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	ARM® Cortex®-M7
Core Size	32-Bit Single-Core
Speed	300MHz
Connectivity	CANbus, I²C, IrDA, LINbus, MMC/SD/SDIO, QSPI, SPI, SSC, UART/USART, USB
Peripherals	Brown-out Detect/Reset, DMA, I²S, POR, PWM, WDT
Number of I/O	75
Program Memory Size	512KB (512K x 8)
Program Memory Type	FLASH
EEPROM Size	-
RAM Size	256K x 8
Voltage - Supply (Vcc/Vdd)	3V ~ 3.6V
Data Converters	A/D 10x12b; D/A 2x12b
Oscillator Type	Internal
Operating Temperature	-40°C ~ 105°C (TA)
Mounting Type	Surface Mount
Package / Case	100-TFBGA
Supplier Device Package	100-TFBGA (9x9)
Purchase URL	https://www.e-xfl.com/product-detail/microchip-technology/atsamv70n19b-cb

Table of Contents

All lock regions must be unlocked before the Full Erase command by using the CLB command. Otherwise, the erase command is aborted and no page is erased.

Table 18-8. Full Erase Command

Step	Handshake Sequence	MODE[3:0]	DATA[15:0]
1	Write handshaking	CMDE	EA
2	Write handshaking	DATA	0

18.3.5.4 Flash Lock Commands

Lock bits can be set using WPL or EWPL commands. They can also be set by using the Set Lock command (SLB). With this command, several lock bits can be activated. A Bit Mask is provided as argument to the command. When bit 0 of the bit mask is set, then the first lock bit is activated.

In the same way, the Clear Lock command (CLB) is used to clear lock bits.

Table 18-9. Set and Clear Lock Bit Command

Step	Handshake Sequence	MODE[3:0]	DATA[15:0]
1	Write handshaking	CMDE	SLB or CLB
2	Write handshaking	DATA	Bit Mask

Lock bits can be read using Get Lock Bit command (GLB). The n^{th} lock bit is active when the bit n of the bit mask is set.

Table 18-10. Get Lock Bit Command

Step	Handshake Sequence	MODE[3:0]	DATA[15:0]
1	Write handshaking	CMDE	GLB
2	Read handshaking	DATA	Lock Bit Mask Status 0 = Lock bit is cleared 1 = Lock bit is set

18.3.5.5 Flash General-purpose NVM Commands

General-purpose NVM bits (GP NVM bits) can be set using the Set GPNVM command (SGPB). This command also activates GP NVM bits. A bit mask is provided as argument to the command. When bit 0 of the bit mask is set, then the first GP NVM bit is activated.

In the same way, the Clear GPNVM command (CGPB) is used to clear general-purpose NVM bits. The general-purpose NVM bit is deactivated when the corresponding bit in the pattern value is set to 1.

Table 18-11. Set/Clear GP NVM Command

Step	Handshake Sequence	MODE[3:0]	DATA[15:0]
1	Write handshaking	CMDE	SGPB or CGPB
2	Write handshaking	DATA	GP NVM bit pattern value

General-purpose NVM bits can be read using the Get GPNVM Bit command (GGPB). The n^{th} GP NVM bit is active when bit n of the bit mask is set.

31.20.29 PMC SleepWalking Enable Register 1

Name: PMC_SLPWK_ER1
Offset: 0x0134
Property: Write-only

This register can only be written if the WPEN bit is cleared in the PMC Write Protection Mode Register.

Bit	31	30	29	28	27	26	25	24
		PID62		PID60	PID59	PID58	PID57	PID56
Access								
Reset								
Bit	23	22	21	20	19	18	17	16
			PID53	PID52	PID51	PID50	PID49	PID48
Access								
Reset								
Bit	15	14	13	12	11	10	9	8
	PID47	PID46	PID45	PID44	PID43	PID42	PID41	PID40
Access								
Reset								
Bit	7	6	5	4	3	2	1	0
	PID39		PID37		PID35	PID34	PID33	PID32
Access								
Reset								

Bits 0:3,5,7:28,30 – PID Peripheral Clock x Disable

Value	Description
0	No effect.
1	Disables the corresponding peripheral clock.

