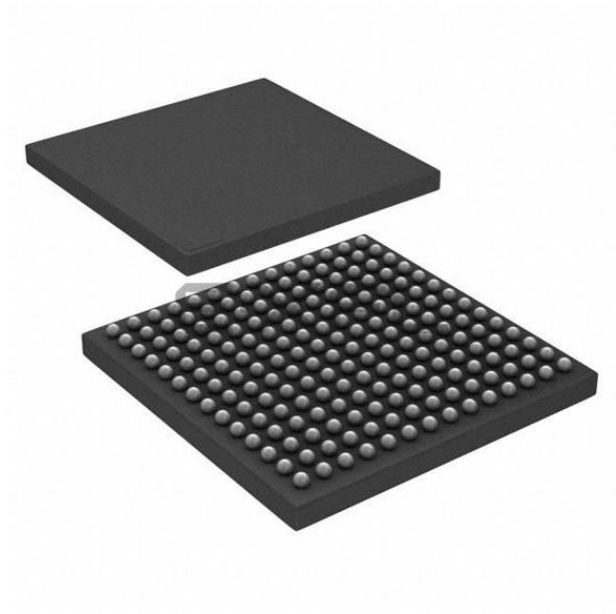


Welcome to E-XFL.COM

Understanding Embedded - Microprocessors

Embedded microprocessors are specialized computing chips designed to perform specific tasks within an embedded system. Unlike general-purpose microprocessors found in personal computers, embedded microprocessors are tailored for dedicated functions within larger systems, offering optimized performance, efficiency, and reliability. These microprocessors are integral to the operation of countless electronic devices, providing the computational power necessary for controlling processes, handling data, and managing communications.

Applications of Embedded - Microprocessors

Embedded microprocessors are utilized across a broad spectrum of applications, making them indispensable in

Details	
Product Status	Active
Core Processor	ARM® Cortex®-A5
Number of Cores/Bus Width	1 Core, 32-Bit
Speed	500MHz
Co-Processors/DSP	Multimedia; NEON™ MPE
RAM Controllers	LPDDR1, LPDDR2, LPDDR3, DDR2, DDR3, DDR3L, QSPI
Graphics Acceleration	Yes
Display & Interface Controllers	Keyboard, LCD, Touchscreen
Ethernet	10/100Mbps (1)
SATA	-
USB	USB 2.0 + HSIC
Voltage - I/O	3.3V
Operating Temperature	-40°C ~ 85°C (TA)
Security Features	ARM TZ, Boot Security, Cryptography, RTIC, Secure Fusebox, Secure JTAG, Secure Memory, Secure RTC
Package / Case	196-TFBGA, CSBGA
Supplier Device Package	196-TFBGA (11x11)
Purchase URL	https://www.e-xfl.com/product-detail/microchip-technology/atsama5d23a-cu

7.4.2 Backup Mode Entry

Figure 7-3 shows the recommended power down sequence to place the SAMA5D2 either in Backup mode or in Backup mode with its DDR in self-refresh. The SHDN signal, output of Shutdown Controller (SHDWC), signals the shutdown request to the power supply. This output is supplied by VDDBU that is present in Backup mode. Placing the external DDR memory in self-refresh while in Backup mode, requires to maintain also VDDIODDR. One possible way to signal this additional need to the power supply is to position one of the general purpose I/Os supplied by VDDBU (PIOBUx) in a predefined state.

Figure 7-3: Recommended Backup Mode Entry

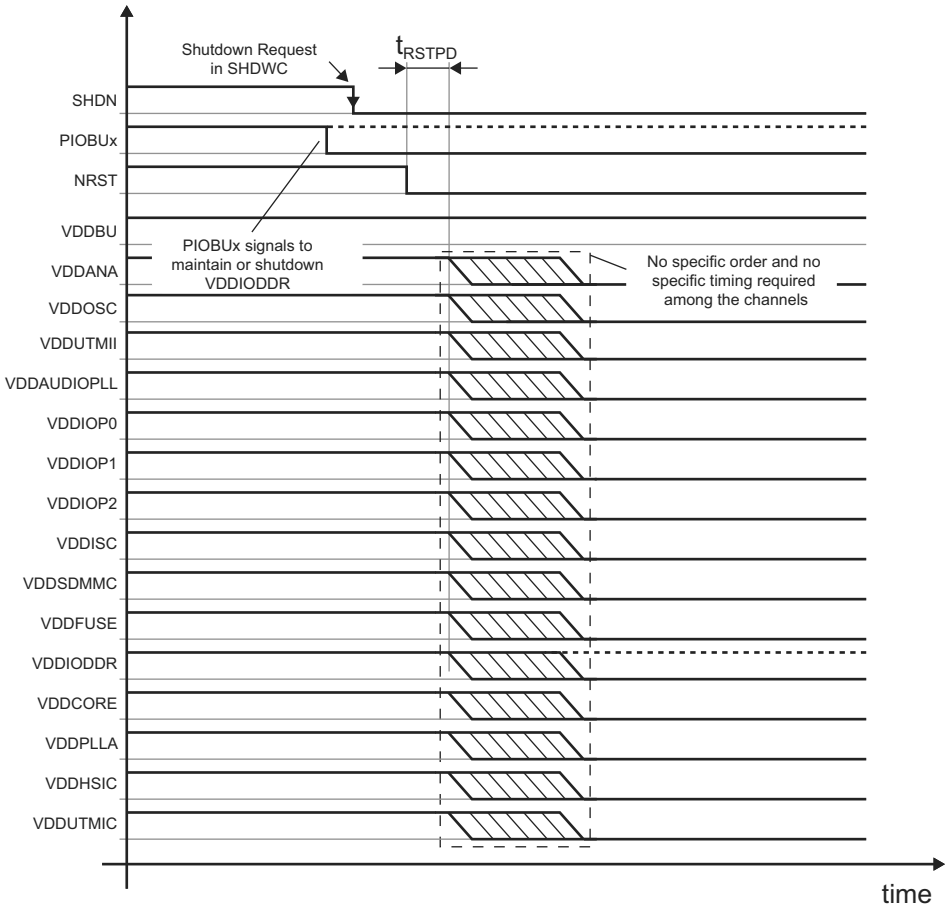


Table 7-4: Powerdown Timing Specification

Symbol	Parameter	Conditions	Min	Max	Unit
t_{RSTPD}	Reset delay at powerdown	From NRST low to the first supply turn-off	0	–	ms

Table 18-10: Register Mapping (Continued)

