Welcome to E-XFL.COM

What is "Embedded - Microcontrollers"?

"Embedded - Microcontrollers" refer to small, integrated circuits designed to perform specific tasks within larger systems. These microcontrollers are essentially compact computers on a single chip, containing a processor core, memory, and programmable input/output peripherals. They are called "embedded" because they are embedded within electronic devices to control various functions, rather than serving as standalone computers. Microcontrollers are crucial in modern electronics, providing the intelligence and control needed for a wide range of applications.

Applications of "Embedded - Microcontrollers"

Details	
Product Status	Active
Core Processor	HCS12X
Core Size	16-Bit
Speed	50MHz
Connectivity	CANbus, EBI/EMI, I²C, IrDA, SCI, SPI
Peripherals	LVD, POR, PWM, WDT
Number of I/O	59
Program Memory Size	256KB (256K x 8)
Program Memory Type	FLASH
EEPROM Size	4K x 8
RAM Size	16K x 8
Voltage - Supply (Vcc/Vdd)	1.72V ~ 5.5V
Data Converters	A/D 8x12b
Oscillator Type	External
Operating Temperature	-40°C ~ 85°C (TA)
Mounting Type	Surface Mount
Package / Case	80-QFP
Supplier Device Package	80-QFP (14x14)
Purchase URL	https://www.e-xfl.com/product-detail/nxp-semiconductors/s912xet256j2caa

2.3.33 Port S Pull Device Enable Register (PERS)

Address 0x024C Access: User read/write(1)

	7	6	5	4	3	2	1	0
R W	PERS7	PERS6	PERS5	PERS4	PERS3	PERS2	PERS1	PERS0
Reset	1	1	1	1	1	1	1	1

Figure 2-31. Port S Pull Device Enable Register (PERS)

1. Read: Anytime.
   Write: Anytime.

Table 2-30. PERS Register Field Descriptions

Field	Description
7-0 PERS	**Port S pull device enable**—Enable pull devices on input pins These bits configure whether a pull device is activated, if the associated pin is used as an input. This bit has no effect if the pin is used as an output. Out of reset all pull devices are enabled. 1 Pull device enabled. 0 Pull device disabled.

2.3.34 Port S Polarity Select Register (PPSS)

Address 0x024D Access: User read/write(1)

	7	6	5	4	3	2	1	0
R W	PPSS7	PPSS6	PPSS5	PPSS4	PPSS3	PPSS2	PPSS1	PPSS0
Reset	0	0	0	0	0	0	0	0

Figure 2-32. Port S Polarity Select Register (PPSS)

1. Read: Anytime.
   Write: Anytime.

Table 2-31. PPSS Register Field Descriptions

Field	Description
7-0 PPSS	**Port S pull device select**—Determine pull device polarity on input pins This register selects whether a pull-down or a pull-up device is connected to the pin. 1 A pull-down device is connected to the associated pin, if enabled and if the pin is used as input. 0 A pull-up device is connected to the associated pin, if enabled and if the pin is used as input.

2.3.106 Port F Polarity Select Register (PPSF)

Address 0x037D

Access: User read/write(1)

	7	6	5	4	3	2	1	0
R W	PPSF7	PPSF6	PPSF5	PPSF4	PPSF3	PPSF2	PPSF1	PPSF0
Reset	0	0	0	0	0	0	0	0

Figure 2-104. Port F Polarity Select Register (PPSF)

1. Read: Anytime.
   Write: Anytime.

Table 2-101. PPSF Register Field Descriptions

Field	Description
7-0 PPSF	**Port F pull device select**—Determine pull device polarity on input pins This register selects whether a pull-down or a pull-up device is connected to the pin. 1 A pull-down device is connected to the associated pin, if enabled and if the pin is used as input. 0 A pull-up device is connected to the associated pin, if enabled and if the pin is used as input.

2.3.107 PIM Reserved Register

Address 0x037E

Access: User read(1)

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

= Unimplemented or Reserved

Figure 2-105. PIM Reserved Register

1. Read: Always reads 0x00
   Write: Unimplemented

2.3.108 Port F Routing Register (PTFRR)

Address 0x037F

Access: User read/write(1)

	7	6	5	4	3	2	1	0
R	0	0	PTFRR5	PTFRR4	PTFRR3	PTFRR2	PTFRR1	PTFRR0
W								
Reset	0	0	0	0	0	0	0	0

= Unimplemented or Reserved

Figure 2-106. Port F Routing Register (PTFRR)

1. Read: Anytime.
   Write: Anytime.

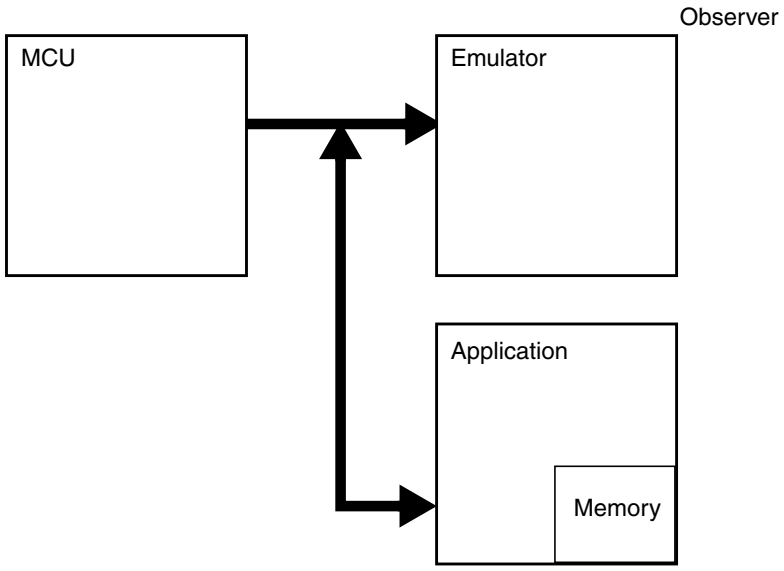

Figure 3-28. ROMON = 0 in Emulation Expanded Mode

3.5.3.5 ROM Control in Special Test Mode

In special test mode the external bus is connected to the application. If the ROMON bit is set, the internal FLASH provides the data, otherwise the application memory provides the data (see Figure 3-29).

