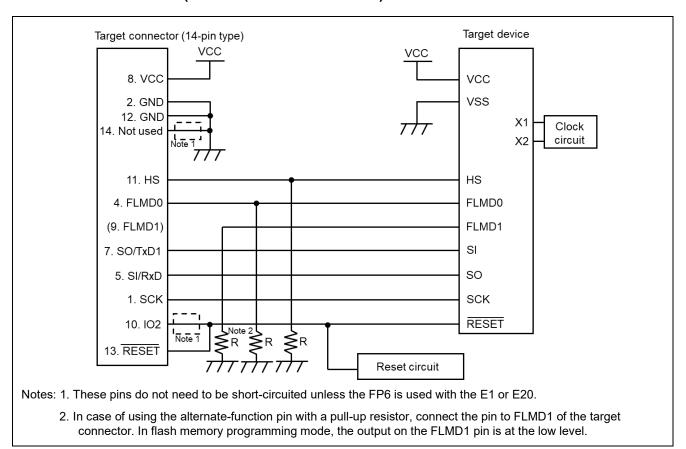


Figure 11.3 Example of a Circuit for 78K and V850 (CSI-H/S - On-Chip Single-Power-Supply Flash **Memory Microcontroller)**

11.4 78K0S (Single-wire UART communications)

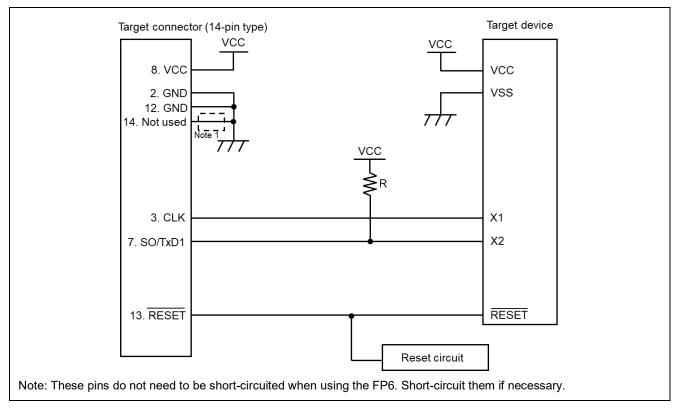


Figure 11.4 Example of a Circuit for 78K0S (Single-Wire UART)

11.5 78K0R (Single-wire UART communications)

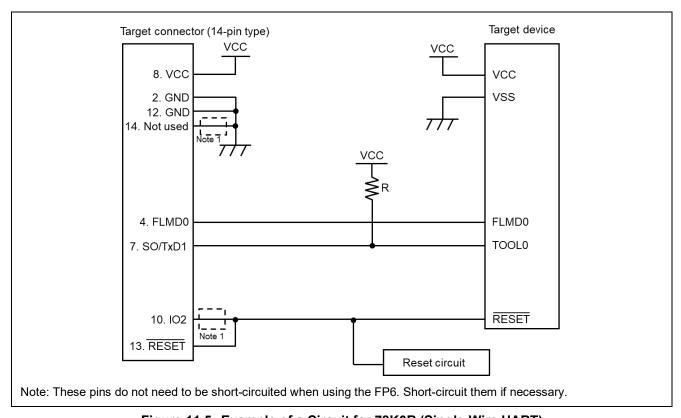


Figure 11.5 Example of a Circuit for 78K0R (Single-Wire UART)

11.6 78K0 (TOOLCx and TOOLDx communications)

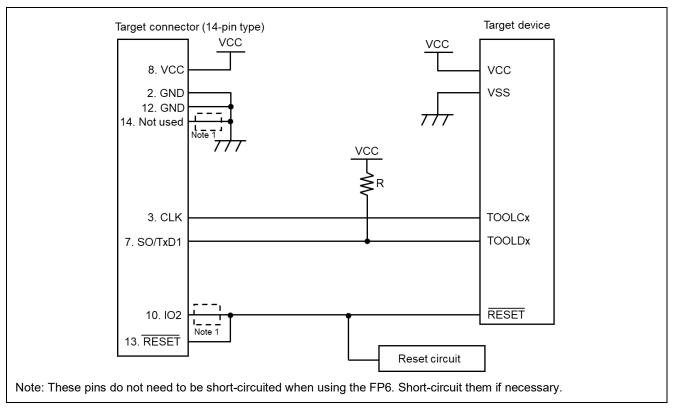


Figure 11.6 Example of a Circuit for 78K0 (TOOLCx and TOOLDx)

11.7 V850E2 (Single-wire UART communications)

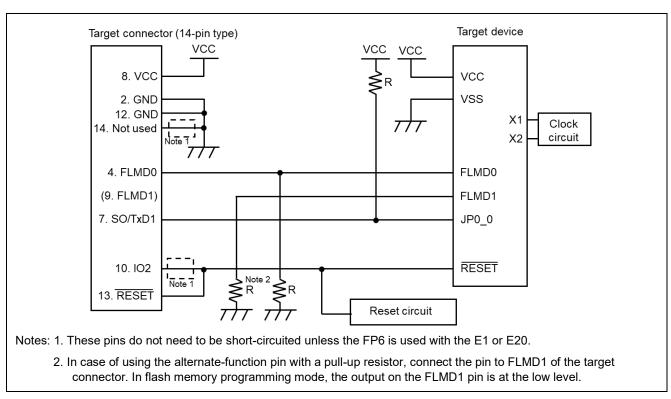


Figure 11.7 Example of a Circuit for V850E2 (Single-Wire UART)

11.8 V850E2 (CSI communications)

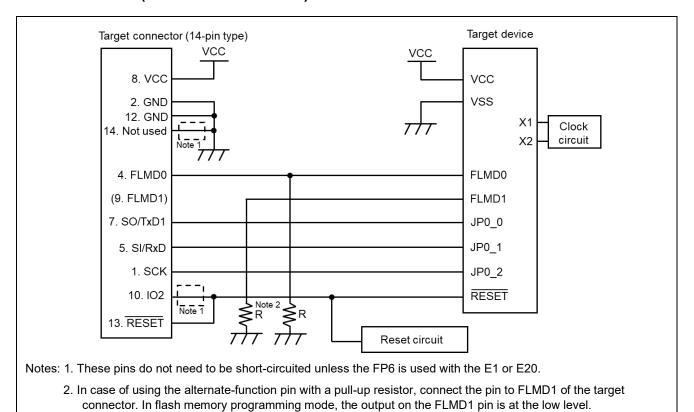


Figure 11.8 Example of a Circuit for V850E2 (CSI)

11.9 RL78 (Single-wire UART communications, VDD = EVDD)

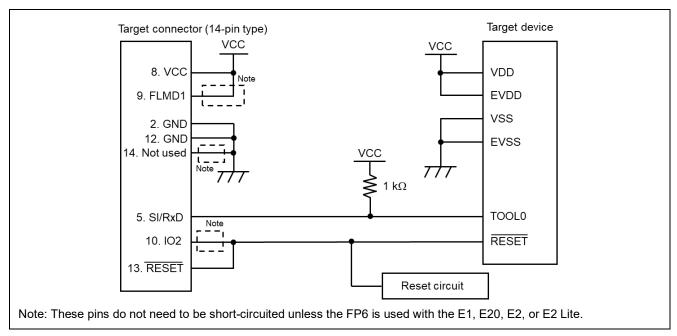


Figure 11.9 Example of a Circuit for RL78 Family (VDD = EVDD)

11.10 RL78 (Single-wire UART communications, VDD ≠ EVDD)

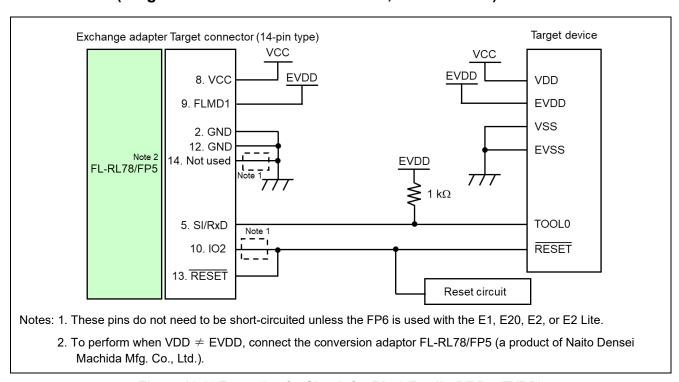
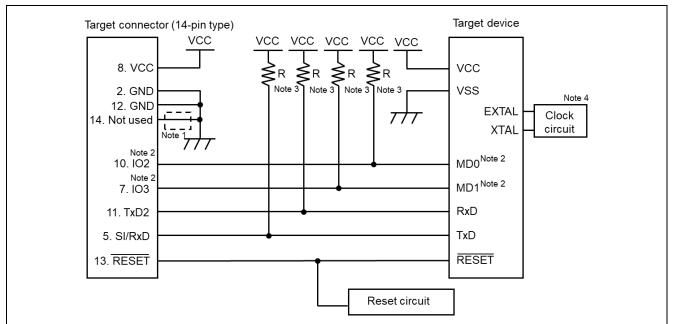


Figure 11.10 Example of a Circuit for RL78 Family (VDD ≠ EVDD)

11.11 RX and SuperH (SCI communications)



Notes: 1. These pins do not need to be short-circuited unless the FP6 is used with the E1, E20, E2, E2 Lite, or E8a.

- 2. Connect the mode setting pins of operating mode to any of the IO0 to IO5 pins. The signal settings for IO0 to IO5 pins can be set in the [Mode Pins Setting] dialog box on the [Connect Setting] tab in the [Setup] dialog box. Normally, use the initial settings in the [IO Signal Settings] area. It is compatible with examples of circuits in the E1/E20 Emulator Additional Document for User's Manual (RX User System Design).
- 3. The value of each resistor should be in the range from 4.7 K Ω to 10 K Ω .
- 4. The need for the clock circuit might differ depending on the target device. Refer to the user's manual of the target device.

