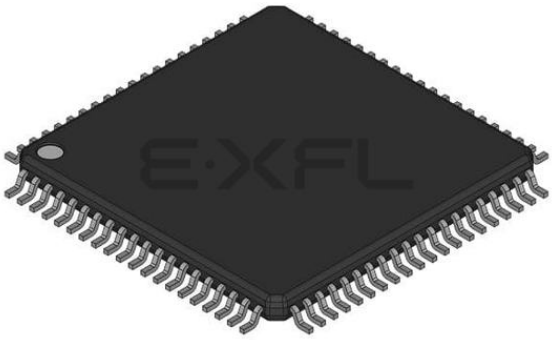


Welcome to E-XFL.COM

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	80MHz
Connectivity	CANbus, EBI/EMI, I²C, IrDA, LINbus, SCI, SPI
Peripherals	LVD, POR, PWM, WDT
Number of I/O	59
Program Memory Size	128KB (128K x 8)
Program Memory Type	FLASH
EEPROM Size	2K x 8
RAM Size	12K x 8
Voltage - Supply (Vcc/Vdd)	2.35V ~ 5.5V
Data Converters	A/D 8x10b
Oscillator Type	External
Operating Temperature	-40°C ~ 125°C (TA)
Mounting Type	Surface Mount
Package / Case	80-QFP
Supplier Device Package	80-QFP (14x14)
Purchase URL	https://www.e-xfl.com/pro/item?MUrl=&PartUrl=mc9s12xdg128maa

NOTE

This documentation covers all devices in the S12XD, S12XB and S12XA families. A full list of these devices and their features can be found in the following chapters:

- E.1 Memory Sizes and Package Options S12XD - Family
- E.2 Memory Sizes and Package Options S12XA & S12XB Family
- E.5 Peripheral Sets S12XD - Family
- E.6 Peripheral Sets S12XA & S12XB - Family
- Table 1-6 Partnames, Masksets and assigned PartID's

This document includes different sections for S12XDPIM, S1XMMC, S12XDBG, S12XEETX and S12XFTX because the different masksets of the S12XD, S12XB and S12XA families include differnt configurations or versions of the modules or have different memory sizes. Table 0-1 shows the maskset specific chapters in this documentation.

Table 0-1. Maskset Specific Documentation

Chapters in this Documentation	L15Y (512k Flash)	M84E (256K Flash)	M42E (128K Flash)
Chapter 21 External Bus Interface (S12XEBIV2) 787	✓	✓	
Chapter 17 Memory Mapping Control (S12XMMCV2) 613	✓		
Chapter 18 Memory Mapping Control (S12XMMCV3) 649		✓	✓
Chapter 19 Debug (S12XDBGV2) 691	✓		
Chapter 20 S12X Debug (S12XDBGV3) Module 743		✓	✓
Chapter 22 DP512 Port Integration Module (S12XDP512PIMV2) 805	✓		
Chapter 23 DQ256 Port Integration Module (S12XDQ256PIMV2) 899		✓	
Chapter 24 DG128 Port Integration Module (S12XDG128PIMV2) 973			✓
Chapter 25 2 Kbyte EEPROM Module (S12XEETX2KV1) 1037			✓
Chapter 26 4 Kbyte EEPROM Module (S12XEETX4KV2) 1071	✓	✓	
Chapter 27 512 Kbyte Flash Module (S12XFTX512K4V2) 1105	✓		
Chapter 28 256 Kbyte Flash Module (S12XFTX256K2V1) 1147		✓	
Chapter 29 128 Kbyte Flash Module (S12XFTX128K1V1) 1189			✓
Chapter 5 Analog-to-Digital Converter (S12ATD10B8CV3) 157	✓	✓	

Table 2-2. CRGFLG Field Descriptions (continued)

Field	Description
5 LVRF	**Low Voltage Reset Flag** — If low voltage reset feature is not available (see device specification) LVRF always reads 0. LVRF is set to 1 when a low voltage reset occurs. This flag can only be cleared by writing a 1. Writing a 0 has no effect. 0 Low voltage reset has not occurred. 1 Low voltage reset has occurred.
4 LOCKIF	**PLL Lock Interrupt Flag** — LOCKIF is set to 1 when LOCK status bit changes. This flag can only be cleared by writing a 1. Writing a 0 has no effect.If enabled (LOCKIE = 1), LOCKIF causes an interrupt request. 0 No change in LOCK bit. 1 LOCK bit has changed.
3 LOCK	**Lock Status Bit** — LOCK reflects the current state of PLL lock condition. This bit is cleared in self clock mode. Writes have no effect. 0 PLL VCO is not within the desired tolerance of the target frequency. 1 PLL VCO is within the desired tolerance of the target frequency.
2 TRACK	**Track Status Bit** — TRACK reflects the current state of PLL track condition. This bit is cleared in self clock mode. Writes have no effect. 0 Acquisition mode status. 1Tracking mode status.
1 SCMIF	**Self Clock Mode Interrupt Flag** — SCMIF is set to 1 when SCM status bit changes. This flag can only be cleared by writing a 1. Writing a 0 has no effect. If enabled (SCMIE = 1), SCMIF causes an interrupt request. 0 No change in SCM bit. 1 SCM bit has changed.
0 SCM	**Self Clock Mode Status Bit** — SCM reflects the current clocking mode. Writes have no effect. 0 MCU is operating normally with OSCCLK available. 1 MCU is operating in self clock mode with OSCCLK in an unknown state. All clocks are derived from PLLCLK running at its minimum frequency f_{SCM}.

EXTAL input frequency. In full stop mode (PSTP = 0), the EXTAL pin is pulled down by an internal resistor of typical 200 kΩ.

NOTE

Freescale recommends an evaluation of the application board and chosen resonator or crystal by the resonator or crystal supplier.

Loop controlled circuit is not suited for overtone resonators and crystals.