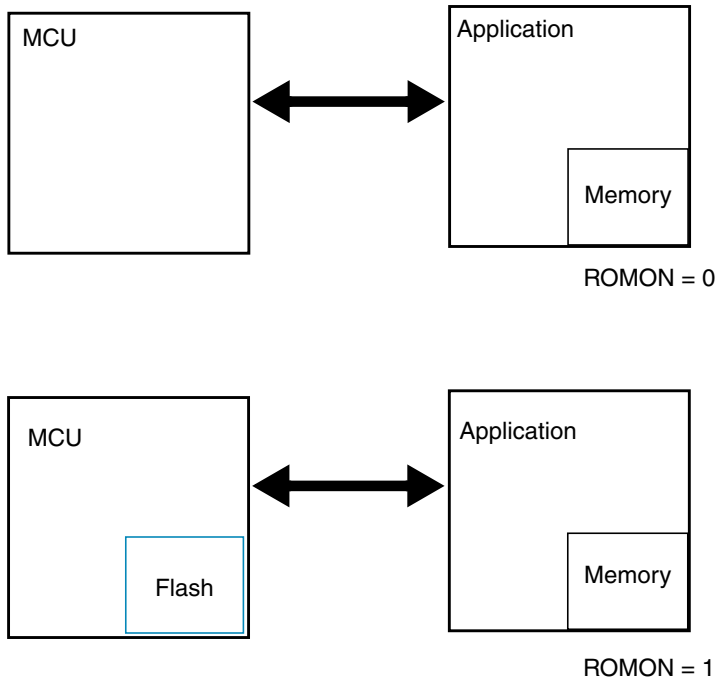

Figure 3-29. ROM in Special Test Mode

Table 7-7. Firmware Commands

Command[1]	Opcode (hex)	Data	Description
READ_NEXT[2]	62	16-bit data out	Increment X index register by 2 (X = X + 2), then read word X points to.
READ_PC	63	16-bit data out	Read program counter.
READ_D	64	16-bit data out	Read D accumulator.
READ_X	65	16-bit data out	Read X index register.
READ_Y	66	16-bit data out	Read Y index register.
READ_SP	67	16-bit data out	Read stack pointer.
WRITE_NEXT	42	16-bit data in	Increment X index register by 2 (X = X + 2), then write word to location pointed to by X.
WRITE_PC	43	16-bit data in	Write program counter.
WRITE_D	44	16-bit data in	Write D accumulator.
WRITE_X	45	16-bit data in	Write X index register.
WRITE_Y	46	16-bit data in	Write Y index register.
WRITE_SP	47	16-bit data in	Write stack pointer.
GO	08	none	Go to user program. If enabled, ACK will occur when leaving active background mode.
GO_UNTIL[3]	0C	none	Go to user program. If enabled, ACK will occur upon returning to active background mode.
TRACE1	10	none	Execute one user instruction then return to active BDM. If enabled, ACK will occur upon returning to active background mode.
TAGGO -> GO	18	none	(Previous enable tagging and go to user program.) This command will be deprecated and should not be used anymore. Opcode will be executed as a GO command.

1. If enabled, ACK will occur when data is ready for transmission for all BDM READ commands and will occur after the write is complete for all BDM WRITE commands.
2. When the firmware command READ_NEXT or WRITE_NEXT is used to access the BDM address space the BDM resources are accessed rather than user code. Writing BDM firmware is not possible.
3. System stop disables the ACK function and ignored commands will not have an ACK-pulse (e.g., CPU in stop or wait mode). The GO_UNTIL command will not get an Acknowledge if CPU executes the wait or stop instruction before the “UNTIL” condition (BDM active again) is reached (see Section 7.4.7, “Serial Interface Hardware Handshake Protocol” last Note).

7.4.5 BDM Command Structure

Hardware and firmware BDM commands start with an 8-bit opcode followed by a 16-bit address and/or a 16-bit data word depending on the command. All the read commands return 16 bits of data despite the byte or word implication in the command name.

8-bit reads return 16-bits of data, of which, only one byte will contain valid data. If reading an even address, the valid data will appear in the MSB. If reading an odd address, the valid data will appear in the LSB.

CMP — Compare — CMP

Operation

RS1 – RS2 ⇒ NONE (translates to SUB R0, RS1, RS2)
RD – IMM16 ⇒ NONE (translates to CMPL RD, #IMM16[7:0]; CPCH RD, #IMM16[15:8])

Subtracts two 16 bit values and discards the result.

CCR Effects

N	Z	V	C
Δ	Δ	Δ	Δ

N: Set if bit 15 of the result is set; cleared otherwise.

Z: Set if the result is $0000; cleared otherwise.

V: Set if a two´s complement overflow resulted from the operation; cleared otherwise.
RS1[15] & $\overline{RS2[15]}$ & $\overline{result[15]}$ | $\overline{RS1[15]}$ & RS2[15] & result[15]
RD[15] & $\overline{IMM16[15]}$ & $\overline{result[15]}$ | $\overline{RD[15]}$ & IMM16[15] & result[15]

C: Set if there is a carry from the bit 15 of the result; cleared otherwise.
$\overline{RS1[15]}$ & RS2[15] | $\overline{RS1[15]}$ & result[15] | RS2[15] & result[15]
$\overline{RD[15]}$ & IMM16[15] | $\overline{RD[15]}$ & result[15] | IMM16[15] & result[15]

Code and CPU Cycles

Source Form	Address Mode	Machine Code											Cycles
CMP RS1, RS2	TRI	0	0	0	1	1	0	0	0	RS1	RS2	0	0	P
CMP RS, #IMM16	IMM8	1	1	0	1	0	RS			IMM16[7:0]				P
	IMM8	1	1	0	1	1	RS			IMM16[15:8]				P

Table 13-13. ATDCTL4 Field Descriptions

Field	Description
7–5 SMP[2:0]	**Sample Time Select** — These three bits select the length of the sample time in units of ATD conversion clock cycles. Note that the ATD conversion clock period is itself a function of the prescaler value (bits PRS4-0). Table 13-14 lists the available sample time lengths.
4–0 PRS[4:0]	**ATD Clock Prescaler** — These 5 bits are the binary prescaler value PRS. The ATD conversion clock frequency is calculated as follows: $f_{ATDCLK} = \frac{f_{BUS}}{2 \times (PRS + 1)}$ Refer to Device Specification for allowed frequency range of f_{ATDCLK}.

Table 13-14. Sample Time Select

SMP2	SMP1	SMP0	Sample Time in Number of ATD Clock Cycles
0	0	0	4
0	0	1	6
0	1	0	8
0	1	1	10
1	0	0	12
1	0	1	16
1	1	0	20
1	1	1	24

13.3.2.6 ATD Control Register 5 (ATDCTL5)

Writes to this register will abort current conversion sequence and start a new conversion sequence. If external trigger is enabled (ETRIGE=1) an initial write to ATDCTL5 is required to allow starting of a conversion sequence which will then occur on each trigger event. Start of conversion means the beginning of the sampling phase.