Figure 11.11 Example of a Circuit for RX Family and SuperH Family (SCI) (Case of RX62T)

11.12 R8C

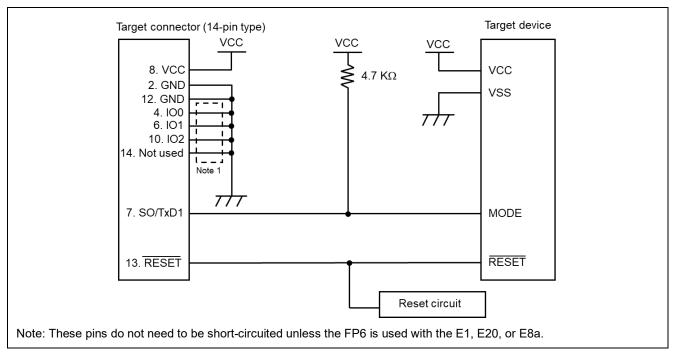


Figure 11.12 Example of a Circuit for R8C Family

11.13 RX100, RX200, RX65x, and RX66T (FINE communications)

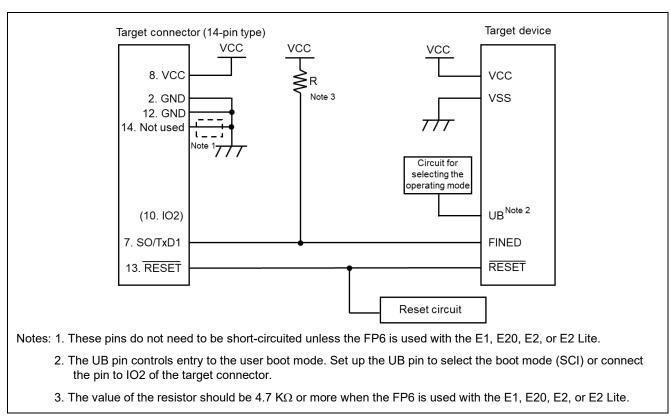
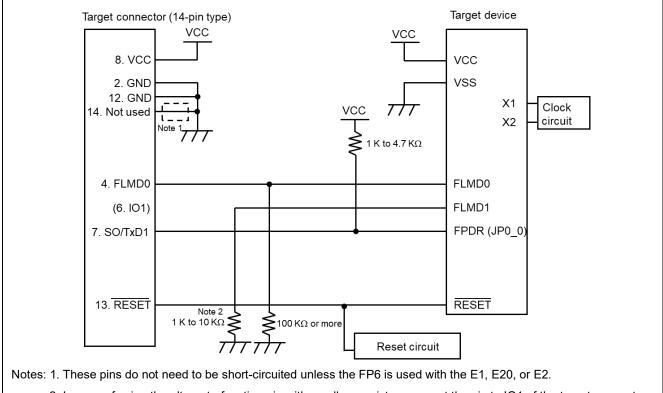


Figure 11.13 Example of a Circuit for RX100, RX200, RX65x, and RX66T (FINE)

11.14 RH850 type 1 (1-wire UART communications)



2. In case of using the alternate-function pin with a pull-up resistor, connect the pin to IO1 of the target connector. In serial programming mode, the output on the IO1 pin is at the low level.

Figure 11.14 Example of a Circuit for RH850 Family (1-Wire UART) (Case of RH850/F1x)

11.15 RH850 type 1 (2-wire UART or CSI communications)

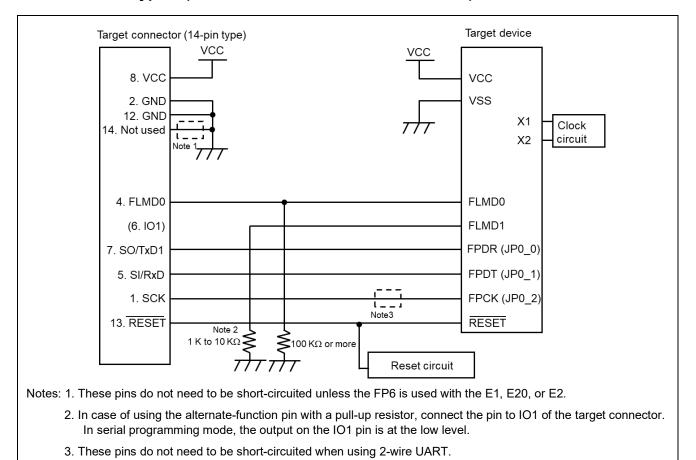


Figure 11.15 Example of a Circuit for RH850 Family (2-Wire UART or CSI) (Case of RH850/F1x)

11.16 RH850 type 2 (2-wire UART or CSI communications)

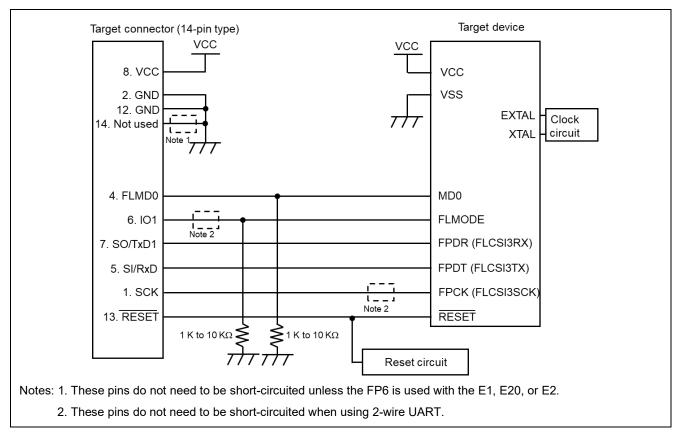


Figure 11.16 Example of a Circuit for RH850 Family (2-wire UART or CSI communications) (Case of RH850/E1x)

11.17 Renesas Synergy™ (UART communications)

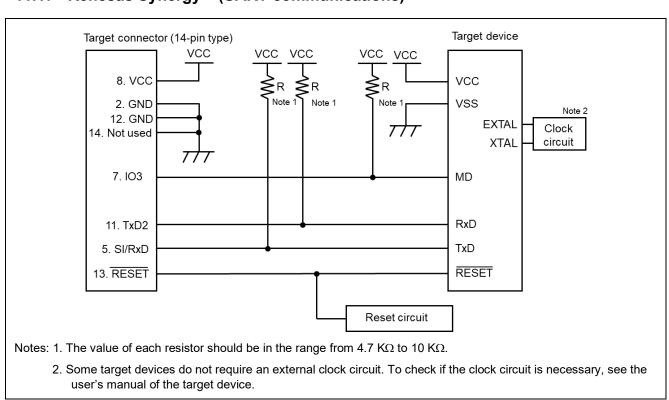


Figure 11.17 Example of a Circuit for an S7G2 (UART communications)

11.18 RE (UART communications)

The following shows the conversion of each signal when a 14-pin target cable and 20-pin conversion adapter are connected to the 15-pin D-sub connector of the PG-FP6.

Table 11.1 List of Signal Connections for RE Family

Signal Name (PG-FP6)	15-Pin D-Sub Male Connector	14-Pin 2.54-mm Pitch Multipurpose Female Connector	CoreSight 20-pin Connector	RE signal name
VCC	8, 9	8	1	VCC
GND	15	2, 12	3, 5, 15, 17, 19	VSS
GND	-	14	9	VSS
TxD2/HS	7	11	8*	MD
SCK/IO4	3	1	4	TxD
FLMD1	6	9	2	RxD
RESET	4	13	10	RESET

Note: Switching pin 8 between use as the MD pin and as the TDI pin during debugging requires a switching circuit.

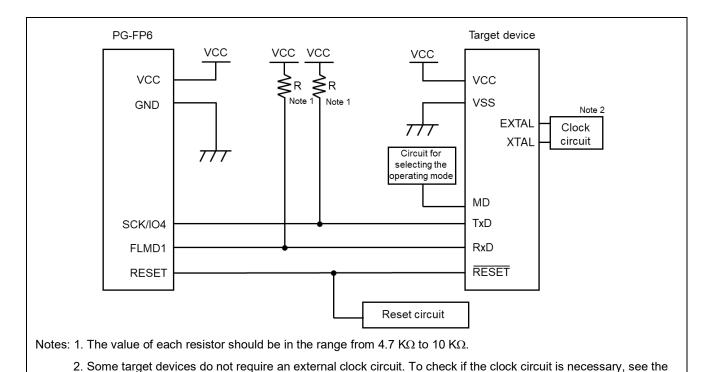


Figure 11.18 Example of a Circuit for R7F0E017D (UART communications)

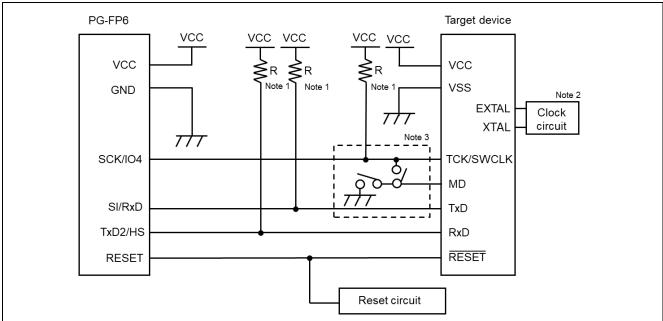
user's manual of the target device.

11.19 RA (UART communications)

The following shows the conversion of each signal when a 14-pin target cable and 20-pin conversion adapter are connected to the 15-pin D-sub connector of the PG-FP6.

Table 11.2 List of Signal Connections for RA Family

Signal Name (PG-FP6)	15-Pin D-Sub Male Connector	14-Pin 2.54-mm Pitch Multipurpose Female Connector	CoreSight 20-pin Connector	RA signal name
VCC	8, 9	8	1	VCC
GND	15	2, 12	3, 5, 15, 17, 19	VSS
GND	-	14	9	VSS
SCK/IO4	3	1	4	MD
SI/RxD	2	5	6	TxD
TxD2/HS	7	11	8	RxD
RESET	4	13	10	RESET



- Notes: 1. The value of each resistor should be in the range from 4.7 K Ω to 10 K Ω .
 - 2. Some target devices do not require an external clock circuit. To check if the clock circuit is necessary, see the user's manual of the target device.
 - 3. Switching pin 4 between use as the MD pin and as the SWCLK/TCK pin during debugging requires a switching circuit.

Figure 11.19 Example of a Circuit for RA6M3 (UART communications)

PG-FP6 V1.05 12. Troubleshooting

12.Troubleshooting

This chapter covers frequently asked questions (FAQ).

12.1 FAQ

For frequently asked questions, refer to the following support portal (FAQ):

https://www.renesas.com/pg-fp6/faq-en

* Using the self-testing function, the user can find out the reason why the FP6 does not operate normally, such as a defect in the FP6, or problems in other hardware. For how to use the tool, refer to 4.4.2.6, [Self Test].

12.2 Problems during Operation

This section describes troubleshooting for problems that may occur during operation.

12.2.1 When an error produces the message 'ERROR: 004 No response'

Cause 1:

The connection with the target system might be wrong.

Action 1:

Check that the connection with the target system is in accord with the recommended circuits shown in chapter 11, Examples of Connections with Microcontrollers.

Cause 2:

The operating mode of the target device might be wrong.

Action 2:

The FP6 is connected to the target device in boot mode or serial programming mode.

- (1) Refer to the user's manual for the target device and check that all required mode pins are being handled correctly.
- (2) For the RX family, check that the settings for I/O signals in the [Tool Details] dialog box match the wiring of the target system.

Cause 3:

The wrong MCU might be selected in the [Create New Setting] dialog box.

The wrong target device might be selected for the settings file.

Action 3:

Select the same MCU as the target device.

Cause 4:

The target device might not be receiving a clock signal.

Action 4:

Check the clock supply on the target system.



PG-FP6 V1.05 12. Troubleshooting

Cause 5:

Power might not be being supplied normally to the target device.

