To our customers,

Old Company Name in Catalogs and Other Documents

On April 1st, 2010, NEC Electronics Corporation merged with Renesas Technology Corporation, and Renesas Electronics Corporation took over all the business of both companies. Therefore, although the old company name remains in this document, it is a valid Renesas Electronics document. We appreciate your understanding.

Renesas Electronics website: http://www.renesas.com

April 1st, 2010
Renesas Electronics Corporation

Issued by: Renesas Electronics Corporation (http://www.renesas.com)

Send any inquiries to http://www.renesas.com/inquiry.

Notice

1. All information included in this document is current as of the date this document is issued. Such information, however, is subject to change without any prior notice. Before purchasing or using any Renesas Electronics products listed herein, please confirm the latest product information with a Renesas Electronics sales office. Also, please pay regular and careful attention to additional and different information to be disclosed by Renesas Electronics such as that disclosed through our website.
2. Renesas Electronics does not assume any liability for infringement of 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. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
3. You should not alter, modify, copy, or otherwise misappropriate any Renesas Electronics product, whether in whole or in part.
4. 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 of these circuits, software, and information in the design of your equipment. Renesas Electronics assumes no responsibility for any losses incurred by you or third parties arising from the use of these circuits, software, or information.
5. When exporting the products or technology described in this document, you should comply with the applicable export control laws and regulations and follow the procedures required by such laws and regulations. You should not use Renesas Electronics products or the technology described in this document for any purpose relating to military applications or use by the military, including but not limited to the development of weapons of mass destruction. Renesas Electronics products and technology may 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.
6. Renesas Electronics has used reasonable care in preparing the information included in this document, but Renesas Electronics does not warrant that such information is error free. Renesas Electronics assumes no liability whatsoever for any damages incurred by you resulting from errors in or omissions from the information included herein.
7. Renesas Electronics products are classified according to the following three quality grades: “Standard”, “High Quality”, and “Specific”. The recommended applications for each Renesas Electronics product depends on the product’s quality grade, as indicated below. You must check the quality grade of each Renesas Electronics product before using it in a particular application. You may not use any Renesas Electronics product for any application categorized as “Specific” without the prior written consent of Renesas Electronics. Further, you may not use any Renesas Electronics product for any application for which it is not intended without the prior written consent of Renesas Electronics. Renesas Electronics shall not be in any way liable for any damages or losses incurred by you or third parties arising from the use of any Renesas Electronics product for an application categorized as “Specific” or for which the product is not intended where you have failed to obtain the prior written consent of Renesas Electronics. The quality grade of each Renesas Electronics product is “Standard” unless otherwise expressly specified in a Renesas Electronics data sheets or data books, etc.

   “Standard”: Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; and industrial robots.

   “High Quality”: Transportation equipment (automobiles, trains, ships, etc.); traffic control systems; anti-disaster systems; anti-crime systems; safety equipment; and medical equipment not specifically designed for life support.

   “Specific”: Aircraft; aerospace equipment; submersible repeaters; nuclear reactor control systems; medical equipment or systems for life support (e.g. artificial life support devices or systems), surgical implantations, or healthcare intervention (e.g. excision, etc.), and any other applications or purposes that pose a direct threat to human life.
8. You should use the Renesas Electronics products described in this document within the range specified by Renesas Electronics, especially with respect to the maximum rating, operating supply voltage range, movement power voltage range, heat radiation characteristics, installation and other product characteristics. Renesas Electronics shall have no liability for malfunctions or damages arising out of the use of Renesas Electronics products beyond such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of its products, semiconductor products have specific characteristics such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Further, Renesas Electronics products are not subject to radiation resistance design. Please be sure to implement safety measures to guard them against the possibility of physical injury, and injury or damage caused by fire in the event of the failure of a Renesas Electronics product, 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, please evaluate the safety of the final products or system 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. Please use Renesas Electronics products in compliance with all applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive. Renesas Electronics assumes no liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. This document may not be reproduced or duplicated, in any form, in whole or in part, without prior written consent of Renesas Electronics.
12. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products, or if you have any other inquiries.

(Note 1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its majority-owned subsidiaries.

(Note 2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

RENESAS

Application Note

78K0/78K0R/V850

8-, 16- and 32-bit Single-chip Microcontrollers

Flash Protection Features and Security Setting Guide

Document No. U20050EU1V0AN00
October 2009. NEC Electronics America, Inc.

The information in this document is current as of October 2009. The information is subject to change without notice. For actual design-in, refer to the latest publications of NEC Electronics data sheets or data books, etc., for the most up-to-date specifications of NEC Electronics products. Not all products and/or types are available in every country. Please check with an NEC Electronics sales representative for availability and additional information.

No part of this document may be copied or reproduced in any form or by any means without prior written consent of NEC Electronics. NEC Electronics assumes no responsibility for any errors that may appear in this document.

NEC Electronics does not assume any liability for infringement of patents, copyrights or other intellectual property rights of third parties by or arising from the use of NEC Electronics products listed in this document or any other liability arising from the use of such NEC Electronics products. No license, express, implied or otherwise, is granted under any patents, copyrights or other intellectual property rights of NEC Electronics or others.

Descriptions of circuits, software and other related information in this document are provided for illustrative purposes in semiconductor product operation and application examples. The incorporation of these circuits, software and information in the design of customer's equipment shall be done under the full responsibility of customer. NEC Electronics no responsibility for any losses incurred by customers or third parties arising from the use of these circuits, software and information.

While NEC Electronics endeavors to enhance the quality, reliability and safety of NEC Electronics products, customers agree and acknowledge that the possibility of defects thereof cannot be eliminated entirely. To minimize risks of damage to property or injury (including death) to persons arising from defects in NEC Electronics products, customers must incorporate sufficient safety measures in their design, such as redundancy, fire-containment and anti-failure features.

NEC Electronics products are classified into the following three quality grades: “Standard”, “Special” and “Specific”.

The "Specific" quality grade applies only to NEC Electronics products developed based on a customer-designated “quality assurance program” for a specific application. The recommended applications of NEC Electronics product depend on its quality grade, as indicated below. Customers must check the quality grade of each NEC Electronics product before using it in a particular application.

