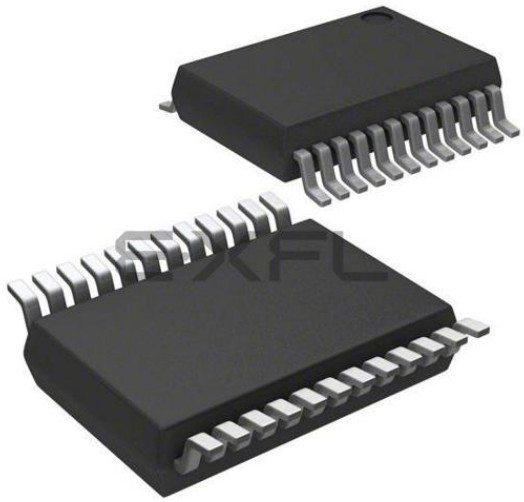


Welcome to E-XFL.COM

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	32KB (32K x 8)
Program Memory Type	FLASH
EEPROM Size	2K x 8
RAM Size	8K 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/atsaml10d15a-yft

Each peripheral can only be configured either in Secure or in Non-Secure mode.

The PAC NONSECx registers (Read Only) contain one bit per peripheral for that purpose, which is the image of the NONSECx fuses from the NVM User row (UROW).

During Boot ROM execution, the NONSECx fuses from the NVM User row are copied in the PAC peripheral NONSECx registers so that they can be read by the application.

All peripherals are marked as "exempt" in the memory map, meaning that all bus transactions are propagated. As a consequence, any illegal accesses are reported back to the PAC and trigger an interrupt if enabled.

The security configuration (Secure or Non-Secure) is propagated to each individual peripheral, thus it is the responsibility of the peripheral to grant or not the access with the following rules:

- If the peripheral is configured as Non-Secure in the PAC:
  - Secure access and Non-Secure 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), a PAC error is triggered

Important: These rules do not apply to the specific peripherals called Mix-Secure peripherals.

Note: The Secure application will usually provide an API for the Non-Secure application using the Non-Secure Callable region (NSC) to allow the Non-Secure application to request specific resources.

Table 13-8. Peripheral PAC Security Attribution (Excluding Mix-Secure Peripherals)

Mode	Secure Master Access	Non-Secure Master Access
Non-Secure	Read / Write	Read / Write
Secure	Read / Write	Discarded (Write ignored / Read 0x0) PAC Error is generated

13.2.5.1 SAM L11 Peripherals Configuration Example

Below is a typical configuration examples where all peripherals except the ADC, TC0, and Event System (EVSYS) are reserved to the Secure application:

- Secure/Non-Secure Peripherals PAC configuration:
  - PAC.NONSECA=PAC.NONSECB=0x0000_0000
  - PAC.NONSECC=0x0000_00091 (ADC, TC0 and EVSYS available for the Non-Secure application)

13.2.6 SAM L11 Memory Space Security Attribution

This table provides the security attributions of the SAM L11 memory space:

16.12.9 Device Identification

Name: DID
Offset: 0x0018
Reset: see related links
Property: PAC Write-Protection

The information in this register is related to the 2. Ordering Information.

Bit	31	30	29	28	27	26	25	24
	PROCESSOR[3:0]				FAMILY[4:1]			
Access	R	R	R	R	R	R	R	R
Reset	p	p	p	p	f	f	f	f

Bit	23	22	21	20	19	18	17	16
	FAMILY[0:0]		SERIES[5:0]					
Access	R		R	R	R	R	R	R
Reset	f		s	s	s	s	s	s

Bit	15	14	13	12	11	10	9	8
	DIE[3:0]				REVISION[3:0]			
Access	R	R	R	R	R	R	R	R
Reset	d	d	d	d	r	r	r	r

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

Bits 31:28 – PROCESSOR[3:0] Processor
The value of this field defines the processor used on the device.

Bits 27:23 – FAMILY[4:0] Product Family
The value of this field corresponds to the Product Family part of the ordering code.

Bits 21:16 – SERIES[5:0] Product Series
The value of this field corresponds to the Product Series part of the ordering code.

Bits 15:12 – DIE[3:0] Die Number
Identifies the die family.

Bits 11:8 – REVISION[3:0] Revision Number
Identifies the die revision number. 0x0=rev.A, 0x1=rev.B etc.

