Application Note

AN2206/D
Rev. 0, 11/2001

Security And Protection On The HCS12 Family

By Andy McKechan
Applications Engineering
East Kilbride, Scotland

Introduction

The purpose of this document is to allow users of HCS12 micro-controllers to understand the non –volatile memory (NVM) protection and the security scheme that is being implemented, including the potential pitfalls. It should be noted that although the 9S12DP256 scheme is used as an example, information included in this document will apply to all future HCS12 family members. This document reflects the status of the mask set 0K79X (Barracuda-2) onwards, and therefore some of the features mentioned are not included in mask set 0K36N (Barracuda-1). Additional information on the HCS12 family of microcontrollers can be found in the relevant specifications and also Engineering Bulletin EB386 which can be obtained from the following web site.

http://www.freescale.com

Protection

Protection is intended to guard the NVM against accidental changes which may be caused by run-away software. It can be bypassed in all special modes (Special Single Chip, Special Expanded or Special Peripheral Mode) until the next reset by writing to the FPROT or EPROT registers. The FPROT and EPROT registers are loaded from Flash and EEPROM respectively during reset.

In normal modes it is possible to write to the protection registers in order to change from the unprotected to the protected state but not from the protected to the unprotected state.

In order to remove the protection beyond the next reset the respective Flash or EEPROM locations must be erased and re-programmed.

freescale semiconductor

NOTE: *It should be noted that the erase size is 512 bytes for the flash and 4 bytes for the EEPROM, while the program size is 2 bytes.*

Flash Configuration

The Flash memory on the Barracuda is 256Kbytes in size and is made up of 4 64Kbyte blocks. Each 64K byte flash block is arranged in a 32K x 16- bit configuration and may be read either as bytes, aligned words or misaligned words. To make the number of Flash blocks easily scalable, 8 out of the 12 control registers are banked as shown in Figure 1. Each bank is associated with a Flash block. The register banks are selected by setting the BKSEL bits in the Flash Configuration Register (FCNFG).

