



Welcome to [E-XFL.COM](https://www.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	HCS12
Core Size	16-Bit
Speed	32MHz
Connectivity	CANbus, SCI, SPI
Peripherals	LVD, POR, PWM, WDT
Number of I/O	49
Program Memory Size	32KB (32K x 8)
Program Memory Type	FLASH
EEPROM Size	4K x 8
RAM Size	2K x 8
Voltage - Supply (Vcc/Vdd)	1.72V ~ 5.5V
Data Converters	A/D 10x12b
Oscillator Type	Internal
Operating Temperature	-40°C ~ 125°C (TA)
Mounting Type	Surface Mount
Package / Case	64-LQFP
Supplier Device Package	64-LQFP (10x10)
Purchase URL	https://www.e-xfl.com/product-detail/nxp-semiconductors/s9s12p32j0mlh

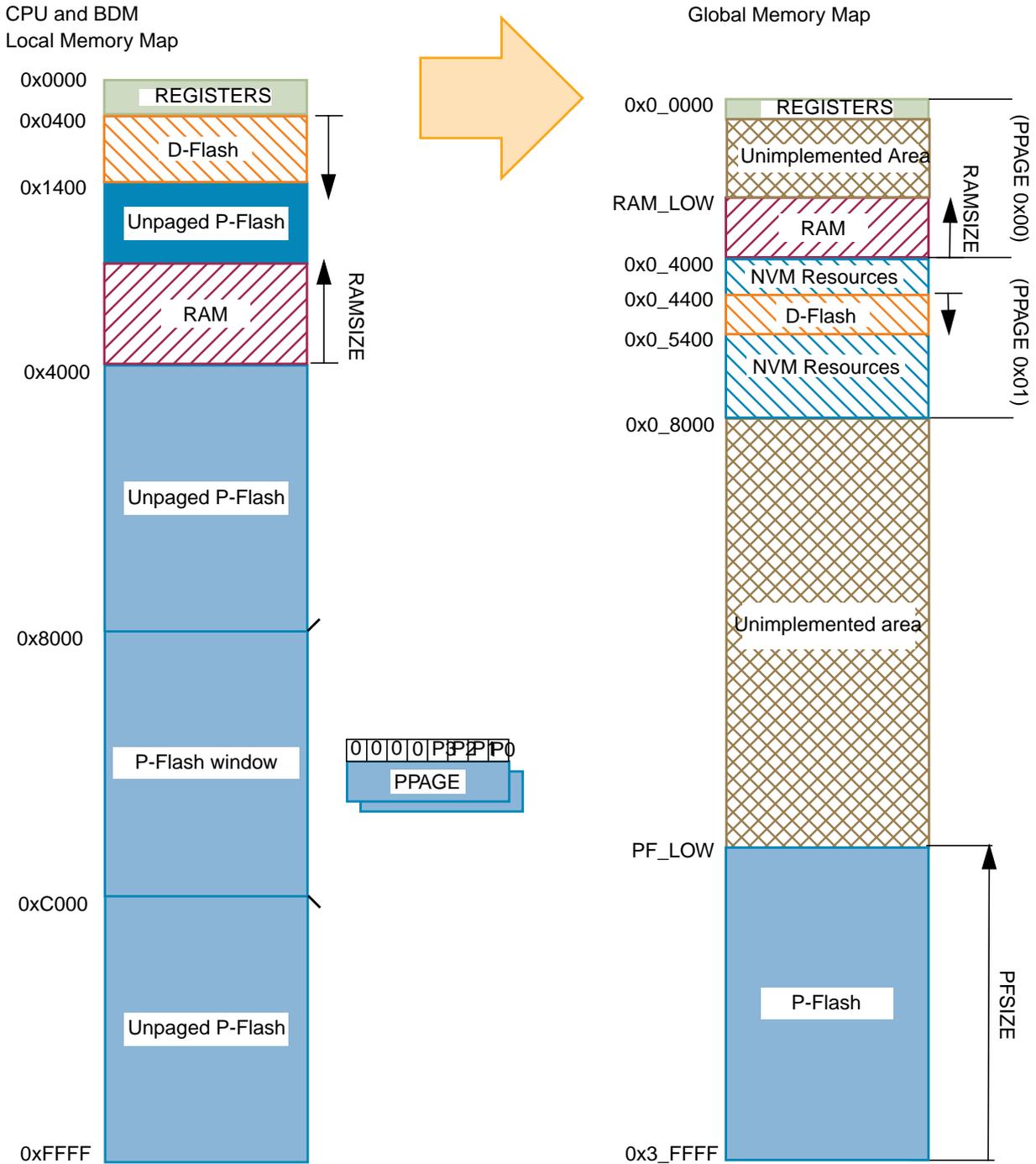


Figure 3-11. Implemented Global Address Mapping

clock please make sure that the communication rate is adapted accordingly and a communication time-out (BDM soft reset) has occurred.

5.3 Memory Map and Register Definition

5.3.1 Module Memory Map

Table 5-1 shows the BDM memory map when BDM is active.

Table 5-1. BDM Memory Map

Global Address	Module	Size (Bytes)
0x3_FF00–0x3_FF0B	BDM registers	12
0x3_FF0C–0x3_FF0E	BDM firmware ROM	3
0x3_FF0F	Family ID (part of BDM firmware ROM)	1
0x3_FF10–0x3_FFFF	BDM firmware ROM	240

5.3.2 Register Descriptions

A summary of the registers associated with the BDM is shown in Figure 5-2. Registers are accessed by host-driven communications to the BDM hardware using READ_BD and WRITE_BD commands.

Global Address	Register Name		Bit 7	6	5	4	3	2	1	Bit 0
0x3_FF00	Reserved	R	X	X	X	X	X	X	0	0
		W								
0x3_FF01	BDMSTS	R	ENBDM	BDMACT	0	SDV	TRACE	0	UNSEC	0
		W								
0x3_FF02	Reserved	R	X	X	X	X	X	X	X	X
		W								
0x3_FF03	Reserved	R	X	X	X	X	X	X	X	X
		W								
0x3_FF04	Reserved	R	X	X	X	X	X	X	X	X
		W								

= Unimplemented, Reserved
 = Implemented (do not alter)

X = Indeterminate
 0 = Always read zero

Figure 5-2. BDM Register Summary

5.3.3 Family ID Assignment

The family ID is an 8-bit value located in the BDM ROM in active BDM (at global address: 0x3_FF0F). The read-only value is a unique family ID which is 0xC2 for devices with an HCS12S core.