Note: The device variant (last letter of the ordering number) is independent of the die revision (DSU.DID.REVISION): The device variant denotes functional differences, whereas the die revision marks evolution of the die.

16.12.14 CoreSight ROM Table Entry 1

Name: ENTRY1
Offset: 0x1004
Reset: 0xXXXXX00X
Property: PAC Write-Protection

Bit	31	30	29	28	27	26	25	24
	ADDOFF[19:12]							
Access	R	R	R	R	R	R	R	R
Reset	x	x	x	x	x	x	x	x

Bit	23	22	21	20	19	18	17	16
	ADDOFF[11:4]							
Access	R	R	R	R	R	R	R	R
Reset	x	x	x	x	x	x	x	x

Bit	15	14	13	12	11	10	9	8
	ADDOFF[3:0]							
Access	R	R	R	R				
Reset	x	x	x	x				

Bit	7	6	5	4	3	2	1	0
							FMT	EPRES
Access							R	R
Reset							1	x

Bits 31:12 – ADDOFF[19:0] Address Offset
The base address of the component, relative to the base address of this ROM table.

Bit 1 – FMT Format
Always read as '1', indicating a 32-bit ROM table.

Bit 0 – EPRES Entry Present
This bit indicates whether an entry is present at this location in the ROM table.

This bit is set at power-up if the device is not protected indicating that the entry is not present.

This bit is cleared at power-up if the device is not protected indicating that the entry is present.

46.14.1 External Reset Pin

21.6.3 Additional Features

Not applicable.

21.6.4 DMA Operation

Not applicable.

21.6.5 Interrupts

Not applicable.