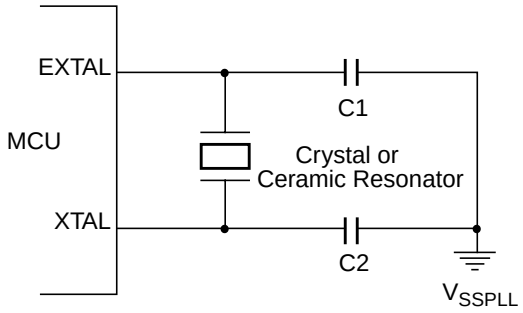
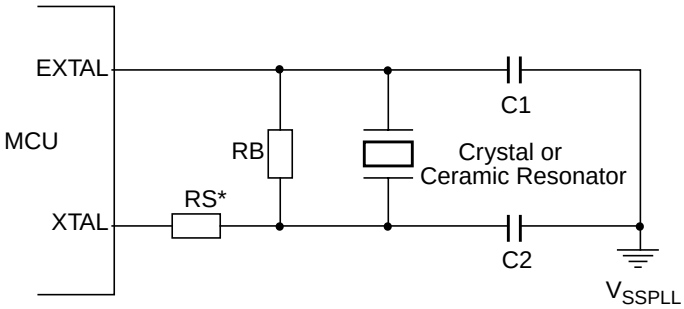


Figure 3-2. Loop Controlled Pierce Oscillator Connections ($\overline{XCLKS}$ = 1)

NOTE

Full swing Pierce circuit is not suited for overtone resonators and crystals without a careful component selection.



* R_S can be zero (shorted) when use with higher frequency crystals. Refer to manufacturer's data.

Figure 3-3. Full Swing Pierce Oscillator Connections ($\overline{XCLKS}$ = 0)

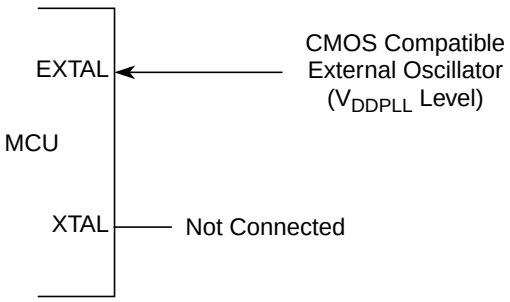


Figure 3-4. External Clock Connections ($\overline{XCLKS}$ = 0)

Chapter 6
XGATE (S12XGATEV2)

6.1 Introduction

The XGATE module is a peripheral co-processor that allows autonomous data transfers between the MCU's peripherals and the internal memories. It has a built in RISC core that is able to pre-process the transferred data and perform complex communication protocols.

The XGATE module is intended to increase the MCU's data throughput by lowering the S12X_CPU's interrupt load.

Figure 6-1 gives an overview on the XGATE architecture.

This document describes the functionality of the XGATE module, including:

- XGATE registers (Section 6.3, "Memory Map and Register Definition")
- XGATE RISC core (Section 6.4.1, "XGATE RISC Core")
- Hardware semaphores (Section 6.4.4, "Semaphores")
- Interrupt handling (Section 6.5, "Interrupts")
- Debug features (Section 6.6, "Debug Mode")
- Security (Section 6.7, "Security")
- Instruction set (Section 6.8, "Instruction Set")

6.1.1 Glossary of Terms

XGATE Request

A service request from a peripheral module which is directed to the XGATE by the S12X_INT module (see Figure 6-1).

XGATE Channel

The resources in the XGATE module (i.e. Channel ID number, Priority level, Service Request Vector, Interrupt Flag) which are associated with a particular XGATE Request.

XGATE Channel ID

A 7-bit identifier associated with an XGATE channel. In S12X designs valid Channel IDs range from $78 to $09.

XGATE Channel Interrupt

An S12X_CPU interrupt that is triggered by a code sequence running on the XGATE module.

XGATE Software Channel

BHS

Branch if Higher or Same (Same as BCC)

BHS

Operation

If C = 0, then PC + $0002 + (REL9 << 1) ⇒ PC

Branch instruction to compare unsigned numbers.

Branch if RS1 ≥ RS2:

```
SUB     R0,RS1,RS2
BHS     REL9
```

CCR Effects

N	Z	V	C
—	—	—	—

N: Not affected.
Z: Not affected.
V: Not affected.
C: Not affected.

Code and CPU Cycles

Source Form	Address Mode	Machine Code								Cycles
BHS REL9	REL9	0	0	1	0	0	0	0	REL9	PP/P

If the bus clock is generated from a PLL, it is recommended to select the oscillator clock rather than the bus clock due to jitter considerations, especially at the faster CAN bus rates.

For microcontrollers without a clock and reset generator (CRG), CANCLK is driven from the crystal oscillator (oscillator clock).

A programmable prescaler generates the time quanta (Tq) clock from CANCLK. A time quantum is the atomic unit of time handled by the MSCAN.

Eqn. 10-2

$$Tq = \frac{f_{CANCLK}}{(\text{Prescaler value})}$$

A bit time is subdivided into three segments as described in the Bosch CAN specification. (see Figure 10-44):

- SYNC_SEG: This segment has a fixed length of one time quantum. Signal edges are expected to happen within this section.
- Time Segment 1: This segment includes the PROP_SEG and the PHASE_SEG1 of the CAN standard. It can be programmed by setting the parameter TSEG1 to consist of 4 to 16 time quanta.
- Time Segment 2: This segment represents the PHASE_SEG2 of the CAN standard. It can be programmed by setting the TSEG2 parameter to be 2 to 8 time quanta long.

