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®-M4F
Core Size	32-Bit Single-Core
Speed	120MHz
Connectivity	EBI/EMI, I²C, IrDA, LINbus, MMC/SD, QSPI, SPI, UART/USART, USB
Peripherals	Brown-out Detect/Reset, DMA, I²S, POR, PWM
Number of I/O	51
Program Memory Size	1MB (1M x 8)
Program Memory Type	FLASH
EEPROM Size	-
RAM Size	256K x 8
Voltage - Supply (Vcc/Vdd)	1.71V ~ 3.63V
Data Converters	A/D 24x12b; D/A 2x12b
Oscillator Type	Internal
Operating Temperature	-40°C ~ 85°C (TA)
Mounting Type	Surface Mount
Package / Case	64-VFQFN Exposed Pad
Supplier Device Package	64-VQFN (9x9)
Purchase URL	https://www.e-xfl.com/product-detail/microchip-technology/atsamd51j20a-mut

Offset	Name	Bit Pos.								
0x1FE8	PID2	7:0	REVISION[3:0]				JEPU	JEPIDCH[2:0]		
		15:8								
		23:16								
		31:24								
0x1FEC	PID3	7:0	REVAND[3:0]				CUSMOD[3:0]			
		15:8								
		23:16								
		31:24								
0x1FF0	CID0	7:0	PREAMBLEB0[7:0]							
		15:8								
		23:16								
		31:24								
0x1FF4	CID1	7:0	CCLASS[3:0]				PREAMBLE[3:0]			
		15:8								
		23:16								
		31:24								
0x1FF8	CID2	7:0	PREAMBLEB2[7:0]							
		15:8								
		23:16								
		31:24								
0x1FFC	CID3	7:0	PREAMBLEB3[7:0]							
		15:8								
		23:16								
		31:24								

12.13 Register Description

Registers can be 8, 16, or 32 bits wide. Atomic 8-, 16- and 32-bit accesses are supported. In addition, the 8-bit quarters and 16-bit halves of a 32-bit register, and the 8-bit halves of a 16-bit register can be accessed directly.

Some registers are optionally write-protected by the Peripheral Access Controller (PAC). Optional PAC write-protection is denoted by the "PAC Write-Protection" property in each individual register description. For details, refer to 12.5.7 Register Access Protection.

18.8.1 Control A

Name: CTRLA
Offset: 0x00
Reset: 0x00
Property: PAC Write-Protection

Bit	7	6	5	4	3	2	1	0
						IORET		
Access						R/W		
Reset						0		

Bit 2 – IORET I/O Retention
Note: This bit is not reset by a hibernate or backup reset. When the IORET feature is used, the debugger access to the chip will not be allowed until the IORET bit is cleared after waking up from hibernate or backup sleep. When the IORET is set in active mode, the PORT can still be controlled by peripherals and the PORT registers. It is only when the device wakes up from hibernate or backup sleep mode that the IORET= 1 will prevent the PORT from being controlled by the peripherals or PORT registers. POR and BOD33 resets can clear the IORET bit.

Value	Description
0	After waking up from Hibernate or Backup mode, I/O lines are not held.
1	After waking up from Hibernate or Backup mode, I/O lines are held until IORET is written to 0.

Value	Name	Description
0xB	DIV4096	Divide clock by 4096
0xC	DIV8192	Divide clock by 8192
0xD	DIV16384	Divide clock by 16384
0xE	DIV32768	Divide clock by 32768
0xF	DIV65536	Divide clock by 65536

Bit 8 – ACTCFG BOD12 Configuration in Active Sleep Mode
This field is not synchronized.

Value	Description
0	In active mode, the BOD12 operates in continuous mode.
1	In active mode, the BOD12 operates in sampling mode.

Bit 6 – RUNSTDBY Run in Standby
This bit is not synchronized.

Value	Description
0	In standby sleep mode, the BOD12 is disabled.
1	In standby sleep mode, the BOD12 is enabled.

Bit 5 – STDBYCFG BOD12 Configuration in Standby Sleep Mode
If the RUNSTDBY bit is set to 1, the STDBYCFG bit sets the BOD12 configuration in standby sleep mode.

This field is not synchronized.

Value	Description
0	In standby sleep mode, the BOD12 is enabled and configured in continuous mode.
1	In standby sleep mode, the BOD12 is enabled and configured in sampling mode.