Action 5:

- (1) Check the power supply setting.
- (2) If the power is being supplied from the FP6, the power might not be sufficient. In such cases, supply power from the target system. Confirm that the supply of power on the target system is possible.

Cause 6:

The security functions of the target device may restrict the connection to the PG-FP6.

Action 6:

None. Change the target device if this is required.

12.2.2 When an error produces the message '023 Inv. Sig. addr.'

Cause 1:

An attempt was made to connect a target device which differs from that when the settings file was created.

Action 1:

Create a new settings file or use the correct settings file with the target device.

Cause 2:

The memory structure might have been changed by the option settings of the target device.

Action 2:

When the MCU has a function that for changing the mapping of the flash memory, such as a dual-bank structure, the FP6 recognizes the MCU as a different one before and after changes to the memory mapping. Accordingly, after a change to the memory mapping in the MCU, the error "023 Inv. Sig. addr." will occur. In the FP6, create and change settings files for use before and after changes to the memory mapping.

12.2.3 When an error produces the message 'Communication failure or timeout'

Cause 1:

The connection to the target system may be wrong.

Action 1:

Confirm that the connection to the target system is correct according to the recommended circuits shown in chapter 11, Examples of Connections with Microcontrollers.



PG-FP6 V1.05 12. Troubleshooting

Cause 2:

Settings of the target system and FP6 may not match.

Action 2:

- (1) Baud rate: Check the operating frequency of the target device to see if the baud rate exceeds the allowable communications rate and if the baud rate is appropriate.
- (2) Clock settings: Check if the clock settings for the target device in the FP6 match the actual clock of the target system.

Cause 3:

The target device might have been reset during communications.

Action 3:

- (1) Power supply of the target device: An internal reset might occur in the target device due to voltage fluctuations during communications with the FP6. Check that the power supply is free of problems.
- (2) External reset: A reset might have been applied to the target device by an external reset circuit during communications with the FP6. Check that the reset circuit is free of problems.

Cause 4:

Communications between the FP6 and target device might not be stable.

Action 4:

Check that there is no noise on the communications line.

Remark: Good communications may not be possible if you are using a self-made cable, a self-made extension cable, or the like for connection with a tool.



PG-FP6 V1.05

13. Points for Caution

This chapter gives some notes on rewriting the memory in the target device.

13.1 Checking before Connection

· Applies to: All MCUs

Connection of the target device in the cases listed below may damage the tool in use or the target system due to conflicts between signals. Be sure to check that the settings and circuit connection are correct.

- The type of the target device to be connected was mistaken.
- The wrong recommended circuit was used for the target device.
- The output setting of mode setting pins was wrong while the setting is for manual entry to boot mode.
- The power-supply setting was wrong.

13.2 Manipulating the User Boot Mat

Applies to: RX610 series

If a valid ID code has not been set before the MCU is connected (i.e. the device is not protected), manipulation of the user boot mat is not possible on completion of the connection. To enable manipulation of the user boot mat, set a valid ID code before connecting the MCU.

Applies to: SH family

Reading and uploading of data in user boot mat areas are not supported.

· Applies to: SH family

If you are using HEX files, do not select [Operate] for both the code flash and user boot flash areas on the [Block Setting] tabbed page of the [Setup] dialog box.

13.3 Erasing a Chip

Applies to: RH850 family

When a chip is erased, the configuration data are cleared after all other data have been erased. In other words, the option settings of the MCU are all erased. Since all settings, including the settings at the time of shipment, are erased, be sure to make the required settings at the same time.

In addition, processing to clear the configuration data is prohibited in some MCUs. When you wish to erase a chip, refer to the user's manual of the target device in use and determine whether the processing is available.

13.4 Auto-Padding with 0xFF

Applies to: All MCUs

When an amount of data is less than the minimum unit for programming a flash memory, the data are always padded with 0xFF before programming.

Applies to: RX

When programming the configuration setting area, parts with no data will be padded with 0xFF.



PG-FP6 V1.05 13. Points for Caution

13.5 Wide Voltage Mode

· Applies to: 78K0R family

If you wish to enable wide voltage mode, select the [Wide Voltage] check box on the [Connect Setting] tabbed page of the [Setup] dialog box. Since the FP6 ignores any wide voltage setting in a HCUHEX file, this is the case regardless of whether you are using an HCUHEX file.

13.6 Switching to Dual Mode

• Applies to: RX-family MCUs with flash memory in a dual-bank structure

When you create a new setting file for the FP6 Terminal, select a target device name that matches the bank mode selected by the Bank Mode Select bits in the option-setting memory.

The following error messages will appear when the FP6 is connected to an MCU with a different bank mode.

Message displayed on the FP6: ERROR:023 Inv. Sig. addr.

FP6 Terminal: Connection or synchronisation failed.

The bank mode for the MCU is changed by the following actions.

- Resetting the MCU after a setting for bank mode which differs from the current setting has been written to the Bank Mode Select bits
- Resetting the MCU after selecting [Erase Chip] to erase a chip that is currently in dual mode

[How to switch a chip from the linear mode to the dual mode]

- 1. Create a new ESF file for an MCU in the linear mode.
- 2. Select the erasure option as [Erase Chip] to erase the chip.
- 3. Program the option-setting memory with a file that specifies the dual mode.
- 4. Reset the MCU.

13.7 RPI Files

Applies to: RL78 family, RX100 series*1, and RX200 series*1

When you are using an RPI file, the following settings will be effective even if the RPI file includes no settings regarding command protection*2 or a flash-access window.

Command Protection*2

Disable Block Erase: No Disable Program: No

Disable Boot Block Cluster Programming: No

Flash Access Window

Beginning: Block 0 in the code flash memory of the target MCU End: The last block in the code flash memory of the target MCU

Notes: 1. Only those MCUs that support flash-access window

2. For the RL78 family only



PG-FP6 V1.05

13.8 RPE Files

Applies to: All MCUs

An RPE file is a file in which a program file is encrypted and can be generated by the encryption utility program that comes with this product.

13.9 Verification after Protecting the MCU

- Applies to: RH850, RX64M, RX71M, RX66T, RX72T
 Setting the following protection functions of the MCU restricts the verification function.
 - ID code protection
 - Proceeding with verification ("Verify by reading the device") without issuing a reset after the ID code protection bit has been set (written) will cause a protection error. To avoid this type of error, be sure to reset the MCU after setting (writing to) the ID code protection bit. The FP6 enters the ID authentication mode and verification is enabled.
 - Read command protect (Reading prohibited)
 After the read command protection bit has been set, the ID code written to the MCU cannot be verified. However, the setting of the read command protection bit becomes effective immediately after a new setting has been written.

13.10 Changing the Speed of Communications with the FP6

Changing the speed of communications with the FP6 in the [PC Connection] dialog box or with the brt command while the FP6 is connected to a serial port will disconnect communications between the FP6 Terminal and the FP6. In such cases, open the [PC Connection] dialog box again, re-connect the FP6 Terminal with the FP6, and restart the FP6 Terminal.



14. Maintenance and Warranty

This chapter covers basic maintenance, warranty information, provisions for repair and the procedures for requesting a repair.

14.1 Maintenance

- (1) If dust or dirt collects on this product, wipe it off with a dry soft cloth. Do not use thinner or other solvents because these chemicals can cause the surface coating to separate.
- (2) When you do not use this product for a long period, disconnect it from the power supply, host PC and user system.

14.2 Warranty

- (1) This product comes with a one-year warranty after purchase.
 - Should the product break down or be damaged while you're using it under normal condition based on its user's manual, it will be repaired or replaced free of cost.
- (2) However, if the following failure or damage occurs to the product under warranty, the product will be repaired or
 - a) Failure or damage attributable to the misuse or abuse of the product or its use under other abnormal conditions.
 - b) Failure or damage attributable to improper handling of the product after purchase, such as dropping of the product when it is transported or moved.
 - c) Failure or damage to the product caused by other pieces of equipment connected to it.
 - d) Failure or damage attributable to fire, earthquakes, thunderbolts, floods, or other natural disasters or abnormal voltages, etc.
 - e) Failure or damage attributable to modifications, repairs, adjustments, or other acts made to the product by other than Renesas Electronics Corporation.
- (3) Consumables (e.g., sockets and adapters) are not covered by the aforementioned repair.

In the above cases, contact your local distributor. If your product is being leased, consult the leasing company or the owner.

14.3 Repair Provisions

(1) Repairs not covered by warranty

Problems arising in products for which more than one year has elapsed since purchase are not covered by warranty.

(2) Replacement not covered by warranty

If your product's fault falls into any of the following categories, the fault will be corrected by replacing the entire product instead of repairing it, or you will be advised to purchase a new product, depending on the severity of the fault.

- Faulty or broken mechanical portions
- Flaws, separation, or rust in coated or plated portions
- Flaws or cracks in plastic portions
- Faults or breakage caused by improper use or unauthorized repair or modification
- Heavily damaged electric circuits due to overvoltage, overcurrent or shorting of power supply
- Cracks in the printed circuit board or burnt-down patterns
- A wide range of faults that make replacement less expensive than repair
- Faults that are not locatable or identifiable



- (3) Expiration of the repair period
 - When a period of one year has elapsed after production of a given model ceased, repairing products of that model may become impossible.
- (4) Carriage fees for sending your product to be repaired Carriage fees for sending your product to us for repair are at your own expense.

14.4 How to Make Request for Repair

If your product is found faulty, fill in the Repair Request Sheet downloadable from the following URL. And email the sheet and send the product to your local distributor. To ensure rapid repair, fill in the sheet as specific as possible.

https://www.renesas.com/repair



Note on Transporting the Product:



When sending your product for repair, use the packing box and cushioning material supplied with the product when it was delivered to you and specify caution in handling (handling as precision equipment). If packing of your product is not complete, it may be damaged during transportation. When you pack your product in a bag, make sure to use the conductive plastic bag supplied with the product (usually a blue bag). If you use a different bag, it may lead to further trouble with your product due to static electricity.

Appendix A. Messages

This chapter explains the messages.