"Standard": Computers, office equipment, communications equipment, test and measurement equipment, audio and visual equipment, home electronic appliances, machine tools, personal electronic equipment and industrial robots.

"Special": Transportation equipment (automobiles, trains, ships, etc.), traffic control systems, anti-disaster systems, anti-crime systems, safety equipment and medical equipment (not specifically designed for life support).

"Specific": Aircraft, aerospace equipment, submersible repeaters, nuclear reactor control systems, life support systems and medical equipment for life support, etc.

The quality grade of NEC Electronics products is “Standard” unless otherwise expressly specified in NEC Electronics data sheets or data books, etc. If customers wish to use NEC Electronics products in applications not intended by NEC Electronics, they must contact NEC Electronics sales representative in advance to determine NEC Electronics’ willingness to support a given application.

Notes:

1. "NEC Electronics" as used in this statement means NEC Electronics Corporation and also includes its majority-owned subsidiaries.
2. "NEC Electronics products" means any product developed or manufactured by or for NEC Electronics (as defined above).

M8E 02.10

Revision History

Date	Revision	Section	Description
October 15, 2009	—	—	First release

Contents

List of Figures

List of Tables

1. Introduction

This application note provides a state-of-the-art protection of the Flash contents against a fraudulent read-out of the flash contents and a guide to security settings on 8-bit, 16-bit and 32-bit NEC Electronics embedded flash microcontrollers (MCUs). The application note first explains which protection features are provided in different access modes and afterward guides through how to achieve a specific protection level by setting a security option.

For specific device security settings, reference the microcontroller's user manual, HEX Consolidation Utility user manual, PG-FP5 user manual and Self-Programming library application note for additional details.

2. Protection Features

The protection of the Flash contents is achieved by implementing a whole range of features. There are different channels to access the Flash which need to be considered independently:

- Flash Programming Interface, or the so called 'Serial Programming Mode'
- Debugging Interface
- Self-programming Mode
- Normal operation mode with instruction and data fetch from the flash

The protection of each of the access types is described independently as those protection features are quite independent of each other.

2.1 Flash Programming Interface

The Flash Programming Interface is active in the so called 'Serial Programming Mode' which allows the user to write to the internal flash memory of a virgin device or to reprogram a previously written device using an external programming tool. Those tools are either offered by NEC Electronics, PG-FP5, or by 3rd parties. As this is a generic interface which could also be misused for read-out attacks, special care was taken to offer a proper protection of this interface. The following protection flags are available:

- Chip Erase
- Block Erase
- Program
- Read, where applicable
- Boot block cluster reprogramming

The disabling of those programming interface functions will have the following effects:

1. **Chip Erase**

   The disabling of this function will prevent any erasure of the internal device flash by a flash programmer. Neither single blocks nor the entire flash can be erased. Thus it is not possible to update the stored memory contents with a flash programmer. As the Self-programming operation is not influenced by this setting, it is possible to erase the flash memory in Self-programming mode, and perform an application update. Please note that this function does not increase the protection against a read-out of the flash contents. This option should only be set if any reprogramming of the device with a flash programmer should be prevented.

2. **Block Erase**

   By disabling the block erase, it is not possible to erase single or multiple blocks of the flash memory. When block erase is disabled, only chip erase is possible. The disabling of the block erase ensures that it is only possible to erase the complete flash memory. This ensures that no data remain in the device

when performing an application update. A malicious software, which would be downloaded into the device with a flash programmer will not be able to find remains of the old application.

3. **Program** [Note]

   By disabling program it is not possible to write any further data into the Flash memory. This feature prevents that a non-written area of the Flash is misused to store malicious software or to overwrite already written Flash areas with invalid data to cause software misbehavior.

4. **Read**

   Devices which offer a read command, also offer a flag to disable this command.

5. **Boot block cluster reprogramming**

   The disabling of this function will prevent any erasure of the internal device flash by a flash programmer and any erasure of the boot blocks by Self-programming. Thus, the boot blocks will behave like as read only memory (ROM) after activating this function.

Abovementioned security functions are also expressed as security flags such as Chip erase disable flag, Block erase disable flag, Write disable flag, Read disable flag, and Boot block cluster rewrite disable flag. Though different description among in documents, they are the same protection features. Section 3 will explain how to set these features for various protection levels.

Note: For flash programming in this document, program and write are interchangeable jargons and so do the same as reprogram and rewrite.

2.1.1 Implementation of flags

All above mentioned flags have no influence on the Self-programming operations except Boot block cluster reprogramming. Even if the flags are set, all operation can be performed in the Self-programming mode. Self-programming, nevertheless, cannot erase boot blocks when Boot block cluster reprogramming function is set. Example: When setting the block erase disable flag, single blocks cannot be erase via an external flash programming tool, but it is still possible to erase a single block, or a set of blocks, in the Self-programming mode. The flags are implemented in such a way that the communication protocol rejects any command which is prohibited by the flags. Furthermore, the programming hardware itself is also configured by the flags in such a way that any operation which is prohibited by the flags is not possible.

2.1.2 Recommendation for usage of flags

Out of those flags, the ‘Block Erase’, ‘Program’, and ‘Read’ flags are considered to be sufficient for an effective read-out protection. The ‘Chip Erase’ and ‘Boot block cluster reprogramming’ disable prevents a reprogramming in serial mode completely and should therefore be used with care.

2.2 Debugging Interface

For the debugging interface a 10 bytes password can be chosen which needs to be transmitted before the debugging interface can be used. For 32-bit device, V850 series, by setting the uppermost bit of this password to '0' it is possible to disable the interface completely. For 8-bit and 16-bit devices, On-chip debug option byte setting will determine whether debug operation is enable or disable. This option byte setting can also be set for additional protection to erase flash content in case of authentication fail.

2.3 Self-programming

The basic idea of Self-programming is to write data, which are already available in the RAM of the device, to the Flash memory. Thus, the application needs the ability to receive those data from the outside. In order to provide the greatest flexibility, there is no limitation on the communication channel to receive those data. Consequently, it is not possible to provide a dedicated protection of those channels by NEC Electronics, but partial protection can be done by Boot block cluster reprogramming and Flash Shield Window, which is explained in section 3.2.2. By setting Boot block cluster reprogramming function and/or Flash Shield Window, Self-programming cannot reprogram to specified flash memory area. It is up to the application program to ensure that those communication channels are not misused to gain an unwanted access to the flash and its contents.