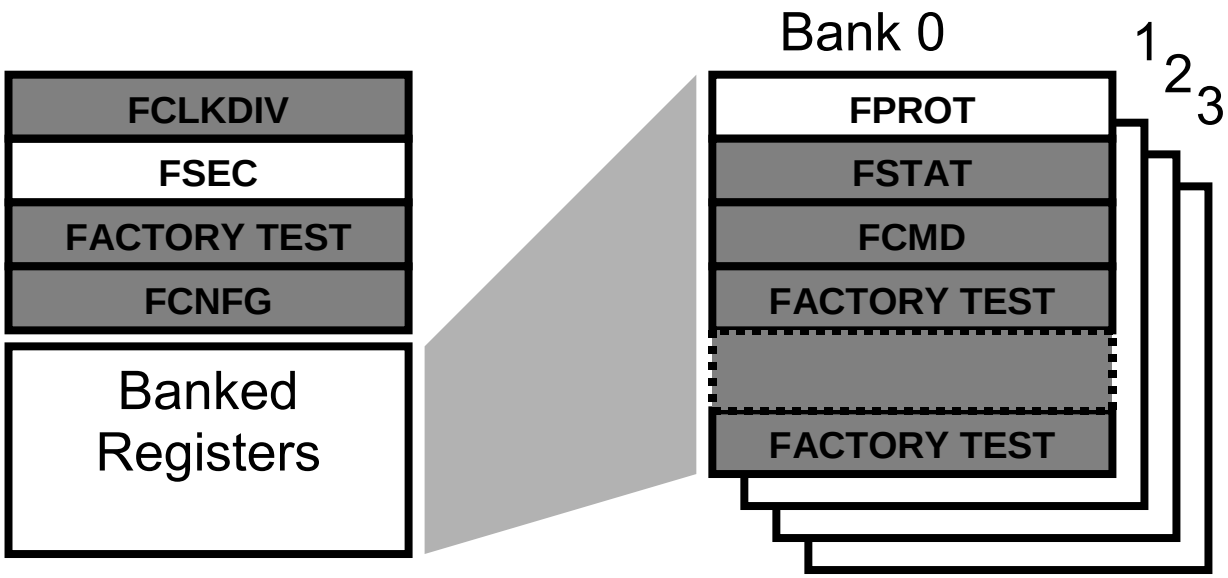

Figure 1. Flash Configuration

Flash Protection

Flash Block 0 contains 16 bytes of protection and security information situated from $FF00 to $FF0F. The details of these bytes are given in the following table.

Table 1. Flash 0 Protection/Security Field

ADDRESS	SIZE	DESCRIPTION
$FF00 – $FF07	8	Backdoor Comparison Key
$FF08–$FF09	2	Reserved
$FF0A	1	Protection byte for Flash block 3
$FF0B	1	Protection byte for Flash block 2
$FF0C	1	Protection byte for Flash block 1
$FF0D	1	Protection byte for Flash block 0
$FF0E	1	Reserved
$FF0F	1	Security byte

Each block of flash contains one protection register (FPROT) which is loaded from Flash block 0 during the reset phase. There is no protection activated in the erased state.

FPROT Register (Base + $0104)

The FPROT register defines which Flash sectors are protected against program or erase. This register is banked.

Bit 7	6	5	4	3	2	1	0
FPOPEN	–	FPHDIS	FPHS1	FPHS0	FPLDIS	FPLS1	FPLS0

FPOPEN, FPHDIS and FPLDIS bits in the FPROT register can only be written to the protected state (i.e. 0). FPLS[1:0] can be written anytime until bit FPLDIS is cleared. FPHS[1:0] bits can be written anytime until bit FPHDIS is cleared. If the FPOPEN bit is cleared, then the state of the FPHDIS, FPHS[1:0], FPLDIS and FPLS[1:0] bits is irrelevant. The FPROT register is loaded from Flash array during reset according to the following table.

Flash Address	Protection byte for
$FF0D	Flash 0
$FF0C	Flash 1
$FF0B	Flash 2
$FF0A	Flash 3

FPOPEN — Opens the flash block or subsections of it for program or erase.
1 = The flash block or subsections are enabled to program or erase.
0 = The whole flash block is protected. In this case the other bits within the protect register are don't care.

FPHDIS — Flash Protection Higher address range disable

This bit determines whether there is a protected area at the higher end of the flash block address map.
1 = Protection disabled
0 = Protection enabled

FPHDIS = 0 and FPHS[1:0] determine the size of the higher protection area (growing downwards from the top of the Flash area)

Table 2. Higher Address Range Protection

FPHS[1:0]	Flash Block	PPAGE	Protected Address Range	Protected Area Size (bytes)
00	0	Unpaged ($3F)	$F800–$FFFF	2K
01	0	Unpaged ($3F)	$F000–$FFFF	4K
10	0	Unpaged ($3F)	$E000–$FFFF	8K
11	0	Unpaged ($3F)	$C000–$FFFF	16K
00	0	$3F	$B800–$BFFF	2K
01	0	$3F	$B000–$BFFF	4K
10	0	$3F	$A000–$BFFF	8K
11	0	$3F	$8000–$BFFF	16K
00	1	$3B	$B800–$BFFF	2K
01	1	$3B	$B000–$BFFF	4K
10	1	$3B	$A000–$BFFF	8K
11	1	$3B	$8000–$BFFF	16K
00	2	$37	$B800–$BFFF	2K
01	2	$37	$B000–$BFFF	4K
10	2	$37	$A000–$BFFF	8K
11	2	$37	$8000–$BFFF	16K
00	3	$33	$B800–$BFFF	2K
01	3	$33	$B000–$BFFF	4K
10	3	$33	$A000–$BFFF	8K
11	3	$33	$8000–$BFFF	16K

FPLDIS — Flash Protection Lower address range disable

This bit determines whether there is a protected area at the lower end of the flash block address map.

