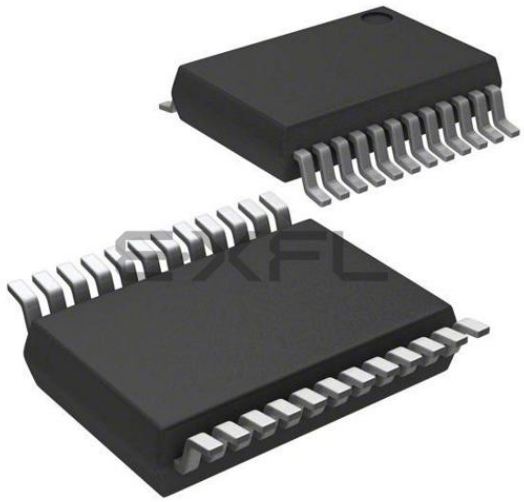


Welcome to E-XFL.COM

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®-M23
Core Size	32-Bit Single-Core
Speed	32MHz
Connectivity	I²C, LINbus, SPI, UART/USART
Peripherals	Brown-out Detect/Reset, DMA, POR, PWM, WDT
Number of I/O	17
Program Memory Size	64KB (64K x 8)
Program Memory Type	FLASH
EEPROM Size	2K x 8
RAM Size	16K x 8
Voltage - Supply (Vcc/Vdd)	1.62V ~ 3.63V
Data Converters	A/D 5x12b; D/A 1x10b
Oscillator Type	Internal
Operating Temperature	-40°C ~ 125°C (TA)
Mounting Type	Surface Mount
Package / Case	24-SSOP (0.209", 5.30mm Width)
Supplier Device Package	24-SSOP
Purchase URL	https://www.e-xfl.com/product-detail/microchip-technology/atsaml10d16a-yf

        - Standby with Full SRAM Retention (0.5 µA) with 5.3 µs wake-up time
        - Off mode (< 100 nA)
    - Static and dynamic power gating architecture
    - Sleepwalking peripherals
    - Two performance levels
    - Embedded Buck/LDO regulator with on-the-fly selection
- **Security**
    - Up to four tamper pins for static and dynamic intrusion detections
    - Data Flash
        - Optimized for secrets storage
        - Data Scrambling with user-defined key (optional)
        - Rapid Tamper erase on scrambling key and on one user-defined row
        - Silent access for side channel attack resistance
    - TrustRAM
        - Address and Data scrambling with user-defined key
        - Chip-level tamper detection on physical RAM to resist microprobing attacks
        - Rapid Tamper Erase on scrambling key and RAM data
        - Silent access for side channel attack resistance
        - Data remanence prevention
    - Peripherals
        - One True Random Generator (TRNG)
        - AES-128, SHA-256, and GCM cryptography accelerators (optional)
        - Secure pin multiplexing to isolate on dedicated I/O pins a secured communication with external devices from the non-secure application (optional)
    - TrustZone for flexible hardware isolation of memories and peripherals (optional)
        - Up to six regions for the Flash
        - Up to two regions for the Data Flash
        - Up to two regions for the SRAM
        - Individual security attribution for each peripheral, I/O, external interrupt line, and Event System Channel
    - Secure Boot with SHA-based authentication (optional)
    - Up to three debug access levels
    - Up to three Chip Erase commands to erase part of or the entire embedded memories
    - Unique 128-bit serial number
- **Advanced Analog and Touch**
    - One 12-bit 1 Msps Analog-to-Digital Converter (ADC) with up to 10 channels
    - Two Analog Comparators (AC) with window compare function
    - One 10-bit 350 kSPS Digital-to-Analog Converter (DAC) with external and internal outputs
    - Three Operational Amplifiers (OPAMP)
    - One enhanced Peripheral Touch Controller (PTC):
        - Up to 20 self-capacitance channels
        - Up to 100 (10 x 10) mutual-capacitance channels
        - Low-power, high-sensitivity, environmentally robust capacitive touch buttons, sliders, and wheels

Table 4-4. Serial Wire Debug Interface Pinout

Signal	Supply	I/O pin
SWCLK	VDDIO	PA30
SWDIO	VDDIO	PA31

4.4 SERCOM Configurations

The following table lists the supported features for each SERCOM instance:

Table 4-5. SERCOM Features Summary

	SERCOM Instance		
Protocol	**SERCOM0**	**SERCOM1**	**SERCOM2**
SPI	Yes	Yes	Yes
I^2C (1)	Yes High-speed mode (≤ 3,4 Mbit/s)	Yes Fast plus Mode (≤ 1 Mbit/s)	No
USART	Yes including: Hardware Handshaking IrDA	Yes including: Hardware Handshaking IrDA	Yes including: Hardware Handshaking IrDA RS-485 Auto-baud mode LIN Slave ISO7816
USART/SPI Receive Buffer Size	Two-level	Four-level	Two-level
Secure Pin Multiplexing (**SAM L11 only**)	No	Yes	No

Note:

1. I^2C is not supported on all SERCOM pins. Refer to the SERCOM I^2C Pins table for more details.

4.4.1 SERCOM I2C Pins

The following table lists the SERCOM pins which support I^2C:

Table 4-6. SERCOM I^2C Pins

Pin Name	SERCOM0 I^2C Pad Name	SERCOM1 I^2C Pad Name
PA16	SERCOM0/PAD[0]	SERCOM1/PAD[0]
PA17	SERCOM0/PAD[1]	SERCOM1/PAD[1]
PA22	SERCOM0/PAD[0]	N/A
PA23	SERCOM0/PAD[1]	N/A

4.4.2 Secure Pin Multiplexing (on SERCOM) Pins

The Secure Pin Multiplexing feature can be used on dedicated SERCOM I/O pins to isolate a secure communication with external devices from the non-secure application.