A.1 Messages Defined in the FP6 Terminal

No.	Message	Description
E0000001	Reading of a product list file failed.	There may be a shortfall of the files required to run the FP6 Terminal. Reinstall the FP6 Terminal.
E0000002	Saving of a configuration file for the FP6 terminal failed.	Permit writing FP6.ini in the document folder.
E0000004	The firmware file for the FP6 was not correct.	There may be a shortfall of the files required to run the FP6 Terminal. Reinstall the FP6 Terminal.
E0000005	Creation or updating of a setting file failed.	Create a setting file in a writable folder.
E0000006	The name of the folder for a setting file or the name of a setting file is too long. The name of a folder must have no more than 244 characters.	Shorten the path of the folder of the setting file.
E0000007	A setting file was not found.	Create a new settings file or select a correct settings file.
E0000008	The setting file was not correct.	Create a new settings file or select a correct settings file.
E0000010	The device information file cannot be opened.	A parameter file is required to be in the same folder as that for the selected settings file. If the correct combination is not clear, create a new file. Reinstall the FP6 Terminal if the error cannot be fixed.
E0000011	The device information file is not correct.	A parameter file is required to be in the same folder as that for the selected settings file. If the correct combination is not clear, create a new file. Reinstall the FP6 Terminal if the error cannot be fixed.
E0000012	Preparation for downloading a program file failed.	Check if writing to the folder that contains the settings file is possible.
E0000014	The selected program file cannot be opened.	The selected program file cannot be opened because it might have been moved or removed. Select a program file again.
E0000015	The format of the selected program file is not supported.	Select a program file in a supported format.
E0000016	Data were overlapping.	Confirm that the program file does not include data for overlapping address ranges.
E0000017	This file format cannot be selected in the second to fourth text fields on the [Program File] tabbed page.	Select the same format from among RPI, HCUHEX, DDI, and RPE as that of the file in the first text field on the [Program File] tabbed page.
E0000018	System error.	Reinstall the FP6 Terminal.
E0000019	Since a write-protected folder or file was specified, creating the file was not possible.	Confirm that the specified folder or file is not protected.
E0000023	Updating of the files failed.	Ensure that the files in the selected folder are not protected.
E0010001	A timeout occurred during communications with FP6.	Check if the USB cable or serial cable has been correctly connected to the FP6 and that the FP6 has been turned on.
E0010002	An error in communications with the FP6 occurred.	Check if the USB cable or serial cable has been correctly connected to the FP6 and that the FP6 has been turned on.
E0010003	Updating of the firmware for the FP6 failed.	Confirm the connection with the FP6.
	The FP6 terminal was started in a limited mode.	The firmware file may be damaged. Reinstall the FP6 Terminal.

No.	Message	Description
E0010006	Setting of a password failed.	Confirm the connection between the PC and the FP6.
E0010007	Authentication of a password failed.	Input a correct password or initialize the FP6.
E0010008	The value input for the password was not correct.	Specify characters that are actually usable for the FP6 password.
		For the usable characters, refer to section 4.4.2.7, [FP6 Manager].
E0010009	Setting the boot protection failed.	When an authentication pattern is set for [Boot Protection] in the [FP6 Manager] dialog box, the pattern as entered the first time does not match that entered the second time. To specify an authentication pattern for [Boot Protection], the same pattern must be entered the first and second times.
E0020001	The value input for VCC was out of range.	Set the VCC value according to the MCU specification.
E0020002	The input is not correct.	Input a correct value.
E0020003	The value input for the input frequency was out of range.	Set the input frequency according to the MCU specification.
E0020004	No target area is selected.	Select at least one target area on the [Block Setting] tabbed page.

A.2 Error Messages Produced by the FP6 Main Unit

The following describes the error messages produced by the FP6 main unit. The first rows of the Message column are messages displayed in the message display of the main unit. The second and subsequent rows of the Message column are messages displayed in the FP6 Terminal.

No.	Message	Possible Workaround
001	Invalid PR5 data	The parameter file might not have been downloaded to the FP6, or the parameter file was
	Invalid Parameter File.	downloaded but is damaged. Download a correct parameter file to the FP6.
002	Not connected	The target device is manually connected. Enable automatic connection with the 'autocon'
	No device connected.	command or execute a 'con' command before the command that leads to this error.
004	No response	The target device is not connected or is not responding. Check the connection to and
	The device is not responding.	operating mode of the target device. Another possibility is disabling of connection by the security functions of the target device. Refer to section 12.2, Problems during Operation.
005	Not supported!	The command issued is not supported on the target device and thus cannot be used.
	Not supported for this device type.	Check if the parameter file for the MCU to be connected has been downloaded to the FP6 main unit.
006	Command aborted!	The [Read] command has been canceled.
	Cancel pressed, command aborted.	
800	Parameter Error!	An illegal option was specified in the communications command. Refer to chapter 7, Usage
	Invalid argument.	of Communications Commands, and specify a correct option.
009	HEX file Error!	The program file data downloaded to the FP6 may have been damaged. Download the
	HEX file contains invalid data!!	program file again.
012	Synchron. Failed	A failure in communications occurred while the FP6 was proceeding with connection to the
	Connection or Synchronisation failed.	target device. Check the connection between the target device and the FP6. Slowing the transfer rate may solve this problem.
013	Addr. Range err	The address given in the command exceeds the address range of the MCU.
014	RDY detect. fail	The target device is not connected or is not responding. Check the connection to and
	Connection or Synchronisation failed.	operating mode of the target device. Refer to section 12.2, Problems during Operation.
015	Freq. set failed	Setting the frequency of the target device failed. Check if the oscillator frequency of the
	Connection or Synchronisation failed.	target system matches the frequency specified in the FP6 Terminal, and if the frequency is selectable for the MCU.
016	Baudrt. set fail	Setting the baud rate of the target device failed. Check if the oscillator frequency of the
	Connection or Synchronisation failed.	target system matches the frequency specified in the FP6 Terminal. The MCU may not support the specified baud rate. Refer to the user's manual of the MCU and specify a supported baud rate.
017	ID code chk. err	This error code and message are displayed when an ID code different from the security
	Security code	code set in the target device is authenticated.
	authentication failed.	If you have forgotten the configured ID code, connection to the target device for serial programming is basically disabled. However, erasure of the whole flash memory is enabled as an exception in some target devices; for details, refer to the user's manual of the target device.

Message	Possible Workaround
Inv. Sig. ID	An attempt was made to connect a target device which differs from that when the settings
Invalid signature code.	file was created. Create a new settings file or use the correct settings file with the target device.
Inv. Sig. code	An attempt was made to connect a target device which differs from that when the settings
Invalid signature code.	file was created. Create a new settings file or use the correct settings file with the target device.
Inv. Sig. func.	An attempt was made to connect a target device which differs from that when the settings
Invalid signature code.	file was created. Create a new settings file or use the correct settings file with the target device.
Inv. Sig. addr.	An attempt was made to connect a target device which differs from that when the settings
Invalid signature code.	file was created or the memory structure might have been changed by the option settings of the target device. Create a new settings file. Refer to section 12.2, Problems during Operation.
Inv. device name	An attempt was made to connect a target device which differs from that when the settings
Invalid signature code.	file was created. Create a new settings file or use the correct settings file with the target device.
Inv. Dev/Firm ver	An attempt was made to connect a target device which differs from that when the settings
Invalid device or firmware version.	file was created. Create a new settings file or use the correct settings file with the target device.
Unkn. Signature	The parameter file downloaded to the FP6 may have been damaged. Download the
Invalid signature code.	parameter file to the FP6 again.
Inv. DeviceInfo	Check the correctness of the correspondence between the parameter file downloaded to
Connection or Synchronisation failed.	the FP6 and the connected MCU.
Endian info err	A timeout occurred when a problem in communications between the target device and the
Communication failure or timeout.	FP6 arose for some reason. Check the connection to the target device and confirm that the target device has not been reset. Refer to section 12.2, Problems during Operation.
Erase Timeout	A timeout occurred when a problem in communications between the target device and the
Communication failure or timeout.	FP6 arose for some reason. Check the connection to the target device and confirm that the target device has not been reset. Refer to section 12.2, Problems during Operation.
Erase failure	This error code and message are displayed when erasure of flash memory in the target
Erase failed	device was attempted but failed. Possible causes of the error (failure to erase) include:
Protect error due	(1) The power-supply voltage for the target device not being correct.
Setting	(2) Flash memory in the target device cannot be erased because of the pin settings or
Receive device	processing.
error (0xXX)	(3) An operation was attempted in an area that is restricted by a security function.
	Check the items (1) through (3) above.
	If this error is not resolved even if there are none of the problems described in (1) through (3) above, the target device may be malfunctioning (including defects in or deterioration of the flash memory).
Bln Timeout	A timeout occurred when a problem in communications between the target device and the
Communication failure or timeout.	FP6 arose for some reason. Check the connection to the target device and confirm that the target device has not been reset. Refer to section 12.2, Problems during Operation.
Blank chk failed	This error code and message are displayed when blank checking is executed for the flash
Not Blank.	memory of the target device and the area is not blank. When the target device is to be programmed, erase the flash memory with the 'ers' command before executing the 'prg' command or execute the 'ep' command.
	Inv. Sig. ID Invalid signature code. Inv. Sig. code Invalid signature code. Inv. Sig. func. Invalid signature code. Inv. Sig. addr. Invalid signature code. Inv. Sig. addr. Invalid signature code. Inv. Dev/Firm ver Invalid signature code. Inv. Dev/Firm ver Invalid device or firmware version. Unkn. Signature Invalid signature code. Inv. DeviceInfo Connection or Synchronisation failed. Endian info err Communication failure or timeout. Erase Timeout Communication failure error due to Security Setting Receive device error (0xXX) BIn Timeout Communication failure or timeout. Blank chk failed



No.	Message	Possible Workaround
070	Write timeout	A timeout occurred when a problem in communications between the target device and the
	Communication failure or timeout.	FP6 arose for some reason. Check the connection to the target device and confirm that the target device has not been reset. Refer to section 12.2, Problems during Operation.
071	Write failed	This error code and message are displayed when programming of flash memory in the target device was attempted but failed.
	Program failed	Possible causes of the error (failure to program) include:
	Protect error due to Security	(1) Programming was attempted in an area where the flash memory had not been erased.
	Setting	(2) The power-supply voltage for the target device not being correct.
	Receive device error (0xXX)	(3) Flash memory in the target device cannot be programmed because of the pin settings or processing.
		(4) An operation was attempted in an area that is restricted by a security function.
		Check the items (1) through (4) above.
		If this error is not resolved even if there are none of the problems described in (1) to (4) above, the target device may be malfunctioning (including defects in or deterioration of the flash memory).
074	No Prog Data	The operation area contains no data for the program file. Check the block setting and
	There is no data in the operating range.	program file downloaded to the FP6.
075	No Flash Option	The flash option settings have not been specified in the setting file.
	No flash options have been set.	When using the Program Flash Option command (pfo command), specify the flash option settings.
080	Vrf Timeout	A timeout occurred when a problem in communications between the target device and the
	Communication failure or timeout.	FP6 arose for some reason. Check the connection to the target device and confirm that the target device has not been reset. Refer to section 12.2, Problems during Operation.
081	Verify failed	This error code and message are displayed when verification of flash memory in the target device was attempted but failed.
	Receive device error (0xXX)	Possible causes of the error include:
		(1) Different data have been written to the program file and the target device.
		(2) The power-supply voltage for the target device not being correct.
		(3) Data cannot be read from flash memory in the target device because of the pin settings
		or processing.
		Check the items (1) through (3) above.
		If this error is not resolved even if there are none of the problems described in (1) to (3) above, the target device may be malfunctioning (including defects in or deterioration of the flash memory).
090	IVrf Timeout	A timeout occurred when a problem in communications between the target device and the
	Communication failure or timeout.	FP6 arose for some reason. Check the connection to the target device and confirm that the target device has not been reset. Refer to section 12.2, Problems during Operation.
091	IVerify failed	An error occurred while the flash memory of the target device was being programmed.
	Internal Verify failed	Erase the flash memory before programming. Also, check that the power-supply voltage for the target device is normal. If the same error occurs even if you try the operation again, the target device may be malfunctioning (including defects in or deterioration of the flash memory).
093	SUM Comm err	An error occurred during execution of the 'sum' command. This might be due to a problem
	Communication failure or timeout.	with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.