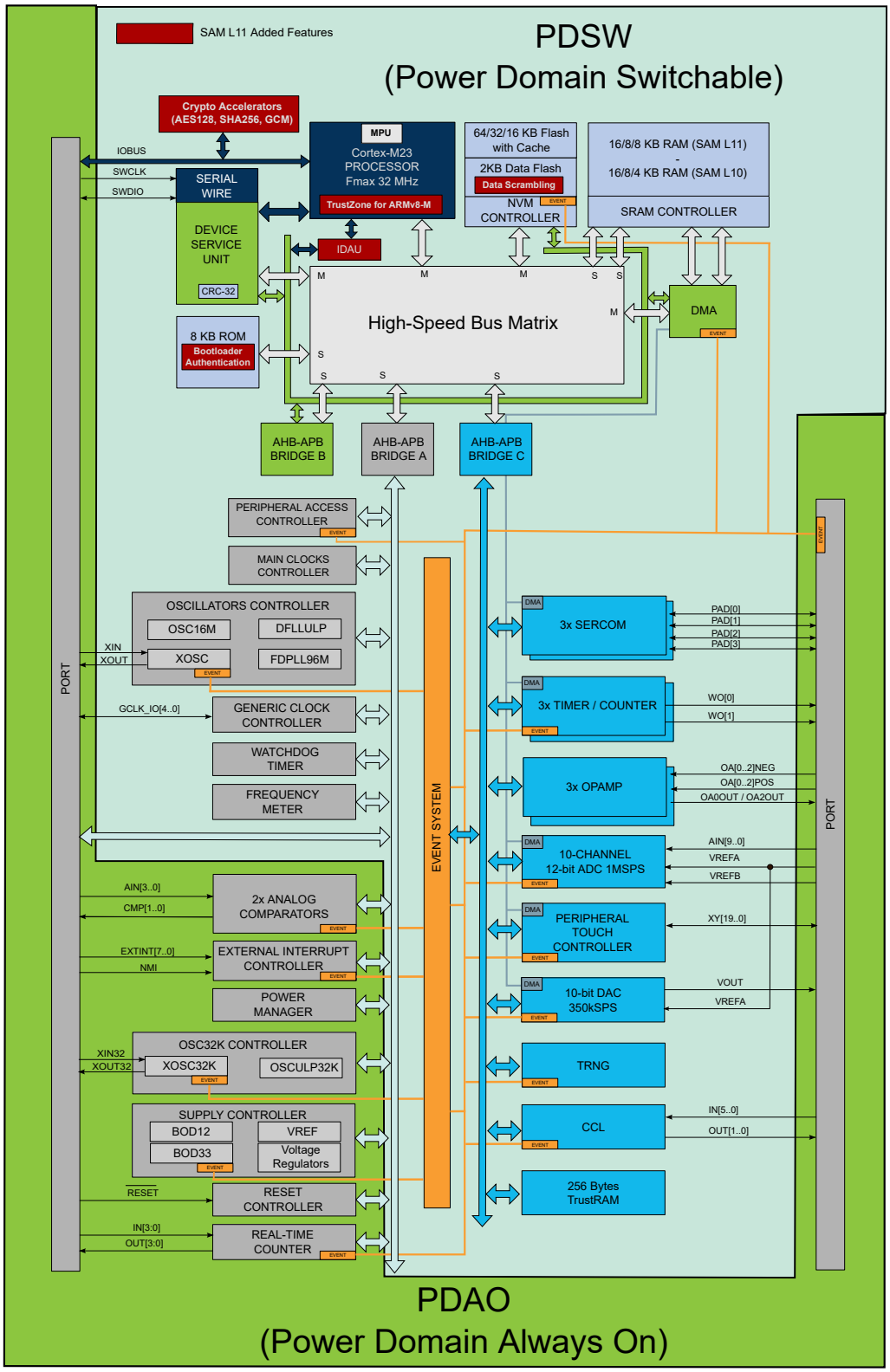
21.6.6 Events

Not applicable.

21.6.7 Sleep Mode Operation

The RSTC module is active in all sleep modes.

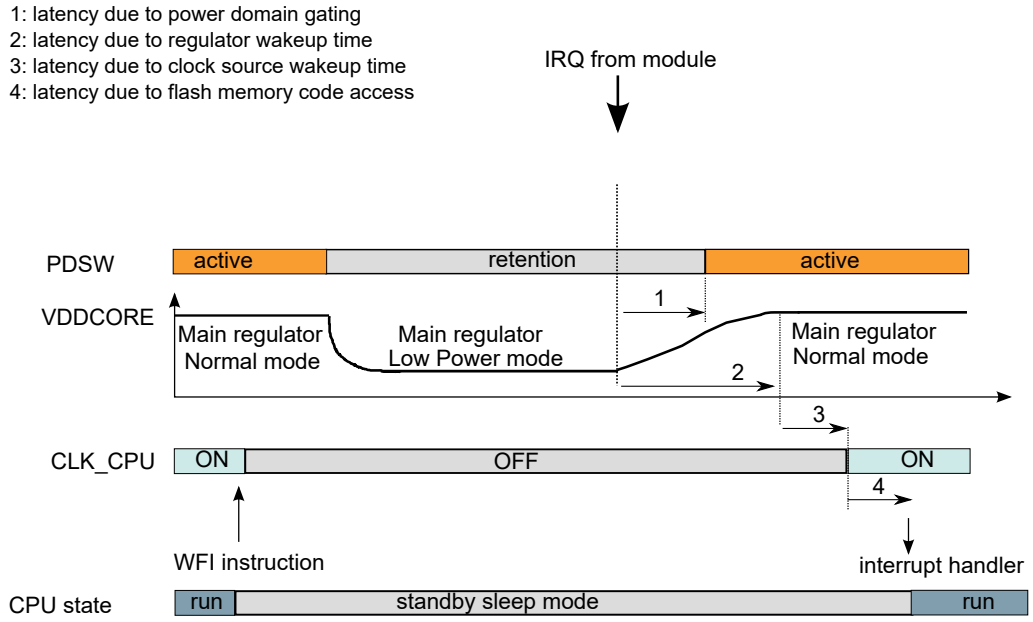
Figure 22-2. Power Domain Partitioning



amount of time for the main regulator to transition to the voltage level corresponding to PL2, causing additional wake-up time.

- Latency due to the CPU clock source wake-up time.
- Latency due to the NVM memory access.
- Latency due to Switchable Power Domain back-bias wake-up time:
  If back-bias is enabled, and the device wakes up from retention, it takes a certain amount of time for the regulator to settle.