Bits 4:3 – ACTION[1:0] BOD12 Action
These bits are used to select the BOD12 action when the supply voltage crosses below the BOD12 threshold.

These bits are loaded from NVM User Row at start-up.

This field is not synchronized.

Value	Name	Description
0x0	NONE	No action.
0x1	RESET	The BOD12 generates a reset.
0x2	INT	The BOD12 generates an interrupt.
0x3	-	Reserved

Bit 2 – HYST Hysteresis
This bit indicates whether hysteresis is enabled for the BOD12 threshold voltage:

This bit is not synchronized.

Value	Description
0	No hysteresis.
1	Hysteresis enabled.

21.12.4 Interrupt Enable Clear in Clock/Calendar mode (CTRLA.MODE=2)

Name: INTENCLR
Offset: 0x08
Reset: 0x0000
Property: PAC Write-Protection

This register allows the user to disable an interrupt without doing a read-modify-write operation. Changes in this register will also be reflected in the Interrupt Enable Set (INTENSET) register.

Bit	15	14	13	12	11	10	9	8
	OVF	TAMPER					ALARMn[1:0]	
Access	R/W	R/W					R/W	R/W
Reset	0	0					0	0

Bit	7	6	5	4	3	2	1	0
	PERn[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

Bit 15 – OVF Overflow Interrupt Enable
Writing a '0' to this bit has no effect. Writing a '1' to this bit will clear the Overflow Interrupt Enable bit, which disables the Overflow interrupt.

Value	Description
0	The Overflow interrupt is disabled.
1	The Overflow interrupt is enabled.

Bit 14 – TAMPER Tamper Interrupt Enable

Bits 9:8 – ALARMn[1:0] Alarm n Interrupt Enable [n = 1..0]
Writing a '0' to this bit has no effect. Writing a '1' to this bit will clear the Alarm n Interrupt Enable bit, which disables the Alarm n interrupt.

Value	Description
0	The Alarm n interrupt is disabled.
1	The Alarm n interrupt is enabled.

Bits 7:0 – PERn[7:0] Periodic Interval n Interrupt Enable [n = 7..0]
Writing a '0' to this bit has no effect. Writing a '1' to this bit will clear the Periodic Interval n Interrupt Enable bit, which disables the Periodic Interval n interrupt.

Value	Description
0	Periodic Interval n interrupt is disabled.
1	Periodic Interval n interrupt is enabled.

21.12.7 Debug Control

Name: DBGCTRL
Offset: 0x0E
Reset: 0x00
Property: PAC Write-Protection

Bit	7	6	5	4	3	2	1	0
								DBGRUN
Access								R/W
Reset								0

Bit 0 – DBGRUN Debug Run
This bit is not reset by a software reset.

This bit controls the functionality when the CPU is halted by an external debugger.

Value	Description
0	The RTC is halted when the CPU is halted by an external debugger.
1	The RTC continues normal operation when the CPU is halted by an external debugger.

Value	Description
0	There is no reset operation ongoing.
1	The reset operation is ongoing.