5.4 Functional Description

The BDM receives and executes commands from a host via a single wire serial interface. There are two types of BDM commands: hardware and firmware commands.

Hardware commands are used to read and write target system memory locations and to enter active background debug mode, see [Section 5.4.3, “BDM Hardware Commands”](#). Target system memory includes all memory that is accessible by the CPU.

Firmware commands are used to read and write CPU resources and to exit from active background debug mode, see [Section 5.4.4, “Standard BDM Firmware Commands”](#). The CPU resources referred to are the accumulator (D), X index register (X), Y index register (Y), stack pointer (SP), and program counter (PC).

Hardware commands can be executed at any time and in any mode excluding a few exceptions as highlighted (see [Section 5.4.3, “BDM Hardware Commands”](#)) and in secure mode (see [Section 5.4.1, “Security”](#)). BDM firmware commands can only be executed when the system is not secure and is in active background debug mode (BDM).

5.4.1 Security

If the user resets into special single chip mode with the system secured, a secured mode BDM firmware lookup table is brought into the map overlapping a portion of the standard BDM firmware lookup table. The secure BDM firmware verifies that the on-chip Flash EEPROM are erased. This being the case, the UNSEC and ENBDM bit will get set. The BDM program jumps to the start of the standard BDM firmware and the secured mode BDM firmware is turned off and all BDM commands are allowed. If the Flash does not verify as erased, the BDM firmware sets the ENBDM bit, without asserting UNSEC, and the firmware enters a loop. This causes the BDM hardware commands to become enabled, but does not enable the firmware commands. This allows the BDM hardware to be used to erase the Flash.

BDM operation is not possible in any other mode than special single chip mode when the device is secured. The device can only be unsecured via BDM serial interface in special single chip mode. For more information regarding security, please see the S12S_9SEC Block Guide.

5.4.2 Enabling and Activating BDM

The system must be in active BDM to execute standard BDM firmware commands. BDM can be activated only after being enabled. BDM is enabled by setting the ENBDM bit in the BDM status (BDMSTS) register. The ENBDM bit is set by writing to the BDM status (BDMSTS) register, via the single-wire interface, using a hardware command such as WRITE_BD_BYTE.

After being enabled, BDM is activated by one of the following¹:

- Hardware BACKGROUND command

1. BDM is enabled and active immediately out of special single-chip reset.

- CPU BGND instruction
- Breakpoint force or tag mechanism¹

When BDM is activated, the CPU finishes executing the current instruction and then begins executing the firmware in the standard BDM firmware lookup table. When BDM is activated by a breakpoint, the type of breakpoint used determines if BDM becomes active before or after execution of the next instruction.

NOTE

If an attempt is made to activate BDM before being enabled, the CPU resumes normal instruction execution after a brief delay. If BDM is not enabled, any hardware BACKGROUND commands issued are ignored by the BDM and the CPU is not delayed.

In active BDM, the BDM registers and standard BDM firmware lookup table are mapped to addresses 0x3_FF00 to 0x3_FFFF. BDM registers are mapped to addresses 0x3_FF00 to 0x3_FF0B. The BDM uses these registers which are readable anytime by the BDM. However, these registers are not readable by user programs.

When BDM is activated while CPU executes code overlapping with BDM firmware space the saved program counter (PC) will be auto incremented by one from the BDM firmware, no matter what caused the entry into BDM active mode (BGND instruction, BACKGROUND command or breakpoints). In such a case the PC must be set to the next valid address via a WRITE_PC command before executing the GO command.

5.4.3 BDM Hardware Commands

Hardware commands are used to read and write target system memory locations and to enter active background debug mode. Target system memory includes all memory that is accessible by the CPU such as on-chip RAM, Flash, I/O and control registers.

Hardware commands are executed with minimal or no CPU intervention and do not require the system to be in active BDM for execution, although, they can still be executed in this mode. When executing a hardware command, the BDM sub-block waits for a free bus cycle so that the background access does not disturb the running application program. If a free cycle is not found within 128 clock cycles, the CPU is momentarily frozen so that the BDM can steal a cycle. When the BDM finds a free cycle, the operation does not intrude on normal CPU operation provided that it can be completed in a single cycle. However, if an operation requires multiple cycles the CPU is frozen until the operation is complete, even though the BDM found a free cycle.

The BDM hardware commands are listed in [Table 5-4](#).

The READ_BD and WRITE_BD commands allow access to the BDM register locations. These locations are not normally in the system memory map but share addresses with the application in memory. To distinguish between physical memory locations that share the same address, BDM memory resources are

1. This method is provided by the S12S_DBG module.

enabled just for the READ_BD and WRITE_BD access cycle. This allows the BDM to access BDM locations unobtrusively, even if the addresses conflict with the application memory map.

Table 5-4. Hardware Commands

Command	Opcode (hex)	Data	Description
BACKGROUND	90	None	Enter background mode if BDM is enabled. If enabled, an ACK will be issued when the part enters active background mode.
ACK_ENABLE	D5	None	Enable Handshake. Issues an ACK pulse after the command is executed.
ACK_DISABLE	D6	None	Disable Handshake. This command does not issue an ACK pulse.
READ_BD_BYTE	E4	16-bit address 16-bit data out	Read from memory with standard BDM firmware lookup table in map. Odd address data on low byte; even address data on high byte.
READ_BD_WORD	EC	16-bit address 16-bit data out	Read from memory with standard BDM firmware lookup table in map. Must be aligned access.
READ_BYTE	E0	16-bit address 16-bit data out	Read from memory with standard BDM firmware lookup table out of map. Odd address data on low byte; even address data on high byte.
READ_WORD	E8	16-bit address 16-bit data out	Read from memory with standard BDM firmware lookup table out of map. Must be aligned access.
WRITE_BD_BYTE	C4	16-bit address 16-bit data in	Write to memory with standard BDM firmware lookup table in map. Odd address data on low byte; even address data on high byte.
WRITE_BD_WORD	CC	16-bit address 16-bit data in	Write to memory with standard BDM firmware lookup table in map. Must be aligned access.
WRITE_BYTE	C0	16-bit address 16-bit data in	Write to memory with standard BDM firmware lookup table out of map. Odd address data on low byte; even address data on high byte.
WRITE_WORD	C8	16-bit address 16-bit data in	Write to memory with standard BDM firmware lookup table out of map. Must be aligned access.