Figure 22-5. Total Wake-up Time from Standby Sleep Mode



22.6.5 Standby with Static Power Domain Gating in Details

In Standby Sleep mode, the switchable power domain (PDSW) of a peripheral can remain in active state to perform the peripheral's tasks. This Static Power Domain Gating feature is supported by all peripherals. For some peripherals it must be enabled by writing a Run in Standby bit in the respective Control A register (CTRLA.RUNSTDBY) to '1'. Refer to each peripheral chapter for details.

The following examples illustrate Standby with static Power Domain Gating:

TC0 Standby with Static Power Domain Gating

TC0 peripheral is used in counter operation mode. An interrupt is generated to wake-up the device based on the TC0 peripheral configuration. To make the TC0 peripheral continue to run in Standby Sleep mode, the RUNSTDBY bit is written to '1'.

- Entering Standby mode: As shown in Figure 22-6, PDSW remains active. Refer to 22.6.3.5 Power Domain Controller for details.
- Exiting Standby mode: When conditions are met, the TC0 peripheral generates an interrupt to wake-up the device, and the CPU is able to operate normally and execute the TC0 interrupt handler accordingly.
- Wake-up time:
  - The required time to set PDSW to active state has to be considered for the global wake-up time, refer to 22.6.4.6 Wake-Up Time for details.

Related Links

33. EVSYS – Event System

27.6.6 Sleep Mode Operation

The RTC will continue to operate in any sleep mode where the source clock is active. The RTC *interrupts* can be used to wake up the device from a sleep mode. RTC *events* can trigger other operations in the system without exiting the sleep mode.

An interrupt request will be generated after the wake-up if the Interrupt Controller is configured accordingly. Otherwise the CPU will wake up directly, without triggering any interrupt. In this case, the CPU will continue executing right from the first instruction that followed the entry into sleep.

The periodic events can also wake up the CPU through the interrupt function of the Event System. In this case, the event must be enabled and connected to an event channel with its interrupt enabled. See *Event System* for more information.

27.6.7 Synchronization

Due to asynchronicity between the main clock domain and the peripheral clock domains, some registers need to be synchronized when written or read.

The following bits are synchronized when written:

- Software Reset bit in Control A register, CTRLA.SWRST
- Enable bit in Control A register, CTRLA.ENABLE
- Count Read Synchronization bit in Control A register (CTRLA.COUNTSYNC)
- Clock Read Synchronization bit in Control A register (CTRLA.COUNTSYNC)

The following registers are synchronized when written:

- Counter Value register, COUNT
- Clock Value register, CLOCK
- Counter Period register, PER
- Compare n Value registers, COMPn
- Alarm n Value registers, ALARMn
- Frequency Correction register, FREQCORR
- Alarm n Mask register, MASKn
- The General Purpose n registers (GPn)

The following registers are synchronized when read:

- The Counter Value register, COUNT, if the Counter Read Sync Enable bit in CTRLA (CTRLA.COUNTSYNC) is '1'
- The Clock Value register, CLOCK, if the Clock Read Sync Enable bit in CTRLA (CTRLA.CLOCKSYNC) is '1'
- The Timestamp Value register (TIMESTAMP)

Required write-synchronization is denoted by the "Write-Synchronized" property in the register description.

Required read-synchronization is denoted by the "Read-Synchronized" property in the register description.

Offset	Name	Bit Pos.								
0x44	GP1	7:0	GP[7:0]							
		15:8	GP[15:8]							
		23:16	GP[23:16]							
		31:24	GP[31:24]							
0x48 ... 0x5F	Reserved									
0x60	TAMPCTRL	7:0	IN3ACT[1:0]		IN2ACT[1:0]		IN1ACT[1:0]		IN0ACT[1:0]	
		15:8								
		23:16					TAMLVL3	TAMLVL2	TAMLVL1	TAMLVL0
		31:24					DEBNC3	DEBNC2	DEBNC1	DEBNC0
0x64	TIMESTAMP	7:0	MINUTE[1:0]		SECOND[5:0]					
		15:8	HOUR[3:0]				MINUTE[5:2]			
		23:16	MONTH[1:0]		DAY[4:0]					HOUR[4:4]
		31:24	YEAR[5:0]						MONTH[3:2]	
0x68	TAMPID	7:0					TAMPID3	TAMPID2	TAMPID1	TAMPID0
		15:8								
		23:16								
		31:24	TAMPEVT							
0x6C	TAMPCTRLB	7:0					ALSI3	ALSI2	ALSI1	ALSI0
		15:8								
		23:16								
		31:24								

27.12 Register Description - Mode 2 - Clock/Calendar

This Register Description section is valid if the RTC is in Clock/Calendar mode (CTRLA.MODE=2).

