Application Note, V1.0, Jul. 2006

AP08049

XC886/888CLM

Migration of Flash to ROM Device: Memory Protection Configurations

Microcontrollers

Never stop thinking

Edition 2006-07

Published by
Infineon Technologies AG
81726 München, Germany

LEGAL DISCLAIMER

THE INFORMATION GIVEN IN THIS APPLICATION NOTE IS GIVEN AS A HINT FOR THE IMPLEMENTATION OF THE INFINEON TECHNOLOGIES COMPONENT ONLY AND SHALL NOT BE REGARDED AS ANY DESCRIPTION OR WARRANTY OF A CERTAIN FUNCTIONALITY, CONDITION OR QUALITY OF THE INFINEON TECHNOLOGIES COMPONENT. THE RECIPIENT OF THIS APPLICATION NOTE MUST VERIFY ANY FUNCTION DESCRIBED HEREIN IN THE REAL APPLICATION. INFINEON TECHNOLOGIES HEREBY DISCLAIMS ANY AND ALL WARRANTIES AND LIABILITIES OF ANY KIND (INCLUDING WITHOUT LIMITATION WARRANTIES OF NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY) WITH RESPECT TO ANY AND ALL INFORMATION GIVEN IN THIS APPLICATION NOTE.

Information

For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office (**www.infineon.com**).

Warnings

Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies Office.

Infineon Technologies Components may only be used in life-support devices or systems with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

XC886/888CLM

Revision History: V1.0, 2006-07

Previous Version(s):
none

Page	Subjects (major changes since last revision)

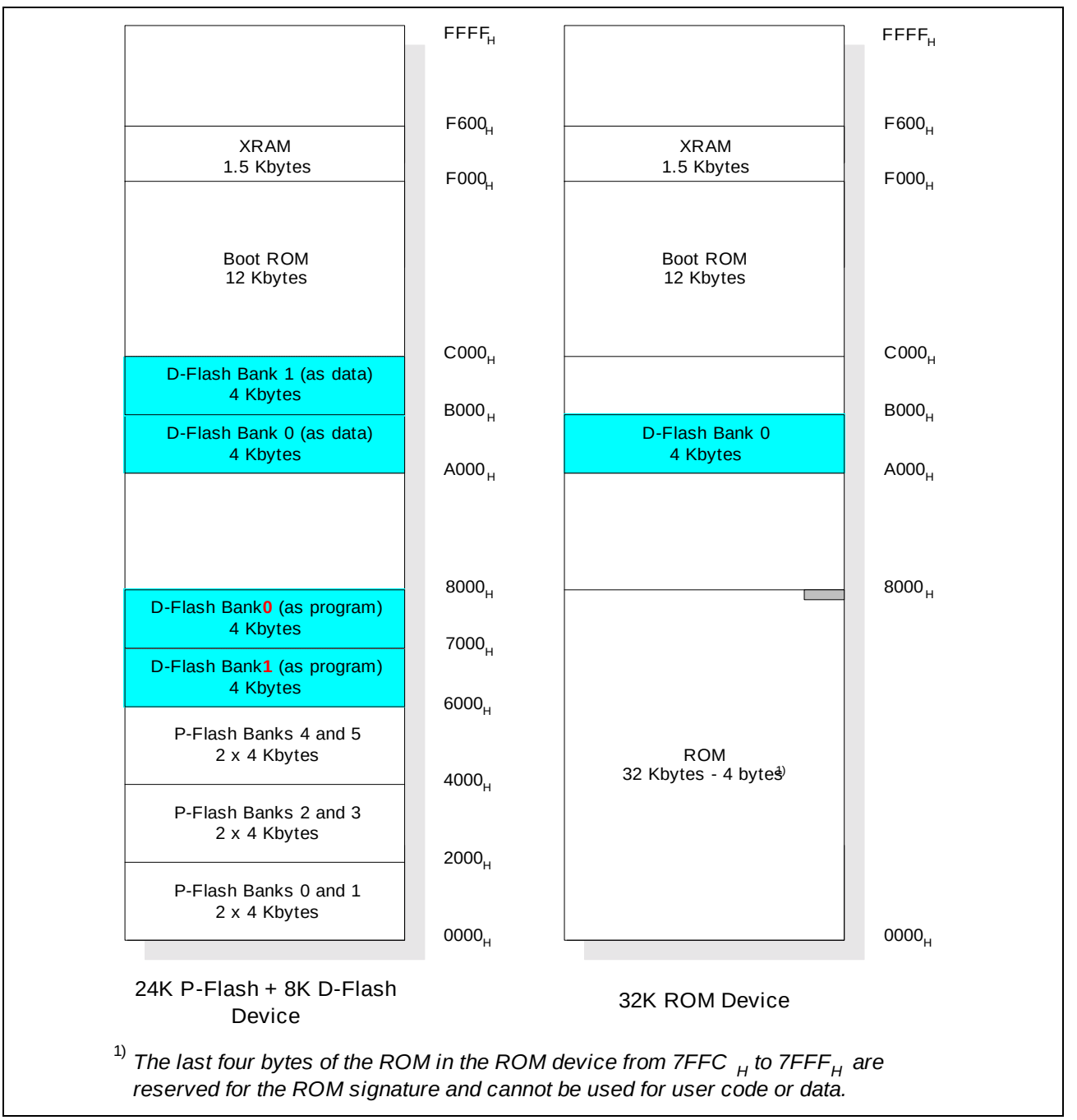
We Listen to Your Comments
Any information within this document that you feel is wrong, unclear or missing at all? Your feedback will help us to continuously improve the quality of this document. Please send your proposal (including a reference to this document) to:
mcdocu.comments@infineon.com