Refer to 13.6 Secure Pin Multiplexing on SERCOM for more details.

The following table lists the SERCOM pins that support the Secure Pin Multiplexing feature:

Features	Cortex-M23 Configurable Options	SAM L10 Implementation	SAM L11 Implementation
Cross Trigger Interface (CTI)	Present or absent	Absent	Absent
Micro Trace Buffer (MTB)	Present or absent	Absent	Absent
Embedded Trace Macrocell (ETM)	Present or absent	Absent	Absent
JTAGnSW debug protocol	Selects between JTAG or Serial-Wire interfaces for the DAP	Serial-Wire	Serial-Wire
Multi-drop for Serial Wire	Present or absent	Absent	Absent

Note:

1. Refer to Table 11-3 for more information.

For more details, refer to the ARM Cortex-M23 Processor Technical Reference Manual (http://www.arm.com).

11.1.2 Cortex-M23 Core Peripherals

The processor has the following core peripheral:

- System Timer (SysTick)
  - The System Timer is a 24-bit timer clocked by the core frequency.

> **Important:** On SAM L11 devices, there are two System timers, one for Secure state and one for Non-secure state.

- Nested Vectored Interrupt Controller (NVIC)
  - The NVIC is an embedded interrupt controller that supports low latency interrupt processing.

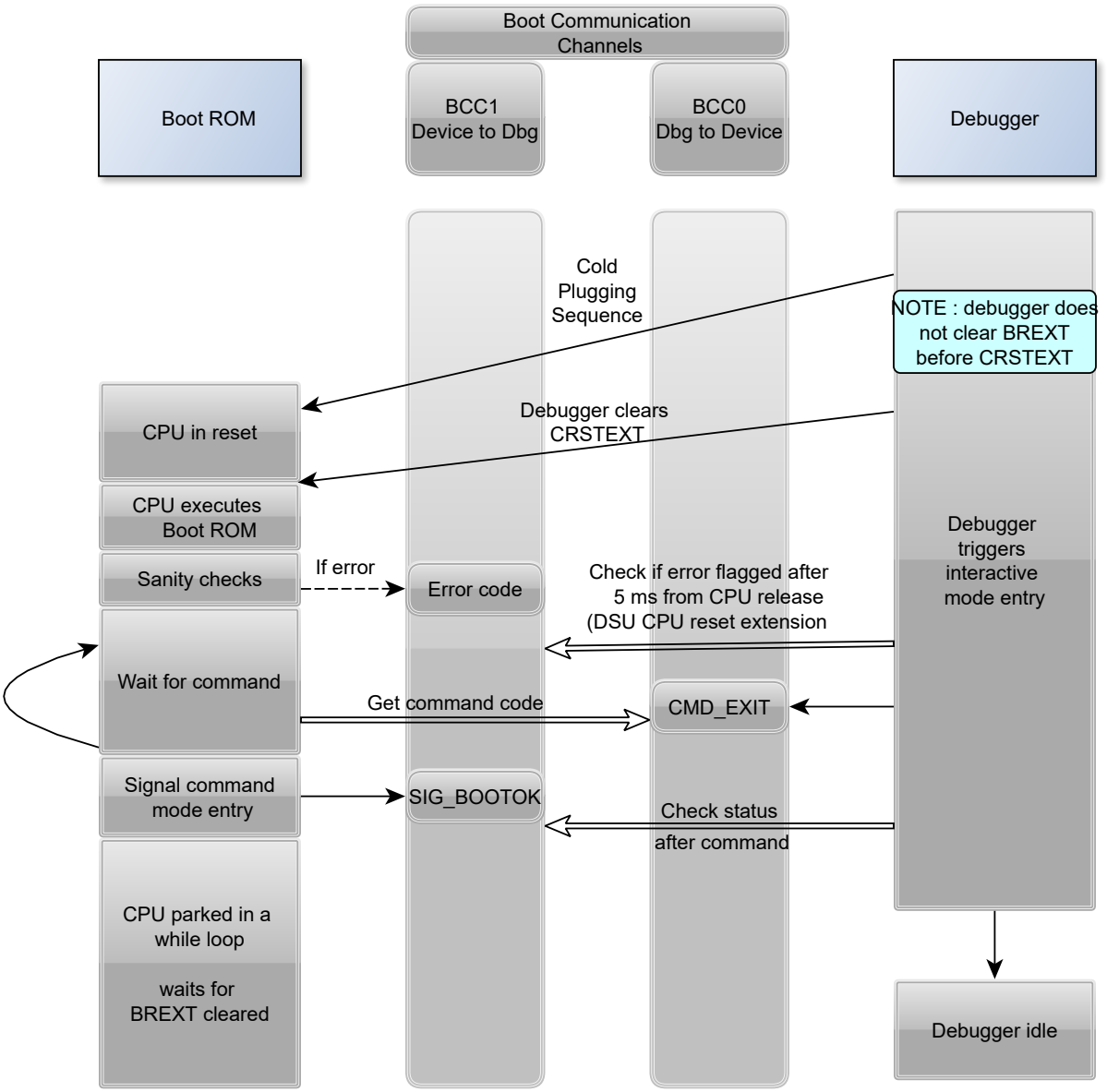
> **Important:** On SAM L11 devices, there are two Vector tables: the Secure Vector table and the Non-Secure Vector table.