2.4 Normal operation mode

During normal operation mode no data which have been fetched from the internal memory can be observed from the outside. As some application offer diagnostic functions, it needs to be ensured that those diagnostic functions are properly protected against a misuse.

2.5 Considerations when using Flash protection flags

2.5.1 Potential influence on the Bootswap function of V850 devices

The programming interface offers a single function to set the security flags. For V850 this command includes also a block number which is used either for the Boot cluster protection or for the Bootswap function. As this block number needs to be transmitted and as the original value of a blank device, which is 0xFF, is not possible, the activation of any security flag necessarily modifies the block number of the Bootswap function.

3. Security Option

Using NEC Electronics dedicated flash programmer PG-FP5 or third party programmer, application code in flash memory is secured by different levels of protection features. The following section will explain in detail on security option.

- Security Settings
- Protection configuration settings
- Setting security option

The security settings can also be set by Self-Programming. Using HEX Consolidation Utility software (HCU), the security settings can be merged with application code to single file and later utilized for factory programming. This section will explain on how to set these protections and their results of individual and combination of the setting.

3.1 Definition of Terms

- **Application code**
  Application code is an HEX file (i.e. program file) which is programmed without security option data into embedded flash memory.

- **[Erase] command**
  The Erase command erases the flash memory in the target device.

- **[Program] command**
  The Program command transmits the memory contents (program files) in the FP5 valid programming area to the target device and writes the programs to the embedded flash memory.

- **[Read] command**
  The Read command loads data on the embedded flash memory in the target device and saves it as a file. The read data can be saved in the Intel HEX format or Motorola HEX format

- **[Security] command**
  The Security command sets the security functions (security settings) for the target device.

- **[Get Security settings] command**
  The Get Security Settings command reads the setting of the security functions from the target device and displays the result in the PG-FP5 GUI. (*See Figure 4*)

- **ESF file**
  ESF file (customized setup file) contains the programming environment settings specific to the user environment. This ESF file is generated by PG-FP5 programmer and not compatible to SET file generated by former programmer, PG-FP4.

- **HCUHEX file**
  An HCUHEX file is created by HEX Consolidation Utility software for merging HEX files and option data.

3.2 Security Settings

NEC Electronics microcontroller has five security functions and Flash Shield Window in embedded flash memory for protection. The following are description of each security and flash shield window function.

3.2.1 Security function

1. **Disable Chip Erase**

   This security setting can prohibit erase command in Chip Operation mode (Chip erase command). Checked Disable Chip Erase box in Figure 3[b], which selects as checked option, activates Chip erase disable flag and can prohibit erasing entire embedded flash memory.

2. **Disable Block Erase**

   This security setting can prohibit erase command in Block Operation mode (Block erase command). Checked Disable Block Erase box in Figure 3 [b], which selects as checked option, activates Block erase disable flag and can prohibit erasing flash block via Programming Interface, but it does not affect on block erase by Self-Programming.

3. **Disable Program**

   This security setting can prohibit program command. Checked Disable Program box in Figure 3[b], which selects as checked option, activates Program disable flag and can prohibit program command, but it allows reprogramming by Self-Programming.

4. **Disable Read** [Note]

   This security setting can prohibit read command via Programming Interface. Checked Disable Read box in Figure 3[b], which selects as checked option, activates Read disable flag and can prohibit reading data from embedded flash memory via Programming Interface.

5. **Disable Boot block cluster reprogramming**

   This security setting can prohibit program command to boot blocks. Checked Disable Boot block cluster reprogramming box in Figure 3[b], which selects as checked option, activates Boot block cluster rewrite disable flag and can prohibit writing boot blocks. After setting this security function, Self-Programming can erase and write individual block except boot blocks.

Note: Disable Read setting is only accessible on supported device. If the device does not support this feature, Disable Read check box will dim in setup dialog box. Refer to specific device's *User Manual* for a detailed description.

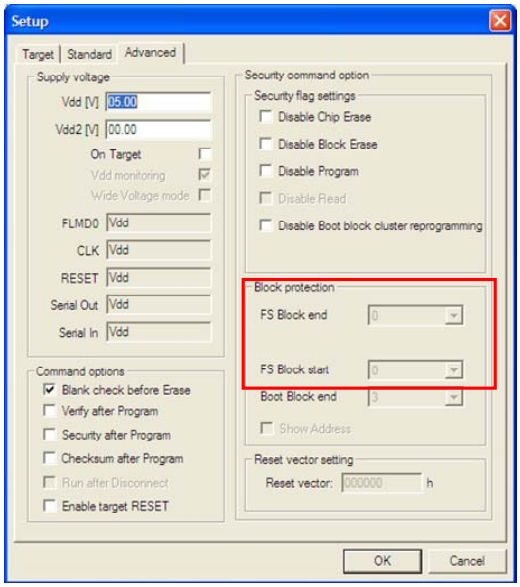
3.2.2 Flash shield window function

Flash shield window function can prevent writing and erasing flash memory area out of specified range in Self-Programming. The window, however, does not limit to Programming Interface command. The flash shield window range can be set or changed via start block and end block of flash memory either under Block protection area form programmer GUI (as shown in Figure 1) or in Self-Programming mode. The relationship between flash shield window function and Programming Interface commands is shown in Table 1. This function can only be available on supported device.

Table 1. Relationship between flash shield window function and Commands

Programming Conditions	Flash shield window range	Command	
		Block Erase	Program
Self-Programming	Specify window range by Self-Programming library function	Enable block erase within specified flash shield window range	Enable program within specified flash shield window range
Programming Interface	Specify window range under Block protection area in programmer GUI	No effect on specified flash shield window range	No effect on specified flash shield window range

Figure 1. Block protection area



Note: Block protection area is only accessible on supported device. If the device does not support this feature, the FS Block end and FS Block start check boxes will dim in Block protection area.

