Freescale Semiconductor
Application Note

Document Number: AN3821
Rev. 1, 2/2009

How to Handle Dual Flash Architecture in MC9S08LG32

by: Saurabh Jhamb
Reference Design and Applications Engineering
Microcontroller Solutions Group

1 Introduction

The MC9S08LG32 is a member of the low-cost, low-power, and high-performance HCS08 family of 8-bit microcontroller units (MCUs). It provides 32 KB of 8-bit flash in parts of two 16 KB blocks. Both the blocks are internally divided into 512 byte pages that are basic units for erasing the flash data.

The flash memory is intended primarily for program code storage. In-circuit programming allows the operating program to be loaded into the flash memory after final assembly of the application product. It is possible to program the entire array through the single-wire background debug interface. Because no special voltages are needed for flash erase and programming operations, in-application programming is also possible through other software-controlled communication paths.

MC9S08LG32 series MCUs contain two flash arrays; therefore program and erase operations can be conducted on one array while code executing from the other. The

Contents

security and protection features treat the two arrays as a single memory entity. It is not possible to page erase or program the array from which code is being executed. The mass erase command erases both arrays, and the blank check command checks both arrays. You cannot page erase or program both arrays at the same time.

Figure 1 shows the on-chip flash memory of MC9S08LG32 series of MCUs.

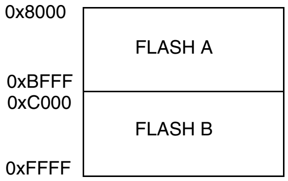


Figure 1. Flash Memory Map

2 Features

- Flash size
  - MC9S08LG32: 32,768 bytes (16,384 bytes in flash A, 16,384 bytes in flash B)
  - MC9S08LG16: 18,432 bytes (2,048 bytes in flash A, 16,384 in flash B)
- Flexible block protection
- Security feature for flash

3 Flash Configuration Registers

The flash module has six 8-bit registers for its configuration and status. Two locations (NVOPT, NVPROT) in the nonvolatile register space in flash memory are copied into corresponding high-page control registers (FOPT, FPROT) at reset.

3.1 Flash Clock Divider Register (FCDIV)

DIVLD is a read-only flag. DIV bits 6:0 may be read at any time, but can be written only one time.

	7	6	5	4	3	2	1	0
R	DIVLD	PRDIV8	DIV					
W	▨							
Reset	0	0	0	0	0	0	0	0

▨ = Unimplemented or Reserved

Figure 2. Flash Clock Divider Register (FCDIV)

Table 1. FCDIV Register Field Descriptions

Field	Description
7 DIVLD	**Divisor Loaded Status Flag** 0 FCDIV has not been written since reset; erase and program operations disabled for flash. 1 FCDIV has been written since reset; erase and program operations enabled for flash.
6 PRDIV8	**Prescale (Divide) Flash Clock by 8** 0 Clock input to the flash clock divider is the bus rate clock. 1 Clock input to the flash clock divider is the bus rate clock divided by 8.
5:0 DIV	**Divisor for Flash Clock Divider** — The flash clock divider divides the bus rate clock (or the bus rate clock divided by 8 if PRDIV8 = 1) by the value in the 6-bit DIV field plus one. See Equation 3-1 and Equation 3-2.

$$\text{if PRDIV8} = 0 \text{ — } f_{FCLK} = f_{Bus} \div (DIV + 1) \qquad \textit{Eqn. 3-1}$$

$$\text{if PRDIV8} = 1 \text{ — } f_{FCLK} = f_{Bus} \div (8 \times (DIV + 1)) \qquad \textit{Eqn. 3-2}$$

3.2 Flash Options Register (FOPT and NVOPT)

During reset, the contents of the nonvolatile location NVOPT are copied from flash into FOPT. To change the value in this register, erase and reprogram the NVOPT location in flash memory as usual and then issue a new MCU reset.

	7	6	5	4	3	2	1	0
R	KEYEN	FNORED	0	0	0	0	SEC01	SEC00
W	▨	▨	▨	▨	▨	▨	▨	▨
Reset	This register is loaded from nonvolatile location NVOPT during reset.							