- System Control Block (SCB)
  - The System Control Block (SCB) provides system implementation information and system control that includes configuration, control, and reporting of system exceptions
- Memory Protection Unit (MPU)
  - The MPU improves system reliability by defining the memory attributes for different memory regions.

> **Important:** On SAM L11 devices, there are two MPUs: one for the Secure state and one for the Non-secure state. Each MPU can define memory access permissions and attributes independently.

- Security Attribution Unit (SAU)
  - The SAU improves system security by defining security attributes for different regions.

Figure 14-9. CMD_EXIT to Park mode flow diagram



14.4.5.3 System Reset Request (CMD_RESET)

This command allows resetting the system using a system reset request. Since the reset is executed immediately after receiving the command, no reply is sent to the debugger.

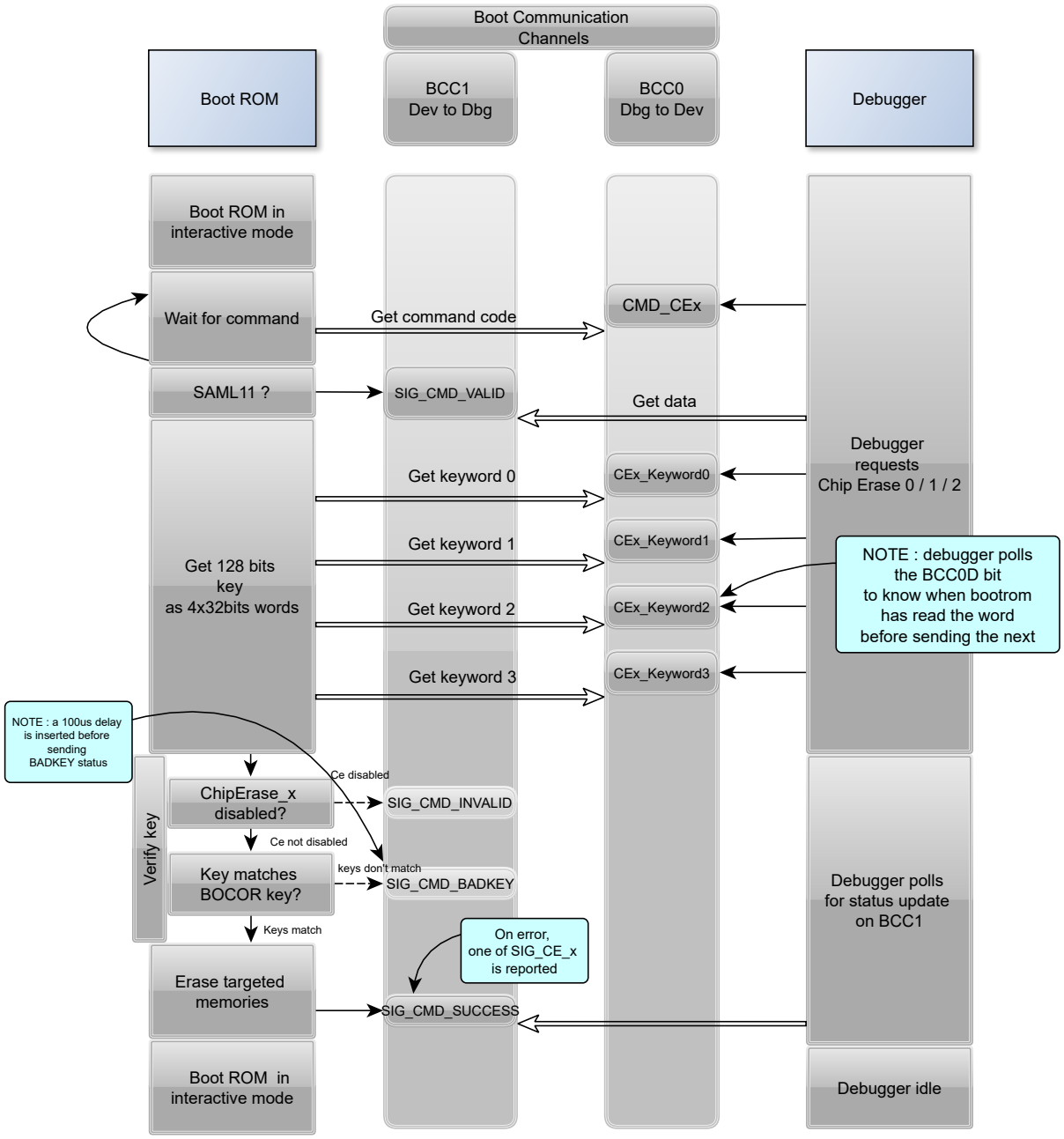
After reset, the CPU executes the Boot ROM code from the beginning

14.4.5.4 Chip Erase (CMD_CHIPERASE) - SAM L10 only

CMD_CHIPERASE command erases the entire device except BOOT area, and reverts to Debug Access Level 2.

14.4.5.5.1 CMD_CEx (SAM L11 only)

Figure 14-11. CMD_CEx Flow diagram



14.4.5.6 NVM Memory Regions Integrity Checks (CMD_CRC)

The Boot ROM provides a way to check the integrity of the embedded non-volatile memories which may be of interest in case of a failure analysis.

This requires the user to place tables describing the memory area to be checked with their expected CRC values.

Note: During this integrity check process, the debugger sends the CRC table address to the device.