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 require synchronization when read and/or written. Synchronization is denoted by the "Read-Synchronized" and/or "Write-Synchronized" property in each individual register description.

Optional write-protection by the Peripheral Access Controller (PAC) is denoted by the "PAC Write-Protection" property in each individual register description.

Some registers are enable-protected, meaning they can only be written when the module is disabled. Enable-protection is denoted by the "Enable-Protected" property in each individual register description.

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

Memory Region	Secure Access	Non-Secure Access	Limitations
FLASH Application non-secure	Y	Y	No if NSULCK.ANS=0
Data FLASH secure	Y	N	No if SULCK.DS=0
Data FLASH non-secure	Y	Y	No if NSULCK.DNS=0
AUX FLASH User Row (UROW)	Y	N	No if BOCOR.URWEN=0
AUX FLASH Boot Configuration (BOCOR)	Y	N	No if BOCOR.BCWEN=0

The NSULCK SULCK bitfields in the user row define respectively the NSULCK and SULCK register default value after a reset.

Special care must be taken when sharing the NVMCTRL between the secure and non-secure domains. When the secure code modifies the NVM it is highly recommended that it disables all write accesses to the APB non-secure alias and writes to AHB non-secure regions by writing a 0 to NONSEC.WRITE. This avoids any interference with non-secure modify operations. Note that in this case even a secure application cannot write the page buffer at a non-secure location since the IDAU changes security attributions of Non-Secure transactions to Non-Secure regions to Non-Secure.

The NONSEC.WRITE reset value is '1', meaning that it is always possible to program a Non-Secure FLASH or Data FLASH region after a debugger probe cold-plugging. But if the debugger connects with the hot-plugging procedure then NONSEC.WRITE must be '1' to let the debugger program Non-Secure regions otherwise the transaction will cause a hardfault (seen as a DAP fault at DAP level).

For applications that don't require Non-Secure regions programming other than from a secure code, it is recommended to always disable Non-Secure writes by disabling NONSEC.WRITE. When disabled secure code needs to enable it to be able to modify Non-Secure regions following this procedure:

- disable interrupts
- write a one to NONSEC.WRITE to allow writes to the non-secure region
- write the page buffer
- write a zero to NONSEC.WRITE
- enable again the interrupts

If the NSCHK interrupt is enabled, a NONSEC.WRITE modification will generate an interrupt so that the non-secure world is aware of this change. Depending on NSCHK.WRITE INTFLAG.NSCHK will rise upon a rising or falling NONSEC.WRITE transition. The interrupt can be configured as secure or non-secure in the NVIC. If secure then a software mechanism can be implemented to call a non-secure NVMCTRL IRQ handler from the secure world.

The NVMCTRL monitors the Page Buffer write accesses and accepts only writes to non-secure regions when the transaction is non-secure. Moreover it checks that any write to the page buffer is in the same page as the previous write when the Page Buffer is not empty. When this check fails, an error is returned to the bus master that initiated the transaction. This ensures that it is not possible to mix different page writes into the Page Buffer. Therefore, any Page Buffer write access must at some point be followed by a manual or automatic Write Page (WP) that automatically clears the page buffer or a Clear Page Buffer (PBC) command.

30.8.10 Secure Region Unlock Bits

Name: SULCK
Offset: 0x20
Reset: x initially determined from NVM User Row after reset
Property: PAC Write-Protection, Write-Secure

Important: This register is only available for **SAM L11** and has no effect for **SAM L10**.

Bit	15	14	13	12	11	10	9	8
	SLKEY[7:0]							
Access	W/-/W	W/-/W	W/-/W	W/-/W	W/-/W	W/-/W	W/-/W	W/-/W
Reset	0	0	0	0	0	0	0	0

Bit	7	6	5	4	3	2	1	0
						DS	AS	BS
Access						RW/R/RW	RW/R/RW	RW/R/RW
Reset						x	x	x

Bits 15:8 – SLKEY[7:0] Secure Unlock Key
When this bit group is written to the key value 0xA5, the write will be performed. If a value different from the key value is tried, the write will be discarded and INTFLAG.KEYE set.