Eqn. 10-3

$$\text{Bit Rate} = \frac{f_{Tq}}{(\text{number of Time Quanta})}$$

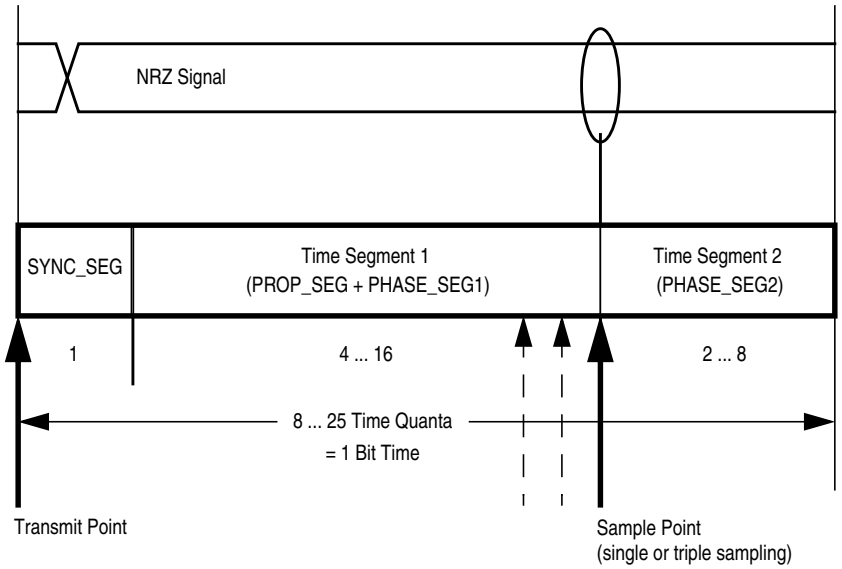


Figure 10-44. Segments within the Bit Time

SPI operation in wait mode is a configurable low power mode, controlled by the SPISWAI bit located in the SPICR2 register. In wait mode, if the SPISWAI bit is clear, the SPI operates like in run mode. If the SPISWAI bit is set, the SPI goes into a power conservative state, with the SPI clock generation turned off. If the SPI is configured as a master, any transmission in progress stops, but is resumed after CPU goes into run mode. If the SPI is configured as a slave, reception and transmission of a byte continues, so that the slave stays synchronized to the master.

- Stop mode

  The SPI is inactive in stop mode for reduced power consumption. If the SPI is configured as a master, any transmission in progress stops, but is resumed after CPU goes into run mode. If the SPI is configured as a slave, reception and transmission of a byte continues, so that the slave stays synchronized to the master.

This is a high level description only, detailed descriptions of operating modes are contained in Section 12.4.7, “Low Power Mode Options”.

12.1.4 Block Diagram

Figure 12-1 gives an overview on the SPI architecture. The main parts of the SPI are status, control and data registers, shifter logic, baud rate generator, master/slave control logic, and port control logic.

12.4.1 Master Mode

The SPI operates in master mode when the MSTR bit is set. Only a master SPI module can initiate transmissions. A transmission begins by writing to the master SPI data register. If the shift register is empty, the byte immediately transfers to the shift register. The byte begins shifting out on the MOSI pin under the control of the serial clock.

- Serial clock

  The SPR2, SPR1, and SPR0 baud rate selection bits, in conjunction with the SPPR2, SPPR1, and SPPR0 baud rate preselection bits in the SPI baud rate register, control the baud rate generator and determine the speed of the transmission. The SCK pin is the SPI clock output. Through the SCK pin, the baud rate generator of the master controls the shift register of the slave peripheral.
- MOSI, MISO pin

  In master mode, the function of the serial data output pin (MOSI) and the serial data input pin (MISO) is determined by the SPC0 and BIDIROE control bits.
- $\overline{SS}$ pin

  If MODFEN and SSOE are set, the $\overline{SS}$ pin is configured as slave select output. The $\overline{SS}$ output becomes low during each transmission and is high when the SPI is in idle state.

  If MODFEN is set and SSOE is cleared, the $\overline{SS}$ pin is configured as input for detecting mode fault error. If the $\overline{SS}$ input becomes low this indicates a mode fault error where another master tries to drive the MOSI and SCK lines. In this case, the SPI immediately switches to slave mode, by clearing the MSTR bit and also disables the slave output buffer MISO (or SISO in bidirectional mode). So the result is that all outputs are disabled and SCK, MOSI, and MISO are inputs. If a transmission is in progress when the mode fault occurs, the transmission is aborted and the SPI is forced into idle state.

  This mode fault error also sets the mode fault (MODF) flag in the SPI status register (SPISR). If the SPI interrupt enable bit (SPIE) is set when the MODF flag becomes set, then an SPI interrupt sequence is also requested.

  When a write to the SPI data register in the master occurs, there is a half SCK-cycle delay. After the delay, SCK is started within the master. The rest of the transfer operation differs slightly, depending on the clock format specified by the SPI clock phase bit, CPHA, in SPI control register 1 (see Section 12.4.3, “Transmission Formats”).

NOTE

A change of the bits CPOL, CPHA, SSOE, LSBFE, MODFEN, SPC0, or BIDIROE with SPC0 set, SPPR2-SPPR0 and SPR2-SPR0 in master mode will abort a transmission in progress and force the SPI into idle state. The remote slave cannot detect this, therefore the master must ensure that the remote slave is returned to idle state.

compared to the serial communication rate. This protocol allows a great flexibility for the POD designers, since it does not rely on any accurate time measurement or short response time to any event in the serial communication.