Module Base + 0x0005

	7	6	5	4	3	2	1	0
R	0	SC	SCAN	MULT	CD	CC	CB	CA
W								
Reset	0	0	0	0	0	0	0	0

Figure 13-8. ATD Control Register 5 (ATDCTL5)

Read: Anytime

Write: Anytime

13.3.2.9 ATD Status Register 2 (ATDSTAT2)

This read-only register contains the Conversion Complete Flags CCF[15:0].

Module Base + 0x000A

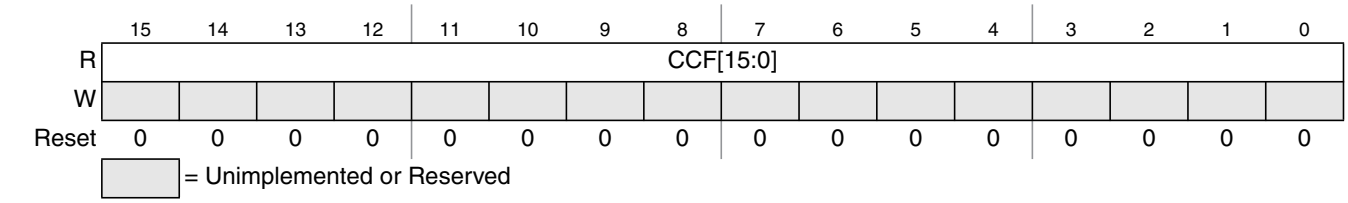

Figure 13-11. ATD Status Register 2 (ATDSTAT2)

Read: Anytime

Write: Anytime, no effect

Table 13-19. ATDSTAT2 Field Descriptions

Field	Description
15–0 CCF[15:0]	**Conversion Complete Flag *n* (*n*= 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1, 0)** — A conversion complete flag is set at the end of each conversion in a sequence. The flags are associated with the conversion position in a sequence (and also the result register number). Therefore in non-fifo mode, CCF[8] is set when the ninth conversion in a sequence is complete and the result is available in result register ATDDR8; CCF[9] is set when the tenth conversion in a sequence is complete and the result is available in ATDDR9, and so forth. If automatic compare of conversion results is enabled (CMPE[*n*]=1 in ATDCMPE), the conversion complete flag is only set if comparison with ATDDR*n* is true and if ACMPIE=1 a compare interrupt will be requested. In this case, as the ATDDR*n* result register is used to hold the compare value, the result will not be stored there at the end of the conversion but is lost. A flag CCF[*n*] is cleared when one of the following occurs: A) Write to ATDCTL5 (a new conversion sequence is started) B) If AFFC=0, write “1” to CCF[*n*] C) If AFFC=1 and CMPE[*n*]=0, read of result register ATDDR*n* D) If AFFC=1 and CMPE[*n*]=1, write to result register ATDDR*n* In case of a concurrent set and clear on CCF[*n*]: The clearing by method A) will overwrite the set. The clearing by methods B) or C) or D) will be overwritten by the set. 0 Conversion number *n* not completed or successfully compared 1 If (CMPE[*n*]=0): Conversion number *n* has completed. Result is ready in ATDDR*n*. If (CMPE[*n*]=1): Compare for conversion result number *n* with compare value in ATDDR*n*, using compare operator CMPGT[*n*] is true. (No result available in ATDDR*n*)

17.5 Initialization

17.5.1 Startup

Set the configuration registers before the PITE bit in the PITCFLMT register is set. Before PITE is set, the configuration registers can be written in arbitrary order.

17.5.2 Shutdown

When the PITCE register bits, the PITINTE register bits or the PITE bit in the PITCFLMT register are cleared, the corresponding PIT interrupt flags are cleared. In case of a pending PIT interrupt request, a spurious interrupt can be generated. Two strategies, which avoid spurious interrupts, are recommended:

1. Reset the PIT interrupt flags only in an ISR. When entering the ISR, the I mask bit in the CCR is set automatically. The I mask bit must not be cleared before the PIT interrupt flags are cleared.
2. After setting the I mask bit with the SEI instruction, the PIT interrupt flags can be cleared. Then clear the I mask bit with the CLI instruction to re-enable interrupts.

17.5.3 Flag Clearing

A flag is cleared by writing a one to the flag bit. Always use store or move instructions to write a one in certain bit positions. Do not use the BSET instructions. Do not use any C-constructs that compile to BSET instructions. “BSET flag_register, #mask” must not be used for flag clearing because BSET is a read-modify-write instruction which writes back the “bit-wise or” of the flag_register and the mask into the flag_register. BSET would clear all flag bits that were set, independent from the mask.

For example, to clear flag bit 0 use: MOVB #$01,PITTF.

17.6 Application Information

To get started quickly with the PIT24B8C module this section provides a small code example how to use the block. Please note that the example provided is only one specific case out of the possible configurations and implementations.

Functionality: Generate an PIT interrupt on channel 0 every 500 PIT clock cycles.

```
                ORG     CODESTART               ; place the program into specific
                                                ; range (to be selected)
                LDS     RAMEND                  ; load stack pointer to top of RAM
                MOVW    #CH0_ISR,VEC_PIT_CH0    ; Change value of channel 0 ISR adr

; ******************** Start PIT Initialization ***************************************************

                CLR     PITCFLMT                ; disable PIT
                MOVB    #$01,PITCE              ; enable timer channel 0
                CLR     PITMUX                  ; ch0 connected to micro timer 0
                MOVB    #$63,PITMTLD0           ; micro time base 0 equals 100 clock cycles
                MOVW    #$0004,PITLD0           ; time base 0 eq. 5 micro time bases 0 =5*100 = 500
```

To calculate the output frequency in center aligned output mode for a particular channel, take the selected clock source frequency for the channel (A, B, SA, or SB) and divide it by twice the value in the period register for that channel.

- PWMx Frequency = Clock (A, B, SA, or SB) / (2*PWMPERx)
- PWMx Duty Cycle (high time as a% of period):
  - Polarity = 0 (PPOLx = 0)

    Duty Cycle = [(PWMPERx-PWMDTYx)/PWMPERx] * 100%
  - Polarity = 1 (PPOLx = 1)

    Duty Cycle = [PWMDTYx / PWMPERx] * 100%

As an example of a center aligned output, consider the following case:

Clock Source = E, where E = 10 MHz (100 ns period)

PPOLx = 0

PWMPERx = 4

PWMDTYx = 1

PWMx Frequency = 10 MHz/8 = 1.25 MHz

PWMx Period = 800 ns

PWMx Duty Cycle = 3/4 *100% = 75%

Shown in Figure 19-23 is the output waveform generated.