Offset	Register	Name	Access	Reset
0x016C	Master 3 Error Address Register	MATRIX_MEAR3	Read-only	0x00000000
0x0170	Master 4 Error Address Register	MATRIX_MEAR4	Read-only	0x00000000
0x0174	Master 5 Error Address Register	MATRIX_MEAR5	Read-only	0x00000000
0x0178	Master 6 Error Address Register	MATRIX_MEAR6	Read-only	0x00000000
0x017C	Master 7 Error Address Register	MATRIX_MEAR7	Read-only	0x00000000
0x0180	Master 8 Error Address Register	MATRIX_MEAR8	Read-only	0x00000000
0x0184	Master 9 Error Address Register	MATRIX_MEAR9	Read-only	0x00000000
0x0188	Master 10 Error Address Register	MATRIX_MEAR10	Read-only	0x00000000
0x018C	Master 11 Error Address Register	MATRIX_MEAR11	Read-only	0x00000000
0x0190–0x01E0	Reserved	–	–	–
0x01E4	Write Protection Mode Register	MATRIX_WPMR	Read/Write	0x00000000
0x01E8	Write Protection Status Register	MATRIX_WPSR	Read-only	0x00000000
0x01EC–0x01FC	Reserved	–	–	–
0x0200	Security Slave 0 Register	MATRIX_SSR0	Read/Write	0x00000000
0x0204	Security Slave 1 Register	MATRIX_SSR1	Read/Write	0x00000000
0x0208	Security Slave 2 Register	MATRIX_SSR2	Read/Write	0x00000000
0x020C	Security Slave 3 Register	MATRIX_SSR3	Read/Write	0x00000000
0x0210	Security Slave 4 Register	MATRIX_SSR4	Read/Write	0x00000000
0x0214	Security Slave 5 Register	MATRIX_SSR5	Read/Write	0x00000000
0x0218	Security Slave 6 Register	MATRIX_SSR6	Read/Write	0x00000000
0x021C	Security Slave 7 Register	MATRIX_SSR7	Read/Write	0x00000000
0x0220	Security Slave 8 Register	MATRIX_SSR8	Read/Write	0x00000000
0x0224	Security Slave 9 Register	MATRIX_SSR9	Read/Write	0x00000000
0x0228	Security Slave 10 Register	MATRIX_SSR10	Read/Write	0x00000000
0x022C	Security Slave 11 Register	MATRIX_SSR11	Read/Write	0x00000000
0x0230	Security Slave 12 Register	MATRIX_SSR12	Read/Write	0x00000000
0x0234	Security Slave 13 Register	MATRIX_SSR13	Read/Write	0x00000000
0x0238	Security Slave 14 Register	MATRIX_SSR14	Read/Write	0x00000000
0x023C	Reserved	–	–	–
0x0240	Security Areas Split Slave 0 Register	MATRIX_SASSR0	Read/Write	(1)
0x0244	Security Areas Split Slave 1 Register	MATRIX_SASSR1	Read/Write	(1)
0x0248	Security Areas Split Slave 2 Register	MATRIX_SASSR2	Read/Write	(1)
0x024C	Security Areas Split Slave 3 Register	MATRIX_SASSR3	Read/Write	(1)
0x0250	Security Areas Split Slave 4 Register	MATRIX_SASSR4	Read/Write	(1)
0x0254	Security Areas Split Slave 5 Register	MATRIX_SASSR5	Read/Write	(1)
0x0258	Security Areas Split Slave 6 Register	MATRIX_SASSR6	Read/Write	(1)

24. Shutdown Controller (SHDWC)

24.1 Description

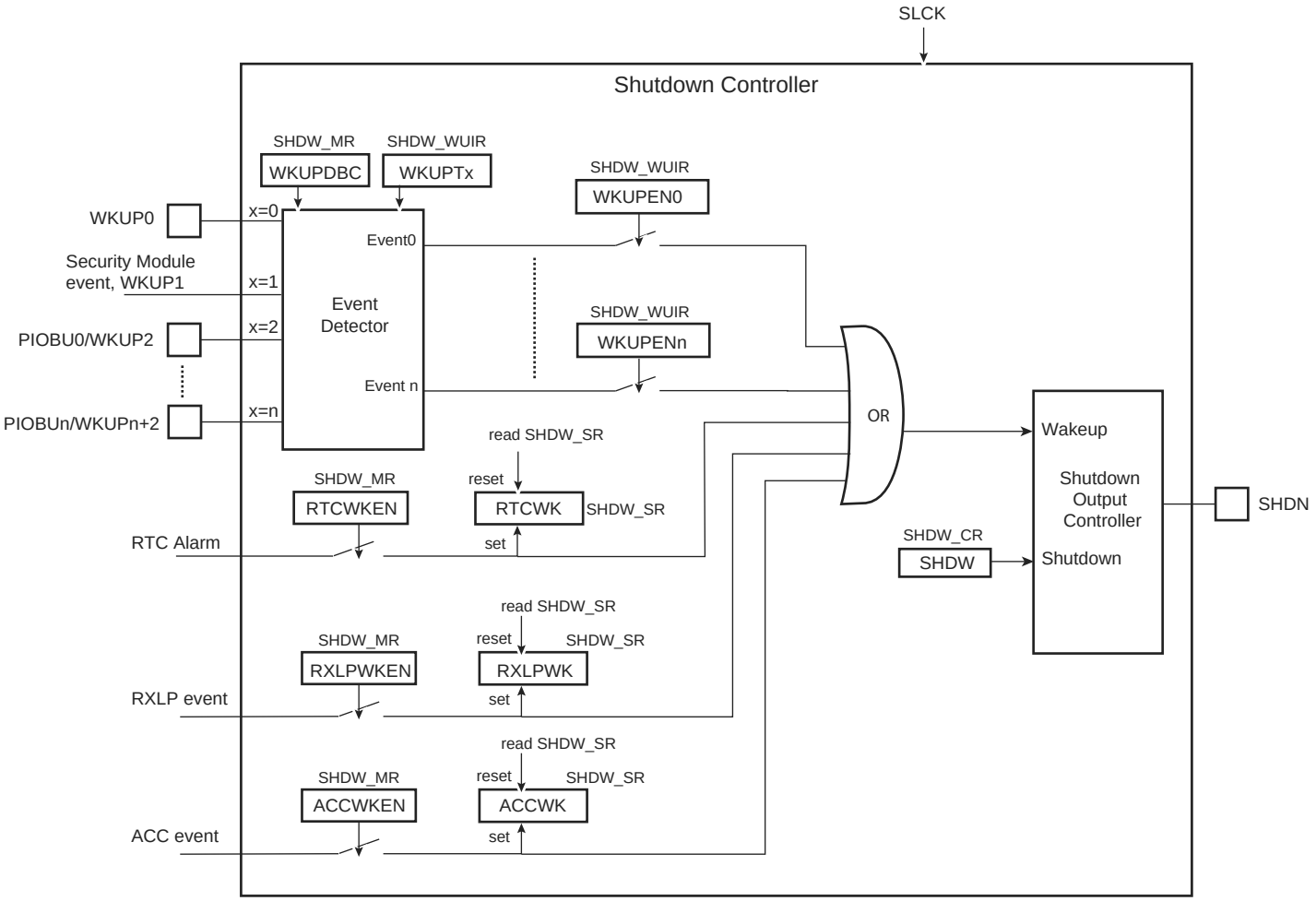
The Shutdown Controller (SHDWC) controls the power supplies VDDIO and VDDCORE and the wakeup detection on debounced input lines.