Table 15-2. PERID Values

Peripheral Bridge Name	BridgeNumber	PERID Values
A	0	0+N
B	1	32+N
C	2	64+N

16.12.6 Data

Name: DATA
Offset: 0x000C
Reset: 0x00000000
Property: PAC Write-Protection

Bit	31	30	29	28	27	26	25	24
	DATA[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
	DATA[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
	DATA[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
	DATA[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 – DATA[31:0] Data
Memory operation initial value or result value.

19.7 Register Summary

Offset	Name	Bit Pos.								
0x00	CTRLA	7:0						CKSEL		
0x01	INTENCLR	7:0								CKRDY
0x02	INTENSET	7:0								CKRDY
0x03	INTFLAG	7:0								CKRDY
0x04	Reserved									
0x05	CPUDIV	7:0	CPUDIV[7:0]							
0x06 ... 0x0F	Reserved									
0x10	AHBMASK	7:0	NVMCTRL	PAC	Reserved	DSU	DMAC	APBC	APBB	APBA
		15:8				TRAM	Reserved	Reserved	Reserved	Reserved
		23:16								
		31:24								
0x14	APBAMASK	7:0	GCLK	SUPC	OSC32KCTRL	OSCCTRL	RSTC	MCLK	PM	PAC
		15:8		Reserved	AC	PORT	FREQM	EIC	RTC	WDT
		23:16								
		31:24								
0x18	APBBMASK	7:0				HMATRIXHS		NVMCTRL	DSU	IDAU
		15:8								
		23:16								
		31:24								
0x1C	APBCMASK	7:0	ADC	TC2	TC1	TC0	SERCOM2	SERCOM1	SERCOM0	EVSYS
		15:8				OPAMP	CCL	TRNG	PTC	DAC
		23:16								
		31:24								

19.8 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 can be write-protected optionally by the Peripheral Access Controller (PAC). This is denoted by the property "PAC Write-Protection" in each individual register description. Refer to the 19.5.8 Register Access Protection for details.

On **SAM L11** devices, this peripheral has different access permissions depending on PAC Security Attribution (Secure or Non-Secure):

- If the peripheral is configured as Non-Secure in the PAC:
  - Secure access and Non-Secure access are granted
- If the peripheral is configured as Secure in the PAC:
  - Secure access is granted
  - Non-Secure access is discarded (Write is ignored, read 0x0) and a PAC error is triggered

20.6.2.2 Enabling, Disabling and Resetting

The FREQM is enabled by writing a '1' to the Enable bit in the Control A register (CTRLA.ENABLE). The peripheral is disabled by writing CTRLA.ENABLE=0.

The FREQM is reset by writing a '1' to the Software Reset bit in the Control A register (CTRLA.SWRST). On software reset, all registers in the FREQM will be reset to their initial state, and the FREQM will be disabled.

Then ENABLE and SWRST bits are write-synchronized.

Related Links

20.6.7 Synchronization

20.6.2.3 Measurement

In the Configuration A register, the Number of Reference Clock Cycles field (CFGA.REFNUM) selects the duration of the measurement. The measurement is given in number of GCLK_FREQM_REF periods.
Note: The REFNUM field must be written before the FREQM is enabled.

After the FREQM is enabled, writing a '1' to the START bit in the Control B register (CTRLB.START) starts the measurement. The BUSY bit in Status register (STATUS.BUSY) is set when the measurement starts, and cleared when the measurement is complete.

There is also an interrupt request for Measurement Done: When the Measurement Done bit in Interrupt Enable Set register (INTENSET.DONE) is '1' and a measurement is finished, the Measurement Done bit in the Interrupt Flag Status and Clear register (INTFLAG.DONE) will be set and an interrupt request is generated.

The result of the measurement can be read from the Value register (VALUE.VALUE). The frequency of the measured clock GCLK_FREQM_MSR is then:

$$f_{CLK\_MSR} = \left(\frac{VALUE}{REFNUM}\right) f_{CLK\_REF}$$

Note: In order to make sure the measurement result (VALUE.VALUE[23:0]) is valid, the overflow status (STATUS.OVF) should be checked.

In case an overflow condition occurred, indicated by the Overflow bit in the STATUS register (STATUS.OVF), either the number of reference clock cycles must be reduced (CFGA.REFNUM), or a faster reference clock must be configured. Once the configuration is adjusted, clear the overflow status by writing a '1' to STATUS.OVF. Then another measurement can be started by writing a '1' to CTRLB.START.

20.6.3 DMA Operation

Not applicable.

20.6.4 Interrupts

The FREQM has one interrupt source:

- DONE: A frequency measurement is done.

The interrupt flag in the Interrupt Flag Status and Clear (20.8.6 INTFLAG) register is set when the interrupt condition occurs. The interrupt can be enabled by writing a '1' to the corresponding bit in the Interrupt Enable Set (20.8.5 INTENSET) register, and disabled by writing a '1' to the corresponding bit in the Interrupt Enable Clear (20.8.4 INTENCLR) register.

An interrupt request is generated when the interrupt flag is set and the corresponding interrupt is enabled. The interrupt request remains active until the interrupt flag is cleared, the interrupt is disabled, or the

Event

If the Event Output Enable bit in the Event Control register (EVCTRL.CFDEO) is set, the CFD clock failure will be output on the Event Output. When the CFD is switched to the safe clock, the CFD clock failure will not be output on the Event Output.

Sleep Mode

The CFD is halted depending on configuration of the XOSC32K and the peripheral clock request. For further details, refer to the Sleep Behavior table above. The CFD interrupt can be used to wake up the device from sleep modes.