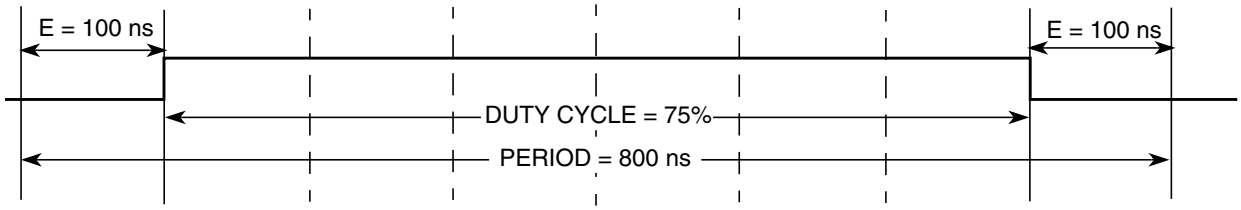

Figure 19-23. PWM Center Aligned Output Example Waveform

19.4.2.7 PWM 16-Bit Functions

The PWM timer also has the option of generating 8-channels of 8-bits or 4-channels of 16-bits for greater PWM resolution. This 16-bit channel option is achieved through the concatenation of two 8-bit channels.

The PWMCTL register contains four control bits, each of which is used to concatenate a pair of PWM channels into one 16-bit channel. Channels 6 and 7 are concatenated with the CON67 bit, channels 4 and 5 are concatenated with the CON45 bit, channels 2 and 3 are concatenated with the CON23 bit, and channels 0 and 1 are concatenated with the CON01 bit.

NOTE

Change these bits only when both corresponding channels are disabled.

When channels 6 and 7 are concatenated, channel 6 registers become the high order bytes of the double byte channel, as shown in Figure 19-24. Similarly, when channels 4 and 5 are concatenated, channel 4 registers become the high order bytes of the double byte channel. When channels 2 and 3 are concatenated,

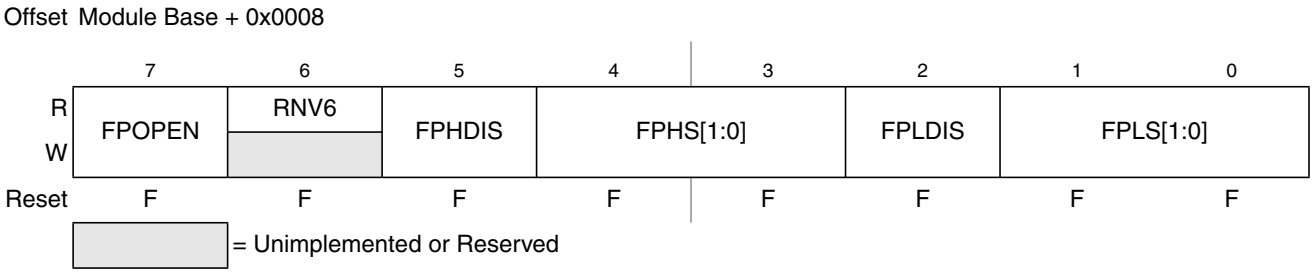

Figure 24-13. Flash Protection Register (FPROT)

The (unreserved) bits of the FPROT register are writable with the restriction that the size of the protected region can only be increased (see Section 24.3.2.9.1, "P-Flash Protection Restrictions," and Table 24-23).

During the reset sequence, the FPROT register is loaded with the contents of the P-Flash protection byte in the Flash configuration field at global address 0x7F_FF0C located in P-Flash memory (see Table 24-3) as indicated by reset condition 'F' in Figure 24-13. To change the P-Flash protection that will be loaded during the reset sequence, the upper sector of the P-Flash memory must be unprotected, then the P-Flash protection byte must be reprogrammed. If a double bit fault is detected while reading the P-Flash phrase containing the P-Flash protection byte during the reset sequence, the FPOPEN bit will be cleared and remaining bits in the FPROT register will be set to leave the P-Flash memory fully protected.

Trying to alter data in any protected area in the P-Flash memory will result in a protection violation error and the FPVIOL bit will be set in the FSTAT register. The block erase of a P-Flash block is not possible if any of the P-Flash sectors contained in the same P-Flash block are protected.

Table 24-19. FPROT Field Descriptions

Field	Description
7 FPOPEN	**Flash Protection Operation Enable** — The FPOPEN bit determines the protection function for program or erase operations as shown in Table 24-20 for the P-Flash block. 0 When FPOPEN is clear, the FPHDIS and FPLDIS bits define unprotected address ranges as specified by the corresponding FPHS and FPLS bits 1 When FPOPEN is set, the FPHDIS and FPLDIS bits enable protection for the address range specified by the corresponding FPHS and FPLS bits
6 RNV[6]	**Reserved Nonvolatile Bit** — The RNV bit should remain in the erased state for future enhancements.
5 FPHDIS	**Flash Protection Higher Address Range Disable** — The FPHDIS bit determines whether there is a protected/unprotected area in a specific region of the P-Flash memory ending with global address 0x7F_FFFF. 0 Protection/Unprotection enabled 1 Protection/Unprotection disabled
4–3 FPHS[1:0]	**Flash Protection Higher Address Size** — The FPHS bits determine the size of the protected/unprotected area in P-Flash memory as shown inTable 24-21. The FPHS bits can only be written to while the FPHDIS bit is set.
2 FPLDIS	**Flash Protection Lower Address Range Disable** — The FPLDIS bit determines whether there is a protected/unprotected area in a specific region of the P-Flash memory beginning with global address 0x7F_8000. 0 Protection/Unprotection enabled 1 Protection/Unprotection disabled
1–0 FPLS[1:0]	**Flash Protection Lower Address Size** — The FPLS bits determine the size of the protected/unprotected area in P-Flash memory as shown in Table 24-22. The FPLS bits can only be written to while the FPLDIS bit is set.

fault information will be recorded until the specific ECC fault flag has been cleared. In the event of simultaneous ECC faults, the priority for fault recording is:

1. Double bit fault over single bit fault
2. CPU over XGATE

Offset Module Base + 0x000E

	7	6	5	4	3	2	1	0
R	ECCR[15:8]							
W								
Reset	0	0	0	0	0	0	0	0

= Unimplemented or Reserved

Figure 24-20. Flash ECC Error Results High Register (FECCRHI)

Offset Module Base + 0x000F

	7	6	5	4	3	2	1	0
R	ECCR[7:0]							
W								
Reset	0	0	0	0	0	0	0	0

= Unimplemented or Reserved

Figure 24-21. Flash ECC Error Results Low Register (FECCRLO)

All FECCR bits are readable but not writable.