3.3 Protection configuration settings

Each security setting has different protection levels and one or more settings can be activated by selecting checked options in parallel to facilitate security functions. After selecting checked option to Disable Chip Erase function, the application code is impossible to update via Programming Interface; it, however, is possible to write by Self-Programming. The effects of Programming Interface commands and Self-Programming by security setting are shown in Table 3 and Table 4 respectively. Protection level, Interface commands and Self-Programming related to Security settings will be described in the following sections.

3.3.1 Security protection level

Basically, protection level can be set as irreversible or reversible setting. Once set to protection level to irreversible setting, the security setting cannot be changed to its original state. In contrast, protection level reversible setting can be possible to alter all security settings to default state by executing chip erase command. Only chip erase command by Programming Interface can alter all security settings to unchecked condition. The security protection level settings are shown in Table 2.

Table 2. Security protection level

Security Setting	Description	Protection Level Setting
Disable Chip Erase	Impossible to erase chip after setting checked option	Irreversible
Disable Boot block cluster reprogramming	Impossible to erase chip after setting checked option	Irreversible
Disable Program	Impossible to program after setting checked option	Reversible
Disable Block Erase	Impossible to erase block after setting checked option	Reversible
Disable Read	Impossible to read after setting checked option	Reversible

3.3.2 Relationship between security settings and Programming Interface command

Depending on security setting, programmer cannot execute any one or more of the Programming Interface commands. For example, by checking to Disable Program and Disable Block Erase boxes as shown in Figure 3[b], programmer can execute Chip erase command and Read command. If you also check to Disable Read box in previous setting, programmer can execute only Chip erase command. Any combination of security settings can be set for different protection levels. The relationship between security settings and Programming Interface commands for V850ES/Jx3-L is shown in Table 3. For specific relationship between security settings and Programming Interface commands, refer to respective device's *User Manual* for additional details.

Table 3. Relationship between security settings and Programming Interface commands

Security setting	Programming Interface command			
	Chip erase	Block erase	Program	Read
Disable Chip erase	Impossible	Impossible	Possible	Possible
Disable Block erase	Possible	Impossible	Possible	Possible
Disable Program	Possible	Impossible	Impossible	Possible
Disable Read	Possible	Possible	Possible	Impossible
Disable Boot block cluster reprogramming	Impossible	Possible[Note]	Possible[Note]	Possible

NOTE: All blocks other than boot blocks.

Impossible : Impossible to execute Programming Interface command after setting checked option
Possible : Possible to execute Programming Interface command after setting checked option

3.3.3 Effect of security setting on Self-Programming functions

All security settings do not affect on Self-Programming except Disable Boot block cluster reprogramming function. Selecting checked option to Disable Boot block cluster reprogramming function prohibits erasing boot blocks so that neither Chip erase command nor Self-Programming can erase the boot blocks. Disable Block erase function, nevertheless, does not affect on blocks except boot blocks for both Programming Interface and Self-Programming. Refer to the device self flash programming library *User Manual* for detailed description.

Table 4. Relationship between security settings and Self-Programming

Security setting	Self-Programming function
Disable Chip erase	No effect on Self-Programming functions after setting checked option
Disable Block erase	
Disable Program	
Disable Read	
Disable Boot block cluster reprogramming	Effect on block erase and write functions to boot block clusters after setting checked option.

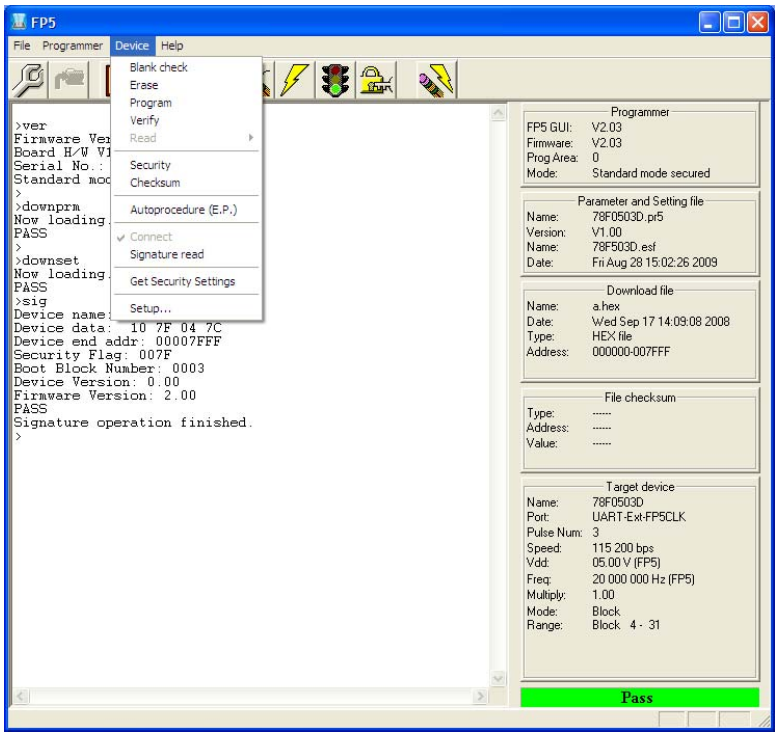
3.4 Setting security option

The security settings can be set in three ways – Programming Interface, HEX Consolidation Utility software and Self-Programming. Programming Interface can set security option using on-board or off-board programming. HEX Consolidation Utility software, on the other hand, allows setting security option in edit mode for factory programming, and Self-Programming can set by self flash programming library when device is executing application code. If HEX Consolidation Utility software cannot support the device, manual security setting will be processed with printed form known as Option Release Form. The form is only available on regional support and contact regional representative for availability. In case of online File Transfer System is available in that region, use online in stead of printed form. For example, the online system can be available at https://romcode.eu.necel.com/rcts/ for Europe region.