▨ = Unimplemented or Reserved

Figure 3. Flash Options Register (FOPT)

Table 2. FOPT Register Field Descriptions

Field	Description
7 KEYEN	**Backdoor Key Mechanism Enable** 0 No backdoor key access allowed. 1 If user firmware writes an 8-byte value that matches the nonvolatile backdoor key (NVBACKKEY through NVBACKKEY+7 in that order), security is temporarily disengaged until the next MCU reset.
6 FNORED	**Vector Redirection Disable** 0 Vector redirection enabled. 1 Vector redirection disabled.
1:0 SEC0[1:0]	**Security State Code** — This 2-bit field determines the security state of the MCU as shown in Table 3.

Table 3. Security States[1]

SEC01:SEC00	Description
0:0	secure

Table 3. Security States[1] (continued)

SEC01:SEC00	Description
0:1	secure
1:0	unsecured
1:1	secure

[1] SEC01:SEC00 changes to 1:0 after successful backdoor key entry or a successful blank check of flash.

3.3 Flash Configuration Register (FCNFG)

	7	6	5	4	3	2	1	0
R	0	0	KEYACC	0	0	0	0	0
W	▨	▨		▨	▨	▨	▨	▨
Reset	0	0	0	0	0	0	0	0

▨ = Unimplemented or Reserved

Figure 4. Flash Configuration Register (FCNFG)

Table 4. FCNFG Register Field Descriptions

Field	Description
5 KEYACC	**Enable Writing of Access Key** 0 Writes to flash are interpreted as the start of a flash programming or erase command. 1 Writes to NVBACKKEY (0xFFB0–0xFFB7) are interpreted as comparison key writes while writes to rest of the flash are ignored.

3.4 Flash Protection Register (FPROT and NVPROT)

During reset, the contents of the nonvolatile location NVPROT are copied from flash into FPROT. With FPDIS set, all bits are writable, but with FPDIS clear, the FPS bits are writable as long as the size of the protected region is being increased. Any FPROT write that attempts to decrease the size of the protected region, is ignored.

	7	6	5	4	3	2	1	0
R	FPS[1]							FPDIS[1]
W								
Reset	This register is loaded from nonvolatile location NVPROT during reset.							

[1] Background commands can be used to change the contents of these bits in FPROT.

Figure 5. Flash Protection Register (FPROT)

Table 5. FPROT Register Field Descriptions

Field	Description
7:1 FPS	**Flash Protect Select Bits** — When FPDIS = 0, this 7-bit field determines the ending address of unprotected flash locations at the high address end of the flash.
0 FPDIS	**Flash Protection Disable** 0 Flash block specified by FPS7:FPS1 is block protected (program and erase not allowed). 1 No flash block is protected.

3.5 Flash Status Register (FSTAT)

	7	6	5	4	3	2	1	0
R	FCBEF	FCCF	FPVIOL	FACCERR	0	FBLANK	0	0
W		▨			▨	▨	▨	▨
Reset	1	1	0	0	0	0	0	0

▨ = Unimplemented or Reserved

Figure 6. Flash Status Register (FSTAT)

Table 6. FSTAT Register Field Descriptions

Field	Description
7 FCBEF	**Flash Command Buffer Empty Flag**—Flag to indicate the status of flash command buffer. 0 Command buffer is full (not ready for additional commands). 1 A new burst program command can be written to the command buffer.
6 FCCF	**Flash Command Complete Flag**—Flag to indicate the active execution of any flash command. 0 Command in progress. 1 All commands complete.
5 FPVIOL	**Protection Violation Flag** 0 No protection violation. 1 An attempt was made to erase or program a protected location.
4 FACCERR	**Access Error Flag** 0 No access error. 1 An access error has occurred.
2 FBLANK	**Flash Verified as All Blank (erased) Flag** 0 After a blank check command is completed and FCCF = 1, FBLANK = 0 indicates the flash array is not completely erased. 1 After a blank check command is completed and FCCF = 1, FBLANK = 1 indicates the flash array is completely erased (all 0xFF).