Table 24-27. FECCR Index Settings

ECCRIX[2:0]	FECCR Register Content		
	Bits [15:8]	**Bit[7]**	**Bits[6:0]**
000	Parity bits read from Flash block	CPU or XGATE source identity	Global address [22:16]
001	Global address [15:0]		
010	Data 0 [15:0]		
011	Data 1 [15:0] (P-Flash only)		
100	Data 2 [15:0] (P-Flash only)		
101	Data 3 [15:0] (P-Flash only)		
110	Not used, returns 0x0000 when read		
111	Not used, returns 0x0000 when read		

Offset Module Base + 0x000A

	7	6	5	4	3	2	1	0
R W	CCOB[15:8]							
Reset	0	0	0	0	0	0	0	0

Figure 26-16. Flash Common Command Object High Register (FCCOBHI)

Offset Module Base + 0x000B

	7	6	5	4	3	2	1	0
R W	CCOB[7:0]							
Reset	0	0	0	0	0	0	0	0

Figure 26-17. Flash Common Command Object Low Register (FCCOBLO)

26.3.2.11.1 FCCOB - NVM Command Mode

NVM command mode uses the indexed FCCOB register to provide a command code and its relevant parameters to the Memory Controller. The user first sets up all required FCCOB fields and then initiates the command's execution by writing a 1 to the CCIF bit in the FSTAT register (a 1 written by the user clears the CCIF command completion flag to 0). When the user clears the CCIF bit in the FSTAT register all FCCOB parameter fields are locked and cannot be changed by the user until the command completes (as evidenced by the Memory Controller returning CCIF to 1). Some commands return information to the FCCOB register array.

The generic format for the FCCOB parameter fields in NVM command mode is shown in Table 26-26. The return values are available for reading after the CCIF flag in the FSTAT register has been returned to 1 by the Memory Controller. Writes to the unimplemented parameter fields (CCOBIX = 110 and CCOBIX = 111) are ignored with reads from these fields returning 0x0000.

Table 26-26 shows the generic Flash command format. The high byte of the first word in the CCOB array contains the command code, followed by the parameters for this specific Flash command. For details on the FCCOB settings required by each command, see the Flash command descriptions in Section 26.4.2.

Table 26-26. FCCOB - NVM Command Mode (Typical Usage)

CCOBIX[2:0]	Byte	FCCOB Parameter Fields (NVM Command Mode)
000	HI	FCMD[7:0] defining Flash command
	LO	0, Global address [22:16]
001	HI	Global address [15:8]
	LO	Global address [7:0]
010	HI	Data 0 [15:8]
	LO	Data 0 [7:0]

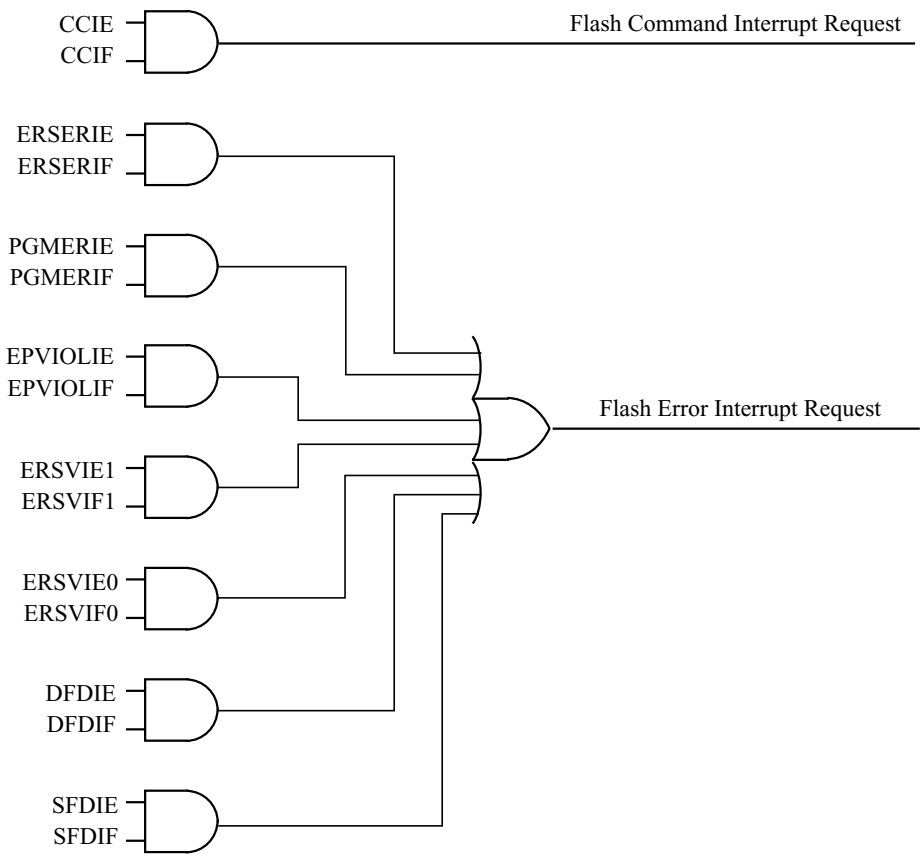

Figure 27-27. Flash Module Interrupts Implementation

27.4.4 Wait Mode

The Flash module is not affected if the MCU enters wait mode. The Flash module can recover the MCU from wait via the CCIF interrupt (see Section 27.4.3, “Interrupts”).

27.4.5 Stop Mode

If a Flash command is active (CCIF = 0) or an EE-Emulation operation is pending when the MCU requests stop mode, the current Flash operation will be completed before the CPU is allowed to enter stop mode.

27.5 Security

The Flash module provides security information to the MCU. The Flash security state is defined by the SEC bits of the FSEC register (see Table 27-12). During reset, the Flash module initializes the FSEC register using data read from the security byte of the Flash configuration field at global address 0x7F_FF0F.

The security state out of reset can be permanently changed by programming the security byte of the Flash configuration field. This assumes that you are starting from a mode where the necessary P-Flash erase and program commands are available and that the upper region of the P-Flash is unprotected. If the Flash security byte is successfully programmed, its new value will take affect after the next MCU reset.