NOTE:

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.

5.4.4 Standard BDM Firmware Commands

BDM firmware commands are used to access and manipulate CPU resources. The system must be in active BDM to execute standard BDM firmware commands, see [Section 5.4.2, “Enabling and Activating BDM”](#). Normal instruction execution is suspended while the CPU executes the firmware located in the standard BDM firmware lookup table. The hardware command BACKGROUND is the usual way to activate BDM.

As the system enters active BDM, the standard BDM firmware lookup table and BDM registers become visible in the on-chip memory map at 0x3_FF00–0x3_FFFF, and the CPU begins executing the standard BDM firmware. The standard BDM firmware watches for serial commands and executes them as they are received.

The firmware commands are shown in [Table 5-5](#).

Chapter 6

S12S Debug Module (S12SDBGV2)

Table 6-1. Revision History

Revision Number	Revision Date	Sections Affected	Summary of Changes
02.07	13.DEC.2007	6.5	Added application information
02.08	09.MAY.2008	General	Spelling corrections. Revision history format changed.
02.09	29.MAY.2008	6.4.5.4	Added note for end aligned, PurePC, rollover case.

6.1 Introduction

The S12SDBG module provides an on-chip trace buffer with flexible triggering capability to allow non-intrusive debug of application software. The S12SDBG module is optimized for S12SCPU debugging.

Typically the S12SDBG module is used in conjunction with the S12SBDM module, whereby the user configures the S12SDBG module for a debugging session over the BDM interface. Once configured the S12SDBG module is armed and the device leaves BDM returning control to the user program, which is then monitored by the S12SDBG module. Alternatively the S12SDBG module can be configured over a serial interface using SWI routines.

6.1.1 Glossary Of Terms

COF: Change Of Flow. Change in the program flow due to a conditional branch, indexed jump or interrupt.

BDM: Background Debug Mode

S12SBDM: Background Debug Module

DUG: Device User Guide, describing the features of the device into which the DBG is integrated.

WORD: 16 bit data entity

Data Line: 20 bit data entity

CPU: S12SCPU module

DBG: S12SDBG module

POR: Power On Reset

Tag: Tags can be attached to CPU opcodes as they enter the instruction pipe. If the tagged opcode reaches the execution stage a tag hit occurs.

Table 6-12. DBGCNT Field Descriptions

Field	Description
7 TBF	Trace Buffer Full — The TBF bit indicates that the trace buffer has stored 64 or more lines of data since it was last armed. If this bit is set, then all 64 lines will be valid data, regardless of the value of DBGCNT bits. The TBF bit is cleared when ARM in DBG1 is written to a one. The TBF is cleared by the power on reset initialization. Other system generated resets have no affect on this bit This bit is also visible at DBGSR[7]
5–0 CNT[5:0]	Count Value — The CNT bits indicate the number of valid data 20-bit data lines stored in the Trace Buffer. Table 6-13 shows the correlation between the CNT bits and the number of valid data lines in the Trace Buffer. When the CNT rolls over to zero, the TBF bit in DBGSR is set and incrementing of CNT will continue in end-trigger mode. The DBGCNT register is cleared when ARM in DBG1 is written to a one. The DBGCNT register is cleared by power-on-reset initialization but is not cleared by other system resets. Thus should a reset occur during a debug session, the DBGCNT register still indicates after the reset, the number of valid trace buffer entries stored before the reset occurred. The DBGCNT register is not decremented when reading from the trace buffer.

Table 6-13. CNT Decoding Table

TBF	CNT[5:0]	Description
0	000000	No data valid
0	000001	1 line valid
	000010	2 lines valid
	000100	4 lines valid
	000110	6 lines valid

	111111	63 lines valid
1	000000	64 lines valid; if using Begin trigger alignment, ARM bit will be cleared and the tracing session ends.
1	000001	64 lines valid,
	..	oldest data has been overwritten by most recent data
	..	
	111110	

6.3.2.7 Debug State Control Registers

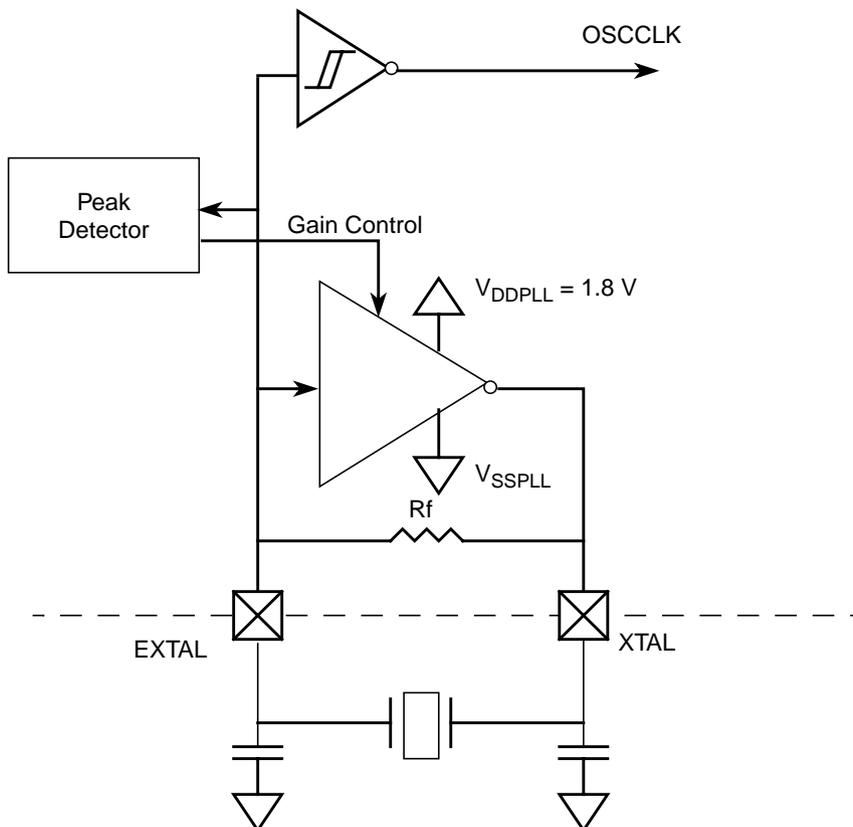
There is a dedicated control register for each of the state sequencer states 1 to 3 that determines if transitions from that state are allowed, depending upon comparator matches or tag hits, and defines the next state for the state sequencer following a match. The three debug state control registers are located at the same address in the register address map (0x0027). Each register can be accessed using the COMRV bits in DBG1 to blend in the required register. The COMRV = 11 value blends in the match flag register (DBGMFR).