24.8 Register Summary

Offset	Name	Bit Pos.								
0x00	NCR	7:0	WESTAT	INCSTAT	CLRSTAT	MPE	TXEN	RXEN	LBL	
		15:8	SRTSM			TXZQPF	TXPF	THALT	TSTART	BP
		23:16					LPI	FNP	TXPBPF	ENPBPR
		31:24								
0x04	NCFGR	7:0	UNIHEN	MTIHEN	NBC	CAF	JFRAME	DNVLAN	FD	SPD
		15:8	RXBUFO[1:0]		PEN	RTY				MAXFS
		23:16	DCPF			CLK[2:0]			RFCS	LFERD
		31:24		IRXER	RXBP	IPGSEN		IRXFCS	EFRHD	RXCOEN
0x08	NSR	7:0						IDLE	MDIO	
		15:8								
		23:16								
		31:24								
0x0C	UR	7:0								MII
		15:8								
		23:16								
		31:24								
0x10	DCFGR	7:0	ESPA	ESMA		FBLDO[4:0]				
		15:8					TXCOEN	TXPBMS	RXBMS[1:0]	
		23:16	DRBS[7:0]							
		31:24								DDRP
0x14	TSR	7:0			TXCOMP	TFC	TXGO	RLE	COL	UBR
		15:8								HRESP
		23:16								
		31:24								
0x18	RBQB	7:0	ADDR[5:0]							
		15:8	ADDR[13:6]							
		23:16	ADDR[21:14]							
		31:24	ADDR[29:22]							
0x1C	TBQB	7:0	ADDR[5:0]							
		15:8	ADDR[13:6]							
		23:16	ADDR[21:14]							
		31:24	ADDR[29:22]							
0x20	RSR	7:0					HNO	RXOVR	REC	BNA
		15:8								
		23:16								
		31:24								
0x24	ISR	7:0	TCOMP	TFC	RLEX	TUR	TXUBR	RXUBR	RCOMP	MFS
		15:8		PFTR	PTZ	PFNZ	HRESP	ROVR		
		23:16	PDRSFR	PDRQFR	SFT	DRQFT	SFR	DRQFR		
		31:24				WOL		SRI	PDRSFT	PDRQFT
0x28	IER	7:0	TCOMP	TFC	RLEX	TUR	TXUBR	RXUBR	RCOMP	MFS
		15:8	EXINT	PFTR	PTZ	PFNZ	HRESP	ROVR		
		23:16	PDRSFR	PDRQFR	SFT	DRQFT	SFR	DRQFR		

24.9.14 GMAC PHY Maintenance Register

Name: MAN
Offset: 0x034
Reset: 0x00000000
Property: Read/Write

This register is a shift register. Writing to it starts a shift operation which is signaled completed when bit 2 is set in the Network Status Register (NSR). It takes about 2000 MCK cycles to complete, when MDC is set for MCK divide by 32 in the Network Configuration Register. An interrupt is generated upon completion.

During this time, the MSB of the register is output on the MDIO pin and the LSB updated from the MDIO pin with each MDC cycle. This causes transmission of a PHY management frame on MDIO. Refer also to section 22.2.4.5 of the IEEE 802.3 standard.

Reading during the shift operation returns the current contents of the shift register. At the end of management operation, the bits will have shifted back to their original locations. For a read operation, the data bits are updated with data read from the PHY. It is important to write the correct values to the register to ensure a valid PHY management frame is produced.

The MDIO interface can read IEEE 802.3 clause 45 PHYs, as well as clause 22 PHYs. To read clause 45 PHYs, bit 30 should be written with a '0' rather than a '1'. To write clause 45 PHYs, bits 31:28 should be written as 0x1:

PHY	Access	Bit Value			
		WZO	CLTTO	OP[1]	OP[0]
Clause 22	Read	0	1	1	0
	Write	0	1	0	1
Clause 45	Read	0	0	1	1
	Write	0	0	0	1
	Read + Address	0	0	1	0

For a description of MDC generation, see also the 'GMAC Network Configuration Register' (NCR) description.

Clock Failure Detection

The CFD is reset only at power-on (POR). The CFD does not monitor the XOSC32K clock when the oscillator is disabled (XOSC32K.ENABLE=0).

Before starting CFD operation, the user must start and enable the safe clock source (OSCULP32K oscillator).

CFD operation is started by writing a '1' to the CFD Enable bit in the External Oscillator Control register (CFDCTRL.CFDEN). After starting or restarting the XOSC32K, the CFD does not detect failure until the start-up time has elapsed. The start-up time is configured by the Oscillator Start-Up Time in the External Multipurpose Crystal Oscillator Control register (XOSC32K.STARTUP). Once the XOSC32K Start-Up Time is elapsed, the XOSC32K clock is constantly monitored.

During a period of 4 safe clocks (monitor period), the CFD watches for a clock activity from the XOSC32K. There must be at least one rising and one falling XOSC32K clock edge during 4 safe clock periods to meet non-failure conditions. If no or insufficient activity is detected, the failure status is asserted: The Clock Failure Detector status bit in the Status register (STATUS.XOSC32KFAIL) and the Clock Failure Detector interrupt flag bit in the Interrupt Flag register (INTFLAG.XOSC32KFAIL) are set. If the XOSC32KFAIL bit in the Interrupt Enable Set register (INTENSET.XOSC32KFAIL) is set, an interrupt is generated as well. If the Event Output enable bit in the Event Control register (EVCTRL.CFDEO) is set, an output event is generated, too.