3.4.1 Setting security option by Programming Interface

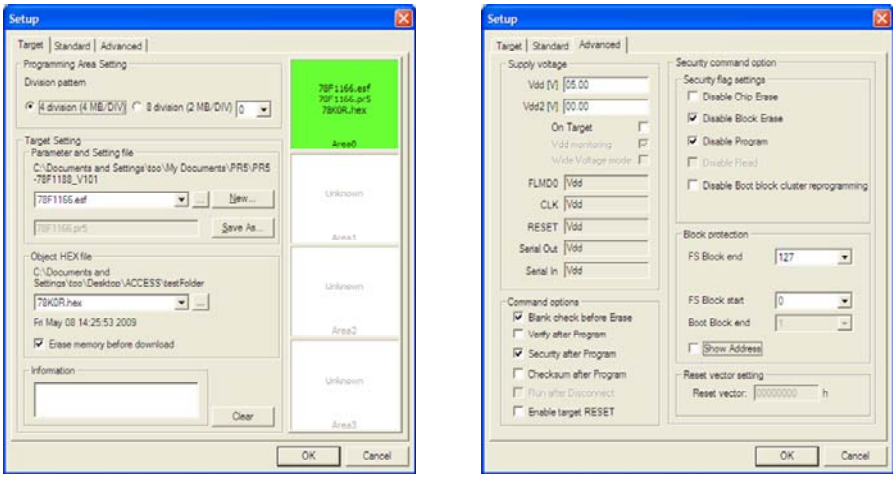
PG-FP5 programmer allows you to set the security option and program application code. To set security option, select setup command under Device pull-down menu from Main window as shown in Figure 2. Setup Dialog box will prompt for setting option data. Select Advanced Tab for selecting Security flag settings – refer to Figure 3 [a] and [b]. Checked appropriate boxes in Security flag settings area will activate the respective security functions. The setting will be saved in ESF file after clicking OK button and back to Main window.

Figure 2. Main Window



Either executing security command under Device pull-down menu or clicking security icon will program the option data to embedded flash memory. Since option data is set differently from Application code, it cannot be written by Program command. Alternatively, executing Program command does not program the Security flag settings. Security command, however, will execute automatically after executing Program command if select checked option to “Security after Program” in Command options, which shown in Figure 3[b].

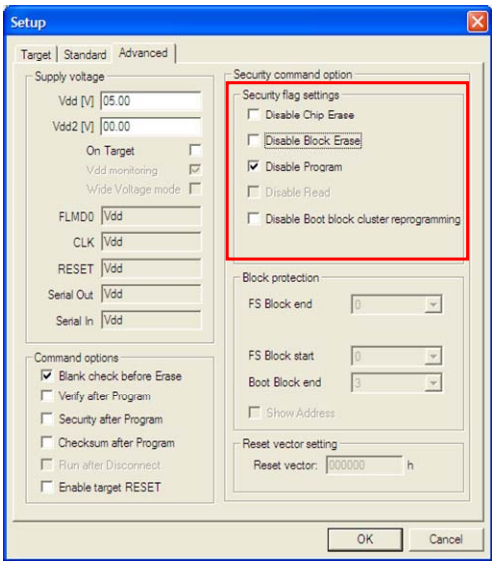
Figure 3. Device Setup Dialog Box



[a] Target Tab [b] Advanced Tab

For retrieving security option from target device, select Get Security Settings command under Device pull-down menu and Setup dialog box will prompt with programmed Security flag settings as shown in Figure 4. In this dialog box, clicking OK button will store up-loaded option data to ESF file and revise the previous setting. Refer to PG-FP5 *User Manual* for a more detailed description.

Figure 4. Security flag settings from target device



3.4.2 Setting security by HEX consolidation utility

HEX Consolidation Utility software (HCU) is a program that combines application code and option data into single HCUHEX file. This program has two modes: Edit mode and Check mode. Edit mode allows you to set security option, and Check mode can review the setting. To set security option, first, run HCU program and select Edit mode from HCU Main selection box, and then click OK button. Second selection box (see Figure 6[a]) will prompt for selecting parameter meter file, hex file and option data. After selecting parameter file and hex file, third selection box shown in Figure 6[b] will prompt for option data selection. Select Set Option data and click OK button. The Option data dialog box will open to set security option. Checked respective boxes in Security flag settings, shown in Figure 7, will activate the respective security functions. Finally, click OK buttons to generate consolidated HCUHEX file and ready for programming. After consolidating application code and option data, the HCUHEX file is needed to verify with PG-FP5 or MINICUBE2 by programming to the selected device. Refer to the HEX Consolidation Utility software *User Manual* for more details.

Figure 5. HCU Main selection box

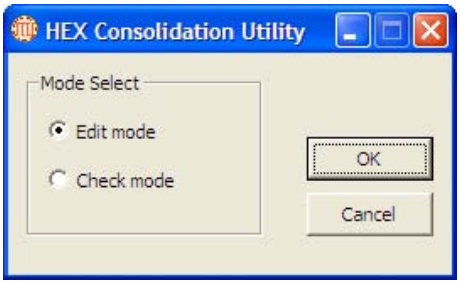
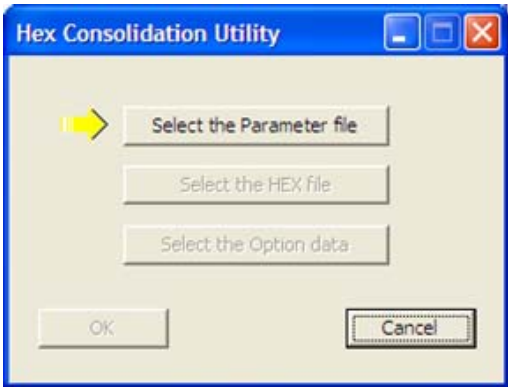
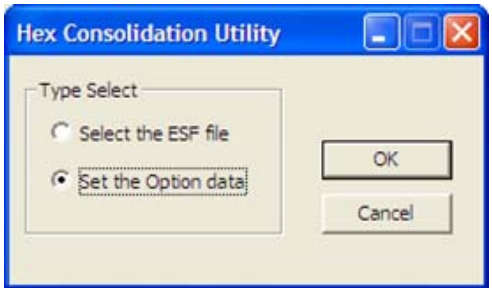