The following subsections describe these security-related subjects:

- Unsecuring the MCU using Backdoor Key Access
- Unsecuring the MCU in Special Single Chip Mode using BDM
- Mode and Security Effects on Flash Command Availability

27.5.1 Unsecuring the MCU using Backdoor Key Access

The MCU may be unsecured by using the backdoor key access feature which requires knowledge of the contents of the backdoor keys (four 16-bit words programmed at addresses 0x7F_FF00–0x7F_FF07). If the KEYEN[1:0] bits are in the enabled state (see Section 27.3.2.2), the Verify Backdoor Access Key command (see Section 27.4.2.12) allows the user to present four prospective keys for comparison to the keys stored in the Flash memory via the Memory Controller. If the keys presented in the Verify Backdoor Access Key command match the backdoor keys stored in the Flash memory, the SEC bits in the FSEC register (see Table 27-12) will be changed to unsecure the MCU. Key values of 0x0000 and 0xFFFF are not permitted as backdoor keys. While the Verify Backdoor Access Key command is active, P-Flash block 0 will not be available for read access and will return invalid data.

The user code stored in the P-Flash memory must have a method of receiving the backdoor keys from an external stimulus. This external stimulus would typically be through one of the on-chip serial ports.

If the KEYEN[1:0] bits are in the enabled state (see Section 27.3.2.2), the MCU can be unsecured by the backdoor key access sequence described below:

1. Follow the command sequence for the Verify Backdoor Access Key command as explained in Section 27.4.2.12
2. If the Verify Backdoor Access Key command is successful, the MCU is unsecured and the SEC[1:0] bits in the FSEC register are forced to the unsecure state of 10

The Verify Backdoor Access Key command is monitored by the Memory Controller and an illegal key will prohibit future use of the Verify Backdoor Access Key command. A reset of the MCU is the only method to re-enable the Verify Backdoor Access Key command.

After the backdoor keys have been correctly matched, the MCU will be unsecured. After the MCU is unsecured, the sector containing the Flash security byte can be erased and the Flash security byte can be reprogrammed to the unsecure state, if desired.

In the unsecure state, the user has full control of the contents of the backdoor keys by programming addresses 0x7F_FF00–0x7F_FF07 in the Flash configuration field.

The security as defined in the Flash security byte (0x7F_FF0F) is not changed by using the Verify Backdoor Access Key command sequence. The backdoor keys stored in addresses 0x7F_FF00–0x7F_FF07 are unaffected by the Verify Backdoor Access Key command sequence. After the next reset of the MCU, the security state of the Flash module is determined by the Flash security byte

state. During the execution of this command (CCIF=0) the user must not write to any Flash module register. The CCIF flag is set after the Unsecure Flash operation has completed.

Table 28-54. Unsecure Flash Command Error Handling

Register	Error Bit	Error Condition
FSTAT	ACCERR	Set if CCOBIX[2:0] != 000 at command launch
		Set if a Load Data Field command sequence is currently active
		Set if command not available in current mode (see Table 28-30)
	FPVIOL	Set if any area of the P-Flash memory is protected
	MGSTAT1	Set if any errors have been encountered during the verify operation(1)
	MGSTAT0	Set if any non-correctable errors have been encountered during the verify operation[1]
FERSTAT	EPVIOLIF	Set if any area of the buffer RAM EEE partition is protected

1. As found in the memory map for FTM1024K5.

28.4.2.12 Verify Backdoor Access Key Command

The Verify Backdoor Access Key command will only execute if it is enabled by the KEYEN bits in the FSEC register (see Table 28-11). The Verify Backdoor Access Key command releases security if user-supplied keys match those stored in the Flash security bytes of the Flash configuration field (see Table 28-3). The Verify Backdoor Access Key command must not be executed from the Flash block containing the backdoor comparison key to avoid code runaway.

Table 28-55. Verify Backdoor Access Key Command FCCOB Requirements

CCOBIX[2:0]	FCCOB Parameters	
000	0x0C	Not required
001	Key 0	
010	Key 1	
011	Key 2	
100	Key 3	

Upon clearing CCIF to launch the Verify Backdoor Access Key command, the Memory Controller will check the FSEC KEYEN bits to verify that this command is enabled. If not enabled, the Memory Controller sets the ACCERR bit in the FSTAT register and terminates. If the command is enabled, the Memory Controller compares the key provided in FCCOB to the backdoor comparison key in the Flash configuration field with Key 0 compared to 0x7F_FF00, etc. If the backdoor keys match, security will be released. If the backdoor keys do not match, security is not released and all future attempts to execute the Verify Backdoor Access Key command are aborted (set ACCERR) until a reset occurs. The CCIF flag is set after the Verify Backdoor Access Key operation has completed.

Chapter 29
1024 KByte Flash Module (S12XFTM1024K5V2)

Table 29-1. Revision History

Revision Number	Revision Date	Sections Affected	Description of Changes
V02.08	14 Nov 2007	29.5.2/29-1200 29.4.2/29-1176 29.4.2.8/29-1182	- Changed terminology from ‘word program’ to “Program P-Flash’ in the BDM unsecuring description, Section 29.5.2 - Added requirement that user not write any Flash module register during execution of commands ‘Erase All Blocks’, Section 29.4.2.8, and ‘Unsecure Flash’, Section 29.4.2.11 - Added statement that security is released upon successful completion of command ‘Erase All Blocks’, Section 29.4.2.8
V02.09	19 Dec 2007	29.4.2/29-1176	- Corrected Error Handling table for Full Partition D-Flash, Partition D-Flash, and EEPROM Emulation Query commands
V02.10	25 Sep 2009	29.1/29-1140 29.3.2.1/29-1152 29.4.2.4/29-1179 29.4.2.7/29-1181 29.4.2.12/29-1185 29.4.2.12/29-1185 29.4.2.12/29-1185 29.4.2.20/29-1194 29.3.2/29-1150 29.3.2.1/29-1152 29.4.1.2/29-1171 29.6/29-1200	- Clarify single bit fault correction for P-Flash phrase - Expand FDIV vs OSCCLK Frequency table - Add statement concerning code runaway when executing Read Once command from Flash block containing associated fields - Add statement concerning code runaway when executing Program Once command from Flash block containing associated fields - Add statement concerning code runaway when executing Verify Backdoor Access Key command from Flash block containing associated fields - Relate Key 0 to associated Backdoor Comparison Key address - Change “power down reset” to “reset” - Add ACCERR condition for Disable EEPROM Emulation command The following changes were made to clarify module behavior related to Flash register access during reset sequence and while Flash commands are active: - Add caution concerning register writes while command is active - Writes to FCLKDIV are allowed during reset sequence while CCIF is clear - Add caution concerning register writes while command is active - Writes to FCCOBIX, FCCOBHI, FCCOBLO registers are ignored during reset sequence

29.3 Memory Map and Registers

This section describes the memory map and registers for the Flash module. Read data from unimplemented memory space in the Flash module is undefined. Write access to unimplemented or reserved memory space in the Flash module will be ignored by the Flash module.