24.2 Embedded Characteristics

- Shutdown Logic
  - Software Assertion of the Shutdown Output Pin (SHDN)
  - Programmable deassertion from the PIOBU, WKUP Input Pins
- Wakeup Logic
  - Programmable Assertion from the PIOBU, WKUP Input Pins, and Internal Wakeup Event from RTC, RXLP, ACC, Security Module

24.3 Block Diagram

Figure 24-1: Shutdown Controller Block Diagram



The value obtained must be rounded to the nearest integer prior to being programmed into CORRECTION field.

If HIGHPPM = 1, then the clock frequency correction range is from 30.5 ppm up to 1950 ppm. The RTC accuracy is less than 1 ppm for a range correction from 30.5 ppm up to 90 ppm.

The correction field must be programmed according to the required correction in ppm; the formula is as follows:

$$\text{CORRECTION} = \frac{3906}{\text{ppm}} - 1$$

The value obtained must be rounded to the nearest integer prior to be programmed into CORRECTION field.

If NEGPPM is set to 1, the ppm correction is negative (used to correct crystals that are faster than the nominal 32.768 kHz).

OUT0: All ADC Channel Trigger Event Source Selection

Value	Name	Description
0	NO_WAVE	No waveform, stuck at ‘0’
1	FREQ1HZ	1 Hz square wave
2	FREQ32HZ	32 Hz square wave
3	FREQ64HZ	64 Hz square wave
4	FREQ512HZ	512 Hz square wave
5	ALARM_TOGGLE	Output toggles when alarm flag rises
6	ALARM_FLAG	Output is a copy of the alarm flag
7	PROG_PULSE	Duty cycle programmable pulse

OUT1: ADC Last Channel Trigger Event Source Selection

Value	Name	Description
0	NO_WAVE	No waveform, stuck at ‘0’
1	FREQ1HZ	1 Hz square wave
2	FREQ32HZ	32 Hz square wave
3	FREQ64HZ	64 Hz square wave
4	FREQ512HZ	512 Hz square wave
5	ALARM_TOGGLE	Output toggles when alarm flag rises
6	ALARM_FLAG	Output is a copy of the alarm flag
7	PROG_PULSE	Duty cycle programmable pulse

THIGH: High Duration of the Output Pulse

Value	Name	Description
0	H_31MS	31.2 ms
1	H_16MS	15.6 ms
2	H_4MS	3.91 ms
3	H_976US	976 µs
4	H_488US	488 µs

28. Slow Clock Controller (SCKC)

28.1 Description

The System Controller embeds a Slow Clock Controller (SCKC). The SCKC selects the slow clock from one of two sources:

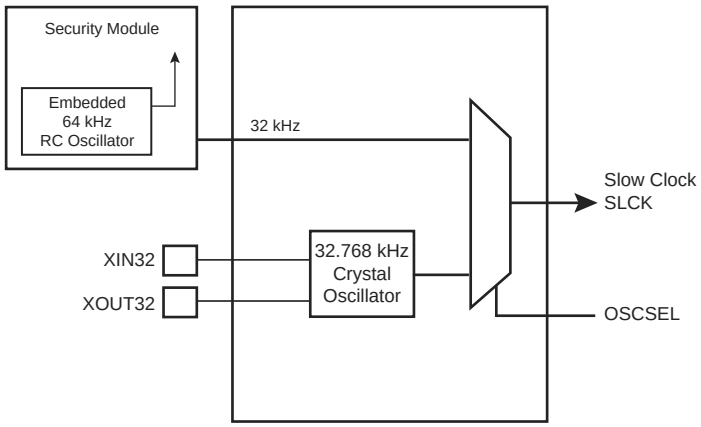
- External 32.768 kHz crystal oscillator
- Embedded 64 kHz (typical) RC oscillator

28.2 Embedded Characteristics

- 64 kHz (typical) RC Oscillator or 32.768 kHz Crystal Oscillator Selector
- VDDBU Powered

28.3 Block Diagram

Figure 28-1: Block Diagram



28.4 Functional Description

The OSCSEL bit is located in the Slow Clock Controller Configuration Register (SCKC_CR) located at the address 0xFC068650 in the backed-up part of the System Controller and, thus, it is preserved while VDDBU is present.

The embedded 64 kHz (typical) RC oscillator and the 32.768 kHz crystal oscillator are always enabled as soon as VDDBU is established. The Slow Clock Selector command (OSCSEL bit) selects the slow clock source.

After the VDDBU power-on reset, the default configuration is OSCSEL = 0, allowing the system to start on the embedded 64 kHz (typical) RC oscillator.

The programmer controls the slow clock switching by software and so must take precautions during the switching phase.