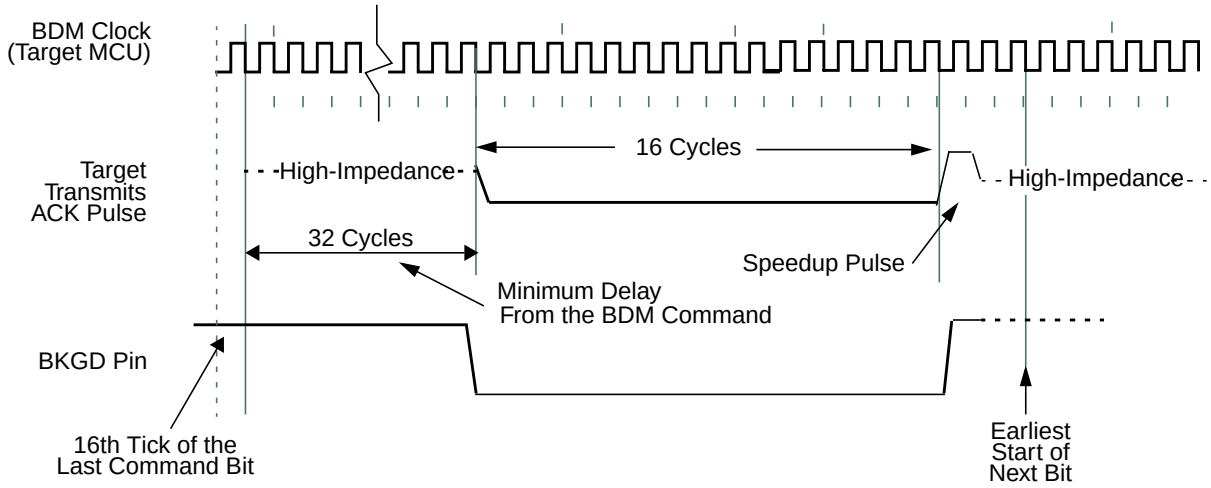


Figure 15-11. Target Acknowledge Pulse (ACK)

NOTE

If the ACK pulse was issued by the target, the host assumes the previous command was executed. If the CPU enters wait or stop prior to executing a hardware command, the ACK pulse will not be issued meaning that the BDM command was not executed. After entering wait or stop mode, the BDM command is no longer pending.

Figure 15-12 shows the ACK handshake protocol in a command level timing diagram. The READ_BYTE instruction is used as an example. First, the 8-bit instruction opcode is sent by the host, followed by the address of the memory location to be read. The target BDM decodes the instruction. A bus cycle is grabbed (free or stolen) by the BDM and it executes the READ_BYTE operation. Having retrieved the data, the BDM issues an ACK pulse to the host controller, indicating that the addressed byte is ready to be retrieved. After detecting the ACK pulse, the host initiates the byte retrieval process. Note that data is sent in the form of a word and the host needs to determine which is the appropriate byte based on whether the address was odd or even.

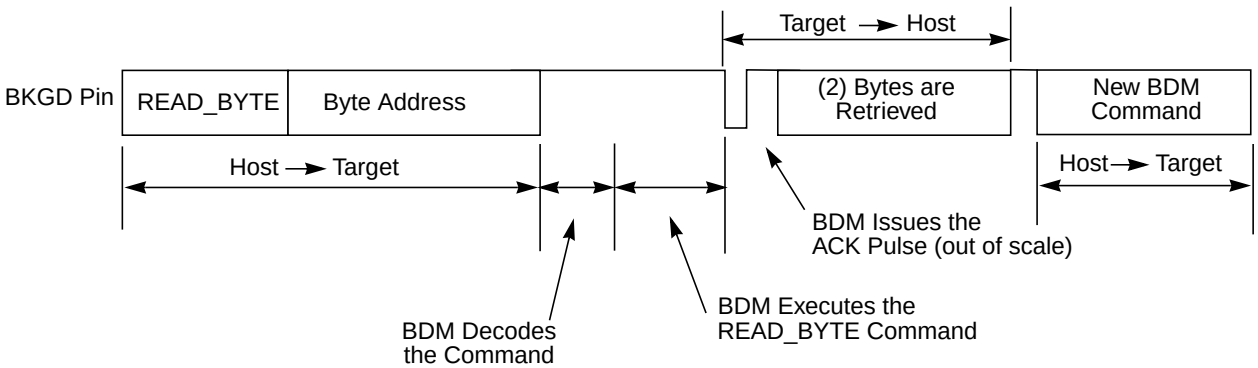


Figure 15-12. Handshake Protocol at Command Level

18.3.2.7 EEPROM Page Index Register (EPAGE)

Address: 0x0017

	7	6	5	4	3	2	1	0
R W	EP7	EP6	EP5	EP4	EP3	EP2	EP1	EP0
Reset	1	1	1	1	1	1	1	0

Figure 18-13. EEPROM Page Index Register (EPAGE)

Read: Anytime

Write: Anytime

These eight index bits are used to page 1 KByte blocks into the EEPROM page window located in the local (CPU or BDM) memory map from address 0x0800 to address 0x0BFF (see Figure 18-14). This supports accessing up to 256 Kbytes of EEPROM (in the Global map) within the 64 KByte Local map. The EEPROM page index register is effectively used to construct paged EEPROM addresses in the Local map format.

CAUTION

XGATE write access to this register during an CPU access which makes use of this register could lead to unexpected results.

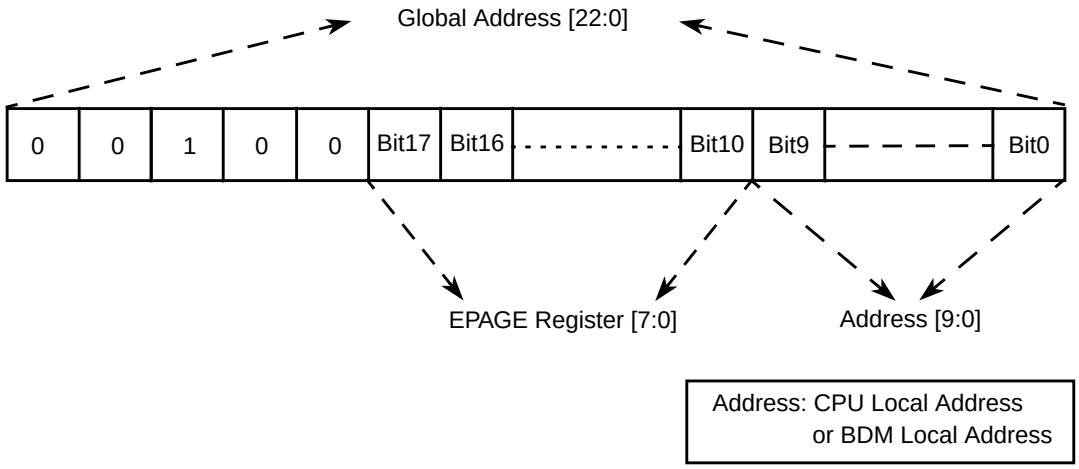


Figure 18-14. EPAGE Address Mapping

Table 18-13. EPAGE Field Descriptions

Field	Description
7–0 EP[7:0]	**EEPROM Page Index Bits 7–0** — These page index bits are used to select which of the 256 EEPROM array pages is to be accessed in the EEPROM Page Window.