1 = Protection disabled
0 = Protection enabled

FPLDIS = 0 and FPLS[1:0] determine the size of the lower protection area (growing upwards from $4000)

Table 3. Lower Address Range Protection

FPLS[1:0]	Flash Block	PPAGE	Protected Address Range	Protected Area Size (bytes)
00	0	Unpaged ($3E)	$4000–$41FF	512
01	0	Unpaged ($3E)	$4000–$43FF	1K
10	0	Unpaged ($3E)	$4000–$47FF	2K
11	0	Unpaged ($3E)	$4000–$4FFF	4K
00	0	$3E	$8000–$81FF	512
01	0	$3E	$8000–$83FF	1K
10	0	$3E	$8000–$87FF	2K
11	0	$3E	$8000–$8FFF	4K
00	1	$3A	$8000–$81FF	512
01	1	$3A	$8000–$83FF	1K
10	1	$3A	$8000–$87FF	2K
11	1	$3A	$8000–$8FFF	4K
00	2	$36	$8000–$81FF	512
01	2	$36	$8000–$83FF	1K
10	2	$36	$8000–$87FF	2K
11	2	$36	$8000–$8FFF	4K
00	3	$32	$8000–$81FF	512
01	3	$32	$8000–$83FF	1K
10	3	$32	$8000–$87FF	2K
11	3	$32	$8000–$8FFF	4K

EEPROM Protection

The EEPROM block is 4K byte in size, organised as 2048 x 16 bit words. The erase sector size is 4 bytes.

During the reset phase, the EEPROM Protection register (EPROT) is loaded from EEPROM relative address $0FFD. No protection is activated in the erased state.

EPROT Register (Base + $0114)

Bit 7	6	5	4	3	2	1	0
EPOPEN	–	–	–	EPDIS	EP2	EP1	EP0

EPOPEN — Opens the EEPROM block or a subsection of it for program or erase.

1 = The EEPROM block or subsections are enabled to program or erase.
0 = The whole EEPROM block is protected. In this case the other bits within the protect register are don't care.

EPDIS — EEPROM Protection address range Disable.

The EPDIS bit determines whether there is a protected area in the space of the EEPROM address map.

1 = Protection disabled.
0 = Protection enabled.

EPDIS = 0 and EP[2:0] determine the size of the protection area growing downwards from the top of the EEPROM area.

Table 4. Address Range Protection

EP[2..0]	Protected Address Range	Protected Area Size (bytes)
000	$_FC0 – $_FFF	64
001	$_F80 – $_FFF	128
010	$_F40 – $_FFF	192
011	$_F00 – $_FFF	256
100	$_EC0 – $_FFF	320
101	$_E80 – $_FFF	384
110	$_E40 – $_FFF	448
111	$_E00 – $_FFF	512

Security

A good security scheme must serve two purposes. On one hand it must prevent under any circumstances, the reading or modification of valuable IP or data stored in NVM by any unauthorised person. On the other hand it must also allow authorised users to do the following -

- Execute programs and read the data
- Debug their software
- Analyse their programmed devices easily
- Re-program their devices in the field

Memory Security Implementation

The security register (FSEC) is loaded from the Flash Block 0 ($FF0F) during the reset phase.

FSEC Register (Base + $0101)

Bit 7	6	5	4	3	2	1	0
KEYEN	–	–	–	–	–	SEC01	SEC00

KEYEN — Enable backdoor key to security
1 = Backdoor key to security is enabled.
0 = Backdoor key to security is disabled.

SEC0 [1: 0] — memory security bits

Those two bits define the secure state of the device.

SEC0[1:0]	Security State
00	Secured
01	Secured
10	Unsecured
11	Secured

Operation of a Secured Device

- Normal single chip – In this mode the BDM is disabled.
- Special Single Chip (BDM) – This mode is disabled unless all of the NVMs are erased. The erased state is verified by firmware and it takes approximately 1 second before the BDM becomes active for an erased chip.
- Expanded mode (executing from external memory) – The internal Flash and EEPROM are disabled when this mode is used.