Table 6-14. State Control Register Access Encoding

COMRV	Visible State Control Register
00	DBGSCR1
01	DBGSCR2
10	DBGSCR3
11	DBGMFR

Figure 7-1. Block diagram of S12CPMU

Figure 7-2 shows a block diagram of the OSCLCP.


Figure 7-2. OSCLCP Block Diagram

7.2 Signal Description

This section lists and describes the signals that connect off chip.

7.2.1 $\overline{\text{RESET}}$

$\overline{\text{RESET}}$ is an active-low bidirectional pin. As an input it initializes the MCU asynchronously to a known start-up state. As an open-drain output it indicates that an MCU-internal reset has been triggered.

7.2.2 EXTAL and XTAL

These pins provide the interface for a crystal to control the internal clock generator circuitry. EXTAL is the external clock input or the input to the crystal oscillator amplifier. XTAL is the output of the crystal oscillator amplifier. The MCU internal OSCCLK is derived from the EXTAL input frequency. If OSCE=0,

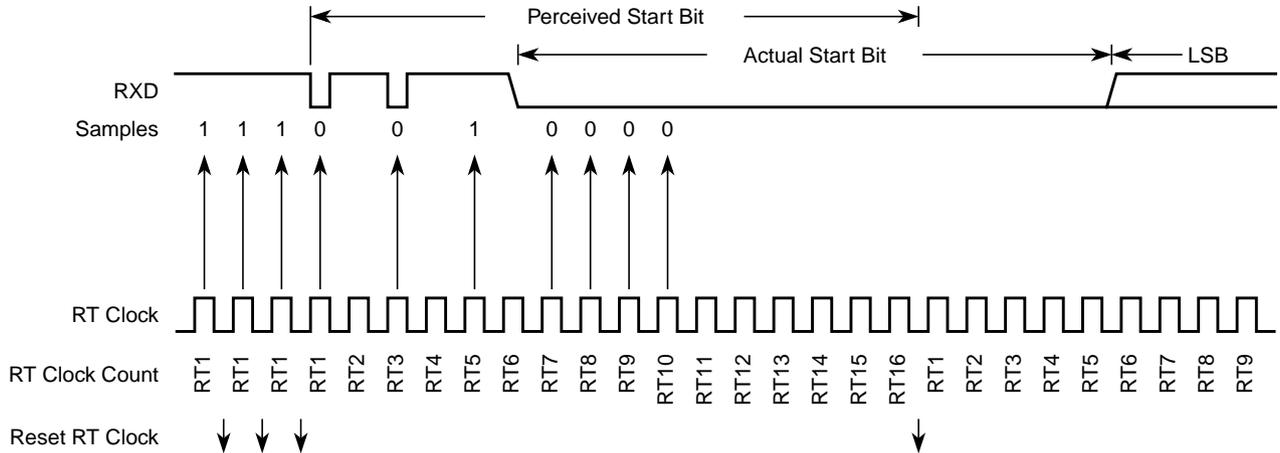


Figure 11-24. Start Bit Search Example 3

Figure 11-25 shows the effect of noise early in the start bit time. Although this noise does not affect proper synchronization with the start bit time, it does set the noise flag.

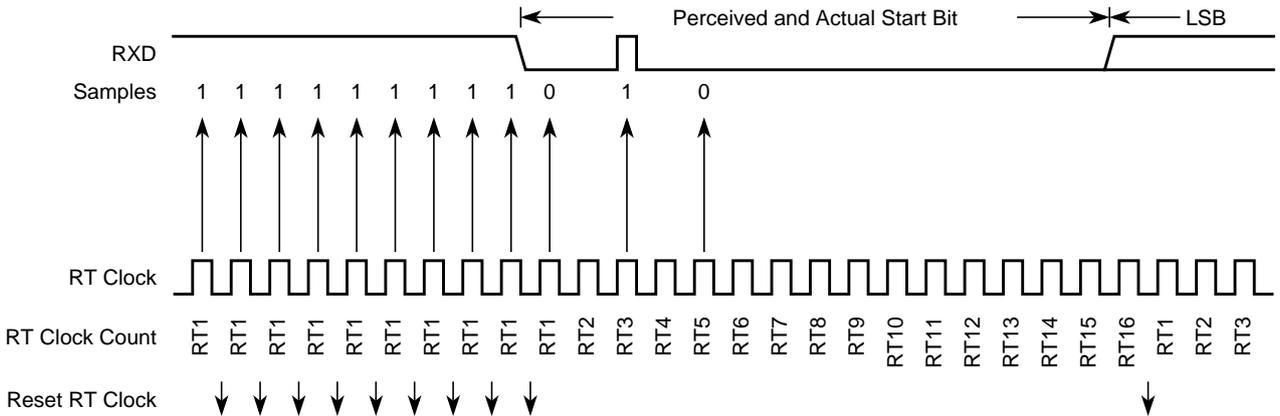


Figure 11-25. Start Bit Search Example 4

Figure 11-26 shows a burst of noise near the beginning of the start bit that resets the RT clock. The sample after the reset is low but is not preceded by three high samples that would qualify as a falling edge. Depending on the timing of the start bit search and on the data, the frame may be missed entirely or it may set the framing error flag.