29.3.1 Module Memory Map

The S12X architecture places the P-Flash memory between global addresses 0x70_0000 and 0x7F_FFFF as shown in Table 29-2. The P-Flash memory map is shown in Figure 29-2.

Table 29-2. P-Flash Memory Addressing

Global Address	Size (Bytes)	Description
0x7C_0000 – 0x7F_FFFF	256 K	P-Flash Block 0 Contains Flash Configuration Field (see Table 29-3)
0x7A_0000 – 0x7B_FFFF	128 K	P-Flash Block 1N
0x78_0000 – 0x79_FFFF	128 K	P-Flash Block 1S
0x74_0000 – 0x77_FFFF	256 K	P-Flash Block 2
0x70_0000 – 0x73_FFFF	256 K	P-Flash Block 3

The FPROT register, described in Section 29.3.2.9, can be set to protect regions in the Flash memory from accidental program or erase. Three separate memory regions, one growing upward from global address 0x7F_8000 in the Flash memory (called the lower region), one growing downward from global address 0x7F_FFFF in the Flash memory (called the higher region), and the remaining addresses in the Flash memory, can be activated for protection. The Flash memory addresses covered by these protectable regions are shown in the P-Flash memory map. The higher address region is mainly targeted to hold the boot loader code since it covers the vector space. Default protection settings as well as security information that allows the MCU to restrict access to the Flash module are stored in the Flash configuration field as described in Table 29-3.

Table 29-3. Flash Configuration Field(1)

Global Address	Size (Bytes)	Description
0x7F_FF00 – 0x7F_FF07	8	Backdoor Comparison Key Refer to Section 29.4.2.12, “Verify Backdoor Access Key Command,” and Section 29.5.1, “Unsecuring the MCU using Backdoor Key Access”
0x7F_FF08 – 0x7F_FF0B(2)	4	Reserved
0x7F_FF0C[2]	1	P-Flash Protection byte. Refer to Section 29.3.2.9, “P-Flash Protection Register (FPROT)”
0x7F_FF0D[2]	1	EEE Protection byte Refer to Section 29.3.2.10, “EEE Protection Register (EPROT)”

Table 29-18. FERSTAT Field Descriptions

Field	Description
7 ERSERIF	**EEE Erase Error Interrupt Flag** — The setting of the ERSERIF flag occurs due to an error in a Flash erase command that resulted in the erase operation not being successful during EEE operations. The ERSERIF flag is cleared by writing a 1 to ERSERIF. Writing a 0 to the ERSERIF flag has no effect on ERSERIF. While ERSERIF is set, it is possible to write to the buffer RAM EEE partition but the data written will not be transferred to the D-Flash EEE partition. 0 Erase command successfully completed on the D-Flash EEE partition 1 Erase command failed on the D-Flash EEE partition
6 PGMERIF	**EEE Program Error Interrupt Flag** — The setting of the PGMERIF flag occurs due to an error in a Flash program command that resulted in the program operation not being successful during EEE operations. The PGMERIF flag is cleared by writing a 1 to PGMERIF. Writing a 0 to the PGMERIF flag has no effect on PGMERIF. While PGMERIF is set, it is possible to write to the buffer RAM EEE partition but the data written will not be transferred to the D-Flash EEE partition. 0 Program command successfully completed on the D-Flash EEE partition 1 Program command failed on the D-Flash EEE partition
4 EPVIOLIF	**EEE Protection Violation Interrupt Flag** —The setting of the EPVIOLIF flag indicates an attempt was made to write to a protected area of the buffer RAM EEE partition. The EPVIOLIF flag is cleared by writing a 1 to EPVIOLIF. Writing a 0 to the EPVIOLIF flag has no effect on EPVIOLIF. While EPVIOLIF is set, it is possible to write to the buffer RAM EEE partition as long as the address written to is not in a protected area. 0 No EEE protection violation 1 EEE protection violation detected
3 ERSVIF1	**EEE Error Interrupt 1 Flag** —The setting of the ERSVIF1 flag indicates that the memory controller was unable to change the state of a D-Flash EEE sector. The ERSVIF1 flag is cleared by writing a 1 to ERSVIF1. Writing a 0 to the ERSVIF1 flag has no effect on ERSVIF1. While ERSVIF1 is set, it is possible to write to the buffer RAM EEE partition but the data written will not be transferred to the D-Flash EEE partition. 0 No EEE sector state change error detected 1 EEE sector state change error detected
2 ERSVIF0	**EEE Error Interrupt 0 Flag** —The setting of the ERSVIF0 flag indicates that the memory controller was unable to format a D-Flash EEE sector for EEE use. The ERSVIF0 flag is cleared by writing a 1 to ERSVIF0. Writing a 0 to the ERSVIF0 flag has no effect on ERSVIF0. While ERSVIF0 is set, it is possible to write to the buffer RAM EEE partition but the data written will not be transferred to the D-Flash EEE partition. 0 No EEE sector format error detected 1 EEE sector format error detected
1 DFDIF	**Double Bit Fault Detect Interrupt Flag** — The setting of the DFDIF flag indicates that a double bit fault was detected in the stored parity and data bits during a Flash array read operation or that a Flash array read operation was attempted on a Flash block that was under a Flash command operation. The DFDIF flag is cleared by writing a 1 to DFDIF. Writing a 0 to DFDIF has no effect on DFDIF. 0 No double bit fault detected 1 Double bit fault detected or an invalid Flash array read operation attempted
0 SFDIF	**Single Bit Fault Detect Interrupt Flag** — With the IGNSF bit in the FCNFG register clear, the SFDIF flag indicates that a single bit fault was detected in the stored parity and data bits during a Flash array read operation or that a Flash array read operation was attempted on a Flash block that was under a Flash command operation. The SFDIF flag is cleared by writing a 1 to SFDIF. Writing a 0 to SFDIF has no effect on SFDIF. 0 No single bit fault detected 1 Single bit fault detected and corrected or an invalid Flash array read operation attempted

29.3.2.9 P-Flash Protection Register (FPROT)

The FPROT register defines which P-Flash sectors are protected against program and erase operations.