Figure 6. HCU selection box

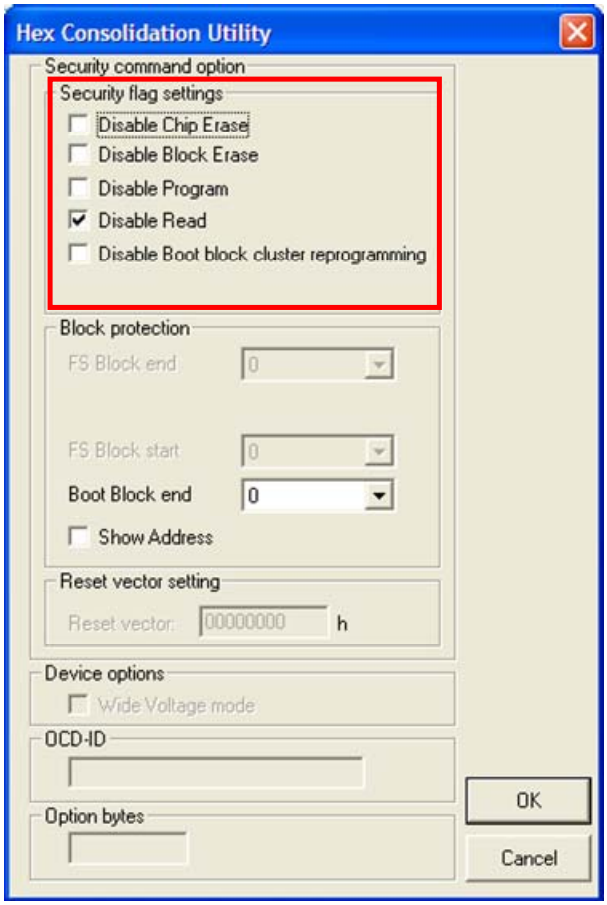


(a)



(b)

Figure 7. HCU Option data dialog box



3.4.3 Setting security settings by Self-Programming

In Self-Programming mode, security option can be set by self flash programming library. Using specific library function calls, individual security function can be activated, but it cannot be reversed by the library. Refer to self flash programming library *User Manual* for a more detailed description.

3.4.4 Setting security option by Option Release Form

For factory programming, if HEX Consolidation Utility software does not support to an intended device, manual entry will be used for setting security option. In this case, NEC Electronics will issue an Option Release Form for each Application code. A sample Option Release Form is shown in Figure 9. Follow the specific instructions on provided Option Release Form for accuracy. For option data setting, the sample form has a couple of groups list from 002 to 005 for Security flag settings and from 007 to 022 for Block protection. Mark with “01” for unchecked option or “02” for checked option in the appropriate bracket to deactivate or activate the security functions respectively. In the Option Release Form, flash shield block start and end values are expressed in binary format for selecting block number. Set bit to one with writing “01” or reset bit to zero with writing “02” in respective bracket. As a sample demonstration, option data

setting in PG-FP5 setup is shown in Figure 8, and its related setting to Option Release form is listed in Table 5. In this example, the Security flag settings permit Disable Boot block cluster reprogramming and Disable Chip erase command via Programming Interface. The Flash Shield Window setting also allows you to rewrite flash memory from 1800H (start address of block 3) to 3C7FFH (end address of block 120) in Self-programming mode.

Figure 8. Example of the option data settings in PG-FP5 and its Flash Shield Window memory map

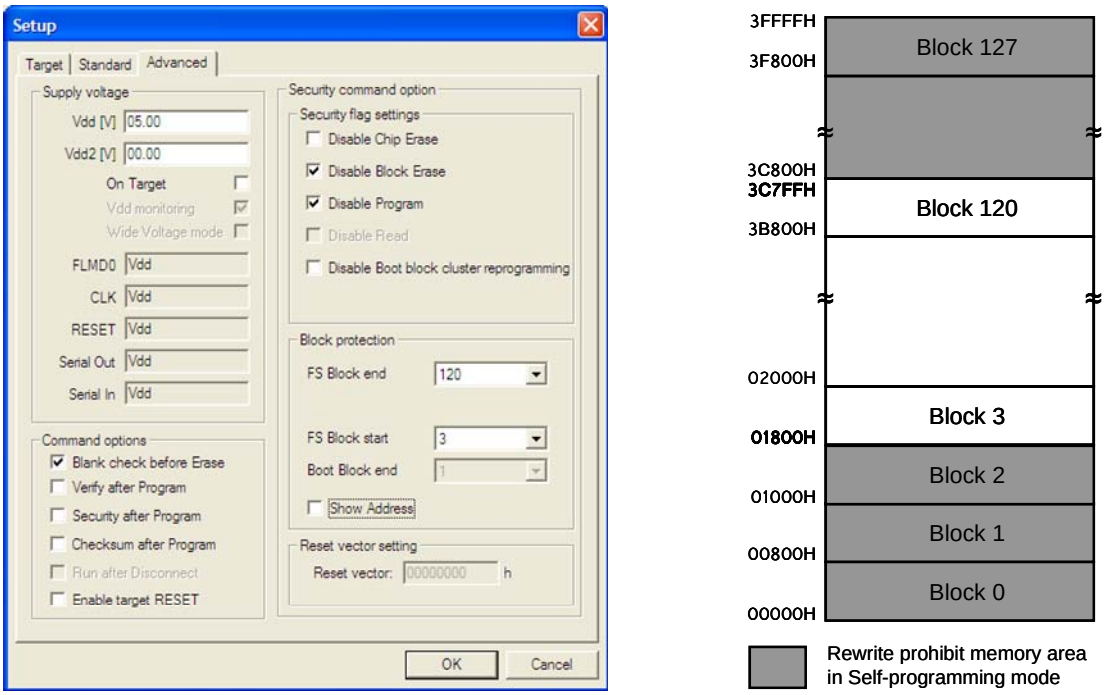
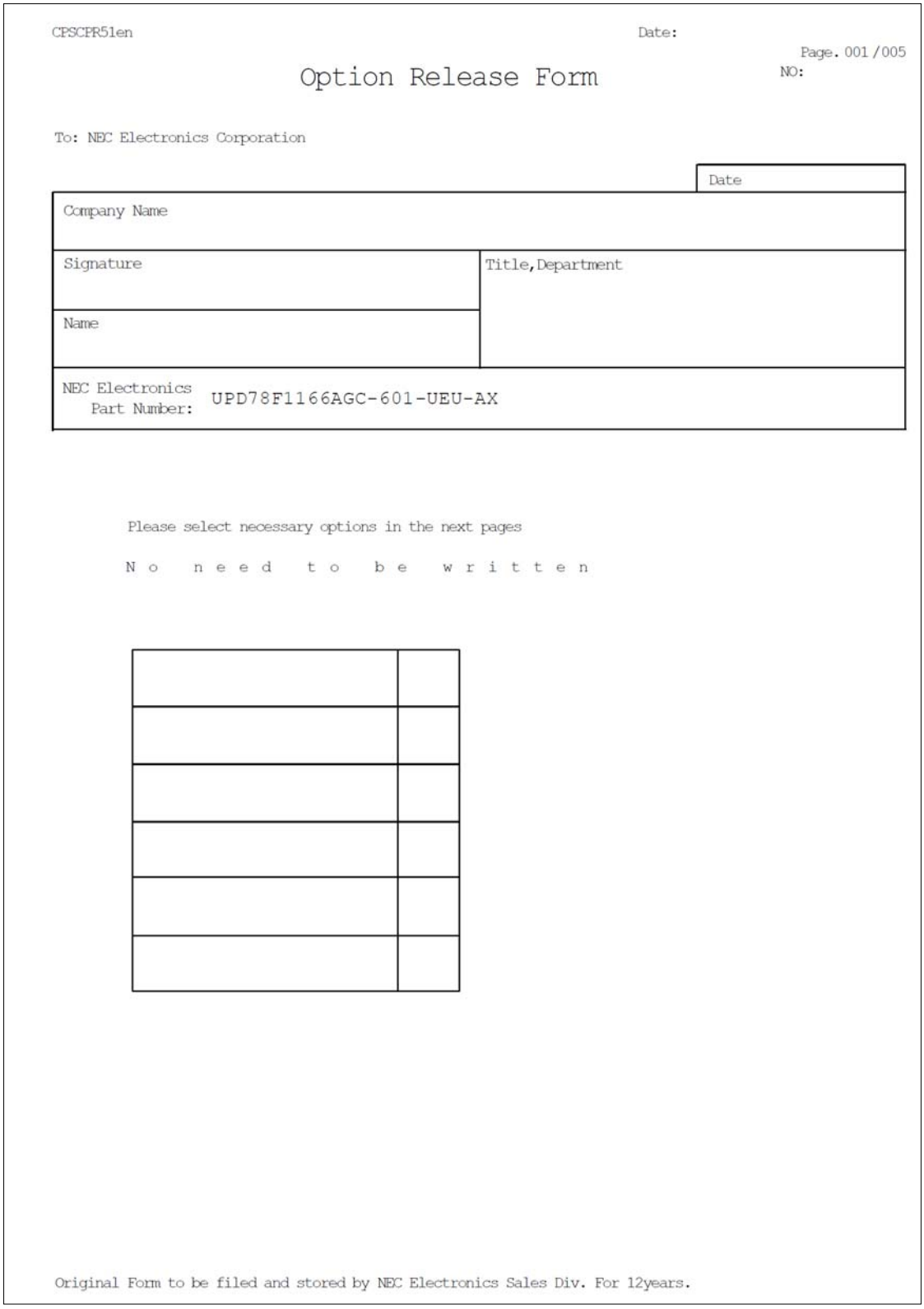