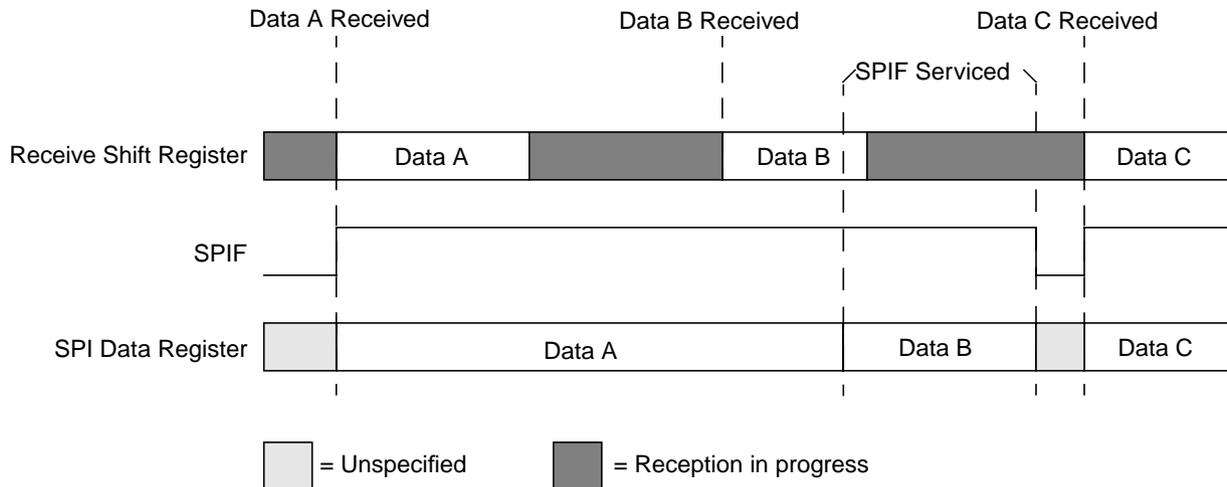


Figure 12-9. Reception with SPIF serviced in Time

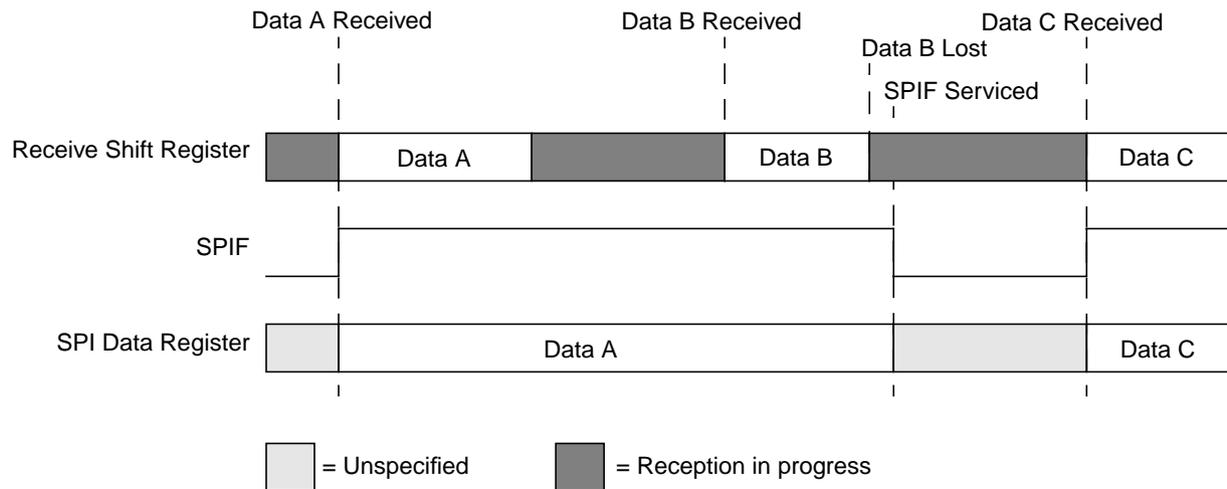


Figure 12-10. Reception with SPIF serviced too late

12.4 Functional Description

The SPI module allows a duplex, synchronous, serial communication between the MCU and peripheral devices. Software can poll the SPI status flags or SPI operation can be interrupt driven.

The SPI system is enabled by setting the SPI enable (SPE) bit in SPI control register 1. While SPE is set, the four associated SPI port pins are dedicated to the SPI function as:

- Slave select (\overline{SS})
- Serial clock (SCK)
- Master out/slave in (MOSI)
- Master in/slave out (MISO)

When the third edge occurs, the value previously latched from the serial data input pin is shifted into the LSB or MSB of the SPI shift register, depending on LSBFE bit. After this edge, the next bit of the master data is coupled out of the serial data output pin of the master to the serial input pin on the slave.