38.8.56 GMAC Deferred Transmission Frames Register

Name: GMAC_DTF
Offset: 0x148
Reset: 0x00000000
Property: Read-only

Bit	31	30	29	28	27	26	25	24
Access								
Reset								

Bit	23	22	21	20	19	18	17	16
							DEFT[17:16]	
Access							R	R
Reset							0	0

Bit	15	14	13	12	11	10	9	8
	DEFT[15:8]							
Access	R	R	R	R	R	R	R	R
Reset	0	0	0	0	0	0	0	0

Bit	7	6	5	4	3	2	1	0
	DEFT[7:0]							
Access	R	R	R	R	R	R	R	R
Reset	0	0	0	0	0	0	0	0

Bits 17:0 – DEFT[17:0] Deferred Transmission
This register counts the number of frames experiencing deferral due to carrier sense being active on their first attempt at transmission. Frames involved in any collision are not counted nor are frames that experienced a transmit underrun.

38.8.62 GMAC Multicast Frames Received Register

Name: GMAC_MFR
Offset: 0x160
Reset: 0x00000000
Property: -

Bit	31	30	29	28	27	26	25	24
	MFRX[31:24]							
Access	R	R	R	R	R	R	R	R
Reset	0	0	0	0	0	0	0	0

Bit	23	22	21	20	19	18	17	16
	MFRX[23:16]							
Access	R	R	R	R	R	R	R	R
Reset	0	0	0	0	0	0	0	0

Bit	15	14	13	12	11	10	9	8
	MFRX[15:8]							
Access	R	R	R	R	R	R	R	R
Reset	0	0	0	0	0	0	0	0

Bit	7	6	5	4	3	2	1	0
	MFRX[7:0]							
Access	R	R	R	R	R	R	R	R
Reset	0	0	0	0	0	0	0	0

Bits 31:0 – MFRX[31:0] Multicast Frames Received without Error
This register counts the number of multicast frames successfully received without error, excluding pause frames, and is only incremented if the frame is successfully filtered and copied to memory.

38.8.80 GMAC IP Header Checksum Errors Register

Name: GMAC_IHCE
Offset: 0x1A8
Reset: 0x00000000
Property: -

Bit	31	30	29	28	27	26	25	24
Access								
Reset								

Bit	23	22	21	20	19	18	17	16
Access								
Reset								

Bit	15	14	13	12	11	10	9	8
Access								
Reset								

Bit	7	6	5	4	3	2	1	0
	HCKER[7:0]							
Access	R	R	R	R	R	R	R	R
Reset	0	0	0	0	0	0	0	0

Bits 7:0 – HCKER[7:0] IP Header Checksum Errors
This register counts the number of frames discarded due to an incorrect IP header checksum, but are between 64 and 1518 Bytes (1536 Bytes if GMAC_NCFGR.MAXFS=1) and do not have a CRC error, an alignment error, nor a symbol error.

Bit 17 – CTRLDIR Control Direction

Value	Description
0	Cleared after a SETUP packet to indicate that the following packet is an OUT packet.
1	Set after a SETUP packet to indicate that the following packet is an IN packet.

Bit 16 – RWALL Read/Write Allowed
This bit is set for IN endpoints when the current bank is not full, i.e., the user can write further data into the FIFO.

This bit is set for OUT endpoints when the current bank is not empty, i.e., the user can read further data from the FIFO.

This bit is never set if USBHS_DEVEPTIMRx.STALLRQ = 1 or in case of error.

This bit is cleared otherwise.

This bit should not be used for control endpoints.

Bits 15:14 – CURRBK[1:0] Current Bank
This bit is set for non-control endpoints, to indicate the current bank:

This field may be updated one clock cycle after the RWALL bit changes, so the user should not poll this field as an interrupt bit.

Value	Name	Description
0	BANK0	Current bank is bank0
1	BANK1	Current bank is bank1
2	BANK2	Current bank is bank2
3	Reserved	

Bits 13:12 – NBUSYBK[1:0] Number of Busy Banks
This field is set to indicate the number of busy banks:

For IN endpoints, it indicates the number of banks filled by the user and ready for IN transfer. When all banks are free, this triggers a PEP_x interrupt if NBUSYBKE = 1.