24.6.4 32 kHz Ultra Low-Power Internal Oscillator (OSCULP32K) Operation

The OSCULP32K provides a tunable, low-speed, and ultra low-power clock source. The OSCULP32K is factory-calibrated under typical voltage and temperature conditions.

The OSCULP32K is enabled by default after a Power-on Reset (POR), and will always run except during POR. The frequency of the OSCULP32K Oscillator is controlled by the value in the Calibration bits in the 32 kHz Ultra Low-Power Internal Oscillator Control register (OSCULP32K.CALIB). This data is used to compensate for process variations.

OSCULP32K.CALIB is automatically loaded from Flash Factory Calibration during start-up. The calibration value can be overridden by the user by writing to OSCULP32K.CALIB.

Users can lock the OSCULP32K configuration by setting the Write Lock bit in the 32 kHz Ultra Low-Power Internal Oscillator Control register (OSCULP32K.WRTLOCK = 1). If set, the OSCULP32K configuration is locked until POR is detected.

The OSCULP32K can be used as a source for Generic Clock Generators (GCLK) or for the Real-Time Counter (RTC). To ensure proper operation, the GCLK or RTC modules must be disabled before the clock selection is changed.

OSCULP32K Clock Switch

The Clock switch operation requires the XOSC32K to be enabled (XOSC32K.ENABLE=1 and STATUS.XOSC32KRDY = 1). When the OSCULP32K Clock Switch Enable bit (OSCULP32K.ULP32KSW) is set, the CLK_OSCULP32K clock is switched to the XOSC32K Clock Oscillator. When the clock switch process is complete, the OSCULP32K Clock Switch bit in Status register (STATUS.ULP32KSW) is set. The OSCULP32K oscillator is shut off, and the XOSC32K oscillator becomes always running. The CFD feature is also disabled by hardware. When set, the OSCULP32K.ULP32KSW can be reset only by POR operation.

Related Links

27. RTC – Real-Time Counter

24.6.6 Real-Time Counter Clock Selection

18. GCLK - Generic Clock Controller

24.6.5 Watchdog Timer Clock Selection

The Watchdog Timer (WDT) uses the internal 1.024kHz OSCULP32K output clock. This clock is running all the time and internally enabled when requested by the WDT module.

Related Links

26. WDT – Watchdog Timer

CTRLA.ENABLE=0 and check whether the write synchronization has finished, then change the desired bit field value. Enable-protected bits in CTRLA register can be written at the same time as CTRLA.ENABLE is written to '1', but not at the same time as CTRLA.ENABLE is written to '0'.

Enable-protection is denoted by the "Enable-Protected" property in the register description.

The RTC prescaler divides the source clock for the RTC counter.

Note: In Clock/Calendar mode, the prescaler must be configured to provide a 1Hz clock to the counter for correct operation.

The frequency of the RTC clock (CLK_RTC_CNT) is given by the following formula:

$$f_{\mathrm{CLK\_RTC\_CNT}} = \frac{f_{\mathrm{CLK\_RTC\_OSC}}}{2^{\mathrm{PRESCALER}}}$$

The frequency of the oscillator clock, CLK_RTC_OSC, is given by $f_{CLK\_RTC\_OSC}$, and $f_{CLK\_RTC\_CNT}$ is the frequency of the internal prescaled RTC clock, CLK_RTC_CNT.

27.6.2.2 Enabling, Disabling, and Resetting

The RTC is enabled by setting the Enable bit in the Control A register (CTRLA.ENABLE=1). The RTC is disabled by writing CTRLA.ENABLE=0.

The RTC is reset by setting the Software Reset bit in the Control A register (CTRLA.SWRST=1). All registers in the RTC, except DEBUG, will be reset to their initial state, and the RTC will be disabled. The RTC must be disabled before resetting it.

27.6.2.3 32-Bit Counter (Mode 0)

When the RTC Operating Mode bits in the Control A register (CTRLA.MODE) are written to 0x0, the counter operates in 32-bit Counter mode. The block diagram of this mode is shown in Figure 27-1. When the RTC is enabled, the counter will increment on every 0-to-1 transition of CLK_RTC_CNT. The counter will increment until it reaches the top value of 0xFFFFFFFF, and then wrap to 0x00000000. This sets the Overflow Interrupt flag in the Interrupt Flag Status and Clear register (INTFLAG.OVF).

The RTC counter value can be read from or written to the Counter Value register (COUNT) in 32-bit format.

The counter value is continuously compared with the 32-bit Compare register (COMP0). When a compare match occurs, the Compare 0 Interrupt flag in the Interrupt Flag Status and Clear register (INTFLAG.CMP0) is set on the next 0-to-1 transition of CLK_RTC_CNT.

If the Clear on Match bit in the Control A register (CTRLA.MATCHCLR) is '1', the counter is cleared on the next counter cycle when a compare match with COMP0 occurs. This allows the RTC to generate periodic interrupts or events with longer periods than the prescaler events. Note that when CTRLA.MATCHCLR is '1', INTFLAG.CMP0 and INTFLAG.OVF will both be set simultaneously on a compare match with COMP0.

27.6.2.4 16-Bit Counter (Mode 1)

When the RTC Operating Mode bits in the Control A register (CTRLA.MODE) are written to 0x1, the counter operates in 16-bit Counter mode as shown in Figure 27-2. When the RTC is enabled, the counter will increment on every 0-to-1 transition of CLK_RTC_CNT. In 16-bit Counter mode, the 16-bit Period register (PER) holds the maximum value of the counter. The counter will increment until it reaches the PER value, and then wrap to 0x0000. This sets the Overflow Interrupt flag in the Interrupt Flag Status and Clear register (INTFLAG.OVF).