28.4.1 Switching from Embedded 64 kHz RC Oscillator to 32.768 kHz Crystal Oscillator

The sequence to switch from the embedded 64 kHz (typical) RC oscillator to the 32.768 kHz crystal oscillator is the following:

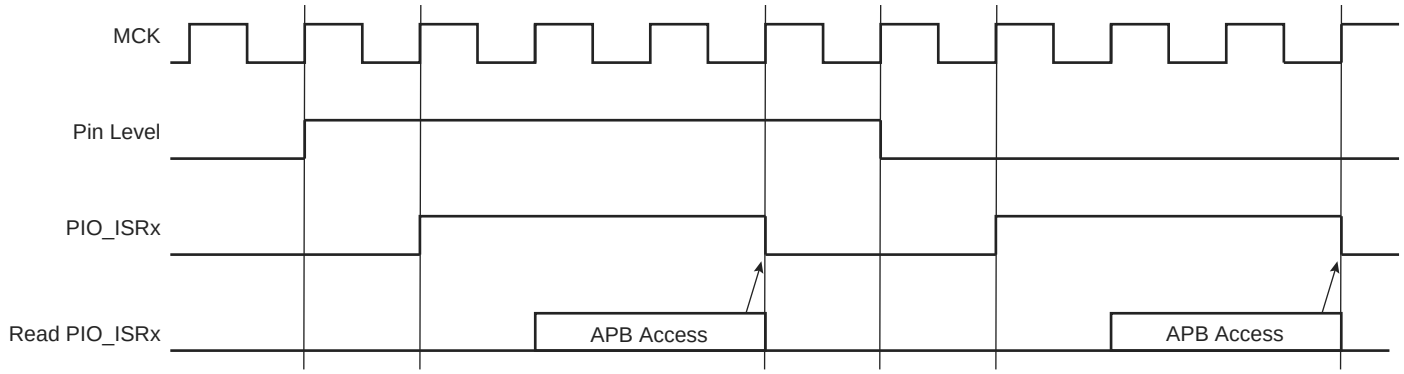
1. Switch the master clock to a source different from slow clock (PLL or Main Oscillator) through the Power Management Controller.
2. Switch from the embedded 64 kHz (typical) RC oscillator to the 32.768 kHz crystal oscillator by writing a 1 to the OSCSEL bit.
3. Wait 5 slow clock cycles for internal resynchronization.

28.4.2 Switching from 32.768 kHz Crystal Oscillator to Embedded 64 kHz RC Oscillator

The sequence to switch from the 32.768 kHz crystal oscillator to the embedded 64 kHz (typical) RC oscillator is the following:

1. Switch the master clock to a source different from slow clock (PLL or Main Oscillator).
2. Switch from the 32.768 kHz crystal oscillator to the embedded RC oscillator by writing a 0 to the OSCSEL bit.
3. Wait 5 slow clock cycles for internal resynchronization.

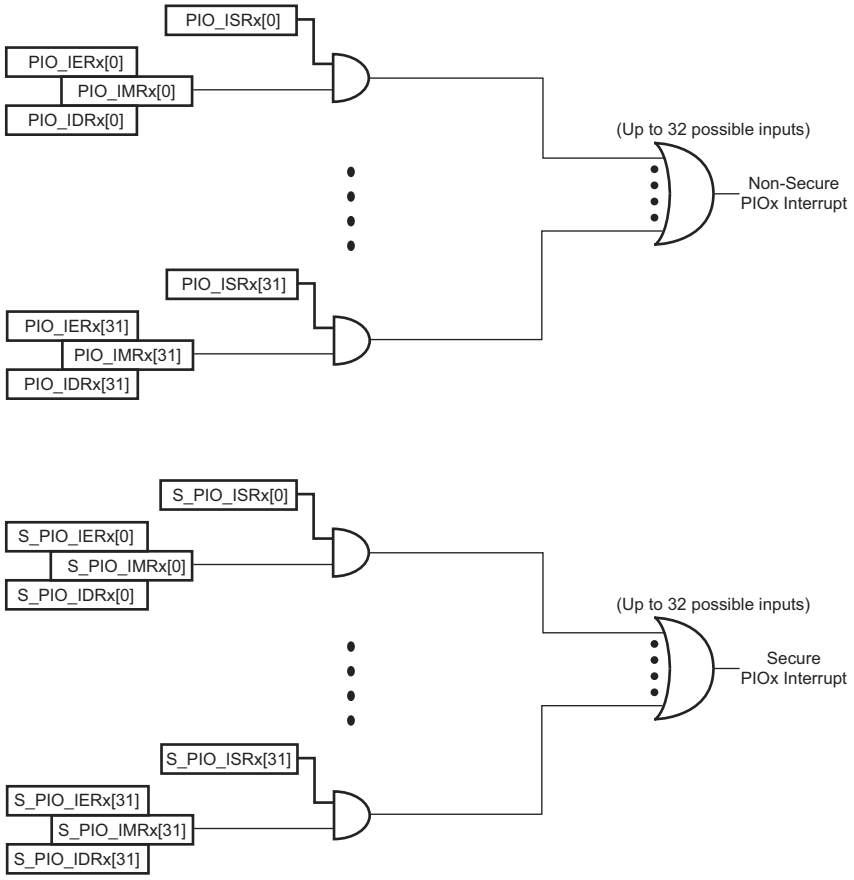
Figure 34-7: Input Change Interrupt Timings When No Additional Interrupt Modes



34.5.11 Interrupt Management

The PIO Controller can drive one secure interrupt signal and one non-secure interrupt signal per I/O group (see Figure 34-1). Secure interrupt signals are connected to the secure interrupt controller of the system. Non-secure interrupt signals are connected to the non-secure interrupt controller of the system.

Figure 34-8: PIO Interrupt Management

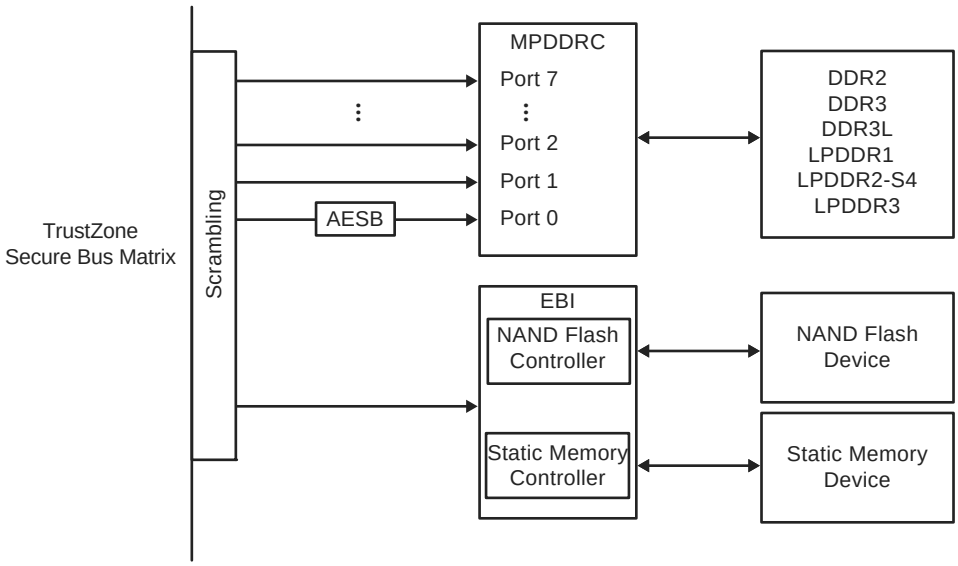


35. External Memories

The product features:

- Multiport DDR-SDRAM Controller (MPDDRC)
- External Bus Interface (EBI) that embeds a NAND Flash controller and a Static Memory Controller (HSMC)

Figure 35-1: External Memory Controllers



- The MPDDRC is a multiport DDRSDR controller supporting DDR2, DDR3, DDR3L, LPDDR1, LPDDR2-S4 and LPDDR3 devices. The MPDDRC user interface is located at 0xF000C000. All the paths can be scrambled and Port 0 can be connected to an AES encryption/decryption engine.
- The HSMC supports Static Memories and MLC/SLC NAND Flash. It embeds MultiBit ECC correction (PMECC). Its user interface is located at 0xF8014000. The HSMC buses can be scrambled.