After a clock failure was issued the monitoring of the XOSC32K clock is continued, and the Clock Failure Detector status bit in the Status register (STATUS.XOSC32KFAIL) reflects the current XOSC32K activity.

Clock Switch

When a clock failure is detected, the XOSC32K clock is replaced by the safe clock in order to maintain an active clock during the XOSC32K clock failure. The safe clock source is the OSCULP32K oscillator clock. Both 32KHz and 1KHz outputs of the XOSC32K are replaced by the respective OSCULP32K 32KHz and 1KHz outputs. The safe clock source can be scaled down by a configurable prescaler to ensure that the safe clock frequency does not exceed the operating conditions selected by the application. When the XOSC32K clock is switched to the safe clock, the Clock Switch bit in the Status register (STATUS.XOSC32KSW) is set.

When the CFD has switched to the safe clock, the XOSC32K is not disabled. If desired, the application must take the necessary actions to disable the oscillator. The application must also take the necessary actions to configure the system clocks to continue normal operations. In the case the application can recover the XOSC32K, the application can switch back to the XOSC32K clock by writing a '1' to Switch Back Enable bit in the Clock Failure Control register (CFDCTRL.SWBACK). Once the XOSC32K clock is switched back, the Switch Back bit (CFDCTRL.SWBACK) is cleared by hardware.

Prescaler

The CFD has an internal configurable prescaler to generate the safe clock from the OSCULP32K oscillator. The prescaler size allows to scale down the OSCULP32K oscillator so the safe clock frequency is not higher than the XOSC32K clock frequency monitored by the CFD. The maximum division factor is 2.

The prescaler is applied on both outputs (32KHz and 1KHz) of the safe clock.

Example 29-1. Example

For an external crystal oscillator at 32KHz and the OSCULP32K frequency is 32KHz, the XOSC32K.CFDPRESC should be set to 0 for a safe clock of equal frequency.

Offset	Name	Bit Pos.								
		15:8	ONDEMAND	RUNSTDBY			EDGSEL[1:0]		PATH[1:0]	
		23:16								
		31:24								
0x8C	CHINTENCLR13	7:0							EVD	OVR
0x8D	CHINTENSET13	7:0							EVD	OVR
0x8E	CHINTFLAG13	7:0							EVD	OVR
0x8F	CHSTATUS13	7:0							BUSYCH	RDYUSR
0x90	CHANNEL14	7:0	EVGEN[7:0]							
		15:8	ONDEMAND	RUNSTDBY			EDGSEL[1:0]		PATH[1:0]	
		23:16								
		31:24								
0x94	CHINTENCLR14	7:0							EVD	OVR
0x95	CHINTENSET14	7:0							EVD	OVR
0x96	CHINTFLAG14	7:0							EVD	OVR
0x97	CHSTATUS14	7:0							BUSYCH	RDYUSR
0x98	CHANNEL15	7:0	EVGEN[7:0]							
		15:8	ONDEMAND	RUNSTDBY			EDGSEL[1:0]		PATH[1:0]	
		23:16								
		31:24								
0x9C	CHINTENCLR15	7:0							EVD	OVR
0x9D	CHINTENSET15	7:0							EVD	OVR
0x9E	CHINTFLAG15	7:0							EVD	OVR
0x9F	CHSTATUS15	7:0							BUSYCH	RDYUSR
0xA0	CHANNEL16	7:0	EVGEN[7:0]							
		15:8	ONDEMAND	RUNSTDBY			EDGSEL[1:0]		PATH[1:0]	
		23:16								
		31:24								
0xA4	CHINTENCLR16	7:0							EVD	OVR
0xA5	CHINTENSET16	7:0							EVD	OVR
0xA6	CHINTFLAG16	7:0							EVD	OVR
0xA7	CHSTATUS16	7:0							BUSYCH	RDYUSR
0xA8	CHANNEL17	7:0	EVGEN[7:0]							
		15:8	ONDEMAND	RUNSTDBY			EDGSEL[1:0]		PATH[1:0]	
		23:16								
		31:24								
0xAC	CHINTENCLR17	7:0							EVD	OVR
0xAD	CHINTENSET17	7:0							EVD	OVR
0xAE	CHINTFLAG17	7:0							EVD	OVR
0xAF	CHSTATUS17	7:0							BUSYCH	RDYUSR
0xB0	CHANNEL18	7:0	EVGEN[7:0]							
		15:8	ONDEMAND	RUNSTDBY			EDGSEL[1:0]		PATH[1:0]	
		23:16								
		31:24								
0xB4	CHINTENCLR18	7:0							EVD	OVR
0xB5	CHINTENSET18	7:0							EVD	OVR
0xB6	CHINTFLAG18	7:0							EVD	OVR