For OUT endpoints, it indicates the number of banks filled by OUT transactions from the host. When all banks are busy, this triggers a PEP_x interrupt if NBUSYBKE = 1.

When the USBHS_DEVEPTIMRx.FIFOCON bit is cleared (by writing a one to the USBHS_DEVEPTIMRx.FIFOCONC bit) to validate a new bank, this field is updated two or three clock cycles later to calculate the address of the next bank.

A PEP_x interrupt is triggered if:

Value	Name	Description
0	0_BUSY	0 busy bank (all banks free)
1	1_BUSY	1 busy bank
2	2_BUSY	2 busy banks
3	3_BUSY	3 busy banks • for IN endpoint, USBHS_DEVEPTIMRx.NBUSYBKE = 1 and all the banks are free;

39.6.45 Host Pipe x Status Register (Control, Bulk Pipes)

Name: USBHS_HSTPIPISRx
Offset: 0x0530 + x*0x04 [x=0..9]
Reset: 0
Property: Read/Write

This register view is relevant only if PTYPE = 0x0 or 0x2 in "Host Pipe x Configuration Register".

Bit	31	30	29	28	27	26	25	24
		PBYCT[10:4]						
Access								
Reset		0	0	0	0	0	0	0

Bit	23	22	21	20	19	18	17	16
	PBYCT[3:0]					CFGOK		RWALL
Access								
Reset	0	0	0	0		0		0

Bit	15	14	13	12	11	10	9	8
	CURRBK[1:0]		NBUSYBK[1:0]				DTSEQ[1:0]	
Access								
Reset	0	0	0	0			0	0

Bit	7	6	5	4	3	2	1	0
	SHORTPACKETI	RXSTALLDI	OVERFI	NAKEDI	PERRI	TXSTPI	TXOUTI	RXINI
Access								
Reset	0	0	0	0	0	0	0	0

Bits 30:20 – PBYCT[10:0] Pipe Byte Count
This field contains the byte count of the FIFO.

For an OUT pipe, the field is incremented after each byte written by the user into the pipe and decremented after each byte sent to the peripheral.

For an IN pipe, the field is incremented after each byte received from the peripheral and decremented after each byte read by the user from the pipe.

This field may be updated 1 clock cycle after the RWALL bit changes, so the user should not poll this field as an interrupt bit.

Bit 18 – CFGOK Configuration OK Status
This bit is set/cleared when the USBHS_HSTPIPCFGx.ALLOC bit is set.

This bit is set if the pipe x number of banks (USBHS_HSTPIPCFGx.PBK) and size (USBHS_HSTPIPCFGx.PSIZE) are correct compared to the maximal allowed number of banks and size for this pipe and to the maximal FIFO size (i.e., the DPRAM size).

If this bit is cleared, the user should rewrite correct values for the PBK and PSIZE fields in the USBHS_HSTPIPCFGx register.

42.6.5.3 Read Memory Transfer

The user can access the data of the serial memory by sending an instruction with QSPI_IFR.DATAEN = 1 and QSPI_IFR.TFRTYP = 1.

In this mode, the QSPI is able to read data at random address into the serial Flash memory, allowing the CPU to execute code directly from it (XIP execute-in-place).

In order to fetch data, the user must first configure the instruction frame by writing the QSPI_IFR. Then data can be read at any address in the QSPI address space mapping. The address of the system bus read accesses match the address of the data inside the serial Flash memory.

When Fetch mode is enabled, several instruction frames can be sent before writing QSPI_CR.LASTXFR. Each time the system bus read accesses become nonsequential (addresses are not consecutive), a new instruction frame is sent with the corresponding address.

42.6.5.4 Continuous Read Mode

The QSPI is compatible with the Continuous Read mode which is implemented in some serial Flash memories.