35.1 Multiport DDR-SDRAM Controller (MPDDRC)

35.1.1 Description

The MPDDRC is an 8-port memory controller supporting DDR-SDRAM and low-power DDR devices. Data transfers are performed through a 16/32-bit data bus on one chip select. The controller operates with a 1.8V power supply for DDR2, DDR3, LPDDR1, 1.35V for DDR3L and 1.2V for LPDDR2, LPDDR3.

For full details, refer to Section 36. “Multiport DDR-SDRAM Controller (MPDDRC)”.

36.5.3.2 Powerdown Mode

This mode is activated by configuring the Low-power Command bit (LPCB) to 2 in the MPDDRC Low-Power Register (MPDDRC_LPR).

Powerdown mode is used when no access to the DDR-SDRAM device is possible. In this mode, power consumption is greater than in Self-refresh mode. This state is similar to Normal mode (no Low-power mode/no Self-refresh mode), but the CKE pin is low and the input and output buffers are deactivated as soon the DDR-SDRAM device is no longer accessible. In contrast to Self-refresh mode, the DDR-SDRAM device cannot remain in Low-power mode longer than one refresh period (64 ms/32 ms). As no autorefresh operations are performed in this mode, the MPDDRC carries out the refresh operation. For the low-power DDR-SDRAM devices, a NOP command must be generated for a minimum period defined in the TXP field of the Timing Parameter 1 register (MPDDRC_TPR1). For DDR-SDRAM devices, a NOP command must be generated for a minimum period defined in the TXP field of MPDDRC_TPR1 (see Section 36.7.5 “MPDDRC Timing Parameter 1 Register”) and in the TXARD and TXARDS fields of MPDDRC_TPR2 (see Section 36.7.6 “MPDDRC Timing Parameter 2 Register”) for DDR2_SDRAM devices. In addition, low-power DDR-SDRAM and DDR-SDRAM must remain in Powerdown mode for a minimum period corresponding to t_{CKE}, t_{PD}, etc. (see the memory device datasheet).

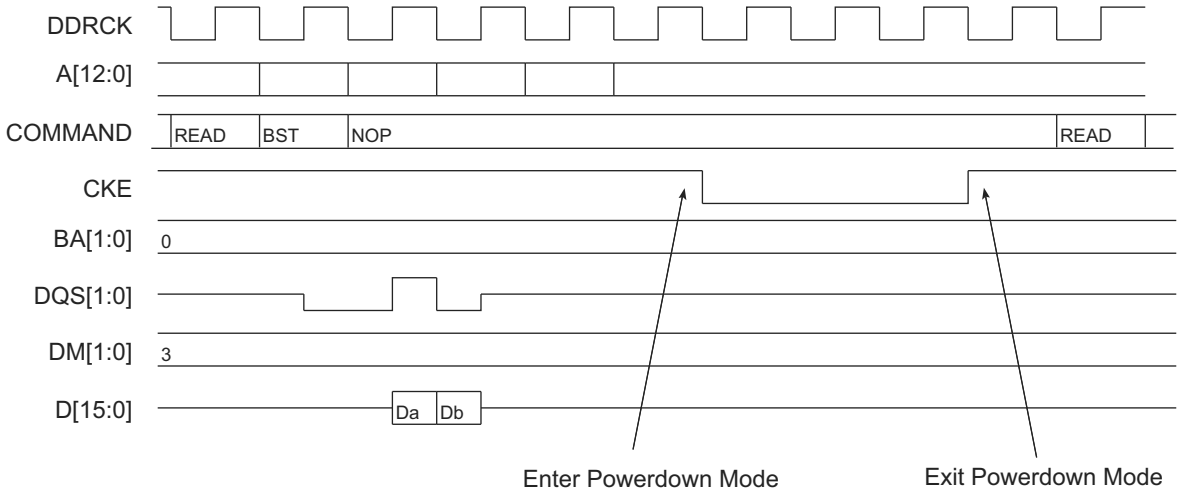
The exit procedure is faster than in Self-refresh mode. See Figure 36-16. The MPDDRC returns to Powerdown mode as soon as the DDR-SDRAM device is not selected. It is possible to define when Powerdown mode is enabled by configuring the TIMEOUT field in the MPDDRC_LPR:

0: Powerdown mode is enabled as soon as the DDR-SDRAM device is not selected.

1: Powerdown mode is enabled 64 clock cycles after completion of the last access.

2: Powerdown mode is enabled 128 clock cycles after completion of the last access.

Figure 36-16: Powerdown Entry/Exit, TIMEOUT = 0



36.5.3.3 Deep Powerdown Mode

The Deep Powerdown mode is a feature of low-power DDR-SDRAM. When this mode is activated, all internal voltage generators inside the device are stopped and all data is lost.

Deep Powerdown mode is activated by configuring the Low-power Command bit (LPCB) to 3 in the MPDDRC Low-Power Register (MPDDRC_LPR). When this mode is enabled, the MPDDRC leaves Normal mode (MPDDRC_MR.MODE = 0) and the controller is frozen. The clock can be stopped during Deep Powerdown mode by setting the CLK_FR field to 1.

Before enabling this mode, the user must make sure there is no access in progress. To exit Deep Powerdown mode, the Low-power Command bit (LPCB) and Clock Frozen bit (CLK_FR) must be 0 and the initialization sequence must be generated by software. See Section 36.4.1 “Low-power DDR1-SDRAM Initialization” or Section 36.4.3 “Low-power DDR2-SDRAM Initialization” or Section 36.4.5 “Low-power DDR3-SDRAM Initialization”.