The RTC counter value can be read from or written to the Counter Value register (COUNT) in 16-bit format.

27.10.14 Tamper Control

Name: TAMPCTRL
Offset: 0x60
Reset: 0x00000000
Property: PAC Write-Protection, Enable-Protected

Bit	31	30	29	28	27	26	25	24
					DEBNC3	DEBNC2	DEBNC1	DEBNC0
Access								
Reset					0	0	0	0

Bit	23	22	21	20	19	18	17	16
					TAMLVL3	TAMLVL2	TAMLVL1	TAMLVL0
Access								
Reset					0	0	0	0

Bit	15	14	13	12	11	10	9	8
Access								
Reset								

Bit	7	6	5	4	3	2	1	0
	IN3ACT[1:0]		IN2ACT[1:0]		IN1ACT[1:0]		IN0ACT[1:0]	
Access								
Reset	0	0	0	0	0	0	0	0

Bits 24, 25, 26, 27 – DEBNC Debounce Enable of Tamper Input INn

Value	Description
0	Debouncing is disabled for Tamper input INn
1	Debouncing is enabled for Tamper input INn

Bits 16, 17, 18, 19 – TAMLVL Tamper Level Select of Tamper Input INn

Value	Description
0	A falling edge condition will be detected on Tamper input INn.
1	A rising edge condition will be detected on Tamper input INn.

Bits 0:1, 2:3, 4:5, 6:7 – INACT Tamper Channel n Action
These bits determine the action taken by Tamper Channel n.

Value	Name	Description
0x0	OFF	Off (Disabled)
0x1	WAKE	Wake and set Tamper flag
0x2	CAPTURE	Capture timestamp and set Tamper flag
0x3	ACTL	Compare RTC signal routed between INn and OUT pins . When a mismatch occurs, capture timestamp and set Tamper flag

TRIGACT[1:0]	Name	Description
0x2	BEAT	One trigger required for each beat transfer
0x3	TRANSACTION	One trigger required for each transaction

Bits 12:8 – TRIGSRC[4:0] Trigger Source
These bits define the peripheral trigger which is source of the transfer. For details on trigger selection and trigger modes, refer to Transfer Triggers and Actions and CHCTRLB.TRIGACT.

Value	Name	Description
0x00	DISABLE	Only software/event triggers
0x01	RTC TIMESTAMP	RTC Timestamp Trigger
0x02	DSU DCC0	ID for DCC0 register
0x03	DSU DCC1	ID for DCC1 register
0x04	SERCOM0 RX	SERCOM0 RX Trigger
0x05	SERCOM0 TX	SERCOM0 TX Trigger
0x06	SERCOM1 RX	SERCOM1 RX Trigger
0x07	SERCOM1 TX	SERCOM1 TX Trigger
0x08	SERCOM2 RX	SERCOM2 RX Trigger
0x09	SERCOM2 TX	SERCOM2 TX Trigger
0x0A	TC0 OVF	TC0 Overflow Trigger
0x0B	TC0 MC0	TC0 Match/Compare 0 Trigger
0x0C	TC0 MC1	TC0 Match/Compare 1 Trigger
0x0D	TC1 OVF	TC1 Overflow Trigger
0x0E	TC1 MC0	TC1 Match/Compare 0 Trigger
0x0F	TC1 MC1	TC1 Match/Compare 1 Trigger
0x10	TC2 OVF	TC2 Overflow Trigger
0x11	TC2 MC0	TC2 Match/Compare 0 Trigger
0x12	TC2 MC1	TC2 Match/Compare 1 Trigger
0x13	ADC RESRDY	ADC Result Ready Trigger
0x14	DAC EMPTY	DAC Empty Trigger
0x15	PTC EOC	PTC End of Conversion Trigger
0x16	PTC SEQ	PTC Sequence Trigger
0x17	PTC WCOMP	PTC Window Compare Trigger

Bits 6:5 – LVL[1:0] Channel Arbitration Level
These bits define the arbitration level used for the DMA channel, where a high level has priority over a low level. For further details on arbitration schemes, refer to 28.6.2.4 Arbitration.

These bits are not enable-protected.

TRIGACT[1:0]	Name	Description
0x0	LVL0	Channel Priority Level 0
0x1	LVL1	Channel Priority Level 1
0x2	LVL2	Channel Priority Level 2
0x3	LVL3	Channel Priority Level 3

- External interrupt pins (EXTINTx). See 29.6.2 Basic Operation.
- Non-maskable interrupt pin (NMI). See 29.6.4 Additional Features.
- Non-secure check interrupt pin (NSCHK). See 29.8.8 INTFLAG

Each interrupt source has an associated interrupt flag. The interrupt flag in the Interrupt Flag Status and Clear register (INTFLAG) is set when an interrupt condition occurs (NMIFLAG for NMI). Each interrupt, except NMI, can be individually enabled by setting the corresponding bit in the Interrupt Enable Set register (INTENSET=1), and disabled by setting the corresponding bit in the Interrupt Enable Clear register (INTENCLR=1).

An interrupt request is generated when the interrupt flag is set and the corresponding interrupt is enabled. The interrupt request remains active until the interrupt flag is cleared, the interrupt is disabled, or the EIC is reset. See the INTFLAG register for details on how to clear interrupt flags. The EIC has at least one common interrupt request line for all the interrupt sources, and one interrupt request line for the NMI. The user must read the INTFLAG (or NMIFLAG) register to determine which interrupt condition is present.