The reset value of 0xFE ensures that there is a linear EEPROM space available between addresses 0x0800 and 0x0FFF out of reset.

The fixed 1K page 0x0C00–0x0FFF of EEPROM is equivalent to page 255 (page number 0xFF).

Table 20-45. Breakpoint Mapping Summary

DBGBRK[1] (DBGC1[3])	BDM Bit (DBGC1[4])	BDM Enabled	BDM Active	S12X Breakpoint Mapping
0	X	X	X	No Breakpoint
1	0	X	0	Breakpoint to SWI
1	0	X	1	No Breakpoint
1	1	0	X	Breakpoint to SWI
1	1	1	0	Breakpoint to BDM
1	1	1	1	No Breakpoint

BDM cannot be entered from a breakpoint unless the ENABLE bit is set in the BDM. If entry to BDM via a BGND instruction is attempted and the ENABLE bit in the BDM is cleared, the S12XCPU actually executes the BDM firmware code. It checks the ENABLE and returns if ENABLE is not set. If not serviced by the monitor then the breakpoint is re-asserted when the BDM returns to normal S12XCPU flow.

If the comparator register contents coincide with the SWI/BDM vector address then an SWI in user code and DBG breakpoint could occur simultaneously. The S12XCPU ensures that BDM requests have a higher priority than SWI requests. Returning from the BDM/SWI service routine care must be taken to avoid re triggering a breakpoint.

NOTE

When program control returns from a tagged breakpoint using an RTI or BDM GO command without program counter modification it will return to the instruction whose tag generated the breakpoint. To avoid re triggering a breakpoint at the same location reconfigure the S12XDBG module in the SWI routine, if configured for an SWI breakpoint, or over the BDM interface by executing a TRACE command before the GO to increment the program flow past the tagged instruction.

An XGATE software breakpoint is forced immediately, the tracing session terminated and the XGATE module execution stops. The user can thus determine if an XGATE breakpoint has occurred by reading out the XGATE program counter over the BDM interface.

21.5.1 Normal Expanded Mode

This mode allows interfacing to external memories or peripherals which are available in the commercial market. In these applications the normal bus operation requires a minimum of 1 cycle stretch for each external access.

21.5.1.1 Example 1a: External Wait Feature Disabled

The first example of bus timing of an external read and write access with the external wait feature disabled is shown in

- Figure ‘Example 1a: Normal Expanded Mode — Read Followed by Write’

The associated supply voltage dependent timing are numbers given in

- Table ‘Example 1a: Normal Expanded Mode Timing V_{DD5} = 5.0 V (EWAITE = 0)’
- Table ‘Example 1a: Normal Expanded Mode Timing V_{DD5} = 3.0 V (EWAITE = 0)’

Systems designed this way rely on the internal programmable access stretching. These systems have predictable external memory access times. The additional stretch time can be programmed up to 8 cycles to provide longer access times.

21.5.1.2 Example 1b: External Wait Feature Enabled

The external wait operation is shown in this example. It can be used to exceed the amount of stretch cycles over the programmed number in EXSTR[2:0]. The feature must be enabled by writing EWAITE = 1.

If the $\overline{\text{EWAIT}}$ signal is not asserted, the number of stretch cycles is forced to a minimum of 2 cycles. If $\overline{\text{EWAIT}}$ is asserted within the predefined time window during the access it will be strobed active and another stretch cycle is added. If strobed inactive, the next cycle will be the last cycle before the access is finished. $\overline{\text{EWAIT}}$ can be held asserted as long as desired to stretch the access.

An access with 1 cycle stretch by $\overline{\text{EWAIT}}$ assertion is shown in

- Figure ‘Example 1b: Normal Expanded Mode — Stretched Read Access’
- Figure ‘Example 1b: Normal Expanded Mode — Stretched Write Access’

The associated timing numbers for both operations are given in

- Table ‘Example 1b: Normal Expanded Mode Timing V_{DD5} = 5.0 V (EWAITE = 1)’
- Table ‘Example 1b: Normal Expanded Mode Timing V_{DD5} = 3.0 V (EWAITE = 1)’

It is recommended to use the free-running clock (ECLK) at the fastest rate (bus clock rate) to synchronize the $\overline{\text{EWAIT}}$ input signal.

22.4.2.10 Port H

This port is associated with the SPI1, SPI2, SCI4, and SCI5. Port H pins PH[7:0] can be used for either general purpose I/O, or with the SPI and SCI subsystems. Port H pins can be used with the routed SPI1 and SPI2 modules. *Refer to Section 22.3.2.37, "Module Routing Register (MODRR)"*.

Port H offers 8 I/O pins with edge triggered interrupt capability (Section 22.4.3, "Pin Interrupts").

NOTE

Port H is not available in 80-pin packages.

22.4.2.11 Port J

This port is associated with the chip selects $\overline{CS0}$, $\overline{CS1}$, $\overline{CS2}$ and $\overline{CS3}$ as well as with CAN4, CAN0, IIC1, IIC0, and SCI2. Port J pins PJ[7:4] and PJ[2:0] can be used for either general purpose I/O, or with the CAN, IIC, or SCI subsystems. If IIC takes precedence the associated pins become IIC open-drain output pins. The CAN4 pins can be re-routed. *Refer to Section 22.3.2.37, "Module Routing Register (MODRR)"*.

Port J pins can be used with the routed CAN0 modules. *Refer to Section 22.3.2.37, "Module Routing Register (MODRR)"*.

Port J offers 7 I/O pins with edge triggered interrupt capability (Section 22.4.3, "Pin Interrupts").