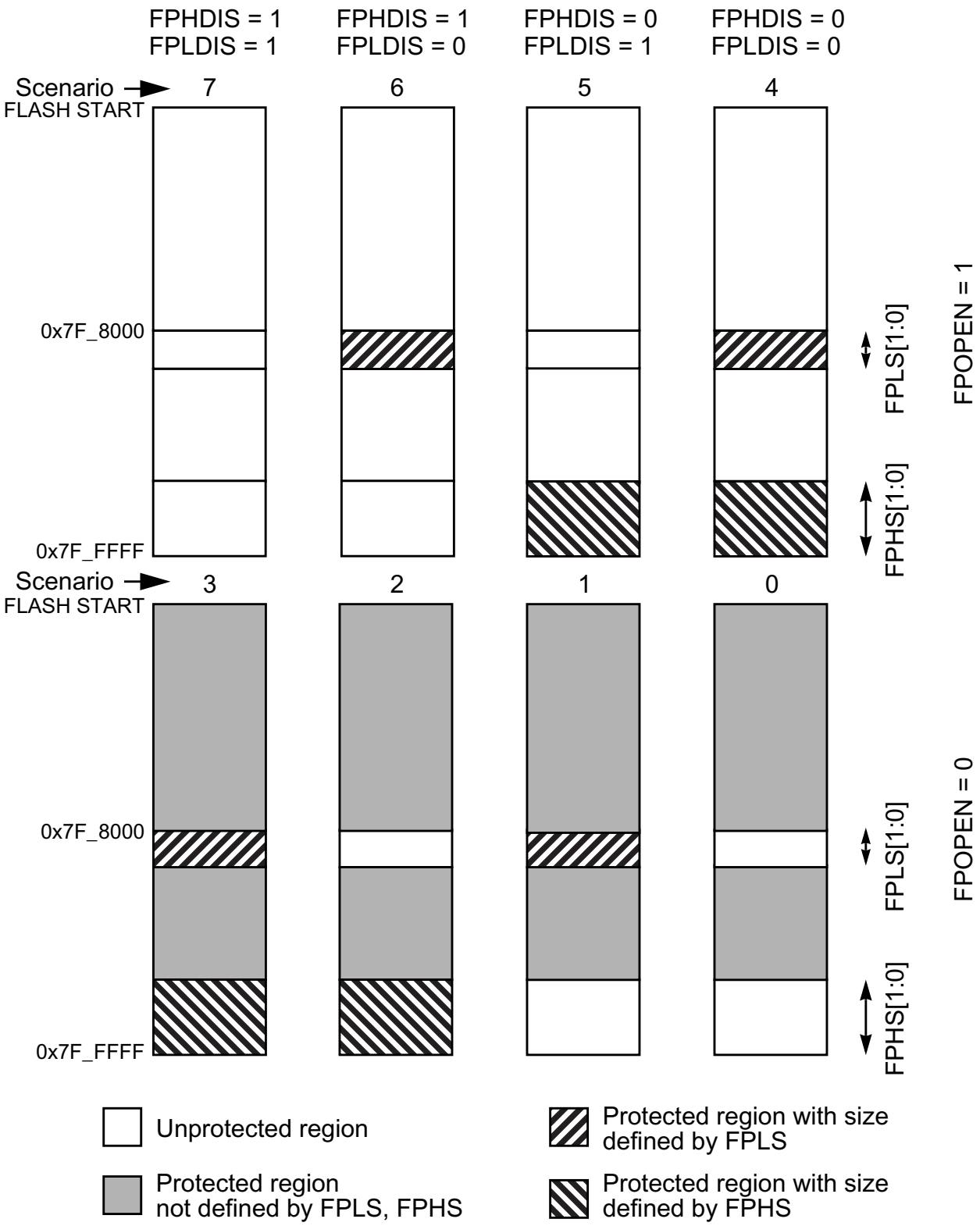

Figure 29-14. P-Flash Protection Scenarios

0x0180–0x01BF MSCAN (CAN1) Map (Sheet 2 of 2)

Address	Name		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0x0196	CAN1IDMR2	R	AM7	AM6	AM5	AM4	AM3	AM2	AM1	AM0
		W								
0x0197	CAN1IDMR3	R	AM7	AM6	AM5	AM4	AM3	AM2	AM1	AM0
		W								
0x0198	CAN1IDAR4	R	AC7	AC6	AC5	AC4	AC3	AC2	AC1	AC0
		W								
0x0199	CAN1IDAR5	R	AC7	AC6	AC5	AC4	AC3	AC2	AC1	AC0
		W								
0x019A	CAN1IDAR6	R	AC7	AC6	AC5	AC4	AC3	AC2	AC1	AC0
		W								
0x019B	CAN1IDAR7	R	AC7	AC6	AC5	AC4	AC3	AC2	AC1	AC0
		W								
0x019C	CAN1IDMR4	R	AM7	AM6	AM5	AM4	AM3	AM2	AM1	AM0
		W								
0x019D	CAN1IDMR5	R	AM7	AM6	AM5	AM4	AM3	AM2	AM1	AM0
		W								
0x019E	CAN1IDMR6	R	AM7	AM6	AM5	AM4	AM3	AM2	AM1	AM0
		W								
0x019F	CAN1IDMR7	R	AM7	AM6	AM5	AM4	AM3	AM2	AM1	AM0
		W								
0x01A0–0x01AF	CAN1RXFG	R	FOREGROUND RECEIVE BUFFER (See Detailed MSCAN Foreground Receive and Transmit Buffer Layout)							
		W								
0x01B0–0x01BF	CAN1TXFG	R	FOREGROUND TRANSMIT BUFFER (See Detailed MSCAN Foreground Receive and Transmit Buffer Layout)							
		W								

0x01C0–0x01FF MSCAN (CAN2) Map (Sheet 1 of 3)

Address	Name		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0x01C0	CAN2CTL0	R	RXFRM	RXACT	CSWAI	SYNCH	TIME	WUPE	SLPRQ	INITRQ
		W								
0x01C1	CAN2CTL1	R	CANE	CLKSRC	LOOPB	LISTEN	BORM	WUPM	SLPAK	INITAK
		W								
0x01C2	CAN2BTR0	R	SJW1	SJW0	BRP5	BRP4	BRP3	BRP2	BRP1	BRP0
		W								
0x01C3	CAN2BTR1	R	SAMP	TSEG22	TSEG21	TSEG20	TSEG13	TSEG12	TSEG11	TSEG10
		W								
0x01C4	CAN2RFLG	R	WUPIF	CSCIF	RSTAT1	RSTAT0	TSTAT1	TSTAT0	OVRIF	RXF
		W								
0x01C5	CAN2RIER	R	WUPIE	CSCIE	RSTATE1	RSTATE0	TSTATE1	TSTATE0	OVRIE	RXFIE
		W								
0x01C6	CAN2TFLG	R	0	0	0	0	0	TXE2	TXE1	TXE0
		W								
0x01C7	CAN2TIER	R	0	0	0	0	0	TXEIE2	TXEIE1	TXEIE0
		W								