Note: Interrupts must be globally enabled for interrupt requests to be generated.

29.6.7 Events

The EIC can generate the following output events:

- External event from pin (EXTINTx).

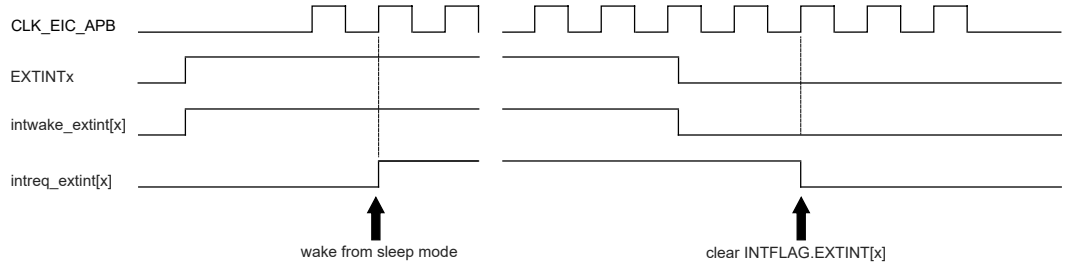
Setting an Event Output Control register (EVCTRL.EXTINTEO) enables the corresponding output event. Clearing this bit disables the corresponding output event. Refer to *Event System* for details on configuring the Event System.

When the condition on pin EXTINTx matches the configuration in the CONFIGn register, the corresponding event is generated, if enabled.

29.6.8 Sleep Mode Operation

In sleep modes, an EXTINTx pin can wake up the device if the corresponding condition matches the configuration in the CONFIG register, and the corresponding bit in the Interrupt Enable Set register (29.8.7 INTENSET) is written to '1'.

Figure 29-5. Wake-up Operation Example (High-Level Detection, No Filter, Interrupt Enable Set)



29.6.9 SAM L11 Secure Access Rights

Non-secure write to CTRLA register or DPRESCALER register is prohibited. Non-secure read to CTRLA or DPRESCALER register or SYNCBUSY register will return zero with no error resulting. Non-secure write to a bit of EVCTRL, ASYNCH, DEBOUNCEN, INTENCLR, INTENSET, INTFLAG and CONFIG registers is prohibited if the related bit of NONSEC.EXTINT is zero. Non-secure write to NMICTRL and NMIFLAG registers is prohibited if NONSECNMI.NMI is zero. Bits relating to secure EXTINT read as zero in non-secure mode with no error resulting.

33.7.7 Ready Users

Name: READYUSR
Offset: 0x1C
Reset: 0x0000000F
Property: Mix-Secure

Important: For **SAM L11 Non-Secure** accesses, read accesses (R*) are allowed only if the security attribution for the corresponding channel (CHANNELx) is set as Non-Secured in the NONSECCHAN register.

Bit	31	30	29	28	27	26	25	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
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
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
					READYUSR3	READYUSR2	READYUSR1	READYUSR0
Access	R	R	R	R	R/R*/R	R/R*/R	R/R*/R	R/R*/R
Reset	0	0	0	0	1	1	1	1

Bits 0, 1, 2, 3 – READYUSR Ready User for Channel n
This bit is set when all event users connected to channel n are ready to handle incoming events on channel n.

This bit is cleared when at least one of the event users connected to the channel is not ready.

When the event channel n path is asynchronous, this bit is always read zero.

37.10.2 Control B

Name: CTRLB
Offset: 0x04
Reset: 0x00000000
Property: PAC Write-Protection, Enable-Protected, Write-Synchronized

Bit	31	30	29	28	27	26	25	24
Access								
Reset								

Bit	23	22	21	20	19	18	17	16
						ACKACT	CMD[1:0]	
Access						R/W	R/W	R/W
Reset						0	0	0

Bit	15	14	13	12	11	10	9	8
							QCEN	SMEN
Access							R	R/W
Reset							0	0

Bit	7	6	5	4	3	2	1	0
Access								
Reset								

Bit 18 – ACKACT Acknowledge Action
This bit defines the I^2C master's acknowledge behavior after a data byte is received from the I^2C slave. The acknowledge action is executed when a command is written to CTRLB.CMD, or if smart mode is enabled (CTRLB.SMEN is written to one), when DATA.DATA is read.

This bit is not enable-protected.

This bit is not write-synchronized.

Value	Description
0	Send ACK.
1	Send NACK.

Bits 17:16 – CMD[1:0] Command
Writing these bits triggers a master operation as described below. The CMD bits are strobe bits, and always read as zero. The acknowledge action is only valid in master read mode. In master write mode, a command will only result in a repeated start or stop condition. The CTRLB.ACKACT bit and the CMD bits can be written at the same time, and then the acknowledge action will be updated before the command is triggered.

Commands can only be issued when either the Slave on Bus interrupt flag (INTFLAG.SB) or Master on Bus interrupt flag (INTFLAG.MB) is '1'.

39.8.6 Output Data

Name: DATA
Offset: 0x20
Reset: 0x00000000
Property: -

Bit	31	30	29	28	27	26	25	24
	DATA[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
	DATA[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
	DATA[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
	DATA[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 – DATA[31:0] Output Data
These bits hold the 32-bit randomly generated output data.