Table 5. Example of relationship between PG-FP5 setup and Option Release Form setting

PG-FP5		Option Release Form									
Disable Boot block cluster reprogramming	unchecked	**002**	Disabling rewriting boot cluster 0 flag	**[01]**	enabled boot block cluster 0 rewriting						
Disable Block erase	checked	**003**	Disabling block erase flag	**[02]**	disabled block erase						
Disable Chip erase	unchecked	**004**	Disabling batch erase flag	**[01]**	enabled batch erase “chip erase”						
Disable Program	checked	**005**	Disabling write flag	**[02]**	disabled write						
Disable Read											
FS Block start	3	**007-014**	Flash Shield Window start block (binary)	**(007) Bit-7**	**(008) Bit-6**	**(009) Bit-5**	**(010) Bit-4**	**(011) Bit-3**	**(012) Bit-2**	**(013) Bit-1**	**(014) Bit-0**
				[02]	**[02]**	**[02]**	**[02]**	**[02]**	**[02]**	**[01]**	**[01]**
FS Block end	120	**015-022**	Flash Shield Window start block (binary)	**(015) Bit-7**	**(016) Bit-6**	**(017) Bit-5**	**(018) Bit-4**	**(019) Bit-3**	**(020) Bit-2**	**(021) Bit-1**	**(022) Bit-0**
				[02]	**[01]**	**[01]**	**[01]**	**[01]**	**[02]**	**[02]**	**[02]**
Boot Block end											

Figure 9. Option Release Form



CPSCPR51en

Date:

Page. 001 /005

NO:

Option Release Form

To: NEC Electronics Corporation

	Date
Company Name	
Signature	Title,Department
Name	
NEC Electronics Part Number:	UPD78F1166AGC-601-UEU-AX

Please select necessary options in the next pages

N o n e e d t o b e w r i t t e n

Original Form to be filed and stored by NEC Electronics Sales Div. For 12years.

CPSCPR52en Date: Thu Sep
Page. 002 /005
NO:

Option data

Title: option 1 /
UPD78F1166AGC-601-UEU-AX

Please choose the corresponding number and fill in the brackets.

Plese specify the following options.
For Blank-ROM product with special marking,
please set all security option such as rewriting boot cluster 0,
block erase, batch erase"chip erase" and writing should be enabled,
set the flash shield window"FSW" start block to "00H",
and set the FSW end block to "7FH".

0 0 2) disabling rewriting boot cluster 0 flag ----------[01]

0 1 enabled boot cluster 0 rewriting

0 2 disabled boot cluster 0 rewriting

0 0 3) disabling block erase flag ----------[02]

0 1 enabled block erase

0 2 disabled block erase

0 0 4) disabling batch erase flag ----------[01]

"chip erase"

0 1 enabled batch erase "chip erase"

0 2 disabled batch erase "chip erase"

0 0 5) disabling write flag ----------[02]

0 1 enabled write

0 2 disabled write

0 0 7) flash shield window start block ----------[02]

Bit 7 of block number(BIN)

0 1 Bit 7 = 1

0 2 Bit 7 = 0

Original Form to be filed and stored by NEC Electronics Sales Div. For 12years.