36.7.15 MPDDRC OCMS KEY2 Register

Name: MPDDRC_OCMS_KEY2

Address: 0xF000C040

Access: Write once

31	30	29	28	27	26	25	24
KEY2							

23	22	21	20	19	18	17	16
KEY2							

15	14	13	12	11	10	9	8
KEY2							

7	6	5	4	3	2	1	0
KEY2							

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

KEY2: Off-chip Memory Scrambling (OCMS) Key Part 2

When Off-chip Memory Scrambling is enabled, the data scrambling depends on KEY1 and KEY2 values.

39.6.9.1 Video Scaler Description

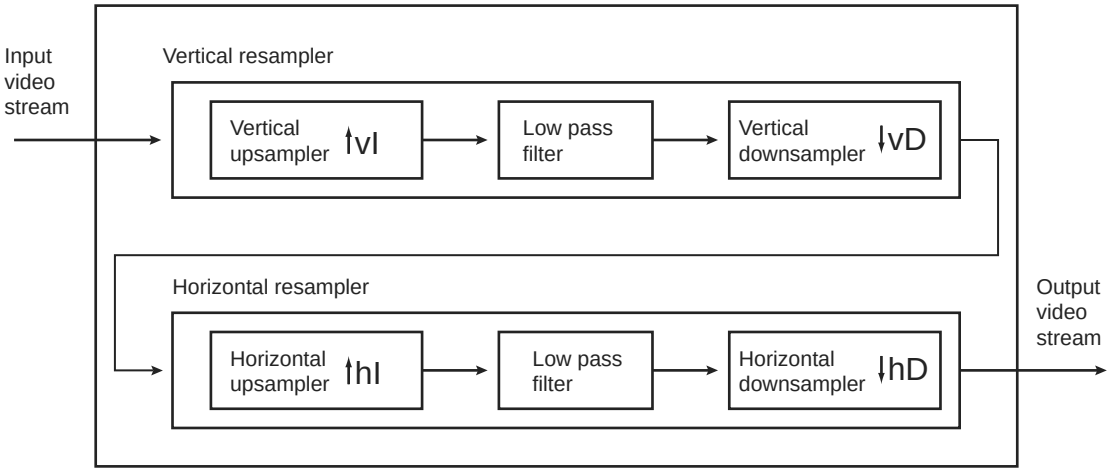
The scaling operation is based on a vertical and horizontal resampling algorithm. The sampling rate of the original image is increased when the video is upscaled, and decreased when the video is downscaled. A Vertical resampler is used to perform a vertical interpolation by a factor of *vI,* and a decimation by a factor of *vD*. A Horizontal resampler is used to perform a vertical interpolation by a factor of *hI,* and a decimation by a factor of *hD.* The horizontal and vertical low pass filters are both designed to minimize the aliasing effect. The frequency response of the low pass filter has the following characteristics:

$$H(\omega) = \begin{cases} I & \text{when } 0 \le |\omega| \le min(\frac{\pi}{I},\frac{\pi}{D}) \\ 0 & \text{otherwise} \end{cases}$$

Taking into account the linear phase condition and anticipating the filter length M, the desired frequency response is modified.

$$H(\omega) = \begin{cases} Ie^{-j\omega\frac{M}{2}} & \text{when } 0 \le |\omega| \le min(\frac{\pi}{I},\frac{\pi}{D}) \\ 0 & \text{otherwise} \end{cases}$$

Figure 39-6: Video Resampler Architecture



The impulse response of the defined low pass filter is:

$$h(n) = \begin{cases} I \times \frac{\omega_c}{\pi} \text{ when } n = 0 \\ I \times \frac{\omega_c}{\pi} \times \frac{\sin(\omega_c n)}{\omega_c n} \text{otherwise} \end{cases}$$

Or, for the filter of length M:

$$h(n) = \begin{cases} I \times \frac{\omega_c}{\pi} \text{ when } n = \frac{M}{2} \\ I \times \frac{\omega_c}{\pi} \times \frac{\sin\left(\omega_c\left(n-\frac{M}{2}\right)\right)}{\omega_c\left(n-\frac{M}{2}\right)} \text{otherwise} \end{cases}$$

39.7.36 Overlay 1 Channel Status Register

Name: LCDC_OVR1CHSR

Address: 0xF0000148

Access: Read-only

31	30	29	28	27	26	25	24
–	–	–	–	–	–	–	–
23	22	21	20	19	18	17	16
–	–	–	–	–	–	–	–
15	14	13	12	11	10	9	8
–	–	–	–	–	–	–	–
7	6	5	4	3	2	1	0
–	–	–	–	–	A2QSR	UPDATESR	CHSR

CHSR: Channel Status

0: Layer disabled

1: Layer enabled

UPDATESR: Update Overlay Attributes In Progress Status

0: No update pending

1: Overlay attributes will be updated on the next frame

A2QSR: Add To Queue Status

0: Add to queue not pending

1: Add to queue pending

39.7.108 High-End Overlay Configuration Register 13

Name: LCDC_HEOCFG13

Address: 0xF00003C0

Access: Read/Write

31	30	29	28	27	26	25	24
SCALEN	–	YFACTOR					

23	22	21	20	19	18	17	16
YFACTOR							

15	14	13	12	11	10	9	8
–	–	XFACTOR					

7	6	5	4	3	2	1	0
XFACTOR							

SCALEN: Hardware Scaler Enable

0: Scaler is disabled

1: Scaler is enabled.

YFACTOR: Vertical Scaling Factor

Scaler Vertical Factor.

XFACTOR: Horizontal Scaling Factor

Scaler Horizontal Factor.

40.8.19 GMAC RX Jumbo Frame Max Length Register

Name: GMAC_RJFML

Address: 0xF8008048

Access: Read/Write

31	30	29	28	27	26	25	24
–	–	–	–	–	–	–	–

23	22	21	20	19	18	17	16
–	–	–	–	–	–	–	–

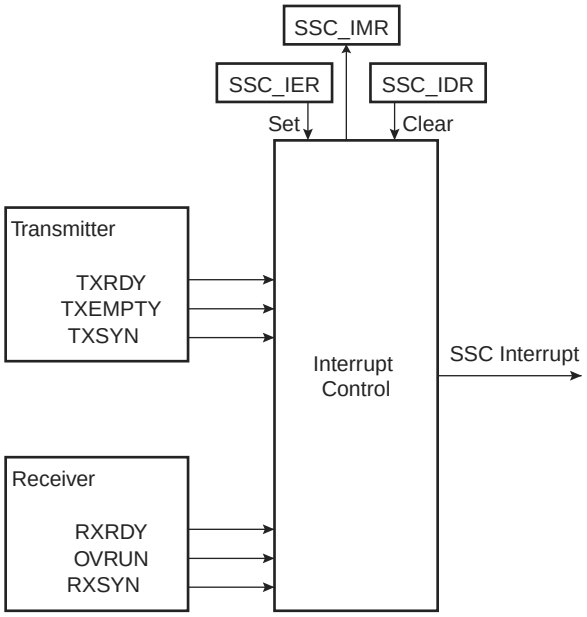
15	14	13	12	11	10	9	8
–	–	FML					

7	6	5	4	3	2	1	0
FML							

FML: Frame Max Length

Rx jumbo frame maximum length.