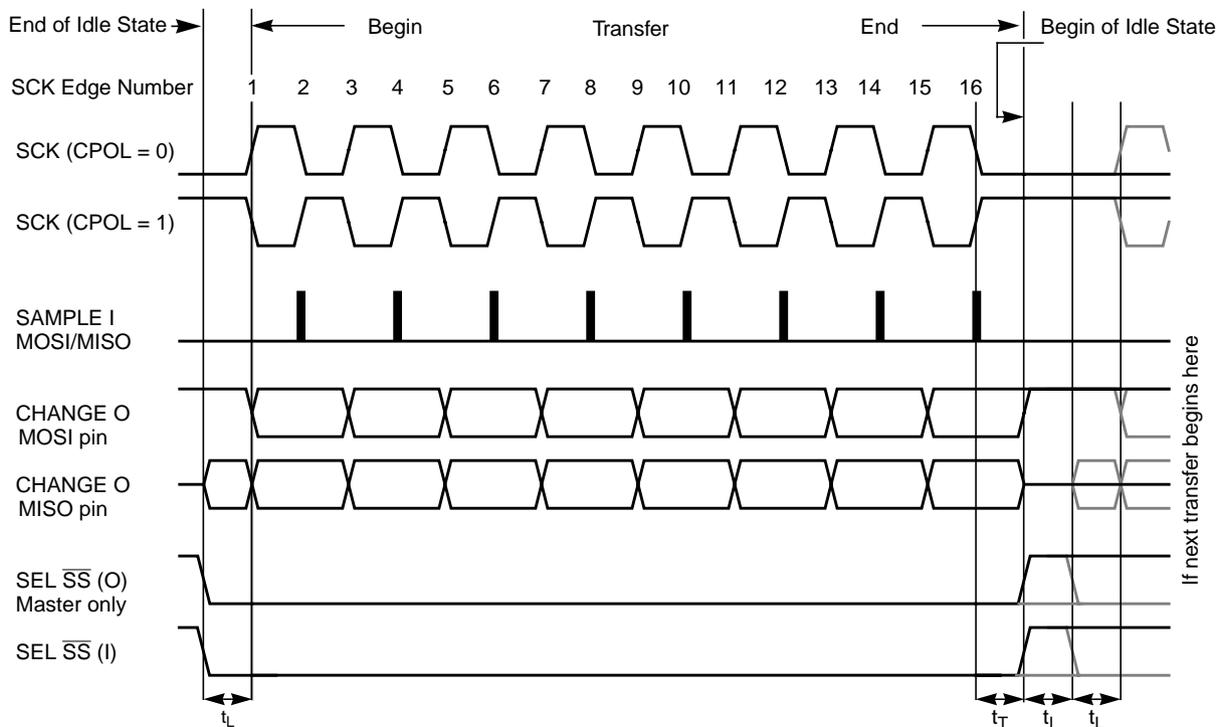
This process continues for a total of n^1 edges on the SCK line with data being latched on even numbered edges and shifting taking place on odd numbered edges.

Data reception is double buffered, data is serially shifted into the SPI shift register during the transfer and is transferred to the parallel SPI data register after the last bit is shifted in.

After $2n^1$ SCK edges:

- Data that was previously in the SPI data register of the master is now in the data register of the slave, and data that was in the data register of the slave is in the master.
- The SPIF flag bit in SPISR is set indicating that the transfer is complete.

Figure 12-14 shows two clocking variations for CPHA = 1. The diagram may be interpreted as a master or slave timing diagram because the SCK, MISO, and MOSI pins are connected directly between the master and the slave. The MISO signal is the output from the slave, and the MOSI signal is the output from the master. The \overline{SS} line is the slave select input to the slave. The \overline{SS} pin of the master must be either high or reconfigured as a general-purpose output not affecting the SPI.



MSB first (LSBFE = 0): MSB Bit 6 Bit 5 Bit 4 Bit 3 Bit 2 Bit 1 LSB Minimum 1/2 SCK
 LSB first (LSBFE = 1): LSB Bit 1 Bit 2 Bit 3 Bit 4 Bit 5 Bit 6 MSB for t_T , t_i , t_L

t_L = Minimum leading time before the first SCK edge, not required for back-to-back transfers

t_T = Minimum trailing time after the last SCK edge

t_i = Minimum idling time between transfers (minimum \overline{SS} high time), not required for back-to-back transfers

Figure 12-14. SPI Clock Format 1 (CPHA = 1), with 8-Bit Transfer Width selected (XFRW = 0)

13.3 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.

13.3.1 Module Memory Map

The S12 architecture places the P-Flash memory between global addresses 0x2_0000 and 0x3_FFFF as shown in Table 13-2. The P-Flash memory map is shown in Figure 13-2.

Table 13-2. P-Flash Memory Addressing

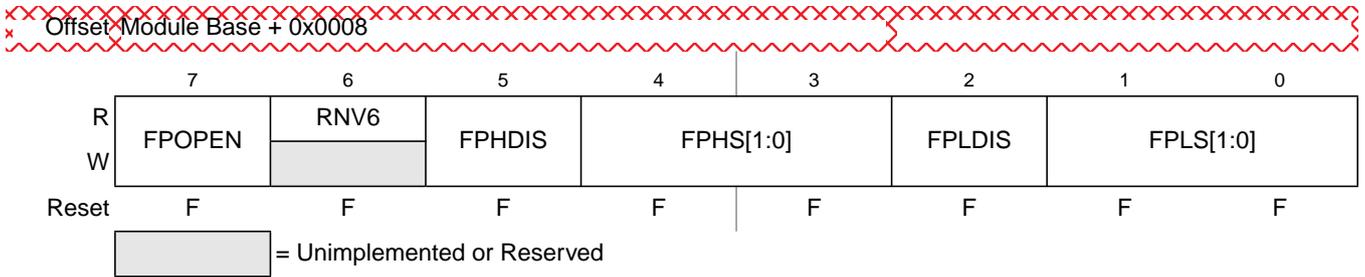
Global Address	Size (Bytes)	Description
0x2_0000 – 0x3_FFFF	128 K	P-Flash Block Contains Flash Configuration Field (see Table 13-3)

The FPROT register, described in Section 13.3.2.9, 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 0x3_8000 in the Flash memory (called the lower region), one growing downward from global address 0x3_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 13-3.

Table 13-3. Flash Configuration Field

Global Address	Size (Bytes)	Description
0x3_FF00-0x3_FF07	8	Backdoor Comparison Key Refer to Section 13.4.5.11, “Verify Backdoor Access Key Command,” and Section 13.5.1, “Unsecuring the MCU using Backdoor Key Access”
0x3_FF08-0x3_FF0B ⁽¹⁾	4	Reserved
0x3_FF0C ¹	1	P-Flash Protection byte. Refer to Section 13.3.2.9, “P-Flash Protection Register (FPROT)”
0x3_FF0D ¹	1	D-Flash Protection byte. Refer to Section 13.3.2.10, “D-Flash Protection Register (DFPROT)”
0x3_FF0E ¹	1	Flash Nonvolatile byte Refer to Section 13.3.2.16, “Flash Option Register (FOPT)”
0x3_FF0F ¹	1	Flash Security byte Refer to Section 13.3.2.2, “Flash Security Register (FSEC)”

1. 0x3FF08-0x3_FF0F form a Flash phrase and must be programmed in a single command write sequence. Each byte in the 0x3_FF08 - 0x3_FF0B reserved field should be programmed to 0xFF.


Figure 13-13. 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 13.3.2.9.1, “P-Flash Protection Restrictions,” and Table 13-20).