CPSCPR53en Date:

Page. 003/005

NO:

Option data

Title: option 2/

UPD78F1166AGC-601-UEU-AX

Please choose the corresponding number and fill in the brackets.

0 0 8) flash shield window start block ----------[02]

Bit 6 of block number(BIN)

0 1 Bit 6 = 1

0 2 Bit 6 = 0

0 0 9) flash shield window start block ----------[02]

Bit 5 of block number(BIN)

0 1 Bit 5 = 1

0 2 Bit 5 = 0

0 1 0) flash shield window start block ----------[02]

Bit 4 of block number(BIN)

0 1 Bit 4 = 1

0 2 Bit 4 = 0

0 1 1) flash shield window start block ----------[02]

Bit 3 of block number(BIN)

0 1 Bit 3 = 1

0 2 Bit 3 = 0

0 1 2) flash shield window start block ----------[02]

Bit 2 of block number(BIN)

0 1 Bit 2 = 1

0 2 Bit 2 = 0

0 1 3) flash shield window start block ----------[01]

Bit 1 of block number(BIN)

0 1 Bit 1 = 1

Original Form to be filed and stored by NEC Electronics Sales Div. For 12years.

CPSCPR53en Date:

Page. 004 / 005

NO:

Option data

Title: option 3 /

UPD78F1166AGC-601-UEU-AX

Please choose the corresponding number and fill in the brackets.

02 Bit 1 = 0

014) flash shield window start block ----------[01]

Bit 0 of block number(BIN)

01 Bit 0 = 1

02 Bit 0 = 0

015) flash shield window end block ----------[02]

Bit 7 of block number(BIN)

01 Bit 7 = 1

02 Bit 7 = 0

016) flash shield window end block ----------[01]

Bit 6 of block number(BIN)

01 Bit 6 = 1

02 Bit 6 = 0

017) flash shield window end block ----------[01]

Bit 5 of block number(BIN)

01 Bit 5 = 1

02 Bit 5 = 0

018) flash shield window end block ----------[01]

Bit 4 of block number(BIN)

01 Bit 4 = 1

02 Bit 4 = 0

Original Form to be filed and stored by NEC Electronics Sales Div. For 12years.

CPSCPR53en Date:

Page. 005 / 005

NO:

Option data

Title: option 4 / 4

UPD78F1166AGC-601-UEU-AX

Please choose the corresponding number and fill in the brackets.

0 1 9) flash shield window end block ----------[01]

Bit 3 of block number(BIN)

0 1 Bit 3 = 1

0 2 Bit 3 = 0

0 2 0) flash shield window end block ----------[02]

Bit 2 of block number(BIN)

0 1 Bit 2 = 1

0 2 Bit 2 = 0

0 2 1) flash shield window end block ----------[02]

Bit 1 of block number(BIN)

0 1 Bit 1 = 1

0 2 Bit 1 = 0

0 2 2) flash shield window end block ----------[02]

Bit 0 of block number(BIN)

0 1 Bit 0 = 1

0 2 Bit 0 = 0

Original Form to be filed and stored by NEC Electronics Sales Div. For 12years.

For more information, contact:

NEC Electronics Corporation
1753, Shimonumabe, Nakahara-ku,
Kawasaki, Kanagawa 211-8668,
Japan
Tel: 044-435-5111
http://www.necel.com/

[America]

NEC Electronics America, Inc.
2880 Scott Blvd.
Santa Clara, CA 95050-2554, U.S.A.
Tel: +1-408-588-6000
U.S. only: 1-800-366-9782
http://www.am.necel.com/

[Europe]

NEC Electronics (Europe) GmbH
Arcadiastrasse 10
40472 Düsseldorf, Germany
Tel: 0211-65030
http://www.eu.necel.com/

Hanover Office
Podbielski Strasse 166 B
30177 Hanover
Tel: 0 511 33 40 2-0

Munich Office
Werner-Eckert-Strasse 9
81829 München
Tel: 0 89 92 10 03-0

Stuttgart Office
Industriestrasse 3
70565 Stuttgart
Tel: 0 711 99 01 0-0

United Kingdom Branch
Cygnus House, Sunrise Parkway
Linford Wood, Milton Keynes
MK14 6NP, U.K.
Tel: 01908-691-133

Succursale Française
9, rue Paul Dautier, B.P. 52180
78142 Velizy-Villacoublay Cédex
France
Tel: 01-3067-5800

Sucursal en España
Juan Esplandiu, 15
28007 Madrid, Spain
Tel: 091-504-2787

Tyskland Filial
Täby Centrum
Entrance S (7th floor)
18322 Täby, Sweden
Tel: 08 638 72 00

Filiale Italiana
Via Fabio Filzi, 25/A
20124 Milano, Italy
Tel: 02-667541

The Netherlands
Limburglaan 5
5616 HR Eindhoven
The Netherlands
Tel: 040 265 40 10

[Asia & Oceania]

NEC Electronics (China) Co., Ltd
7th Floor, Quantum Plaza, No. 27 ZhiChunLu
Haidian
District, Beijing 100083, P.R.China
TEL: 010-8235-1155
http://www.cn.necel.com/

NEC Electronics Shanghai Ltd.
Room 2509-2510, Bank of China Tower,
200 Yincheng Road Central,
Pudong New Area, Shanghai P.R. China
P.C:200120
Tel: 021-5888-5400
http://www.cn.necel.com/

NEC Electronics Hong Kong Ltd.
12/F., Cityplaza 4,
12 Taikoo Wan Road, Hong Kong
Tel: 2886-9318
http://www.hk.necel.com/

Seoul Branch
11F., Samik Lavied'or Bldg., 720-2,
Yeoksam-Dong, Kangnam-Ku,
Seoul, 135-080, Korea
Tel: 02-558-3737

NEC Electronics Taiwan Ltd.
7F, No. 363 Fu Shing North Road
Taipei, Taiwan, R. O. C.
Tel: 02-2719-2377

NEC Electronics Singapore Pte. Ltd.
238A Thomson Road,
#12-08 Novena Square,
Singapore 307684
Tel: 6253-8311
http://www.sg.necel.com/

G05.12A