31.7.10 Channel n Interrupt Enable Set

Name: CHINTENSET
Offset: 0x25 + n*0x08 [n=0..31]
Reset: 0x00
Property: PAC Write-Protection

Bit	7	6	5	4	3	2	1	0
							EVD	OVR
Access							RW	RW
Reset							0	0

Bit 1 – EVD Channel Event Detected Interrupt Enable
Writing a '0' to this bit has no effect.

Writing a '1' to this bit will set the Event Detected Channel Interrupt Enable bit, which enables the Event Detected Channel interrupt.

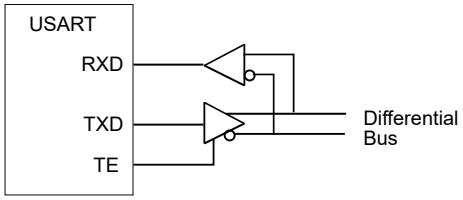
Value	Description
0	The Event Detected Channel interrupt is disabled.
1	The Event Detected Channel interrupt is enabled.

Bit 0 – OVR Channel Overrun Interrupt Enable
Writing a '0' to this bit has no effect.

Writing a '1' to this bit will set the Overrun Channel Interrupt Enable bit, which enables the Overrun Channel interrupt.

Value	Description
0	The Overrun Channel interrupt is disabled.
1	The Overrun Channel interrupt is enabled.

Figure 34-15. RS485 Bus Connection



The TE pin will remain high for the complete frame including stop bit(s). If a Guard Time is programmed in the Control C register (CTRLC.GTIME), the line will remain driven after the last character completion. The following figure shows a transfer with one stop bit and CTRLC.GTIME=3.

Figure 34-16. Example of TE Drive with Guard Time

The Transmit Complete interrupt flag (INTFLAG.TXC) will be raised after the guard time is complete and TE goes low.

34.6.3.7 ISO 7816 for Smart Card Interfacing

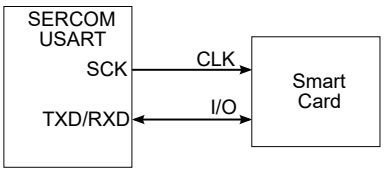
The SERCOM USART features an ISO/IEC 7816-compatible operating mode. This mode permits interfacing with smart cards and Security Access Modules (SAM) communicating through an ISO 7816 link. Both T=0 and T=1 protocols defined by the ISO 7816 specification are supported.

ISO 7816 is available with the following configuration:

- ISO 7816 format (CTRLA.FORM = 0x07)
- Inverse transmission and reception (CTRLA.RXINV=1 and CTRLA.TXINV=1)
- Single bidirectional data line (CTRLA.TXPO and CTRLA.RXPO configured to use the same data pin)
- Even parity (CTRLB.PMODE=0)
- 8-bit character size (CTRLB.CHSIZE=0)
- T=0 (CTRLA.CMODE=1) or T=1 (CTRLA.CMODE=0)

ISO 7816 is a half duplex communication on a single bidirectional line. The USART connects to a smart card as shown below. The output is only driven when the USART is transmitting. The USART is considered as the master of the communication as it generates the clock.

Figure 34-17. Connection of a Smart Card to the SERCOM USART



ISO 7816 characters are specified as 8 bits with even parity. The USART must be configured accordingly.

The USART cannot operate concurrently in both receiver and transmitter modes as the communication is unidirectional. It has to be configured according to the required mode by enabling or disabling either the receiver or the transmitter as desired. Enabling both the receiver and the transmitter at the same time in ISO 7816 mode may lead to unpredictable results.

The ISO 7816 specification defines an inverse transmission format. Data bits of the character must be transmitted on the I/O line at their negative value (CTRLA.RXINV=1 and CTRLA.TXINV=1).