No.	Message	Possible Workaround
094	SCF Comm err	This error code and message are displayed when programming of flash options in the
	Communication	target device was attempted but failed.
	failure or timeout.	Possible causes of the error (failure to program) include:
		(1) An attempt was made to enable a command that had already been disabled.
		(2) An operation that is not possible in the security state of the target device was attempted.
		(3) The power-supply voltage for the target device not being correct.
		(4) Data cannot be read from flash memory in the target device because of the pin settings or processing.
		(5) The target device is malfunctioning (including defect or deterioration in the flash memory).
		Reset the target device or re-check its security state. In some target devices, this problem may be rectified by erasing the flash options (selecting the erasure option as [Erase Chip] to erase the chip). For details, refer to the user's manual of the target device. Another possibility is a problem with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
095	GSC Comm err	An error occurred during execution of the 'gsc' command. This might be due to a problem
	Communication failure or timeout.	with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
096	CLR Comm err	This error occurs when the flash memory in the target device is not blank and the 'clr' or
	Communication failure or timeout.	'rsc' command is executed. Erase all of the flash memory in the target device before executing these commands. Another possibility is a problem with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
099	READ Comm err	An error occurred during execution of the 'read' command. Read prohibition may be set in
	Communication	the security settings for the target device. Another possibility is a problem with communications between the FP6 and target device. Refer to section 12.2, Problems
	failure or timeout.	during Operation.
	Protect error due to Security Setting	
	Receive device error (0xXX)	
100	Pattern mismatch	
	The first and second patterns do not match.	box, the pattern as entered the first time does not match that entered the second time. To specify an authentication pattern for [Boot Protection], the same pattern must be entered the first and second times.
101	ep/prg/vrf Limit	Due to the restriction on the number of times the target device is programmed which is set
	The number of	for [Limit Target Programming] in the [FP6 Manager] dialog box, no more programming or verification commands can be executed.
	executions of ep/prg/vrf command exceeded the upper limit.	The FP6 Manager function is available for removing this restriction.
102	Cmd restricted	Due to the restriction which is set for [Restrict FP6 Operations] in the [FP6 Manager] dialog
	Execution of this	box, executing the command is prohibited.
	command is restricted.	The FP6 Manager function is available for removing this restriction.
103	Cmd restricted	Executing a command is prohibited during the downloading of a HCUHEX or RPI file.
	Execution of this command is restricted when using RPI file.	
106	DLM Comm err.	

No.	Message	Possible Workaround
	DLM error. (0xXX)	An error occurred during execution of the 'dlm' command. This might be due to a problem with communications between the FP6 and target device. If the same error occurs even if you try the operation again, improve the connection environment between the FP6 and MCU. Slowing the transfer rate may solve this problem.

No.	Message	Possible Workaround
107	Require Authen This operation requires authentication.	A transition in the life cycle that requires authentication may have been made with the 'pfo' command. However, use the 'dlm' command in such cases ([DLM Transition] in the FP6 Terminal menu). Alternatively, execute the 'ers_chip' command ([Initialize device] in the FP6 Terminal menu) to initialize the target device.
108	DLM Comm err. Cannot transition to the specified state from the current state.	A transition in the life cycle by the target device failed. A state that does not allow transitions from the current life cycle may have been specified. Acquire the flash options of the target device and confirm that the state that can transit has been specified.
204	Not connected No Device connected.	A 'dcon' command was issued when the target device was already disconnected from the FP6.
210	Already conn. Device already connected.	A 'con' command was issued when the target device was already connected to the FP6. The FP6 target commands can be issued.
302	HEX range err HEX file exceeds target device flash range.	The address range of the downloaded program file extends beyond the set address range. Check the specified program file. When there is no problem even if data out of the range have been included, deselect [Program File Size Monitor] in the [FP6 Manager] dialog box.
303	Invalid ID Tag	The format of the ID Tag is not correct. Download the correct file.
	Invalid ID Tag	For information on the ID Tag, refer to the Terminology table of this user's manual.
400	Targ. power det. Power failure.	This error message is displayed when the FP6 should supply VCC power but VCC has been detected as already being 0.2 V or higher in the target system before VCC is supplied. Check VCC in the target system. If there is no problem with the target system, the FP6 main unit might be damaged. Run a self-test. If this does not resolve the problem, contact a Renesas Electronics sales representative or distributor.
402	FP6 int Vcc fail	The FP6 main unit might be damaged. Contact a Renesas Electronics sales representative
	Power failure.	or distributor.
404	Targ. power fail Power failure.	This error message is displayed when [VCC Monitor] is selected in the [FP6 Manager] dialog box but the VCC voltage is outside the range of the VCC setting by ±5% just before starting communication. Check VCC in the target system. If there is no problem with the target system, the FP6 main unit might be damaged. Run a self-test. If this does not resolve the problem, contact a Renesas Electronics sales representative or distributor.
405	Power failure Power failure.	An overcurrent was detected when VCC was output. Check the connection with the MCU and VCC on the target system. If there is no problem with the target system, the FP6 main unit might be damaged. Run a self-test. If this does not resolve the problem, contact a Renesas Electronics sales representative or distributor.
407	Input Power fail.	The voltage of the USB and the power adapter is not correct. When the same error occurs
	Power failure.	even after the connected PC or AC adapter is changed, the FP6 main unit might be damaged. Contact a Renesas Electronics sales representative or distributor.
585	GOB Comm err	An error occurred during execution of the 'gob' command. This might be due to a problem
	Communication failure or timeout.	with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
586	GID Comm err	An error occurred during execution of the 'gid' command. This might be due to a problem
	Communication failure or timeout.	with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
587	SLB Comm err Communication failure or timeout.	An error occurred during execution of the 'slb' command. A block for which the lock bit has already been set might be disabled in the target device. To disable the lock bit, do not use the 'slb' command but erase the target block. Alternatively, it might be due to a problem with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.



No.	Message	Possible Workaround
588	GOT Comm err	An error occurred during execution of the 'got' command. This might be due to a problem
	Communication failure or timeout.	with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
589	GLB Comm err	An error occurred during execution of the 'glb' command. This might be due to a problem
	Communication failure or timeout.	with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
590	IDC Comn err	An error occurred during execution of the 'idc' command. The OCD ID of a V850E2 cannot
	Communication failure or timeout.	be overwritten. This problem may be resolved by selecting [Erase Chip] as the erasure option and erasing the flash options. Alternatively, it might be due to a problem with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
591	OPB Comn err	An error occurred during execution of the 'opb' command. The option bytes of a V850E2
	Communication failure or timeout.	cannot be overwritten. This problem may be resolved by selecting [Erase Chip] as the erasure option and erasing the flash options. Alternatively, it might be due to a problem with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
592	OTP Comm err	An error occurred during execution of the 'otp' command. A block which has already been
	Communication failure or timeout.	set as OTP might be disabled in the target device. The block once an OTP has been set cannot be released. Alternatively, it might be due to a problem with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
593	SID Comm err	An error occurred during execution of the 'sid' command. This might be due to a problem
	Communication failure or timeout.	with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
595	SED Comm err	An error occurred during execution of the 'sed' command. This might be due to a problem
	Communication failure or timeout.	with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
596	GED Comm err	An error occurred during execution of the 'ged' command. This might be due to a problem
	Communication failure or timeout.	with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
597	SPD Comm err	An error occurred during execution of the 'spd' command. This might be due to a problem with communications between the FP6 and target device. Refer to section 12.2, Problems
	Communication failure or timeout.	during Operation.
599	STM Comm err	An error occurred during execution of the 'stm' command. This might be due to a problem with communications between the FP6 and target device. Refer to section 12.2, Problems
	Communication failure or timeout.	during Operation.
600	GTM Comm err	An error occurred during execution of the 'gtm' command. This might be due to a problem
	Communication failure or timeout.	with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.
601	SPD is active	This error occurs when the security setting to prohibit connection has been made. The
	SPD is active.	serial programming function then cannot be used. In some target devices, this error does not occur even if connection has been prohibited but the 004 error occurs instead.
603	SWAS Recover err	An error occurred during execution of the 'swas_recover' command. This might be due to a problem with communications between the FP6 and target device. Refer to section 12.2,
	Communication failure or timeout.	Problems during Operation.
604	GOS Comm err	An error occurred during execution of the 'gos' command. This might be due to a problem
	Communication failure or timeout.	with communications between the FP6 and target device. Refer to section 12.2, Problems during Operation.



No.	Message	Possible Workaround
605	PFO Comm err	An error occurred during execution of the 'pfo' command. In some target devices, one of
	Communication failure or timeout.	the problems described as responsible for error Nos. 094, 108, 587, 590, 591, or 592 might have occurred.
801	FP6 Power err	The FP6 main unit might be damaged. Contact a Renesas Electronics sales representative
	Power Failure detected.	or distributor.
802	LCD Timeout	The FP6 main unit might be damaged. Contact a Renesas Electronics sales representative
	-(No display)-	or distributor.
803	NAND flash err	The FP6 main unit might be damaged. Contact a Renesas Electronics sales representative
	NAND flash - ECC error	or distributor.
804	NAND flash err	The FP6 main unit might be damaged. Contact a Renesas Electronics sales representative
	NAND flash - Timeout	or distributor.
805	NAND flash err	Execute the 'init' command (click on the [Initialize FP6] button in the [FP6 Manager] dialog
	box selected from the FP6 Terminal menu). The FP6 main unit might be damaged if the error cannot be fixed. Contact a Renesas Electronics sales representative or distributor.	
808	NAND flash err	The FP6 main unit might be damaged. Contact a Renesas Electronics sales representative
	NAND flash - Mapping Error	or distributor.
809	FP6 Config err	The FP6 main unit might be damaged. Contact a Renesas Electronics sales representative
	NAND flash - Mapping Error	or distributor.
810	FP6 Config err	The FP6 main unit might be damaged. Contact a Renesas Electronics sales representative
	FP6 Configuration - Erase/Write fail	or distributor.
811	Statistics err	The FP6 main unit might be damaged. Contact a Renesas Electronics sales representative
	FP6 Statistics - Erase/Write fail	or distributor.
820	FP6 FW err	The firmware of the FP6 is incorrect.
	Firmware data is invalid.	This error may occur when the power of the FP6 main unit is turned off during updating the version of firmware.
		Contact a Renesas Electronics sales representative or distributor.
830	ProgareaSize err	There is no space in the programming area although the required programming area was reserved when the parameter file was downloaded.
	This device requires setting of a larger programming area	Other programming areas must be erased.