NOTE

PJ[5,4,2] are not available in 112-pin packages. PJ[5,4,2,1,0] are not available in 80-pin packages.

22.4.2.12 Port AD0

This port is associated with the ATD0. Port AD0 pins PAD07–PAD00 can be used for either general purpose I/O, or with the ATD0 subsystem.

22.4.2.13 Port AD1

This port is associated with the ATD1. Port AD1 pins PAD23–PAD08 can be used for either general purpose I/O, or with the ATD1 subsystem.

NOTE

PAD[23:16] are not available in 112-pin packages. PAD[23:08] are not available in 80-pin packages.

A valid edge on an input is detected if 4 consecutive samples of a passive level are followed by 4 consecutive samples of an active level directly or indirectly.

The filters are continuously clocked by the bus clock in run and wait mode. In stop mode, the clock is generated by an RC-oscillator in the port integration module. To maximize current saving the RC oscillator runs only if the following condition is true on any pin individually:

Sample count <= 4 and interrupt enabled (PIE = 1) and interrupt flag not set (PIF = 0).

22.4.4 Expanded Bus Pin Functions

All peripheral ports T, S, M, P, H, J, AD0, and AD1 start up as general purpose inputs after reset.

Depending on the external mode pin condition, the external bus interface related ports A, B, C, D, E, and K start up as general purpose inputs on reset or are configured for their alternate functions.

Table 22-70 lists the pin functions in relationship with the different operating modes. If two entries per pin are displayed, a ‘mux’ indicates time-multiplexing between the two functions and an ‘or’ means that a configuration bit exists which can be altered after reset to select the respective function (displayed in *italics*). *Refer to S12X_EBI section for details.*

Table 22-70. Expanded Bus Pin Functions versus Operating Modes

Pin	Single-Chip Modes		Expanded Modes			
	Normal Single-Chip	Special Single-Chip	Normal Expanded	Emulation Single-Chip	Emulation Expanded	Special Test
PK7	GPIO	GPIO	GPIO *or* $\overline{EWAIT}$	GPIO	GPIO *or* $\overline{EWAIT}$	GPIO
PK[6:4]	GPIO	GPIO	ADDR[22:20] *or* *GPIO*	ADDR[22:20] mux ACC[2:0]	ADDR[22:20] mux ACC[2:0]	ADDR[22:20]
PK[3:0]	GPIO	GPIO	ADDR[19:16] *or* *GPIO*	ADDR[19:16] mux IQSTAT[3:0]	ADDR[19:16] mux IQSTAT[3:0]	ADDR[19:16]
PA[7:0]	GPIO	GPIO	ADDR[15:8] *or* *GPIO*	ADDR[15:8] mux IVD[15:8]	ADDR[15:8] mux IVD[15:8]	ADDR[15:8]
PB[7:1]	GPIO	GPIO	ADDR[7:1] *or* *GPIO*	ADDR[7:1] mux IVD[7:1]	ADDR[7:1] mux IVD[7:1]	ADDR[7:1]
PB0	GPIO	GPIO	UDS *or* *GPIO*	ADDR0 mux IVD0	ADDR0 mux IVD0	ADDR0
PC[7:0]	GPIO	GPIO	DATA[15:8] *or* *GPIO*	DATA[15:8]	DATA[15:8]	DATA[15:8] *or* *GPIO*
PD[7:0]	GPIO	GPIO	DATA[7:0]	DATA[7:0]	DATA[7:0]	DATA[7:0]
PE7	GPIO *or* *ECLKX2*	GPIO *or* *ECLKX2*	GPIO *or* *ECLKX2*	ECLKX2	ECLKX2	GPIO *or* *ECLKX2*

open-drain output pins. The CAN4 pins can be re-routed. *Refer to Section 23.0.5.37, "Module Routing Register (MODRR)".*

Port J pins can be used with the routed CAN0 modules. *Refer to Section 23.0.5.37, "Module Routing Register (MODRR)".*

Port J offers 7 I/O pins with edge triggered interrupt capability (Section 23.0.8, "Pin Interrupts").

NOTE

PJ[5,4,2] are not available in 112-pin packages. PJ[5,4,2,1,0] are not available in 80-pin packages.

23.0.7.12 Port AD0

This port is associated with the ATD0. Port AD0 pins PAD07–PAD00 can be used for either general purpose I/O, or with the ATD0 subsystem.

23.0.7.13 Port AD1

This port is associated with the ATD1. Port AD1 pins PAD23–PAD8 can be used for either general purpose I/O, or with the ATD1 subsystem.

NOTE

PAD[23:16] are not available in 112-pin packages. PAD[23:8] are not available in 80-pin packages.

23.0.8 Pin Interrupts

Ports P, H and J offer pin interrupt capability. The interrupt enable as well as the sensitivity to rising or falling edges can be individually configured on per-pin basis. All bits/pins in a port share the same interrupt vector. Interrupts can be used with the pins configured as inputs or outputs.

An interrupt is generated when a bit in the port interrupt flag register and its corresponding port interrupt enable bit are both set. The pin interrupt feature is also capable to wake up the CPU when it is in STOP or WAIT mode.

A digital filter on each pin prevents pulses (Figure 23-78) shorter than a specified time from generating an interrupt. The minimum time varies over process conditions, temperature and voltage (Figure 23-77 and Table 23-69).