39.8.17 Interrupt Enable

Name: IE
Offset: 0x54
Reset: 0x00000000
Property: -

The settings in the Interrupt Enable register determine which status changes in the Interrupt Register will be signalled on an interrupt line.

Bit	31	30	29	28	27	26	25	24
			ARAE	PEDE	PEAE	WDIE	BOE	EWE
Access			R/W	R/W	R/W	R/W	R/W	R/W
Reset			0	0	0	0	0	0

Bit	23	22	21	20	19	18	17	16
	EPE	ELOE	BEUE	BECE	DRXE	TOOE	MRAFE	TSWE
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
	TEFLE	TEFFE	TEFWE	TEFNE	TFEE	TCFE	TCE	HPME
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
	RF1LE	RF1FE	RF1WE	RF1NE	RF0LE	RF0FE	RF0WE	RF0NE
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 29 – ARAE Access to Reserved Address Interrupt Enable

Value	Description
0	Interrupt disabled.
1	Interrupt enabled.

Bit 28 – PEDE Protocol Error in Data Phase Interrupt Enable

Value	Description
0	Interrupt disabled.
1	Interrupt enabled.

Bit 27 – PEAE Protocol Error in Arbitration Phase Interrupt Enable

Value	Description
0	Interrupt disabled.
1	Interrupt enabled.

Bit 26 – WDIE Watchdog Interrupt Enable

39.8.28 Rx FIFO 0 Status

Name: RXF0S
Offset: 0xA4
Reset: 0x00000000
Property: Read-only

Bit	31	30	29	28	27	26	25	24
							RF0L	F0F
Access							R	R
Reset							0	0

Bit	23	22	21	20	19	18	17	16
			F0PI[5:0]					
Access			R	R	R	R	R	R
Reset			0	0	0	0	0	0

Bit	15	14	13	12	11	10	9	8
			F0GI[5:0]					
Access			R	R	R	R	R	R
Reset			0	0	0	0	0	0

Bit	7	6	5	4	3	2	1	0
		F0FL[6:0]						
Access		R	R	R	R	R	R	R
Reset		0	0	0	0	0	0	0

Bit 25 – RF0L Rx FIFO 0 Message Lost
This bit is a copy of interrupt flag IR.RF0L. When IR.RF0L is reset, this bit is also reset.

Overwriting the oldest message when RXF0C.F0OM = '1' will not set this flag.

Value	Description
0	No Rx FIFO 0 message lost.
1	Rx FIFO 0 message lost, also set after write attempt to Rx FIFO 0 of size zero.

Bit 24 – F0F Rx FIFO 0 Full

Value	Description
0	Rx FIFO 0 not full.
1	Rx FIFO 0 full.

Bits 21:16 – F0PI[5:0] Rx FIFO 0 Put Index
Rx FIFO 0 write index pointer, range 0 to 63.

Bits 13:8 – F0GI[5:0] Rx FIFO 0 Get Index
Rx FIFO 0 read index pointer, range 0 to 63.

Bits 6:0 – F0FL[6:0] Rx FIFO 0 Fill Level
Number of elements stored in Rx FIFO 0, range 0 to 64.

40. SD/MMC Host Controller (SDHC)

40.1 Overview

The SD/MMC Host Controller (SDHC) supports the embedded MultiMedia Card (e.MMC) Specification, the SD Memory Card Specification, and the SDIO Specification. It is compliant with the SD Host Controller Standard specifications. Refer to 40.1.1 Reference Documents for details.

The SDHC includes the register set defined in the “SD Host Controller Simplified Specification V3.00” and additional registers to manage e.MMC devices and enhanced features.

The SDHC is clocked by up to three clocks (bus clock, SDHC core clock, and a slow clock for certain functions). Both the MCLK and GCLK must be configured before the SDHC can be used.

The SAM D5x/E5x provides two instances of the SDHC, SDHC0 and SDHC1.