3.6 Flash Command Register (FCMD)

Only five command codes are recognized in normal user modes as shown in Table 7.

	7	6	5	4	3	2	1	0
R	0	0	0	0	0	0	0	0
W	FCMD							
Reset	0	0	0	0	0	0	0	0

Figure 7. Flash Command Register (FCMD)

Table 7. Flash Commands

Command	FCMD	Equate File Label
Blank check	0x05	mBlank
Byte program	0x20	mByteProg
Byte program — burst mode	0x25	mBurstProg
Page erase (512 bytes/page)	0x40	mPageErase
Mass erase (all flash)	0x41	mMassErase

All other command codes are illegal and generate an access error. It is not necessary to perform a blank check command after a mass erase operation. Only blank check is required as part of the security unlocking mechanism.

4 Flash Configuration

Flash frequency is supported between 150 kHz and 200 kHz and it must be programmed in the FCDIV register. FCDIV cannot be written if the access error flag, FACCERR in FSTAT, is set.You must ensure that FACCERR is not set before writing to the FCDIV register.

Flash block has two types of registers for configuration:

1. Nonvolatile Registers—There are three registers that are mapped to flash locations that make them nonvolatile, and are used for storing the reset configuration of flash. NVOPT and NVPROT registers are copied into FOPT and FPROT respectively at the time of reset.
   - NVPROT—This register is used for protection settings of available flash. It specifies whether protection is enabled at reset. It also provides (if protection enabled) the last unprotected address in the flash memory, after which all flash locations are write-protected. In erased form, protection is disabled.
   - NVOPT—This register provides various configuration options to flash. It specifies whether or not the backdoor key entry mechanism is on and vector redirection is enabled. Most importantly, it specifies the security status of flash at the time of reset.
   - NVBACKKEY[0-7]—This provides the 8-byte key to be matched when backdoor key entry mechanism is enabled (refer to NVOPT).
2. Volatile Registers—These are the registers which control the run-time configuration of flash.
   - FCDIV—This register configures the flash frequency. Flash frequency must lie in a range of 150 kHz – 200 kHz.

- FOPT—This register is a replica of NVOPT register, whose content is copied into FOPT register at reset. This is a read-only register.
- FCNFG—This register specifies whether the writes belong to flash addresses or the backdoor key is being entered. When key writes are enabled, all access of flash locations are ignored.
- FPROT—This register is a replica of NVPROT register, whose contents are copied into FPROT register at reset. If protection is enabled, then protected area can only be increased, but not decreased. All bits in this register are writable.
- FSTAT—This register conveys the state of flash in MC9S08LG32. It has flags for access violation, command complete, buffer empty, and flash blank flags, which notify the application about the flash status.
- FCMD—This is the register in which erase, write, blank check, etc., commands are written and thus sent to flash.

5 Flash Operation

Before any program or erase command can be accepted, the flash clock divider register (FCDIV) must be written to set the internal clock for the flash module to a frequency between 150 kHz and 200 kHz. This register can be written only once, so normally this write is done during reset initialization. The bus clock frequency and FCDIV determine the frequency of FCLK. The time for one cycle of FCLK is 1/FCLK.

6 Flash Security

The MC9S08LG32 series MCUs include circuitry to prevent unauthorized access to the contents of flash and RAM memory. When security is engaged, flash and RAM are considered secure resources. Programs executing within secure memory have normal access to any MCU memory locations and resources. Attempts to access a secure memory location with a program executing from an unsecured memory space or through the background debug interface are blocked (writes are ignored and reads return all 0s).

Security is engaged or disengaged based on the state of two nonvolatile register bits (SEC01:SEC00) in the FOPT register. During reset, the contents of the nonvolatile location NVOPT are copied from flash into the working FOPT register in high-page register space. To engage/disengage security, write SEC01:SEC00 bits in NVOPT registers with appropriate values and issue a MCU reset. The on-chip debug module cannot be enabled while the MCU is secure. The separate background debug controller can still be used for background memory access commands of unsecured resources.