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 0x3_FF0C located in P-Flash memory (see Table 13-3) as indicated by reset condition ‘F’ in Figure 13-13. 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 13-16. 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 13-17 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 0x3_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 in Table 13-18. 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 0x3_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 13-19. The FPLS bits can only be written to while the FPLDIS bit is set.

P-Flash phrase containing the D-Flash protection byte during the reset sequence, the DPOPEN bit will be cleared and DPS bits will be set to leave the D-Flash memory fully protected.

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

Table 13-21. DFPROT Field Descriptions

Field	Description
7 DPOPEN	D-Flash Protection Control 0 Enables D-Flash memory protection from program and erase with protected address range defined by DPS bits 1 Disables D-Flash memory protection from program and erase
3–0 DPS[3:0]	D-Flash Protection Size — The DPS[3:0] bits determine the size of the protected area in the D-Flash memory as shown in Table 13-22 .

Table 13-22. D-Flash Protection Address Range

DPS[3:0]	Global Address Range	Protected Size
0000	0x0_4400 – 0x0_44FF	256 bytes
0001	0x0_4400 – 0x0_45FF	512 bytes
0010	0x0_4400 – 0x0_46FF	768 bytes
0011	0x0_4400 – 0x0_47FF	1024 bytes
0100	0x0_4400 – 0x0_48FF	1280 bytes
0101	0x0_4400 – 0x0_49FF	1536 bytes
0110	0x0_4400 – 0x0_4AFF	1792 bytes
0111	0x0_4400 – 0x0_4BFF	2048 bytes
1000	0x0_4400 – 0x0_4CFF	2304 bytes
1001	0x0_4400 – 0x0_4DFF	2560 bytes
1010	0x0_4400 – 0x0_4EFF	2816 bytes
1011	0x0_4400 – 0x0_4FFF	3072 bytes
1100	0x0_4400 – 0x0_50FF	3328 bytes
1101	0x0_4400 – 0x0_51FF	3584 bytes
1110	0x0_4400 – 0x0_52FF	3840 bytes
1111	0x0_4400 – 0x0_53FF	4096 bytes

13.3.2.11 Flash Common Command Object Register (FCCOB)

The FCCOB is an array of six words addressed via the CCOBIX index found in the FCCOBIX register. Byte wide reads and writes are allowed to the FCCOB register.

Read: Anytime but will always return 0x0000 (1 state is transient)

Write: Anytime

Table 14-3. CFORC Field Descriptions

Field	Description
7:0 FOC[7:0]	<p>Force Output Compare Action for Channel 7:0 — A write to this register with the corresponding data bit(s) set causes the action which is programmed for output compare “x” to occur immediately. The action taken is the same as if a successful comparison had just taken place with the TCx register except the interrupt flag does not get set.</p> <p>Note: A channel 7 event, which can be a counter overflow when TTOV[7] is set or a successful output compare on channel 7, overrides any channel 6:0 compares. If forced output compare on any channel occurs at the same time as the successful output compare then forced output compare action will take precedence and interrupt flag won't get set.</p>

14.3.2.3 Output Compare 7 Mask Register (OC7M)

Module Base + 0x0002

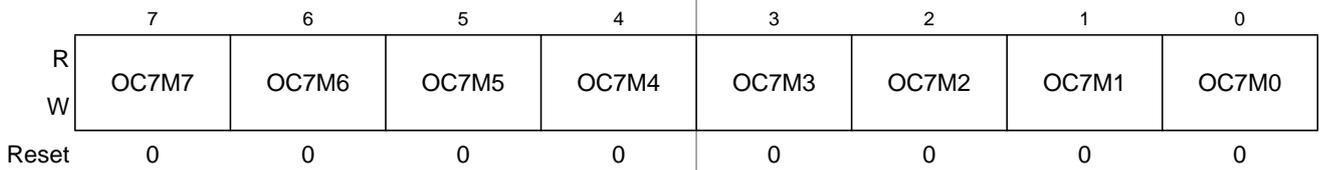


Figure 14-8. Output Compare 7 Mask Register (OC7M)

Read: Anytime

Write: Anytime

Table 14-4. OC7M Field Descriptions

Field	Description
7:0 OC7M[7:0]	<p>Output Compare 7 Mask — A channel 7 event, which can be a counter overflow when TTOV[7] is set or a successful output compare on channel 7, overrides any channel 6:0 compares. For each OC7M bit that is set, the output compare action reflects the corresponding OC7D bit.</p> <p>0 The corresponding OC7Dx bit in the output compare 7 data register will not be transferred to the timer port on a channel 7 event, even if the corresponding pin is setup for output compare.</p> <p>1 The corresponding OC7Dx bit in the output compare 7 data register will be transferred to the timer port on a channel 7 event.</p> <p>Note: The corresponding channel must also be setup for output compare (IOSx = 1 and OCPDx = 0) for data to be transferred from the output compare 7 data register to the timer port.</p>

NOTE

In the following context V_{DD35} is used for either VDDA, VDDR, and VDDX; V_{SS35} is used for either VSSA and VSSX unless otherwise noted.

I_{DD35} denotes the sum of the currents flowing into the VDDA, VDDX and VDDR pins.

A.1.3 Pins

There are four groups of functional pins.

A.1.3.1 I/O Pins

The I/O pins have a level in the range of 3.15V to 5.5V. This class of pins is comprised of all port I/O pins, the analog inputs, BKGD and the $\overline{\text{RESET}}$ pins. Some functionality may be disabled.

A.1.3.2 Analog Reference

This group is made up by the VRH and VRL pins.

A.1.3.3 Oscillator

The pins EXTAL, XTAL dedicated to the oscillator have a nominal 1.8V level.

A.1.3.4 TEST

This pin is used for production testing only. The TEST pin must be tied to ground in all applications.

A.1.4 Current Injection

Power supply must maintain regulation within operating V_{DD35} or V_{DD} range during instantaneous and operating maximum current conditions. If positive injection current ($V_{in} > V_{DD35}$) is greater than I_{DD35} , the injection current may flow out of V_{DD35} and could result in external power supply going out of regulation. Ensure external V_{DD35} load will shunt current greater than maximum injection current. This will be the greatest risk when the MCU is not consuming power; e.g., if no system clock is present, or if clock rate is very low which would reduce overall power consumption.