Figure 45-19: Interrupt Block Diagram



45.8.10 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

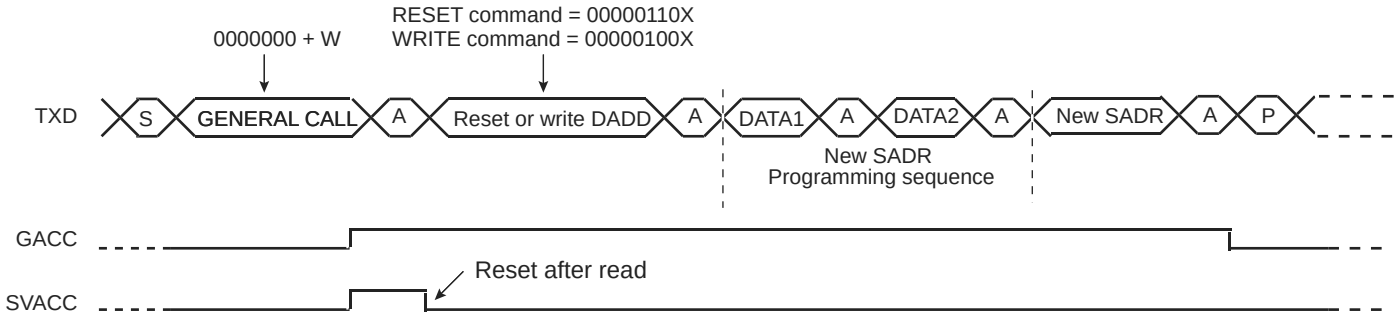
If a GENERAL CALL is detected, GACC is set.

After the detection of general call, it is up to the user to decode the commands which follow.

In case of a WRITE command, the user has to decode the programming sequence and program a new SADR if the programming sequence matches.

Figure 47-115 describes the general call access.

Figure 47-115: Master Performs a General Call



Note: This method allows to create a user-specific programming sequence by choosing the number of programming bytes. The programming sequence has to be provided to the master.

- Clock Stretching

In both Read and Write modes, it may happen that the FLEX_TWI_THR/FLEX_TWI_RHR buffer is not filled/emptied before the transmission/reception of a new character. In this case, to avoid sending/receiving undesired data, a clock stretching mechanism is implemented.

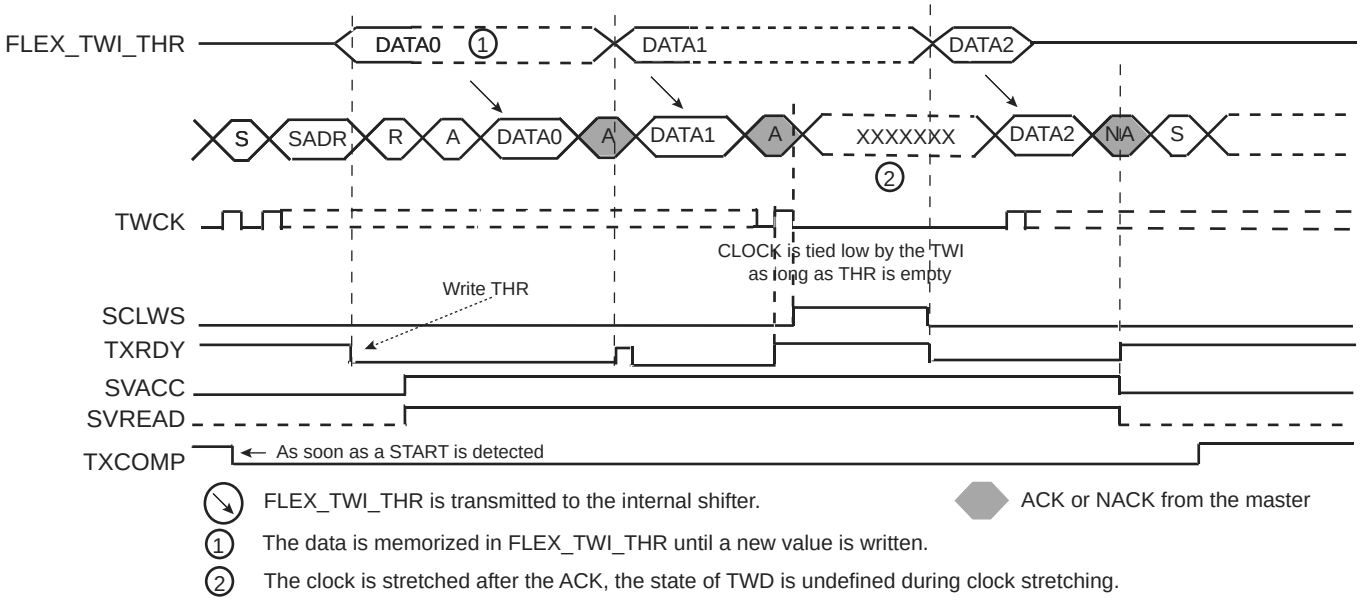
Note: Clock stretching can be disabled by setting the FLEX_TWI_SMR.SCLWSDIS bit. In that case, the UNRE and OVRE flags will indicate an underrun (when FLEX_TWI_THR is not filled on time) or an overrun (when FLEX_TWI_RHR is not read on time).

Clock Stretching in Read Mode

The clock is tied low if the internal shifter is empty and if a STOP or REPEATED START condition was not detected. It is tied low until the internal shifter is loaded.

Figure 47-116 describes the clock stretching in Read mode.