Security is engaged after a mass erase command completion and the NVOPT register security bits should be programmed 0b10 to make flash permanently unsecure.

A blank check procedure immediately after a mass erase makes flash unsecure until the next reset.

7 Backdoor Key Entry Mechanism

There is a mechanism to disengage security for a single run on the fly using backdoor key entry mechanism. If KEYEN bit in NVOPT/FOPT is 1, then this method is enabled, else disabled. If KEYEN = 0, there is no way to disengage security without completely erasing all flash locations.

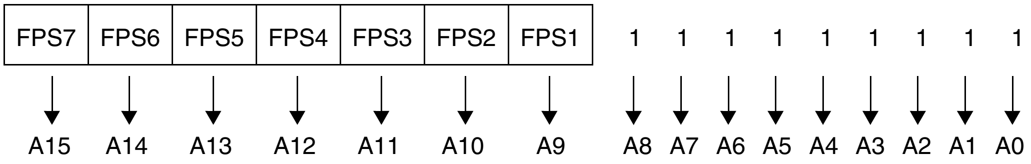
Following are the steps to disengage security temporarily:

1. Write 1 to KEYACC bit in FCNFG register to indicate that the next writes are interpreted as backdoor key.
2. Write the 8 bytes of the key at locations NVBACKKEY through NVBACKKEY+7, respectively.
3. Write 0 to KEYACC bit in FCNFG to indicate end of backdoor key entry.
4. Read security bits in FOPT. If SEC0[1:0] = 0x2, then key entered is correct and flash is unsecure until next reset, else key entered is invalid, flash is secure.

8 Flash Protection Mechanism

The block protection feature prevents the protected region of flash from program or erases. Block protection is controlled through the flash protection register (FPROT). When enabled, block protection begins at any 512-byte boundary below the last address of flash, 0xFFFF.

At reset, FPROT is loaded with the contents of NVPROT. FPROT cannot be changed directly from application software to prevent runaway programs from altering the block protection settings. Because NVPROT is within to the last 512 bytes of flash, if any amount of memory is protected, NVPROT is itself protected and cannot be altered (intentionally or unintentionally) by the application software. FPROT can be written through background debug commands that allows a protected flash memory to be erased and reprogrammed.



The FPS bits are used as the upper bits of the last address of unprotected memory. This address is formed by concatenating FPS7:FPS1 with logic 1 bits, as shown. For example, to protect the last 1536 bytes of memory (addresses 0xFA00 through 0xFFFF), the FPS bits must be set to 1111 100 that results in the value 0xF9FF as the last address of unprotected memory. In addition to programming the FPS bits to the appropriate value, FPDIS (bit 0 of NVPROT) must be programmed to logic 0 to enable block protection. Therefore, the value 0xF8 must be programmed into NVPROT to protect addresses 0xFA00 through 0xFFFF.