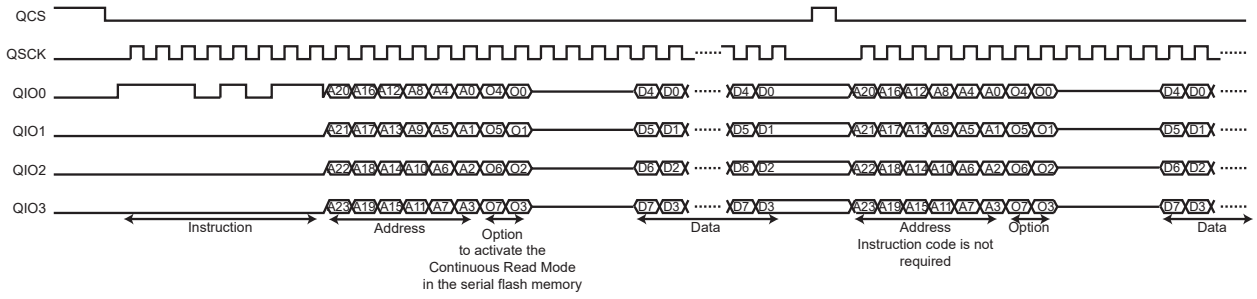
In Continuous Read mode, the instruction overhead is reduced by excluding the instruction code from the instruction frame. When the Continuous Read mode is activated in a serial Flash memory by a specific option code, the instruction code is stored in the memory. For the next instruction frames, the instruction code is not required as the memory uses the stored one.

In the QSPI, Continuous Read mode is used when reading data from the memory (QSPI_IFR.TFRTYP = 1). The addresses of the system bus read accesses are often nonsequential and this leads to many instruction frames that have the same instruction code. By disabling the send of the instruction code, the Continuous Read mode reduces the access time of the data.

To be functional, this mode must be enabled in both the QSPI and the serial Flash memory. The Continuous Read mode is enabled in the QSPI by writing CRM to ‘1’ in the QSPI_IFR (TFRTYP must equal 1). The Continuous Read mode is enabled in the serial Flash memory by sending a specific option code.

⚠ CAUTION If the Continuous Read mode is not supported by the serial Flash memory or disabled, CRM bit must not be written to ‘1’, otherwise data read out of the serial Flash memory is unpredictable.

Figure 42-10. Continuous Read Mode

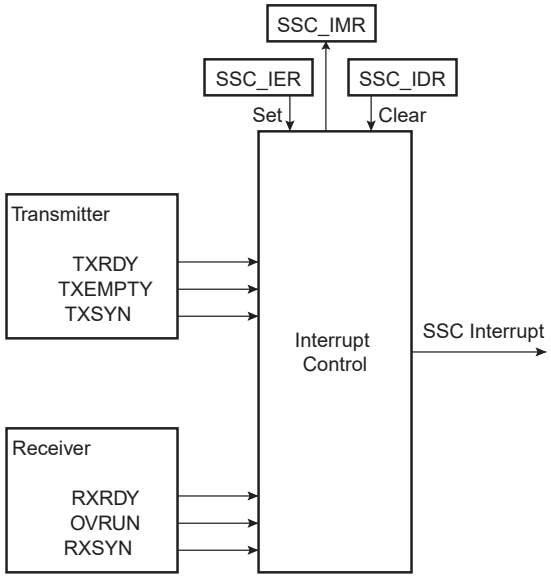


42.6.5.5 Instruction Frame Transmission Examples

All waveforms in the following examples describe SPI transfers in SPI Clock mode 0 (QSPI_SCR.CPOL = 0 and QSPI_SCR.CPHA = 0; see section Serial Clock Phase and Polarity).

All system bus accesses described below refer to the system bus address phase. System bus wait cycles and system bus data phases are not shown.

Figure 44-19. Interrupt Block Diagram



44.8.10 Register Write Protection

To prevent any single software error from corrupting SSC behavior, certain registers in the address space can be write-protected by setting the WPEN bit in the SSC Write Protection Mode Register (SSC_WPMR).

If a write access to a write-protected register is detected, the WPVS flag in the SSC Write Protection Status Register (SSC_WPSR) is set and the field WPVSRC indicates the register in which the write access has been attempted.

The WPVS bit is automatically cleared after reading the SSC_WPSR.