A.3 Error Messages Produced by the FP6 Main Unit that are Only Displayed in the Terminal

The following describes the error messages produced by the FP6 main unit that are only displayed in the USB- or serial-connected terminal.

No.	Message	Description
_	Invalid Parameter File.	A parameter file has not been downloaded to the active programming area of the FP6. Download the parameter file and settings file to the FP6.
_	Password of RPE File not set.	A password for the RPE file has not been set. Set the password for the FP6 in the [FP6 Manager] dialog box before downloading an RPE file to the FP6.
_	Invalid MDE	The endian specified on the [Program File] tabbed page of the [Setup] dialog box may not match that of the downloaded program file. Confirm that the endians of the program file and settings file match.
_	Consolidated HEX file has no Option and Security data.	An HCUHEX file downloaded to the FP6 does not include flash options data. Use HCU.exe to create a HCUHEX file that includes the options.
_	This file format does not support uploading.	Uploading of RPE, RPI, and HCUHEX files is not supported.
_	Command not found (enter 'hlp' for help).	The FP6 does not support the communications command. Check the executable commands by issuing the 'hlp' command.
_	Please update to latest firmware version.	When you use a downloaded parameter file, the FP6 firmware must have been updated to the latest version. Use the FP6 Terminal to update the FP6 firmware.
	Aborted in line: xx Invalid file format.	The format of the downloaded program file might be wrong.
		Check the line indicated by "Aborted in line: xx". This error will also occur when the password given for the RPE file does not match the actual password.

A.4 List of Security and Safety Functions of the Target Device that May Affect the Operation of the Programmer

The following lists the security and safety functions of the target device that may affect the error messages with descriptions that include security functions.

- · Access window
- · Flash shield window
- OTP
- Disable Debugger and Serial Programming
- Disable Serial Programming
- DLM
- · Disable Initialize Command
- Disable Chip Erase
- Disable Block Erase
- Disable Program
- Disable Rewriting boot cluster
- ICU

Remark: The security functions included in a target device and the operation when the security function has been set depends on the target device. Some security functions may not be cleared by using the [Erase Chip] option or the [Initialize Device] menu. For details, refer to the user's manual of the target device.

Appendix B. Supplementary Information

This chapter covers supplementary information referred to by the user's manual of the FP6.

B.1 32-Bit CRC Method

```
*/
       The generator polynomial used for this table is
      x^32+x^26+x^23+x^22+x^16+x^12+x^11+x^10+x^8+x^7+x^5+x^4+x^2+x^1+x^0 */
    according to Autodin/Ethernet/ADCCP protocol standards
                                                                                                                              * /
/* Binary: 0x04c11db7
const uint32_t CRC32_Tab [256] = {
       0 \\ x \\ 0 \\ 
       0x2608edb8, 0x22c9f00f, 0x2f8ad6d6, 0x2b4bcb61, 0x350c9b64, 0x31cd86d3, 0x3c8ea00a, 0x384fbdbd,
       0x4c11db70, 0x48d0c6c7, 0x4593e01e, 0x4152fda9, 0x5f15adac, 0x5bd4b01b, 0x569796c2, 0x52568b75,
       0x6a1936c8, 0x6ed82b7f, 0x639b0da6, 0x675a1011, 0x791d4014, 0x7ddc5da3, 0x709f7b7a, 0x745e66cd,
       0x9823b6e0, 0x9ce2ab57, 0x91a18d8e, 0x95609039, 0x8b27c03c, 0x8fe6dd8b, 0x82a5fb52, 0x8664e6e5,
       0xbe2b5b58, 0xbaea46ef, 0xb7a96036, 0xb3687d81, 0xad2f2d84, 0xa9ee3033, 0xa4ad16ea, 0xa06c0b5d,
       0xd4326d90, 0xd0f37027, 0xddb056fe, 0xd9714b49, 0xc7361b4c, 0xc3f706fb, 0xceb42022, 0xca753d95,
       0xf23a8028, 0xf6fb9d9f, 0xfbb8bb46, 0xff79a6f1, 0xe13ef6f4, 0xe5ffeb43, 0xe8bccd9a, 0xec7dd02d,
       0x34867077, 0x30476dc0, 0x3d044b19, 0x39c556ae, 0x278206ab, 0x23431b1c, 0x2e003dc5, 0x2ac12072,
       0x128e9dcf, 0x164f8078, 0x1b0ca6a1, 0x1fcdbb16, 0x018aeb13, 0x054bf6a4, 0x0808d07d, 0x0cc9cdca,
       0x7897ab07. 0x7c56b6b0. 0x71159069. 0x75d48dde. 0x6b93dddb. 0x6f52c06c. 0x6211e6b5. 0x66d0fb02.
       0x5e9f46bf, 0x5a5e5b08, 0x571d7dd1, 0x53dc6066, 0x4d9b3063, 0x495a2dd4, 0x44190b0d, 0x40d816ba,
       0xaca5c697, 0xa864db20, 0xa527fdf9, 0xa1e6e04e, 0xbfa1b04b, 0xbb60adfc, 0xb6238b25, 0xb2e29692,
       0x8aad2b2f. 0x8e6c3698. 0x832f1041. 0x87ee0df6. 0x99a95df3. 0x9d684044. 0x902b669d. 0x94ea7b2a.
       0xe0b41de7, 0xe4750050, 0xe9362689, 0xedf73b3e, 0xf3b06b3b, 0xf771768c, 0xfa325055, 0xfef34de2,
       0xc6bcf05f, 0xc27dede8, 0xcf3ecb31, 0xcbffd686, 0xd5b88683, 0xd1799b34, 0xdc3abded, 0xd8fba05a,
       0x690ce0ee, 0x6dcdfd59, 0x608edb80, 0x644fc637, 0x7a089632, 0x7ec98b85, 0x738aad5c, 0x774bb0eb,
       0x4f040d56. 0x4bc510e1. 0x46863638. 0x42472b8f. 0x5c007b8a. 0x58c1663d. 0x558240e4. 0x51435d53.
       0x251d3b9e, 0x21dc2629, 0x2c9f00f0, 0x285e1d47, 0x36194d42, 0x32d850f5, 0x3f9b762c, 0x3b5a6b9b,
       0x0315d626, 0x07d4cb91, 0x0a97ed48, 0x0e56f0ff, 0x1011a0fa, 0x14d0bd4d, 0x19939b94, 0x1d528623,
       0xf12f560e, 0xf5ee4bb9, 0xf8ad6d60, 0xfc6c70d7, 0xe22b20d2, 0xe6ea3d65, 0xeba91bbc, 0xef68060b,
       0xd727bbb6, 0xd3e6a601, 0xdea580d8, 0xda649d6f, 0xc423cd6a, 0xc0e2d0dd, 0xcda1f604, 0xc960ebb3,
       0xbd3e8d7e, 0xb9ff90c9, 0xb4bcb610, 0xb07daba7, 0xae3afba2, 0xaafbe615, 0xa7b8c0cc, 0xa379dd7b,
       0x9b3660c6, 0x9ff77d71, 0x92b45ba8, 0x9675461f, 0x8832161a, 0x8cf30bad, 0x81b02d74, 0x857130c3,
       0x5d8a9099, 0x594b8d2e, 0x5408abf7, 0x50c9b640, 0x4e8ee645, 0x4a4ffbf2, 0x470cdd2b, 0x43cdc09c,
       0x7b827d21, 0x7f436096, 0x7200464f, 0x76c15bf8, 0x68860bfd, 0x6c47164a, 0x61043093, 0x65c52d24,
       0x119b4be9, 0x155a565e, 0x18197087, 0x1cd86d30, 0x029f3d35, 0x065e2082, 0x0b1d065b, 0x0fdc1bec,
       0x3793a651, 0x3352bbe6, 0x3e119d3f, 0x3ad08088, 0x2497d08d, 0x2056cd3a, 0x2d15ebe3, 0x29d4f654,
       0xc5a92679, 0xc1683bce, 0xcc2b1d17, 0xc8ea00a0, 0xd6ad50a5, 0xd26c4d12, 0xdf2f6bcb, 0xdbee767c,
       0xe3alcbc1, 0xe760d676, 0xea23f0af, 0xeee2ed18, 0xf0a5bd1d, 0xf464a0aa, 0xf9278673, 0xfde69bc4,
       0x89b8fd09, 0x8d79e0be, 0x803ac667, 0x84fbdbd0, 0x9abc8bd5, 0x9e7d9662, 0x933eb0bb, 0x97ffad0c,
       0xafb010b1, 0xab710d06, 0xa6322bdf, 0xa2f33668, 0xbcb4666d, 0xb8757bda, 0xb5365d03, 0xb1f740b4
};
uint32 t CalcMemoryCRC32 (uint32 t address, uint32 t length)
       uint32 t i, rd ptr, crc accum;
       uint8 t byte, data [16];
```

```
crc_accum= 0xFFFFFFFF; /* Init Pattern */
for (i= 0, rd_ptr= 16; i < length; i++)
{
    /* Check flash read buffer and fill if needed */
    if (rd_ptr == 16)
    {
        Memory_Read (address, 16, data);
        rd_ptr= 0;
        address+= 16;
    }
    byte= ((crc_accum >> 24) ^ data [rd_ptr++]) & 0xFF;
        crc_accum= (crc_accum << 8) ^ CRC32_Tab [byte];
}
return crc_accum;
}</pre>
```

Figure B.1 32-bit CRC Calculation Specifications

B.2 Division Method

```
#define BLOCKSIZ 256
/* You have to store 1-Block ROM data. */
unsigned char rom_data[BLOCKSIZ];
unsigned char
bist_calc()
{
int i;
unsigned short bist, bist_temp;
bist = 0;
for(i = 0; i < BLOCKSIZ; i++) {</pre>
bist_temp = bist & 0x1;
bist_temp = (bist_temp << 8) | (bist_temp << 9) |</pre>
    (bist temp << 11) | (bist temp << 12);
bist = (bist >> 1) ^ rom_data[i] ^ bist_temp;
          }
return((unsigned char)bist);
}
```

