NEC

Application Note

78K0/78K0R/V850

8-, 16- and 32-bit Single-Chip Microcontroller

Flash Protection Features

Document No. U19330EE1V0AN00
Date published June 2008

Printed in Germany

Legal Notes

- **The information in this document is current as of May, 2008. 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 the 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 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 a customer's equipment shall be done under the full responsibility of the customer. NEC Electronics assumes 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 an 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 an NEC Electronics sales representative in advance to determine NEC Electronics' willingness to support a given application.

(Note)
(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).

Regional Information

Some information contained in this document may vary from country to country. Before using any NEC product in your application, please contact the NEC office in your country to obtain a list of authorized representatives anddistributors. They will verify:

- Device availability
- Ordering information
- Product release schedule
- Availability of related technical literature
- Development environment specifications (for example, specifications for third-party tools and components, host computers, power plugs, AC supply voltages, and so forth)
- Network requirements

In addition, trademarks, registered trademarks, export restrictions, and otherlegal issues may also vary from country to country.

NEC Electronics Corporation
1753, Shimonumabe, Nakahara-ku,
Kawasaki, Kanagawa 211-8668, Japan
Tel: 044 4355111
http://www.necel.com/

[America]

NEC Electronics America, Inc.
2880 Scott Blvd.
Santa Clara, CA 95050-2554,
U.S.A.
Tel: 408 5886000
http://www.am.necel.com/

[Europe]

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

United Kingdom Branch
Cygnus House, Sunrise Parkway
Linford Wood, Milton Keynes
MK14 6NP, U.K.
Tel: 01908 691133

Succursale Française
9, rue Paul Dautier, B.P. 52
78142 Velizy-Villacoublay Cédex
France
Tel: 01 30675800

Tyskland Filial
Täby Centrum
Entrance S (7th floor)
18322 Täby, Sweden
Tel: 08 6387200

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

Branch The Netherlands
Steijgerweg 6
5616 HS Eindhoven,
The Netherlands
Tel: 040 2654010

[Asia & Oceania]

NEC Electronics (China) Co., Ltd
7th Floor, Quantum Plaza, No. 27
ZhiChunLu Haidian District,
Beijing 100083, P.R.China
Tel: 010 82351155
http://www.cn.necel.com/

NEC Electronics Shanghai Ltd.
Room 2511-2512, Bank of China
Tower,
200 Yincheng Road Central,
Pudong New Area,
Shanghai 200120, P.R. China
Tel: 021 58885400
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/

NEC Electronics Taiwan Ltd.
7F, No. 363 Fu Shing North Road
Taipei, Taiwan, R.O.C.
Tel: 02 27192377

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

NEC Electronics Korea Ltd.
11F., Samik Lavied'or Bldg., 720-2,
Yeoksam-Dong, Kangnam-Ku, Seoul,
135-080, Korea Tel: 02-558-3737
http://www.kr.necel.com/

Table of Contents

Chapter 1 Introduction

NEC devices offer a state of the art protection of the Flash contents against a fraudulent read-out of the flash contents. This protection 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
- Selfprogramming Mode
- normal operation mode with instruction and data fetch from the flash

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

Chapter 2 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, 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

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

2.1 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 Selfprogramming operation is not influenced by this setting, it is possible to erase the flash memory in Selfprogramming 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.

2.2 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.

2.3 Program

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.

2.4 Read

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

2.5 Implementation of flags

All above mentioned flags have no influence on the Selfprogramming operations. Even if the flags are set, all operation can be performed in the Selfprogramming mode.

Example: When setting the block erase disable flags, 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 Selfprogramming 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.

2.6 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’ disable prevents a reprogramming in serial mode completely and should therefore be used with care.

Chapter 3 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. By setting the uppermost bit of this password to ‘0’ it is possible to disable the interface completely.

Chapter 4 Selfprogramming

The basic idea of Selfprogramming 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, NEC did not impose any limitations on the communication channel to receive those date. Consequently, it is not possible to provide a dedicated protection of those channels by NEC. 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.

Chapter 5 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.

Chapter 6 Considerations when using Flash protection flags

6.1 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 Bootcluster 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.