1 Introduction

This Application Note serves as a guideline for memory protection considerations when migrating from a XC886/888 Flash device to a XC886/888 ROM device.

The XC886/888 product family offers both Flash and ROM devices with either 24 Kbytes or 32 Kbytes of program memory. For Flash devices, this consists of several P-Flash and D-Flash banks, while for ROM devices, this consists of a single ROM block.

Figure 1 shows the memory maps of 32-Kbyte Flash and ROM devices.



1) *The last four bytes of the ROM in the ROM device from 7FFC $_H$ to 7FFF$_H$ are reserved for the ROM signature and cannot be used for user code or data.*

Figure 1 Memory Maps of 32 Kbyte Flash and ROM Devices

Introduction

ROM devices have an additional 4-Kbyte D-Flash bank on top of the 24- or 32-Kbyte ROM size. However, the last four bytes of the ROM ($7FFC_H$ to $7FFF_H$ in both 24- and 32-Kbyte variants) are reserved for the ROM signature and cannot be used to store user code or data.

Note: Although the ROM device contains either a 24- or 32-Kbyte ROM, the maximum size of code that can be placed in the ROM is the given size less 4 bytes.

Note: If a Flash to ROM device migration is being considered, user should not use the 4 bytes from $7FFC_H$ to $7FFF_H$ in the Flash device.

When migrating from a Flash to ROM device, it is possible to put all of the code (up to 32 Kbytes less 4 bytes) from the Flash device (whether it is in P-Flash or D-Flash) inside the ROM. **Table 1** and **Table 2** show two examples of Flash to ROM migration.

Table 1 Example 1: Migrating from 32-Kbyte Flash to ROM Device (27 Kbytes of Code and 5 Kbytes of Data)

Flash Device Configuration	→	ROM Device Configuration
Code size: 27 Kbytes	→	Code size: 27 Kbytes
Data size: 5 Kbytes	→	Data size: 4 Kbytes (ROM device only has 4 Kbytes of D-Flash memory)
Physical memory used for code: All 24 Kbytes of P-Flash + 3 Kbytes of D-Flash bank 1	→	Physical memory used for code: 27 Kbytes of ROM
Physical memory used for data: All 4 Kbytes of D-Flash bank 0 + 1 Kbyte of D-Flash bank 1	→	Physical memory used for data: All 4 Kbytes of D-Flash bank

Table 2 Example 2: Migrating from 32-Kbyte Flash to ROM Device (31 Kbytes of Code and 1 Kbyte of Data)

Flash Device Configuration	→	ROM Device Configuration
Code size: 31 Kbytes	→	Code size: 31 Kbytes
Data size: 1 Kbyte	→	Data size: 1 Kbyte
Physical memory used for code: All 24 Kbytes of P-Flash + All 4 Kbytes of D-Flash bank 1 + 3 Kbytes of D-Flash bank 0	→	Physical memory used for code: 31 Kbytes of ROM
Physical memory used for data: 1 Kbyte of D-Flash bank 0	→	Physical memory used for data: 1 Kbyte of D-Flash bank

2 Memory Protection Scheme

The protection scheme of XC886/888 is based on the single byte password, which is programmable by user via BSL mode 6.

Once a valid password (user-defined password field must be non-zero) has been programmed, all external access to the device will be blocked. This will automatically disable the debug mode as well.

The format of the user programmable password is shown in **Table 3**.

Table 3 User Programmable Password Bit Fields

Bits	Size	Usage	Value
7	1-bit	Flash hardware protection mode selection bit	0 Flash hardware protection mode 0 is selected. 1 Flash hardware protection mode 1 is selected.
6:5	2-bit	Select field for Flash banks to be erased during unprotection	This field has no effect if Flash hardware protection mode 1 is selected (bit 7 = 1). In this mode, all Flash banks will be erased during unprotection. 00 Only P-Flash banks are erased during unprotection. 01 P-Flash banks and D-Flash bank 0 are erased during unprotection. 10 P-Flash banks and D-Flash bank 1 are erased during unprotection. 11 All Flash banks (P-Flash and D-Flash) are erased during unprotection.
4	1-bit	Flash hardware protection enable bit	0 Flash hardware protection will not be activated. 1 Flash hardware protection will be activated. *Note: For ROM devices, this bit refers to protection from accidental erase of D-Flash, i.e. DFLASHEN bit must be set to 1 prior to each erase operation.*
3:0	4-bit	User-defined password field	This password field must be a non-zero value.