Unsecuring the Chip

There are a number of methods available for unsecuring a device.

Single Chip or Expanded modes:

The backdoor key access feature can be used. To implement this the KEYEN bit in the FSEC register must be set (i.e.loaded from $FF0Fon reset.) The keys are four 16-bit words programmed in the Flash 0 at addresses $FF00 – $FF07.

The customer must provide means to receive backdoor keys. The following example shows key 0–3 from an external stimulus (e.g. CAN, SCI, etc.)

```
movb    #KEYACC,FCNFG           ; enable security key writing
movw    key0,$FF00              ; write 64 bits in 4 words – in the correct sequence
movw    key1,$FF02              ; to the flash array
movw    key2,$FF04
movw    key3,$FF06              ; if keys match the Flash contents
movb    #0,FCNFG                ; the chip should be unsecured now
```

Any reset will cause the microcontroller to return to secure operation unless $FF0F is reprogrammed.

Special Single Chip Mode:

Execute a “Mass erase” by writing the sequence via BDM commands. “Mass erase” is the only command allowed in Special Single Chip for a secured device. This method would be most convenient for unsecuring a small number of devices on the bench. The following steps should be followed in order to perform a mass erase in this mode.

1. Write the required value to the FCLKDIV register (0x100)
2. Write 0x10 to the FTSTMOD register (0x102)
3. Write 0xFF to the FPROT register (0x104)
4. Write Array Address and Program Data
5. Write 0x20 to the FCMD register (0x106)
6. Write 0x80 to the FSTAT register (0x105)
7. Loop until the FSTAT register reads 0xC0

A similar procedure is available for the EEPROM The necessary steps are outlined below.

1. Write the required value to the ECLKDIV register (0x110)
2. Write 0xFF to the EPROT register (0x114)
3. Write Array Address and Program Data
4. Write 0x20 to the ECMD register (0x116)
5. Write 0x80 to the ESTAT register (0x115)
6. Loop until the ESTAT register reads 0xC0

Special Test mode:

Execute a “Mass erase” from external memory. Again, it is necessary to reprogram register $FF0F in order to fully unsecure the device.
This is the best method for erasing a large number of devices on the bench and would be suitable for programming houses. The mass erase procedures outlined in the Special Single Chip Mode section above should be used.

Summary

The HCS12 Family of microcontrollers have been designed to offer the maximum possible security of the EEPROM and Flash contents, while at the same time allowing certified users access to carry out important tasks. However, it is extremely important to realise that even the best security scheme can be by-passed if it has not been implemented correctly. Therefore great care should be taken within customer’s code to ensure that the available security scheme is utilised to its maximum potential.

This Page Is Intentionally Left Blank

This Page Is Intentionally Left Blank

[redacted]

How to Reach Us:

Home Page:
www.freescale.com

E-mail:
support@freescale.com

USA/Europe or Locations Not Listed:
Freescale Semiconductor
Technical Information Center, CH370
1300 N. Alma School Road
Chandler, Arizona 85224
+1-800-521-6274 or +1-480-768-2130
support@freescale.com

Europe, Middle East, and Africa:
Freescale Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
support@freescale.com

Japan:
Freescale Semiconductor Japan Ltd.
Headquarters
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku,
Tokyo 153-0064
Japan
0120 191014 or +81 3 5437 9125
support.japan@freescale.com

Asia/Pacific:
Freescale Semiconductor Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@freescale.com

For Literature Requests Only:
Freescale Semiconductor Literature Distribution Center
P.O. Box 5405
Denver, Colorado 80217
1-800-441-2447 or 303-675-2140
Fax: 303-675-2150
LDCForFreescaleSemiconductor@hibbertgroup.com

freescale™
semiconductor