The following registers can be write-protected:

- SSC Clock Mode Register
- SSC Receive Clock Mode Register
- SSC Receive Frame Mode Register
- SSC Transmit Clock Mode Register
- SSC Transmit Frame Mode Register
- SSC Receive Compare 0 Register
- SSC Receive Compare 1 Register

46.7.3 USART Mode Register

Name: US_MR
Offset: 0x0004
Reset: 0x0
Property: Read/Write

This register can only be written if the WPEN bit is cleared in the USART Write Protection Mode Register.

For SPI configuration, see "USART Mode Register (SPI_MODE)".

Bit	31	30	29	28	27	26	25	24
	ONEBIT	MODSYNC	MAN	FILTER		MAX_ITERATION[2:0]		
Access								
Reset	0	0	0	0		0	0	0

Bit	23	22	21	20	19	18	17	16
	INVDATA	VAR_SYNC	DSNACK	INACK	OVER	CLKO	MODE9	MSBF
Access								
Reset	0	0	0	0	0	0	0	0

Bit	15	14	13	12	11	10	9	8
	CHMODE[1:0]		NBSTOP[1:0]		PAR[2:0]			SYNC
Access								
Reset	0	0	0	0	0	0	0	0

Bit	7	6	5	4	3	2	1	0
	CHRL[1:0]		USCLKS[1:0]		USART_MODE[3:0]			
Access								
Reset	0	0	0	0	0	0	0	0

Bit 31 – ONEBIT Start Frame Delimiter Selector

Value	Description
0	Start frame delimiter is COMMAND or DATA SYNC.
1	Start frame delimiter is one bit.

Bit 30 – MODSYNC Manchester Synchronization Mode

Value	Description
0	The Manchester start bit is a 0 to 1 transition
1	The Manchester start bit is a 1 to 0 transition.

Bit 29 – MAN Manchester Encoder/Decoder Enable

Value	Description
0	Manchester encoder/decoder are disabled.
1	Manchester encoder/decoder are enabled.

Bit 28 – FILTER Receive Line Filter

Value	Description
0	There are characters in either US_THR or the Transmit Shift Register, or the transmitter is disabled.
1	There are no characters in US_THR, nor in the Transmit Shift Register.

Bit 5 – OVRE Overrun Error (cleared by writing a one to bit US_CR.RSTSTA)

Value	Description
0	No overrun error has occurred since the last RSTSTA.
1	At least one overrun error has occurred since the last RSTSTA.

Bit 1 – TXRDY Transmitter Ready (cleared by writing US_THR)

Value	Description
0	A character is in the US_THR waiting to be transferred to the Transmit Shift Register or the transmitter is disabled. As soon as the transmitter is enabled, TXRDY becomes 1.
1	There is no character in the US_THR.

Bit 0 – RXRDY Receiver Ready (cleared by reading US_RHR)

Value	Description
0	No complete character has been received since the last read of US_RHR or the receiver is disabled. If characters were being received when the receiver was disabled, RXRDY changes to 1 when the receiver is enabled.
1	At least one complete character has been received and US_RHR has not yet been read.

Value	Description
0	Setting the bit LINWKUP in US_CR sends a LIN 2.0 wakeup signal.
1	Setting the bit LINWKUP in US_CR sends a LIN 1.3 wakeup signal.

Bit 6 – FSDIS Frame Slot Mode Disable

Value	Description
0	The Frame Slot mode is enabled.
1	The Frame Slot mode is disabled.

Bit 5 – DLM Data Length Mode

Value	Description
0	The response data length is defined by field DLC of this register.
1	The response data length is defined by bits 5 and 6 of the identifier (IDCHR in US_LINIR).

Bit 4 – CHKTYP Checksum Type

Value	Description
0	LIN 2.0 “enhanced” checksum
1	LIN 1.3 “classic” checksum

Bit 3 – CHKDIS Checksum Disable

Value	Description
0	In master node configuration, the checksum is computed and sent automatically. In slave node configuration, the checksum is checked automatically.
1	Whatever the node configuration is, the checksum is not computed/sent and it is not checked.

Bit 2 – PARDIS Parity Disable

Value	Description
0	In master node configuration, the identifier parity is computed and sent automatically. In master node and slave node configuration, the parity is checked automatically.
1	Whatever the node configuration is, the Identifier parity is not computed/sent and it is not checked.