Figure B.2 Division (Original) Calculation Specifications

B.3 16-Bit CRC Method

```
/* The generator polynomial used for this table is: */
/* x^16+x^12+x^5+x^0 according to CCITT-16 standard. */
/* Binary: 0x1021 */
const uint16 t CRC16 Tab [256]= {
    0x0000,0x1021,0x2042,0x3063,0x4084,0x50A5,0x60C6,0x70E7,
    0x8108,0x9129,0xA14A,0xB16B,0xC18C,0xD1AD,0xE1CE,0xF1EF,
    0x1231,0x0210,0x3273,0x2252,0x52B5,0x4294,0x72F7,0x62D6,
    0x9339,0x8318,0xB37B,0xA35A,0xD3BD,0xC39C,0xF3FF,0xE3DE,
    0x2462,0x3443,0x0420,0x1401,0x64E6,0x74C7,0x44A4,0x5485,
    0xA56A, 0xB54B, 0x8528, 0x9509, 0xE5EE, 0xF5CF, 0xC5AC, 0xD58D,
    0x3653,0x2672,0x1611,0x0630,0x76D7,0x66F6,0x5695,0x46B4,
    0xB75B, 0xA77A, 0x9719, 0x8738, 0xF7DF, 0xE7FE, 0xD79D, 0xC7BC,
    0x48C4,0x58E5,0x6886,0x78A7,0x0840,0x1861,0x2802,0x3823,
    0xC9CC, 0xD9ED, 0xE98E, 0xF9AF, 0x8948, 0x9969, 0xA90A, 0xB92B,
    0x5AF5,0x4AD4,0x7AB7,0x6A96,0x1A71,0x0A50,0x3A33,0x2A12,
    0xDBFD, 0xCBDC, 0xFBBF, 0xEB9E, 0x9B79, 0x8B58, 0xBB3B, 0xAB1A,
    0x6CA6,0x7C87,0x4CE4,0x5CC5,0x2C22,0x3C03,0x0C60,0x1C41,
    0xEDAE, 0xFD8F, 0xCDEC, 0xDDCD, 0xAD2A, 0xBD0B, 0x8D68, 0x9D49,
    0x7E97,0x6EB6,0x5ED5,0x4EF4,0x3E13,0x2E32,0x1E51,0x0E70,
    0xFF9F, 0xEFBE, 0xDFDD, 0xCFFC, 0xBF1B, 0xAF3A, 0x9F59, 0x8F78,
    0x9188,0x81A9,0xB1CA,0xA1EB,0xD10C,0xC12D,0xF14E,0xE16F,
    0x1080,0x00A1,0x30C2,0x20E3,0x5004,0x4025,0x7046,0x6067,
    0x83B9,0x9398,0xA3FB,0xB3DA,0xC33D,0xD31C,0xE37F,0xF35E,
    0x02B1,0x1290,0x22F3,0x32D2,0x4235,0x5214,0x6277,0x7256,
    0xB5EA, 0xA5CB, 0x95A8, 0x8589, 0xF56E, 0xE54F, 0xD52C, 0xC50D,
    0x34E2,0x24C3,0x14A0,0x0481,0x7466,0x6447,0x5424,0x4405,
    0xA7DB, 0xB7FA, 0x8799, 0x97B8, 0xE75F, 0xF77E, 0xC71D, 0xD73C,
    0x26D3,0x36F2,0x0691,0x16B0,0x6657,0x7676,0x4615,0x5634,
    0xD94C,0xC96D,0xF90E,0xE92F,0x99C8,0x89E9,0xB98A,0xA9AB,
    0x5844,0x4865,0x7806,0x6827,0x18C0,0x08E1,0x3882,0x28A3,
    0xCB7D, 0xDB5C, 0xEB3F, 0xFB1E, 0x8BF9, 0x9BD8, 0xABBB, 0xBB9A,
    0x4A75,0x5A54,0x6A37,0x7A16,0x0AF1,0x1AD0,0x2AB3,0x3A92,
    0xFD2E, 0xED0F, 0xDD6C, 0xCD4D, 0xBDAA, 0xAD8B, 0x9DE8, 0x8DC9,
    0x7C26,0x6C07,0x5C64,0x4C45,0x3CA2,0x2C83,0x1CE0,0x0CC1,
    0xEF1F, 0xFF3E, 0xCF5D, 0xDF7C, 0xAF9B, 0xBFBA, 0x8FD9, 0x9FF8,
    0x6E17,0x7E36,0x4E55,0x5E74,0x2E93,0x3EB2,0x0ED1,0x1EF0
};
uint16_t CalcMemoryCRC16 (uint32_t address, uint32_t length)
    uint32_t i, rd_ptr;
    uint16_t crc_accum;
    uint8_t byte, data [4];
    crc accum= 0x0000; /* Init Pattern */
    for (i= 0, rd_ptr= 0; i < length; i++)
```

```
/* Check flash read buffer and fill if needed */
    if (rd_ptr == 0)
    {
         Memory_Read (address, 4, data);
         rd_ptr= 4;
         address+= 4;
    byte= (crc_accum >> 8) ^ data [--rd_ptr];
    crc_accum= (crc_accum << 8) ^ CRC16_Tab [byte];</pre>
return crc_accum;
```

Figure B.3 16-bit CRC Calculation Specifications

Appendix C. Equivalent Circuits of the Target Interface

This chapter shows equivalent circuits of the target interface.

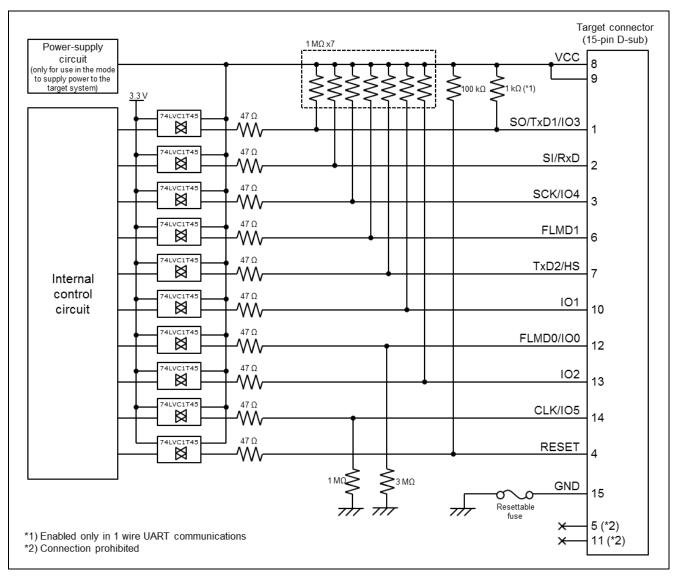


Figure C.1 Equivalent Circuits of the Target Interface

Appendix D. Electrical Specifications of the Remote Interface

This chapter gives the electrical specifications of the remote interface.

D.1 Absolute Maximum Ratings (TA=0 to 40°C)

Pin name	Symbol	Parameter or Conditions	Ratings	Unit
CONN	Vı	Input voltage	-0.5 to +6.0	٧
BUSY	lo	Output current	±50	mA
PASS ERROR	I _{IK}	Input current (V _I < 0 V)	-50	mA
CANCEL ENTER				
NEXT VRF				
START				
CLEAR				

Note: Product quality may suffer if the absolute maximum rating is exceeded even momentarily for any parameter.

That is, the absolute maximum ratings are rated values at which the product is on the verge of suffering physical damage, and therefore the product must be used under conditions that ensure that the absolute maximum ratings are not exceeded.

D.2 DC Characteristics (T_A=0 to 40°C, C=0pF (Unloaded Condition))

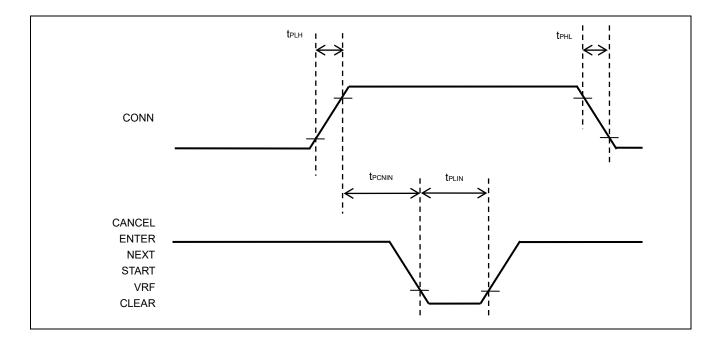
Pin name	Symbol	Parameter or Conditions	MIN.	TYP.	MAX.	Unit
CONN	Vон	Output voltage, high (Iон=8mA)	2.3	_	_	V
BUSY		Output voltage, high (I _{OH} =100µA)	3.0	3.3	_	V
PASS	V _{OL}	Output voltage, low (I _{OL} =8mA)	_	_	0.8	V
ERROR		Output voltage, low (I _{OH} =100µA)		0	0.1	V
CANCEL	ViH	Input voltage, high	2	_	_	V
ENTER NEXT VRF START CLEAR CONN BUSY	VIL IOH IOL	Input voltage, low Output current, high Output current, low			0.8 -8 +8	MA mA
PASS ERROR	IOL					mA
CANCEL	I	Input current	_	_	±1	mA
	R _{IPU}	Internal pull-up resistor (3.3V)	_	4.7	_	ΚΩ

D.3 AC Characteristics (T_A=0 to 40°C, C=0pF (Unloaded Condition))

D.3.1 Standard mode

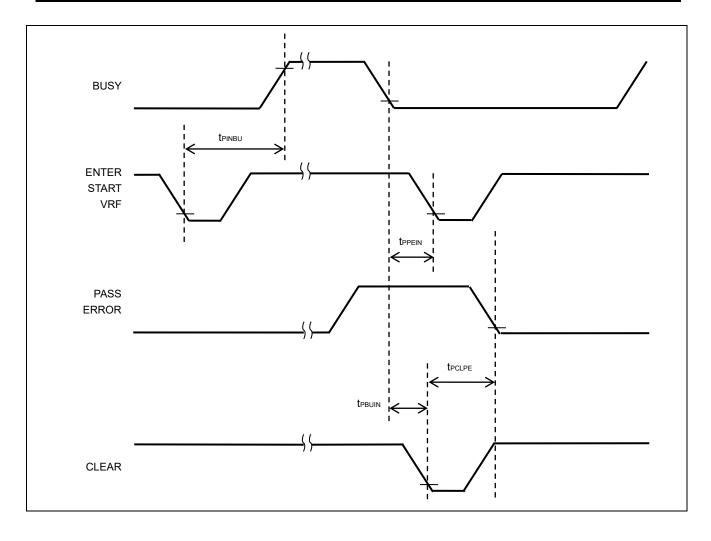
(1)

Pin name	Symbol	Parameter or Conditions	MIN.	TYP.	MAX.	Unit
CONN	t _{PLH}	Rise time(I ₀ =8mA)	_	_	5	ns
BUSY PASS ERROR	t _{PHL}	Fall time (Io=8mA)	_	_	5	ns
CANCEL ENTER NEXT VRF START CLEAR	t _{PLIN}	Low-level width of input signal	50			ms
	tpcnin	Time from the rise of the CONN signal until the input signal is acknowledged	1	_	_	ms



(2)