Related Links

40.3.1 Block Diagram

40.1.1 Reference Documents

Name	Link
SD Host Controller Simplified Specification V3.00	https://www.sdcard.org
SDIO Simplified Specification V3.00	
Physical Layer Simplified Specification V3.01	
Embedded MultiMedia Card (e.MMC) Electrical Standard 4.51	http://www.jedec.org

40.2 Features

- Compatibility:
  - SD Host Controller Standard Specification
  - MultiMedia Card Specification
  - SD Memory Card Specification
  - SDIO Specification Version

  Refer to 40.1.1 Reference Documents for details.
- Support for 1-bit/ 4-bit SD/SDIO Devices
- Support for 1-bit/4-bit e.MMC Devices
- Support for SD/SDIO Default Speed (Maximum SDCLK Frequency = 25 MHz)
- Support for SD/SDIO High Speed (Maximum SDCLK Frequency = 50 MHz)
- Support for e.MMC Default Speed (Maximum SDCLK Frequency = 26 MHz)
- e.MMC Boot Operation Mode Support
- Support for Block Size from 1 to 512 bytes
- Support for Stream, Block and Multi-block Data Read and Write – Advanced DMA and SDMA Capability

The CCL can take the following actions on an input event:

- INSELx: The event is used as input for the TRUTH table. For further details refer to 41.5.6 Events.

Writing a '1' to the LUT Control Event Input Enable bit (LUTCTRL.LUTEI) enables the corresponding action on input event. Writing a '0' to this bit disables the corresponding action on input event.

Related Links

31. EVSYS – Event System

41.6.4 Sleep Mode Operation

When using the GCLK_CCL internal clocking, writing the Run In Standby bit in the Control register (CTRL.RUNSTDBY) to '1' will allow GCLK_CCL to be enabled in Standby Sleep mode.

If CTRL.RUNSTDBY=0, the GCLK_CCL will be disabled in Standby Sleep mode. If the Filter, Edge Detector or Sequential logic are enabled, the LUT output will be forced to zero in STANDBY mode. In all other cases, the TRUTH table decoder will continue operation and the LUT output will be refreshed accordingly.

Related Links

18. PM – Power Manager

42.8.12 Galois Hash (GCM mode only)

Name: GHASH
Offset: 0x6C + n*0x04 [n=0..3]
Reset: 0x00000000
Property: PAC Write-Protection

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] Galois Hash Value
The four 32-bit Hash Word registers GHASHcontain the GHASH value after GF128 multiplication in GCM mode. Writing a new key to KEYWORD registers causes GHASH to be initialized with zeroes. These registers can also be programmed.

There is no difference on the final result when using any of the options for this service. The choice has to be made according to the available resources (RAM, Time) and also taking into account the expected security level.

For this service, two exclusive Calculus Modes are possible. The following table describes the Calculus Mode Options.

Table 43-51. ExpMod Service Calculus Mode Option

Option	Explanation
PUKCL_EXPMOD_FASTRSA	Performs a Fast computation
PUKCL_EXPMOD_REGULARRSA	Performs a Regular computation, slower than the Fast version, but using Regular calculus methods

For this service, four window sizes are possible. The window size in bits is those of the windowing method used for the exponent.

The choice of the window size is a balance between the size of the parameters and the computation time:

- Increasing the window size increases the precomputation workspace.
- Increasing the window size reduces the computation time (may not be relevant for very small exponents).

The following table details the size of the precomputation workspace, depending on the chosen window size option.

Table 43-52. ExpMode Service Window Size Options and Precomputation Space Size

Option specified	Size of the PrecompBase Workspace (bytes)	Content of the Workspace
PUKCL_EXPMOD_WINDOWSIZE_1	3*(u2ModLength + 4) + 8	x
PUKCL_EXPMOD_WINDOWSIZE_2	4*(u2ModLength + 4) + 8	$x\ x^3$
PUKCL_EXPMOD_WINDOWSIZE_3	6*(u2ModLength + 4) + 8	$x\ x^3\ x^5\ x^7$
PUKCL_EXPMOD_WINDOWSIZE_4	10*(u2ModLength + 4) + 8	$x\ x^3\ x^5\ x^7\ x^9\ x^{11}\ x^{13}\ x^{15}$

The exponent can be located in RAM or in the data space. If one part of the exponent is in Crypto RAM this must be mandatory signaled by using the option PUKCL_EXPMOD_EXPINPUKCCRAM.

The following table describes this option.

Table 43-53. ExpMod Service Exponent in Crypto RAM Option

Option	Purpose
PUKCL_EXPMOD_EXPINPUKCCRAM	The exponent can be read from any data space of memory, including Flash, RAM or even Crypto RAM. When at least one word the exponent is in Crypto RAM, this option has to be set.