Bits 1:0 – NACT[1:0] LIN Node Action
Values which are not listed in the table must be considered as “reserved”.

Value	Name	Description
00	PUBLISH	The USART transmits the response.
01	SUBSCRIBE	The USART receives the response.
10	IGNORE	The USART does not transmit and does not receive the response.

47.6.1 UART Control Register

Name: UART_CR
Offset: 0x00
Reset: –
Property: Write-only

Bit	31	30	29	28	27	26	25	24
Access								
Reset								

Bit	23	22	21	20	19	18	17	16
Access								
Reset								

Bit	15	14	13	12	11	10	9	8
				REQCLR				RSTSTA
Access				W				W
Reset				–				–

Bit	7	6	5	4	3	2	1	0
	TXDIS	TXEN	RXDIS	RXEN	RSTTX	RSTRX		
Access	W	W	W	W	W	W		
Reset	–	–	–	–	–	–		

Bit 12 – REQCLR Request Clear

- SleepWalking enabled:

0: No effect.

1: Bit REQCLR clears the potential clock request currently issued by UART, thus the potential system wake-up is cancelled.

- SleepWalking disabled:

0: No effect.

1: Bit REQCLR restarts the comparison trigger to enable receive holding register loading.

Bit 8 – RSTSTA Reset Status

Value	Description
0	No effect.
1	Resets the status bits PARE, FRAME, CMP and OVRE in the UART_SR.

Bit 7 – TXDIS Transmitter Disable

48.7 Register Summary

Offset	Name	Bit Pos.								
0x00	MLB_MLBC0	7:0	MLBLK		ZERO	MLBCLK[2:0]				MLBEN
		15:8	FCNT[0:0]	CTLRETRY		ASYRETRY				
		23:16							FCNT[2:1]	
		31:24								
0x04 ... 0x0B	Reserved									
0x0C	MLB_MS0	7:0	MCS: MediaLB Channel Status [31[7:0]							
		15:8	MCS: MediaLB Channel Status [31[15:8]							
		23:16	MCS: MediaLB Channel Status [31[23:16]							
		31:24	MCS: MediaLB Channel Status [31[31:24]							
0x10 ... 0x13	Reserved									
0x14	MLB_MS1	7:0	MCS: MediaLB Channel Status [63[7:0]							
		15:8	MCS: MediaLB Channel Status [63[15:8]							
		23:16	MCS: MediaLB Channel Status [63[23:16]							
		31:24	MCS: MediaLB Channel Status [63[31:24]							
0x18 ... 0x1F	Reserved									
0x20	MLB_MSS	7:0			SERVREQ	SWSYSCMD	CSSYSCMD	ULKSYSCMD	LKSYSCMD	RSTSYSCMD
		15:8								
		23:16								
		31:24								
0x24	MLB_MSD	7:0	SD0[7:0]							
		15:8	SD1[7:0]							
		23:16	SD2[7:0]							
		31:24	SD3[7:0]							
0x28 ... 0x2B	Reserved									
0x2C	MLB_MIEN	7:0							ISOC_BUFO	ISOC_PE
		15:8								
		23:16		ATX_BREAK	ATX_PE	ATX_DONE	ARX_BREAK	ARX_PE	ARX_DONE	SYNC_PE
		31:24			CTX_BREAK	CTX_PE	CTX_DONE	CRX_BREAK	CRX_PE	CRX_DONE
0x30 ... 0x3B	Reserved									
0x3C	MLB_MLBC1	7:0	CLKM	LOCK						
		15:8	NDA[7:0]							
		23:16								
		31:24								
0x40	Reserved									

Value	Description
0	No counter overflow has occurred since the last read of the Status Register.
1	A counter overflow has occurred since the last read of the Status Register.

Register	UPDM = 0	UPDM = 1	UPDM = 2
	Update is triggered at the next PWM period as soon as the bit UPDULOCK is set to '1'	Update is triggered at the next PWM period as soon as the update period counter has reached the value UPR.	
Update Period Value (PWM_SCUPUPD)	Not applicable	Write by the processor	
	Not applicable	Update is triggered at the next PWM period as soon as the update period counter has reached the value UPR.	