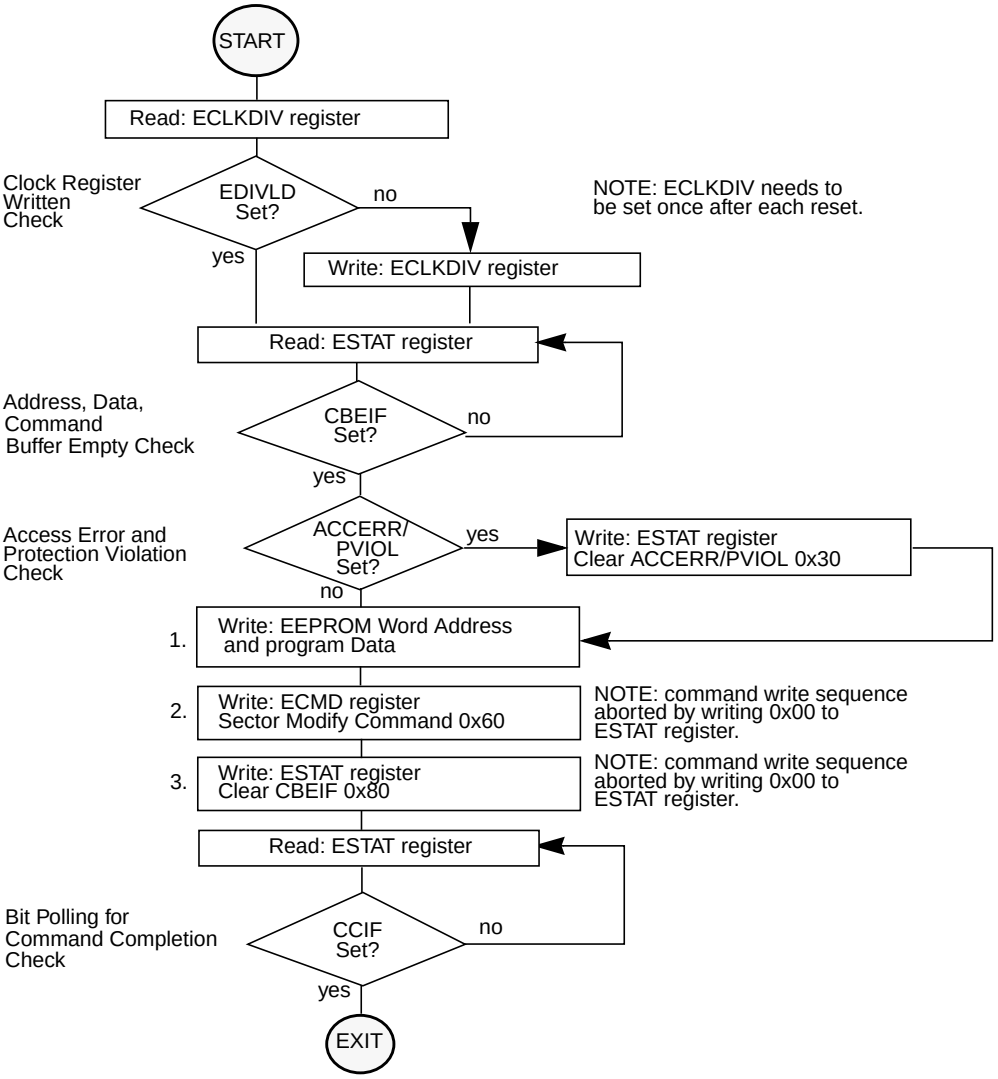


Figure 25-23. Example Sector Modify Command Flow

26.5 Operating Modes

26.5.1 Wait Mode

If a command is active (CCIF = 0) when the MCU enters the wait mode, the active command and any buffered command will be completed.

The EEPROM module can recover the MCU from wait mode if the CBEIF and CCIF interrupts are enabled (see Section 26.8, “Interrupts”).

26.5.2 Stop Mode

If a command is active (CCIF = 0) when the MCU enters the stop mode, the operation will be aborted and, if the operation is program, sector erase, mass erase, or sector modify, the EEPROM array data being programmed or erased may be corrupted and the CCIF and ACCERR flags will be set. If active, the high voltage circuitry to the EEPROM memory will immediately be switched off when entering stop mode. Upon exit from stop mode, the CBEIF flag is set and any buffered command will not be launched. The ACCERR flag must be cleared before starting a command write sequence (see Section 26.4.1.2, “Command Write Sequence”).

NOTE

As active commands are immediately aborted when the MCU enters stop mode, it is strongly recommended that the user does not use the STOP instruction during program, sector erase, mass erase, or sector modify operations.

26.5.3 Background Debug Mode

In background debug mode (BDM), the EPROT register is writable. If the MCU is unsecured, then all EEPROM commands listed in Table 26-10 can be executed. If the MCU is secured and is in special single chip mode, the only command available to execute is mass erase.

26.6 EEPROM Module Security

The EEPROM module does not provide any security information to the MCU. After each reset, the security state of the MCU is a function of information provided by the Flash module (see the specific FTX Block Guide).

27.6.1 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, “Flash Security Register (FSEC)”) and the KEYACC bit is set, a write to a backdoor key address in the Flash memory triggers a comparison between the written data and the backdoor key data stored in the Flash memory. If all four words of data are written to the correct addresses in the correct order and the data matches the backdoor keys stored in the Flash memory, the MCU will be unsecured. The data must be written to the backdoor keys sequentially starting with 0x7F_FF00–1 and ending with 0x7F_FF06–7. 0x0000 and 0xFFFF are not permitted as backdoor keys. While the KEYACC bit is set, reads of the Flash memory will return invalid data.

The user code stored in the 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, “Flash Security Register (FSEC)”), the MCU can be unsecured by the backdoor key access sequence described below:

1. Set the KEYACC bit in the Flash Configuration Register (FCNFG).
2. Write the correct four 16-bit words to Flash addresses 0xFF00–0xFF07 sequentially starting with 0x7F_FF00.
3. Clear the KEYACC bit. Depending on the user code used to write the backdoor keys, a wait cycle (NOP) may be required before clearing the KEYACC bit.
4. If all four 16-bit words match the backdoor keys stored in Flash addresses 0x7F_FF00–0x7F_FF07, the MCU is unsecured and the SEC[1:0] bits in the FSEC register are forced to the unsecure state of 1:0.