Figure 47-116: Clock Stretching in Read Mode



59.4.4 AESB Interrupt Disable Register

Name: AESB_IDR

Address: 0xF001C014

Access: Write-only

31	30	29	28	27	26	25	24
–	–	–	–	–	–	–	–
23	22	21	20	19	18	17	16
–	–	–	–	–	–	–	–
15	14	13	12	11	10	9	8
–	–	–	–	–	–	–	URAD
7	6	5	4	3	2	1	0
–	–	–	–	–	–	–	DATRDY

The following configuration values are valid for all listed bit names of this register:

0: No effect.

1: Disables the corresponding interrupt.

DATRDY: Data Ready Interrupt Disable

URAD: Unspecified Register Access Detection Interrupt Disable

60.3 Product Dependencies

60.3.1 Power Management

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

60.3.2 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.

Table 60-1: Peripheral IDs

Instance	ID
AES	9

60.4 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.

60.4.1 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

62. Triple Data Encryption Standard (TDES)

62.1 Description

The Triple Data Encryption Standard (TDES) is compliant with the American *FIPS (Federal Information Processing Standard) Publication 46-3* specification.

The TDES supports the four different confidentiality modes of operation (ECB, CBC, OFB and CFB), specified in the *FIPS (Federal Information Processing Standard) Publication 81* and is compatible with the Peripheral Data Controller channels for all of these modes, minimizing processor intervention for large buffer transfers.

The TDES key is loaded by the software. The software can write up to three 64-bit keys, each stored in two 32-bit write-only registers, i.e., Key x Word Registers TDES_KEYxWR0 and TDES_KEYxWR1.

The input data (and initialization vector for some modes) are stored in two corresponding 32-bit write-only registers:

Input Data Registers TDES_IDATAR0 and TDES_IDATAR1

Initialization Vector Registers TDES_IVR0 and TDES_IVR1

As soon as the initialization vector, the input data and the keys are configured, the encryption/decryption process may be started. Then the encrypted/decrypted data is ready to be read out on the two 32-bit Output Data registers (TDES_ODATARx) or through the DMA channels.

62.2 Embedded Characteristics

- Supports Single Data Encryption Standard (DES) and Triple Data Encryption Standard (TDES)
- Compliant with *FIPS Publication 46-3, Data Encryption Standard (DES)*
- 64-bit Cryptographic Key for TDES
- Two-key or Three-key Algorithms for TDES
- 18-clock Cycles Encryption/Decryption Processing Time for DES
- 50-clock Cycles Encryption/Decryption Processing Time for TDES
- Supports eXtended Tiny Encryption Algorithm (XTEA)
- 128-bit key for XTEA and Programmable Round Number up to 64
- Supports the Four Standard Modes of Operation specified in the *FIPS Publication 81, DES Modes of Operation*
  - Electronic Code Book (ECB)
  - Cipher Block Chaining (CBC)
  - Cipher Feedback (CFB)
  - Output Feedback (OFB)
- 8-, 16-, 32- and 64-bit Data Sizes Possible in CFB Mode
- Last Output Data Mode Allowing Optimized Message (Data) Authentication Code (MAC) Generation
- Connection to DMA Optimizes Data Transfers for all Operating Modes

62.3 Product Dependencies

62.3.1 Power Management

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

62.3.2 Interrupt Sources

The TDES interface has an interrupt line connected to the Interrupt Controller. In order to handle interrupts, the Interrupt Controller must be programmed before configuring the TDES.

Table 62-1: Peripheral IDs

Instance	ID
TDES	11

When TSMODE = 1 or 3, each trigger event adds two half-words in the buffer (assuming TSAV = 0), first half-word being XPOS of ADC_XPOSR then YPOS of ADC_YPOSR. If TSAV/TSFREQ ≠ 0, the data structure remains unchanged. Not all trigger events add data to the buffer.

When TSMODE = 2, each trigger event adds four half-words to the buffer (assuming TSAV = 0), first half-word being XPOS of ADC_XPOSR followed by YPOS of ADC_YPOSR and finally Z1 followed by Z2, both located in ADC_PRESSR.

When TAG is set (ADC_EMR), the CHNB field (four most significant bits of ADC_LCDR) is cleared when XPOS is transmitted and set when YPOS is transmitted, allowing an easier post-processing of the buffer or a better checking of the buffer integrity. In case 4-wire with Pressure mode is selected, Z1 value is transmitted to the buffer along with tag set to 2 and Z2 is tagged with value 3.

XSCALE and YSCALE (calibration values) are not transmitted to the buffer because they are supposed to be constant and moreover only measured at the very first startup of the controller or upon user request.

There is no change in buffer structure whatever the value of PENDET bit configuration in ADC_TSMR but it is recommended to use the pen detection function for buffer post-processing (see Section 65.6.17.4 “Pen Detection Status”).

Table 72-2: SAMA5D2 Datasheet DS60001476 Rev. A Revision History

Issue Date	Changes
Mar-2017	General - Template update: Moved from Atmel to Microchip template. - The datasheet is assigned a new document number (DS60001476) and revision letter is reset to A. --- Document number DS60001476 revision A corresponds to what would have been 11267 revision F. - ISBN number assigned.
	“Features” : added PTC.
	Table 2. “Configuration Summary”: added PTC. Corrected number of Timers.
	Section 3. “Block Diagram” Figure 3-1. SAMA5D2 Series Block Diagram: corrected SDMMC signals. Updated peripheral bridge naming. Added PTC. Removed signal names.
	Section 4. “Signal Description” Table 4-1 “Signal Description List”: renamed SDMMCx_VDDSEL to SDMMCx_1V8SEL. Added PTC pins on PD0 to PD18.
	Added Section 5. “Safety and Security Features”.
	Section 6. “Package and Pinout” Added Note on IO sets. Table 6-2 “Pin Description”: for P15/R14 renamed SDMMC0_VDDSEL to SDMMC0_1V8SEL.
	Section 7. “Power Considerations” Table 7-1 “SAMA5D2 Power Supplies”: in VDDBU row, corrected RC Oscillator frequency to 64 kHz.
	Section 8. “Memories” Figure 8-1. Memory Mapping: renamed MATRIXx blocks. Added PTC. Renamed TC blocks. Added SYSCWP block.
	Section 12. “Chip Identifier (CHIPID)” Table 12-1 “SAMA5D2 Chip ID Registers”: added chip ids for MRL C revision.
	Section 11. “Peripherals” Table 11-1 “Peripheral Identifiers”: corrected reference to SDMMC. Assigned ID 58 to Peripheral Touch Controller (PTC). Section 11.4 “Peripheral Clock Types”: removed clock type HCLOCK and PCLOCK from table.
	Section 13. “ARM Cortex-A5” Section 13.4.7.3 “Debug”: updated Note.

cont’d on next page