51.6.2.9.1 Method 1: Manual write of duty-cycle values and manual trigger of the update

In this mode, the update of the period value, the duty-cycle values and the dead-time values must be done by writing in their respective update registers with the processor (respectively PWM_CPRDUPDx, PWM_CDTYUPDx and PWM_DTUPDx).

To trigger the update, the user must use the bit UPDULOCK in the PWM_SCUC register which allows to update synchronously (at the same PWM period) the synchronous channels:

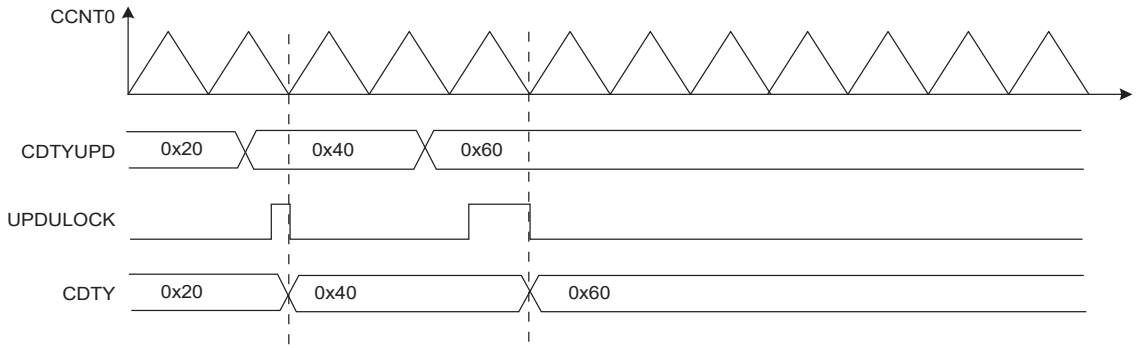
- If the bit UPDULOCK is set to '1', the update is done at the next PWM period of the synchronous channels.
- If the UPDULOCK bit is not set to '1', the update is locked and cannot be performed.

After writing the UPDULOCK bit to '1', it is held at this value until the update occurs, then it is read 0.

Sequence for Method 1:

1. Select the manual write of duty-cycle values and the manual update by setting the UPDM field to '0' in the PWM_SCM register.
2. Define the synchronous channels by the SYNCx bits in the PWM_SCM register.
3. Enable the synchronous channels by writing CHID0 in the PWM_ENA register.
4. If an update of the period value and/or the duty-cycle values and/or the dead-time values is required, write registers that need to be updated (PWM_CPRDUPDx, PWM_CDTYUPDx and PWM_DTUPDx).
5. Set UPDULOCK to '1' in PWM_SCUC.
6. The update of the registers will occur at the beginning of the next PWM period. When the UPDULOCK bit is reset, go to Step 4. for new values.

Figure 51-19. Method 1 (UPDM = 0)



Value	Name	Description
2	SUT16	16 periods of AFE clock
3	SUT24	24 periods of AFE clock
4	SUT64	64 periods of AFE clock
5	SUT80	80 periods of AFE clock
6	SUT96	96 periods of AFE clock
7	SUT112	112 periods of AFE clock
8	SUT512	512 periods of AFE clock
9	SUT576	576 periods of AFE clock
10	SUT640	640 periods of AFE clock
11	SUT704	704 periods of AFE clock
12	SUT768	768 periods of AFE clock
13	SUT832	832 periods of AFE clock
14	SUT896	896 periods of AFE clock
15	SUT960	960 periods of AFE clock

Bits 15:8 – PRESCAL[7:0] Prescaler Rate Selection
PRESCAL = $f_{peripheral\ clock}$/ $f_{AFE\ Clock}$ - 1

When PRESCAL is cleared, no conversion is performed.

Bit 7 – FREERUN Free Run Mode

Value	Name	Description
0	OFF	Normal mode
1	ON	Free Run mode: never wait for any trigger.