43.3.5.2.6 Code Example

```
PUKCL_PARAM PUKCLParam;
PPUKCL_PARAM pvPUKCLParam = &PUKCLParam;


PUKCL(u2Option) =...;
```

- Calculate D from E with the formula:
  $D = E^{-1} mod((P - 1) \times (Q - 1))$
- Calculate the parameters from E:
  $EP = E^{-1} mod(P - 1)$ $EQ = E^{-1} mod(Q - 1)$ $Rval = P^{-1} mod(Q)$

In this computation, the following parameters need to be provided:

- X the input number (pointed by {nu1XBase,2*u2ModLength +16})
- P and Q the primes (pointed by {nu1ModBase,2*u2ModLength +8}).
- EP and EQ the reduced exponents (pointed by {pfu1ExpBase,2*u2ExpLength +8})
- Rval and Precomp (pointed by{nu1PrecompBase,RAndPrecompLen})
- Blinding the exponent blinding value (provided inu1Blinding)

The length RAndPrecompLen depends on the lengths and options chosen; its calculus is detailed in Options below.

The service for this operation is CRT.

Note: The minimum value for u2ModLength is 12 bytes. Therefore, the significant length of P or Q must be at least three 32-bit words.

43.3.5.4.4 Parameters Definition

The following table shows the parameter block for the CRT service.

Many parameters have complex placement in memory; therefore, detailed figures are provided in CRT Service Placement below.

Table 43-62. CRT Service Parameters

Parameter	Type	Direction	Location	Data Length	Before Executing the Service	After Executing the Service
u2Options	u2	I	–	–	Options (see below)	Options (see below)
nu1ModBase	nu1	I	Crypto RAM	2*u2ModLength + 8	Base of P, Q	Base of P, Q untouched
u2ModLength	u2	I	–	–	Length of P or Q greater than or equal to 12	Length of P or Q
nu1XBase (see **Note 1**)	nu1	I	Crypto RAM	2*u2ModLength + 16	Base of X	Base of X Filled with the result
nu1PrecompBase	nu1	I	Crypto RAM	See Options below	Base of Rvalue and Pre computations workspace	Corrupted
pfu1ExpBase (see **Note 2**)	pfu1	I	Any place	2*u2ExpLength + 8	Base of EP, EQ	Base of EP, EQ untouched

Parameter	Type	Direction	Location	Data Length	Before Executing the Service	After Executing the Service
u2ScalarLength	u2	I	–	–	Length of scalar	Length of scalar
pu1PointABase	pu1	I/O	Crypto RAM	(3*u2ModLength + 12) * (2(WA-2))	Generator point	Corrupted
pu1PointPublicKeyGen	pu1	I/O	Crypto RAM	(3*u2ModLength + 12) * (2(WB-2))	Public Key point	Corrupted
pu1AWorkBase	pu1	I	Crypto RAM	(u2ModLength + 4) + (8*u2MaxLength + 44)	Parameter a of the elliptic curve and Workspace	Corrupted

Note:

1. 1. The hash value calculus is defined by the ECDSA norm and depends on the elliptic curve domain parameters. To construct the input parameter, the 4 Most Significant Bytes must be set to zero.

A suggested parameters placement in Crypto RAM is:

- ModCnsBase
- OrderPointBase
- Signature may be placed here or in Classical RAM
- HashBase
- PointABase
- PointPublicKeyGen
- AWorkBase

43.3.6.13.5 Options

The options are set by the u2Options input parameter, which is composed of:

- the mandatory windows sizes WA (window for Point A) and WB (window for Point Public Key)
- the indication of the presence of the Point Signature in system RAM

Important: Please check precisely if the Point Signature is in Crypto RAM. If this is the case the PUKCL_ZPECCMUL_SCAL_IN_CLASSIC_RAM must not be used.

The u2Options number is calculated by an “Inclusive OR” of the options. Some Examples in C language are:

- ```
  // Point Signature in system RAM
  // The Point A window size is 3
  // The Point Public Key window size is 4
  PUKCL(u2Options) = PUKCL_ZPECCMUL_SCAL_IN_CLASSIC_RAM |
  ```
  ```