A.1.5 Absolute Maximum Ratings

Absolute maximum ratings are stress ratings only. A functional operation under or outside those maxima is not guaranteed. Stress beyond those limits may affect the reliability or cause permanent damage of the device.

This device contains circuitry protecting against damage due to high static voltage or electrical fields; however, it is advised that normal precautions be taken to avoid application of any voltages higher than maximum-rated voltages to this high-impedance circuit. Reliability of operation is enhanced if unused inputs are tied to an appropriate logic voltage level (e.g., either V_{SS35} or V_{DD35}).

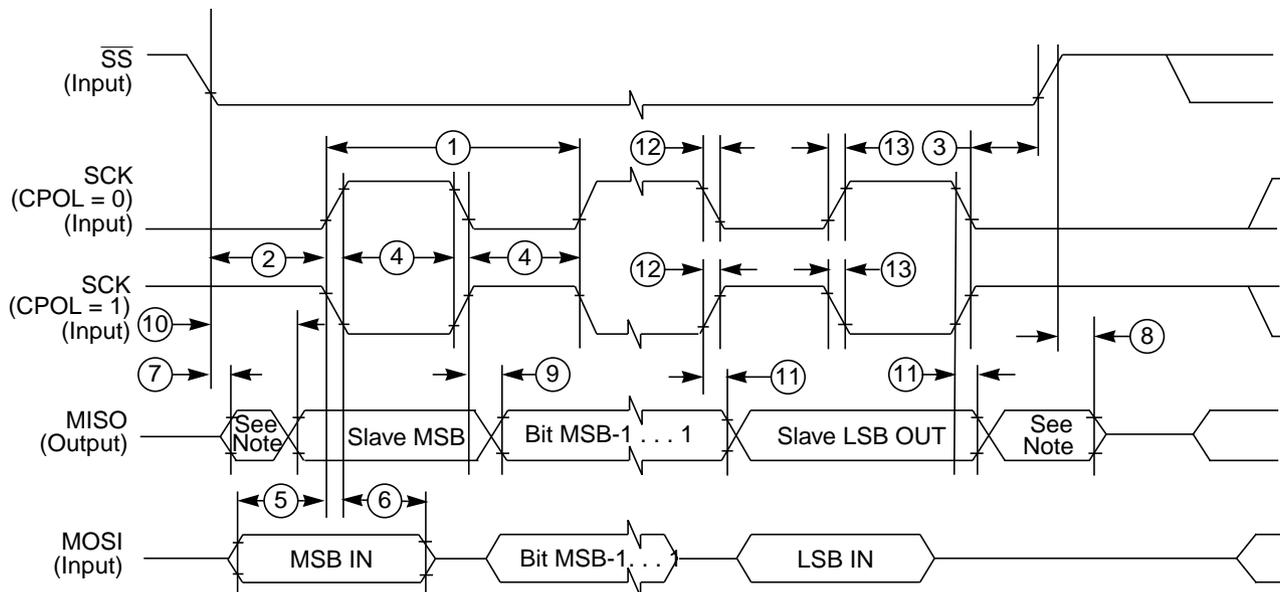
In Table A-27 the timing characteristics for master mode are listed.

Table A-27. SPI Master Mode Timing Characteristics

Num	C	Characteristic	Symbol	Min	Typ	Max	Unit
1	D	SCK frequency	f_{sck}	1/2048	—	1/2	f_{bus}
1	D	SCK period	t_{sck}	2	—	2048	t_{bus}
2	D	Enable lead time	t_{lead}	—	1/2	—	t_{sck}
3	D	Enable lag time	t_{lag}	—	1/2	—	t_{sck}
4	D	Clock (SCK) high or low time	t_{wsck}	—	1/2	—	t_{sck}
5	D	Data setup time (inputs)	t_{su}	8	—	—	ns
6	D	Data hold time (inputs)	t_{hi}	8	—	—	ns
9	D	Data valid after SCK edge	t_{vsck}	—	—	29	ns
10	D	Data valid after \overline{SS} fall (CPHA = 0)	t_{vss}	—	—	15	ns
11	D	Data hold time (outputs)	t_{ho}	20	—	—	ns
12	D	Rise and fall time inputs	t_{rfi}	—	—	8	ns
13	D	Rise and fall time outputs	t_{rfo}	—	—	8	ns

A.11.2 Slave Mode

In Figure A-7 the timing diagram for slave mode with transmission format CPHA = 0 is depicted.



NOTE: Not defined

Figure A-7. SPI Slave Timing (CPHA = 0)



0x0100-0x0113 NVM Contol Register (FTMRC) Map

Address	Name		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0x010D	FRSV2	R	0	0	0	0	0	0	0	0
		W								
0x010E	FRSC3	R	0	0	0	0	0	0	0	0
		W								
0x010F	FRSV4	R	0	0	0	0	0	0	0	0
		W								
0x0110	FOPT	R	NV7	NV6	NV5	NV4	NV3	NV2	NV1	NV0
		W								
0x0111	FRSV5	R	0	0	0	0	0	0	0	0
		W								
0x0112	FRSV6	R	0	0	0	0	0	0	0	0
		W								
0x0113	FRSV7	R	0	0	0	0	0	0	0	0
		W								

0x0114-0x011F Reserved

Address	Name		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0x0114-0x011F	Reserved	R	0	0	0	0	0	0	0	0
		W								

0x0120 Interrupt Vector Base Register

Address	Name		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0x0120	IVBR	R	IVB_ADDR[7:0]							
		W								

0x0121-0x013F Reserved

Address	Name		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0x0114-0x011F	Reserved	R	0	0	0	0	0	0	0	0
		W								

0x0140-0x017F MSCAN Map

Address	Name		Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0x0140	CAN0CTL0	R	RXFRM	RXACT	CSWAI	SYNCH	TIME	WUPE	SLPRQ	INITRQ
		W								
0x0141	CAN0CTL1	R	CANE	CLKSRC	LOOPB	LISTEN	BORM	WUPM	SLPAK	INITAK
		W								
0x0142	CAN0BTR0	R	SJW1	SJW0	BRP5	BRP4	BRP3	BRP2	BRP1	BRP0
		W								