Bit 6 – FWUP Fast Wakeup

Value	Name	Description
0	OFF	Normal Sleep mode: the sleep mode is defined by the SLEEP bit.
1	ON	Fast Wakeup Sleep mode: the voltage reference is ON between conversions and AFE is OFF.

Bit 5 – SLEEP Sleep Mode

Value	Name	Description
0	NORMAL	Normal mode: the AFE and reference voltage circuitry are kept ON between conversions.
1	SLEEP	Sleep mode: the AFE and reference voltage circuitry are OFF between conversions.

Bits 3:1 – TRGSEL[2:0] Trigger Selection

Value	Name	Description
0	AFEC_TRIG0	AFE0_ADTRG for AFEC0 / AFE1_ADTRG for AFEC1
1	AFEC_TRIG1	TIOA Output of the Timer Counter Channel 0 for AFEC0/TIOA Output of the Timer Counter Channel 3 for AFEC1
2	AFEC_TRIG2	TIOA Output of the Timer Counter Channel 1 for AFEC0/TIOA Output of the Timer Counter Channel 4 for AFEC1

57.3 Product Dependencies

57.3.1 Power Management

The AES is clocked through the Power Management Controller (PMC), so the programmer must first configure the PMC to enable the AES clock.

57.3.2 Interrupt Sources

The AES interface has an interrupt line connected to the Interrupt Controller.

Handling the AES interrupt requires programming the Interrupt Controller before configuring the AES.

57.4 Functional Description

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.

Encryption converts data to an unintelligible form called ciphertext. Decrypting the ciphertext converts the data back into its original form, called plaintext. The CIPHER bit in the AES Mode register (AES_MR) allows selection between the encryption and the decryption processes.

The AES is capable of using cryptographic keys of 128/192/256 bits to encrypt and decrypt data in blocks of 128 bits. This 128-bit/192-bit/256-bit key is defined in the user interface AES_KEYWRx register.

The input to the encryption processes of the CBC, CFB, and OFB modes includes, in addition to the plaintext, a 128-bit data block called the initialization vector (IV), which must be set in AES_IVRx. The initialization vector is used in an initial step in the encryption of a message and in the corresponding decryption of the message. AES_IVRx are also used by the CTR mode to set the counter value.

57.4.1 AES Register Endianness

In ARM processor-based products, the system bus and processors manipulate data in little-endian form. The AES interface requires little-endian format words. However, in accordance with the protocol of the FIPS 197 specification, data is collected, processed and stored by the AES algorithm in big-endian form.

The following example illustrates how to configure the AES:

If the first 64 bits of a message (according to FIPS 197, i.e., big-endian format) to be processed is 0xcafedeca_01234567, then AES_IDATAR0 and AES_IDATAR1 registers must be written with the following pattern:

- AES_IDATAR0 = 0xcadefeca
- AES_IDATAR1 = 0x67452301

57.4.2 Operating Modes

The AES supports the following modes of operation:

- ECB: Electronic Codebook
- CBC: Cipher Block Chaining
  - CBC-MAC: Useful for CMAC hardware acceleration
- OFB: Output Feedback
- CFB: Cipher Feedback

57.5.13 AES GCM Intermediate Hash Word Register x

Name: AES_GHASHRx
Offset: 0x78 + x*0x04 [x=0..3]
Reset: 0x00000000
Property: R/W

Bit	31	30	29	28	27	26	25	24
	GHASH[31:24]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bit	23	22	21	20	19	18	17	16
	GHASH[23:16]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bit	15	14	13	12	11	10	9	8
	GHASH[15:8]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bit	7	6	5	4	3	2	1	0
	GHASH[7:0]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bits 31:0 – GHASH[31:0] Intermediate GCM Hash Word x
The four 32-bit Intermediate Hash Word registers expose the intermediate GHASH value. May be read to save the current GHASH value so processing can later be resumed, presumably on a later message fragment. Whenever a new key is written to the AES Key Register two automatic actions are processed:

- GCM hash subkey generation
- AES_GHASHRx Clear

See Key Writing and Automatic Hash Subkey Calculation for details.

If an application software-specific hash initial value is needed for the GHASH, it must be written to AES_GHASHRx:

- after a write to the AES Key Register, if any,
- before starting the input data feed.