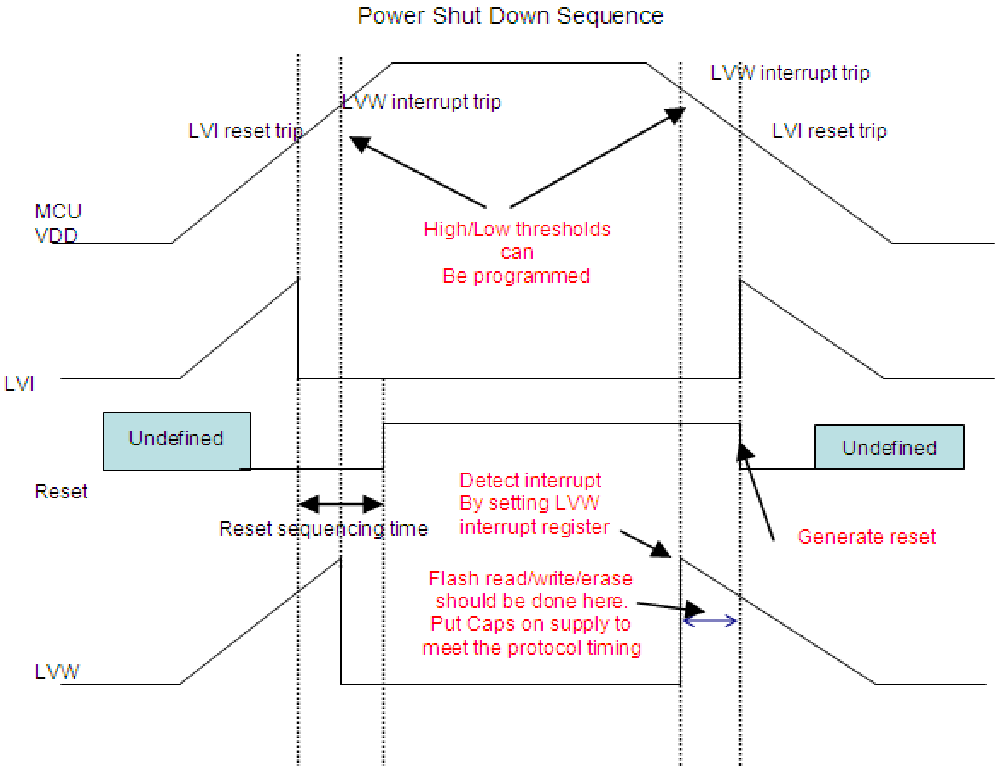
9 Special Consideration in Software

To avoid risk and to prevent loss of important data, software/application must use the LVD system inside the MC9S08LG32 series MCUs.

Here are the steps to achieve the above-mentioned protection:

1. Write SPMSC1_LVDE = 1.
2. Write SPMSC1_LVDRE = 1.
3. Write SPMSC1_LVWIE = 1.

4. Set SPMSC2_LVDV and SPMSC2_LVWV accordingly to set the LVD and LVW trip points. (Refer to *MC9S08LG32 Reference Manual* for details).
5. Insert an interrupt handler routine for low voltage warning to handle critical things in it.
6. Software must be developed to program the flash with critical data as soon as the LVW interrupt comes, and complete the programming of flash before supply reaches LVD trip point.



10 References

See S08LG Product Summary Page for more information and the documents released for MC9S08LG32.

How to Reach Us:

Home Page:
www.freescale.com

Web Support:
http://www.freescale.com/support

USA/Europe or Locations Not Listed:
Freescale Semiconductor, Inc.
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
+1-800-521-6274 or +1-480-768-2130
www.freescale.com/support

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)
www.freescale.com/support

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 China Ltd.
Exchange Building 23F
No. 118 Jianguo Road
Chaoyang District
Beijing 100022
China
+86 10 5879 8000
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

Document Number: AN3821
Rev. 1
2/2009

Information in this document is provided solely to enable system and software implementers to use Freescale Semiconductor products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits or integrated circuits based on the information in this document.

Freescale Semiconductor reserves the right to make changes without further notice to any products herein. Freescale Semiconductor makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale Semiconductor assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters that may be provided in Freescale Semiconductor data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including “Typicals”, must be validated for each customer application by customer’s technical experts. Freescale Semiconductor does not convey any license under its patent rights nor the rights of others. Freescale Semiconductor products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the Freescale Semiconductor product could create a situation where personal injury or death may occur. Should Buyer purchase or use Freescale Semiconductor products for any such unintended or unauthorized application, Buyer shall indemnify and hold Freescale Semiconductor and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Freescale Semiconductor was negligent regarding the design or manufacture of the part.

RoHS-compliant and/or Pb-free versions of Freescale products have the functionality and electrical characteristics as their non-RoHS-compliant and/or non-Pb-free counterparts. For further information, see http://www.freescale.com or contact your Freescale sales representative.

For information on Freescale’s Environmental Products program, go to http://www.freescale.com/epp.