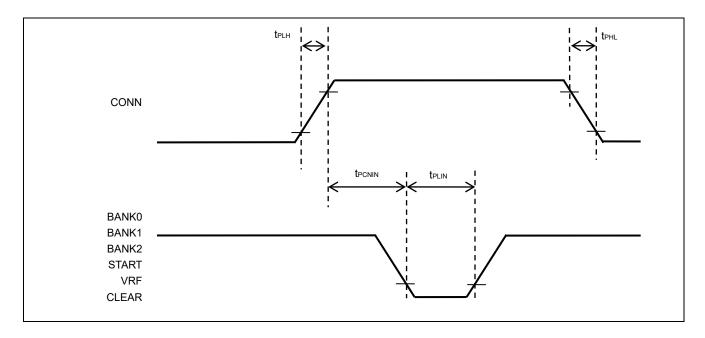
Pin name	Symbol	Parameter or Conditions	MIN.	TYP.	MAX.	Unit
	t _{PINBU}	Time from the fall of the VRF, START,	_	_	50	ms
		or ENTER signal until the rise of the				
		BUSY signal				
	t _{PBUIN}	Time from the fall of the BUSY signal	1	_	_	ms
		until the CLEAR signal can be input				
	t _{PCLPE}	Time from the fall of the CLEAR signal	_	_	50	ms
		until the fall of the PASS or ERROR				
		signal				
	t _{PPEIN}	Time from the fall of the BUSY signal until the VRF, START, or ENTER signal can be input	_	_	1	ms



D.3.2 Bank mode

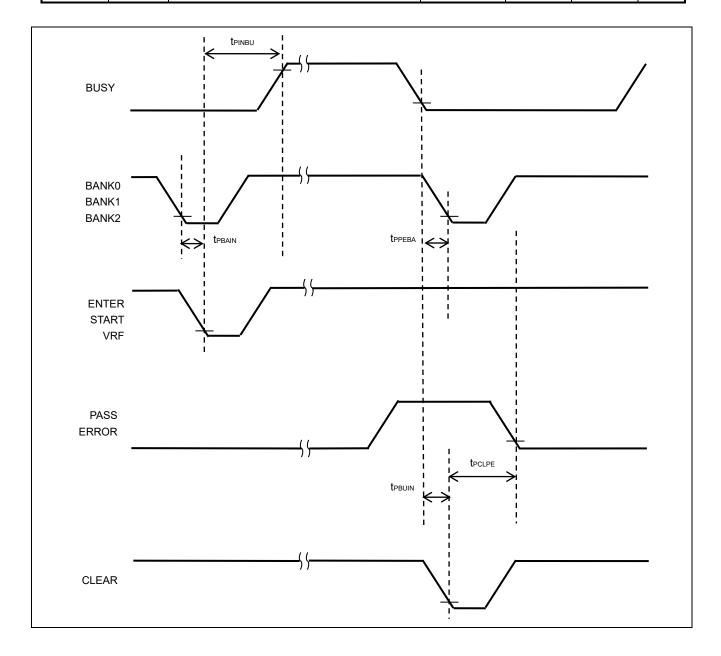
(1)

Pin name	Symbol	Parameter or Conditions	MIN.	TYP.	MAX.	Unit
CONN	t _{PLH}	Rise time (Io=8mA)	_	_	5	ns
BUSY PASS ERROR	t _{PHL}	Fall time (I _O =8mA)		_	5	ns
BANK0	t _{PLIN}	Low-level width of input signal	50	_	_	ms
BANK1 BANK2 VRF START CLEAR	t _P CNIN	Time from the rise of the CONN signal until the input signal is acknowledged	1	_	_	ms



(2)

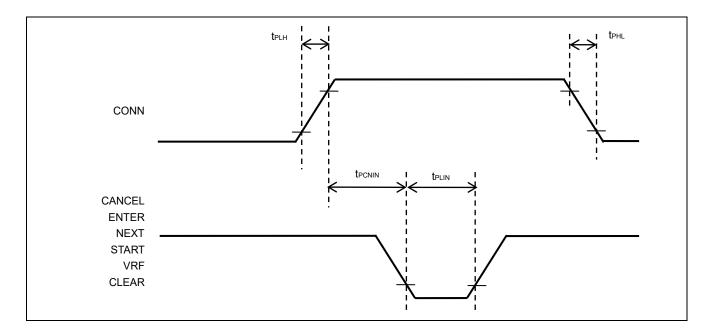
Pin name	Symbol	Parameter or Conditions	MIN.	TYP.	MAX.	Unit
	t _{PBAIN}	Time from the fall of the BANK signal	1	_	_	ms
		until the VRF or START signal can be				
		input				
	t _{PINBU}	Time from the fall of the VRF, START	_	_	100	ms
		or ENTER signal until the rise of the				
		BUSY signal				
	t _{PBUIN}	Time from the fall of the BUSY signal	5	_	_	ms
		until the CLEAR signal can be input				
	t _{PCLPE}	Time from the fall of the CLEAR signal	_	_	50	ms
		until the fall of the PASS or ERROR				
		signal				
	tррева	Time from the fall of the BUSY signal until the BANK signal can be input	10	_	_	ms



D.3.3 Simple mode

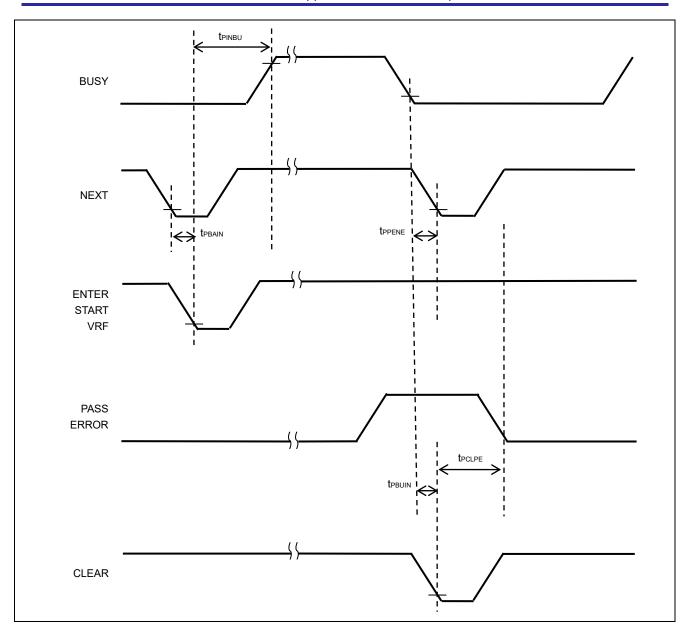
(1)

Pin name	Symbol	Parameter or Conditions	MIN.	TYP.	MAX.	Unit
CONN	t _{PLH}	Rise time (IO=8mA)	_	_	5	ns
BUSY PASS ERROR	t _{PHL}	Fall time (IO=8mA)	_	_	5	ns
CANCEL	t _{PLIN}	Low-level width of input signal	50	_	_	ms
ENTER NEXT VRF START CLEAR	tpcnin	Time from the rise of the CONN signal until the input signal is acknowledged	1	_	_	ms



(2)

Pin name	Symbol	Parameter or Conditions	MIN.	TYP.	MAX.	Unit
	t _{PBAIN}	Time from the fall of the NEXT signal until the VRF or START signal can be input	1	_	_	ms
	tPINBU	Time from the fall of the VRF, START or ENTER signal until the rise of the BUSY signal (When the input signal is input after having changed the program area)	_	_	8000	ms
		Time from the fall of the VRF, START or ENTER signal until the rise of the BUSY signal (When the input signal is input without changing the program area)	_	_	50	ms
	t _{PBUIN}	Time from the fall of the BUSY signal until the CLEAR signal can be input	1	_	_	ms
	t PCLPE	Time from the fall of the CLEAR signal until the fall of the PASS or ERROR signal	_	_	50	ms
	t _{PPENE}	Time from the fall of the BUSY signal until the NEXT signal can be input	1			ms



Appendix E. Electrical Specifications of the Target Interface

This chapter gives the electrical specifications of the target interface.

E.1 Absolute Maximum Ratings (TA=0 to 40°C)

Pin name	Symbol	Parameter or Conditions	Ratings	Unit
Vcc	_	Input power-supply voltage	-0.5 to +6.5	V
SO/TxD1/IO3	Vo	Output voltage	-0.5 to Vcc + 0.5 V*1	V
SI/RxD	Vı	Input voltage	-0.5 to +6.5	V
SCK/IO4				
RESET				
FLMD1				
TxD2/HS				
IO1				
FLMD0/IO0				
IO2				
CLK/IO5				
Vcc	lo	Output current	+500	mA
SO/TxD1/IO3	Io	Output current (-0.3 V $<$ V _O $<$ V _{CC} + 0.5 V)	±50	mA
SI/RxD				
SCK/IO4				
RESET				
FLMD1				
TxD2/HS				
IO1				
FLMD0/IO0				
IO2				
CLK/IO5				

Notes: 1. The value must be less than 6.5 V.

^{2.} Product quality may suffer if the absolute maximum rating is exceeded even momentarily for any parameter. That is, the absolute maximum ratings are rated values at which the product is on the verge of suffering physical damage, and therefore the product must be used under conditions that ensure that the absolute maximum ratings are not exceeded.

E.2 DC Characteristics (T_A=0 to 40°C)

Pin name	Symbol	Parameter or Conditions	MIN.	TYP.	MAX.	Unit
Vcc	V _{OH}	Output voltage, high	1.2	_	5.5	V
		Output voltage, high (I _{OH} = 100 mA)	Vcc - 5%	Vcc	Vcc + 5%	V
	Іін	Input current, high	_	_	+10	mA
SO/TxD1/IO3	V _{OL1}	Output voltage, low (I _{OL} = 100 μA)	_	0	0.2	V
SI/RxD SCK/IO4	V _{OL2}	Output voltage, low (Vcc = 1.65 V, I _{OL} =8mA)	_	_	0.45	V
RESET FLMD1	V _{OL3}	Output voltage, low (Vcc = 4.5 V, I _{OL} = 32 mA)	_	_	0.55	V
TxD2/HS IO1	V _{OH1}	Output voltage, high (I _{OH} = 100 μA)	V _{CC} - 0.1	Vcc	_	V
FLMD0/IO0 IO2	V _{OH2}	Output voltage, high (Vcc = 1.65 V, I _{OH} = 8 mA)	1.2	_	_	V
CLK/IO5	Vонз	Output voltage, high (Vcc = 4.5 V, I _{OH} = 32 mA)	3.8	_	_	V
	V _{IL1}	Input voltage, low (V _{CC} = 1.2 V)	_	_	V _{CC} × 0.2	V
	V _{IL2}	Input voltage, low (3.0 V < V _{CC} < 3.6 V)	_	_	0.8	V
	V _{IL3}	Input voltage, low (4.5 V < V _{CC} < 5.5 V)	_	_	Vcc × 0.3	V
	V _{IH1}	Input voltage, high (Vcc = 1.2 V)	Vcc × 0.8	_	_	V
	V _{IH2}	Input voltage, high (3.0 V < V _{CC} < 3.6 V)	2.0	_	_	V
	V _{IH3}	Input voltage, high (4.5 V < V _{CC} < 5.5 V)	V _{CC} × 0.7	_	_	V

PG-FP6 V1.05 User's Manual

Publication Date: Rev.7.00 Jul.01.21

Published by: Renesas Electronics Corporation

PG-FP6 V1.05