The backdoor key access sequence is monitored by an internal security state machine. An illegal operation during the backdoor key access sequence will cause the security state machine to lock, leaving the MCU in the secured state. A reset of the MCU will cause the security state machine to exit the lock state and allow a new backdoor key access sequence to be attempted. The following operations during the backdoor key access sequence will lock the security state machine:

1. If any of the four 16-bit words does not match the backdoor keys programmed in the Flash array.
2. If the four 16-bit words are written in the wrong sequence.
3. If more than four 16-bit words are written.
4. If any of the four 16-bit words written are 0x0000 or 0xFFFF.
5. If the KEYACC bit does not remain set while the four 16-bit words are written.
6. If any two of the four 16-bit words are written on successive MCU clock cycles.

After the backdoor keys have been correctly matched, the MCU will be unsecured. Once the MCU is unsecured, the Flash security byte can be programmed 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 backdoor key access sequence to unsecure. The backdoor keys stored in addresses 0x7F_FF00–0x7F_FF07 are

28.6.1 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 28.3.2.2, “Flash Security Register (FSEC)”) and the KEYACC bit is set, a write to a backdoor key address in the Flash memory triggers a comparison between the written data and the backdoor key data stored in the Flash memory. If all four words of data are written to the correct addresses in the correct order and the data matches the backdoor keys stored in the Flash memory, the MCU will be unsecured. The data must be written to the backdoor keys sequentially starting with 0x7F_FF00–1 and ending with 0x7F_FF06–7. 0x0000 and 0xFFFF are not permitted as backdoor keys. While the KEYACC bit is set, reads of the Flash memory will return invalid data.

The user code stored in the 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 28.3.2.2, “Flash Security Register (FSEC)”), the MCU can be unsecured by the backdoor key access sequence described below:

1. Set the KEYACC bit in the Flash Configuration Register (FCNFG).
2. Write the correct four 16-bit words to Flash addresses 0xFF00–0xFF07 sequentially starting with 0x7F_FF00.
3. Clear the KEYACC bit. Depending on the user code used to write the backdoor keys, a wait cycle (NOP) may be required before clearing the KEYACC bit.
4. If all four 16-bit words match the backdoor keys stored in Flash addresses 0x7F_FF00–0x7F_FF07, the MCU is unsecured and the SEC[1:0] bits in the FSEC register are forced to the unsecure state of 1:0.

The backdoor key access sequence is monitored by an internal security state machine. An illegal operation during the backdoor key access sequence will cause the security state machine to lock, leaving the MCU in the secured state. A reset of the MCU will cause the security state machine to exit the lock state and allow a new backdoor key access sequence to be attempted. The following operations during the backdoor key access sequence will lock the security state machine:

1. If any of the four 16-bit words does not match the backdoor keys programmed in the Flash array.
2. If the four 16-bit words are written in the wrong sequence.
3. If more than four 16-bit words are written.
4. If any of the four 16-bit words written are 0x0000 or 0xFFFF.
5. If the KEYACC bit does not remain set while the four 16-bit words are written.
6. If any two of the four 16-bit words are written on successive MCU clock cycles.

After the backdoor keys have been correctly matched, the MCU will be unsecured. Once the MCU is unsecured, the Flash security byte can be programmed 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 backdoor key access sequence to unsecure. The backdoor keys stored in addresses 0x7F_FF00–0x7F_FF07 are

0x0040–0x007F Enhanced Capture Timer 16-Bit 8-Channels (ECT) Map (Sheet 1 of 3)

Address	Name		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0x0040	TIOS	R	IOS7	IOS6	IOS5	IOS4	IOS3	IOS2	IOS1	IOS0
		W								
0x0041	CFORC	R	0	0	0	0	0	0	0	0
		W	FOC7	FOC6	FOC5	FOC4	FOC3	FOC2	FOC1	FOC0
0x0042	OC7M	R	OC7M7	OC7M6	OC7M5	OC7M4	OC7M3	OC7M2	OC7M1	OC7M0
		W								
0x0043	OC7D	R	OC7D7	OC7D6	OC7D5	OC7D4	OC7D3	OC7D2	OC7D1	OC7D0
		W								
0x0044	TCNT (hi)	R	Bit 15	14	13	12	11	10	9	Bit 8
		W								
0x0045	TCNT (lo)	R	Bit 7	6	5	4	3	2	1	Bit 0
		W								
0x0046	TSCR1	R	TEN	TSWAI	TSFRZ	TFFCA	PRNT	0	0	0
		W								
0x0047	TTOV	R	TOV7	TOV6	TOV5	TOV4	TOV3	TOV2	TOV1	TOV0
		W								
0x0048	TCTL1	R	OM7	OL7	OM6	OL6	OM5	OL5	OM4	OL4
		W								
0x0049	TCTL2	R	OM3	OL3	OM2	OL2	OM1	OL1	OM0	OL0
		W								
0x004A	TCTL3	R	EDG7B	EDG7A	EDG6B	EDG6A	EDG5B	EDG5A	EDG4B	EDG4A
		W								
0x004B	TCTL4	R	EDG3B	EDG3A	EDG2B	EDG2A	EDG1B	EDG1A	EDG0B	EDG0A
		W								
0x004C	TIE	R	C7I	C6I	C5I	C4I	C3I	C2I	C1I	C0I
		W								
0x004D	TSCR2	R	TOI	0	0	0	TCRE	PR2	PR1	PR0
		W								
0x004E	TFLG1	R	C7F	C6F	C5F	C4F	C3F	C2F	C1F	C0F
		W								
0x004F	TFLG2	R	TOF	0	0	0	0	0	0	0
		W								
0x0050	TC0 (hi)	R	Bit 15	14	13	12	11	10	9	Bit 8
		W								
0x0051	TC0 (lo)	R	Bit 7	6	5	4	3	2	1	Bit 0
		W								
0x0052	TC1 (hi)	R	Bit 15	14	13	12	11	10	9	Bit 8
		W								
0x0053	TC1 (lo)	R	Bit 7	6	5	4	3	2	1	Bit 0
		W								
0x0054	TC2 (hi)	R	Bit 15	14	13	12	11	10	9	Bit 8
		W								
0x0055	TC2 (lo)	R	Bit 7	6	5	4	3	2	1	Bit 0
		W								