Note: For ROM devices, bits 5 to 7 are not applicable and should be written with zeros.

Memory Protection Scheme

BSL mode 6, which is used for enabling memory protection, can also be used for disabling memory protection for the Flash device. Here, the programmed password must be provided by the user. A password match triggers an automatic erase of the protected P-Flash and D-Flash contents, including the programmed password. The memory protection is then disabled upon the next reset.

For the ROM device, the ROM is protected at all times and BSL mode 6 is used only to block external access to the device. However, unlike the Flash device, it is not possible to disable the memory protection of the ROM device. Here, entering BSL mode 6 will result in a protection error.

3 Memory Protection Configurations

To enable a smooth migration from Flash device to the ROM device, user is strongly encouraged to follow the suggestions shown in **Table 4**, **Table 5** and **Table 6** for the various code sizes. A different usage other than the recommendations below should be clarified with Infineon Technologies.

For code size less than or equal to 24 Kbytes, the recommended password bits [7:4] setting is shown in **Table 4**. This setting ensures full compatibility between Flash and ROM device.

Table 4 Recommendation For Code Size ≤ 24 Kbytes

Protection	Flash Device	ROM Device
Recommended setting of Password bits [7:4]	$0XX1_B$	0001_B
Disabling of Memory Protection (During Software Upgrade)	All P-Flash banks will be erased. Erase of D-Flash bank(s) depends on bits 5 to 7. See **Table 3**.	It is not possible to disable the memory protection in ROM devices.
Read Protection	P-Flash contents cannot be read from other address spaces including D-Flash. D-Flash contents can be read from any address space.	ROM contents can be read only by itself. D-Flash contents can be read from any address space.
Program Protection	P-Flash banks cannot be programmed. D-Flash banks can be programmed.	D-Flash bank can be programmed.
Erase Protection	P-Flash banks cannot be erased. D-Flash banks can be erased if DFLASHEN bit is set to 1 prior to each erase operation.	D-Flash bank can be erased if DFLASHEN bit is set to 1 prior to each erase operation.

For code size greater than 24 Kbytes, the recommended password bits [7:4] setting is shown in **Table 5**. It is required that all of the code in the Flash device is located inside the ROM for compatibility.

Table 5 Recommendation For Code Size > 24 Kbytes

Protection	Flash Device	ROM Device
Recommended setting of Password bits [7:4]	$XXX0_B$	0000_B
Disabling of Memory Protection (During Software Upgrade)	All P-Flash banks will be erased. Erase of D-Flash bank(s) depends on bits 5 to 7. See **Table 3**.	It is not possible to disable the memory protection in ROM devices.
Read Protection	Flash contents can be read from any address space.	ROM contents can be read only by itself. D-Flash contents can be read from any address space.
Program Protection	All Flash banks can be programmed.	D-Flash bank can be programmed.
Erase Protection	All Flash banks can be erased regardless of the value of DFLASHEN bit.	D-Flash bank can be erased regardless of the value of DFLASHEN bit.

Memory Protection Configurations

For code size equal to 32 Kbytes, there is no compatible configuration in the ROM device as the Flash memory can always be programmed and erased.

However, if all 32-byte of Flash contents can be moved to ROM, i.e. there is no D-Flash needed in the ROM device, the password bits [7:4] setting shown in **Table 6** may be used for compatibility.

Table 6 Recommendation For Code Size = 32 Kbytes

Protection	Flash Device	ROM Device
Recommended setting of Password bits [7:4]	$1XX1_B$	$000X_B$
Disabling of Memory Protection (During Software Upgrade)	All Flash banks will be erased.	It is not possible to disable the memory protection in ROM devices.
Read Protection	Flash contents can be read from any Flash address space.	ROM contents can be read only by itself. D-Flash contents can be read from any address space.
Program Protection	All Flash banks cannot be programmed.	D-Flash bank can be programmed.
Erase Protection	All Flash banks cannot be erased regardless of the value of DFLASHEN bit.	D-Flash bank can be erased. If bit 4 of password is 1, DFLASHEN needs to be set prior to each erase operation.

Note: In the ROM device, the ROM contents are always read protected regardless of password setting. If user still needs to read ROM contents during execution from D-Flash or XRAM, user needs to put a function in the ROM to be able to read the entire ROM content.

w w w . i n f i n e o n . c o m

Published by Infineon Technologies AG