41.8.3 Reference Control

Name: REFCTRL
Offset: 0x02
Reset: 0x00
Property: PAC Write-Protection, Enable-Protected

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

Bit 7 – REFCOMP Reference Buffer Offset Compensation Enable
The gain error can be reduced by enabling the reference buffer offset compensation. This will increase the start-up time of the reference.

Value	Description
0	Reference buffer offset compensation is disabled.
1	Reference buffer offset compensation is enabled.

Bits 3:0 – REFSEL[3:0] Reference Selection
These bits select the reference for the ADC.

Value	Name	Description
0x0	INTREF	Internal variable reference voltage, refer to the SUPC.VREF register for voltage reference value
x01	INTVCC0	1/1.6 VDDANA
0x2	INTVCC1	1/2 VDDANA (only for VDDANA > 2.0V)
0x3	VREFA	External reference
0x4	VREFB	External reference
0x5	INTVCC2	VDDANA
0x6 - 0xF		Reserved

44.7 Register Summary

Offset	Name	Bit Pos.								
0x00	CTRLA	7:0	LPMUX						ENABLE	SWRST
0x01	Reserved									
0x02	STATUS	7:0						READYx	READYx	READYx
0x03	Reserved									
0x04	OPAMPCTRL0	7:0	ONDEMAND	RUNSTDBY	RES2VCC	BIAS[1:0]		ANAOUT	ENABLE	
		15:8	POTMUX[2:0]			RES1MUX[2:0]			RES1EN	RES2OUT
		23:16	MUXNEG[3:0]				MUXPOS[3:0]			
		31:24								
0x08	OPAMPCTRL1	7:0	ONDEMAND	RUNSTDBY	RES2VCC	BIAS[1:0]		ANAOUT	ENABLE	
		15:8	POTMUX[2:0]			RES1MUX[2:0]			RES1EN	RES2OUT
		23:16	MUXNEG[3:0]				MUXPOS[3:0]			
		31:24								
0x0C	OPAMPCTRL2	7:0	ONDEMAND	RUNSTDBY	RES2VCC	BIAS[1:0]		ANAOUT	ENABLE	
		15:8	POTMUX[2:0]			RES1MUX[2:0]			RES1EN	RES2OUT
		23:16	MUXNEG[3:0]				MUXPOS[3:0]			
		31:24								
0x10	RESCTRL	7:0	REFBUFLEVEL[1:0]			POTMUX[2:0]		RES1MUX	RES1EN	RES2OUT

44.8 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.

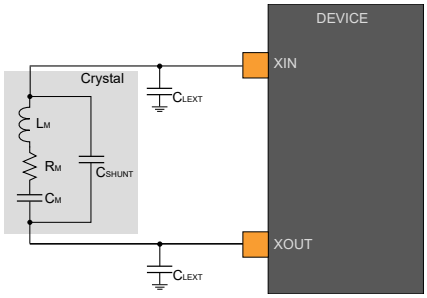
Some registers are optionally write-protected by the Peripheral Access Controller (PAC). Optional PAC write-protection is denoted by the "PAC Write-Protection" property in each individual register description. For details, refer to Register Access Protection.

On **SAM L11** devices, this peripheral has different access permissions depending on PAC Security Attribution (Secure or Non-Secure):

- If the peripheral is configured as Non-Secure in the PAC:
  - Secure access and Non-Secure access are granted
- If the peripheral is configured as Secure in the PAC:
  - Secure access is granted
  - Non-Secure access is discarded (Write is ignored, read 0x0) and a PAC error is triggered

Refer to *Peripherals Security Attribution* for more information.

Figure 46-3. Oscillator Connection



The user must choose a crystal oscillator where the crystal load capacitance C_L is within the range given in the Table. The exact value of C_L can be found in the crystal data sheet. The capacitance of the external capacitors (C_{LEXT}) can then be computed as follows:

$C_{LEXT} = 2(C_L - C_{PARA} - C_{PCB} - C_{SHUNT})$

Where:

- C_{PARA} is the internal load capacitor parasitic between XIN and XOUT ($C_{PARA} = (C_{XIN} * C_{XOUT})/(C_{XIN} + C_{XOUT})$)
- C_{PCB} is the capacitance of the PCB
- C_{SHUNT} is the shunt capacity of the crystal.

Table 46-44. Multi Crystal Oscillator Electrical Characteristics

Symbol	Parameter	Conditions	Min.	Typ.	Max	Units
Fout	Crystal oscillator frequency		0.4	-	32	MHz
ESR(2)	Crystal Equivalent Series Resistance - SF = 3	F = 0,4MHz - CL=100 pF XOSC,GAIN=0	-	-	5.6K	Ω
		F = 2MHz - CL=20 pF XOSC,GAIN=0, Cshunt=3.3pF	-	-	330	
		F = 4MHz - CL=20 pF XOSC,GAIN=1, Cshunt=2.5pF	-	-	240	
		F = 8MHz - CL=20 pF XOSC,GAIN=2, Cshunt=5.5pF	-	-	105	
		F = 16MHz - CL=20 pF XOSC,GAIN=3, Cshunt=4pF	-	-	60	
		F = 32MHz - CL=20 pF XOSC,GAIN=4, Cshunt=3.9pF	-	-	55	
Cxin(2)	Parasitic load capacitor		-	6.7	-	pF
Cxout(2)			-	4.2	-	pF
Tstart(2)	Startup time	F = 2MHz - CL=20 pF XOSC,GAIN=0, Cshunt=3.3pF	-	15.6K	81.6K	Cycles
		F = 4MHz - CL=20 pF XOSC,GAIN=1, Cshunt=2.5pF	-	6.3K	25.2K	