Bit 2 – DS DATA Secure Unlock Bit
Default state after erase will be unlocked (0x1).

Value	Description
0	The DS region is locked.
1	The DS region is not locked.

Bit 1 – AS Application Secure Unlock Bit
Default state after erase will be unlocked (0x1).

Value	Description
0	The AS region is locked.
1	The AS region is not locked.

Bit 0 – BS BOOT Secure Unlock Bit
Default state after erase will be unlocked (0x1).

Value	Description
0	The BS region is locked.
1	The BS region is not locked.

31.5 Product Dependencies

In order to use this peripheral, other parts of the system must be configured correctly, as described below.

31.5.1 I/O Lines

Not applicable.

31.5.2 Power Management

The TRAM will continue to operate in any sleep mode, as long as its source clock is running. The TRAM interrupts can be used to wake up the device from sleep modes. Events connected to the event system can trigger other operations in the system without exiting sleep modes. Refer *PM – Power Manager* for details on the different sleep modes.

31.5.3 Clocks

The TRAM bus clock (CLK_TRAM_AHB) can be enabled and disabled by the Main Clock module, and the default state of CLK_TRAM_AHB can be found in the *Peripheral Clock Masking* section.

31.5.4 DMA

Not applicable

31.5.5 Interrupts

The interrupt request lines are connected to the interrupt controller. Using the TRAM interrupts requires the interrupt controller to be configured first. Refer to NVIC - Nested Interrupt *Nested Vector Interrupt Controller* for details.

31.5.6 Events

Data Remanence Prevention and Tamper events are connected directly from the RTC to the TRAM, without going through the Event System.

31.5.7 Debug Operation

Not applicable.

31.5.8 Register Access Protection

All registers with write-access are optionally write-protected by the Peripheral Access Controller (PAC), except for the following registers:

- Interrupt Flag (INTFLAG) register
- Data Scramble Control (DSCC) register
- Permutation Write (PERMW) register
- All RAM (RAM[0:63]) addresses

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

Write-protection does not apply to accesses through an external debugger. Refer to the Peripheral Access Controller chapter for details.

31.5.9 SAM L11 TrustZone Specific 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:

The tamper full erase routine operates at the highest priority. If a remanence routine executing when a tamper full erase occurs, the remanence routine is immediately terminated. If the CPU attempts to write a new scramble key at the same time the tamper key erase routine is active, the CPU data is ignored, but no bus error will occur. If a CPU security routine access is requested during a tamper full erase, the CPU transaction will be ignored and treated as a bus error similar to accessing the module during a software reset.

Important: In STANDBY low power mode, it is mandatory to enable the dynamic power gating feature (STDBYCFG.DPGPDSW) to ensure TrustRAM erasing when the power domain PDSW is in a retention state.

31.6.3 Interrupts

The TRAM has the following interrupt sources:

- Data Remanence Prevention (DRP): Indicates that the data remanence prevention routine has ended.
- Data Read Error (ERR): Indicates when there is a RAM readout error.

Each interrupt source has an interrupt flag associated with it. The interrupt flag in the Interrupt Flag Status and Clear (INTFLAG) register is set when the interrupt condition occurs. Each interrupt can be individually enabled by writing a one to the corresponding bit in the Interrupt Enable Set (INTENSET) register, and disabled by writing a one to the corresponding bit in the Interrupt Enable Clear (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 TRAM is reset. See 22.8.6 INTFLAG for details on how to clear interrupt flags. All interrupt requests from the peripheral are ORed together on system level to generate one combined interrupt request to the NVIC. Refer to *Nested Vector Interrupt Controller* for details. The user must read the INTFLAG register to determine which interrupt condition is present.

Note that interrupts must be globally enabled for interrupt requests to be generated. Refer to *Nested Vector Interrupt Controller* for details.

31.6.4 Sleep Mode Operation

The TRAM continues to operate during sleep. When it receives events from the Event System, it will request its own clock in order to perform the requested operation.

An interrupt request will be generated after the wake-up if the Interrupt Controller is configured accordingly. Otherwise the CPU will wake up directly, without triggering an interrupt. In this case, the CPU will continue executing from the instruction following the entry into sleep.

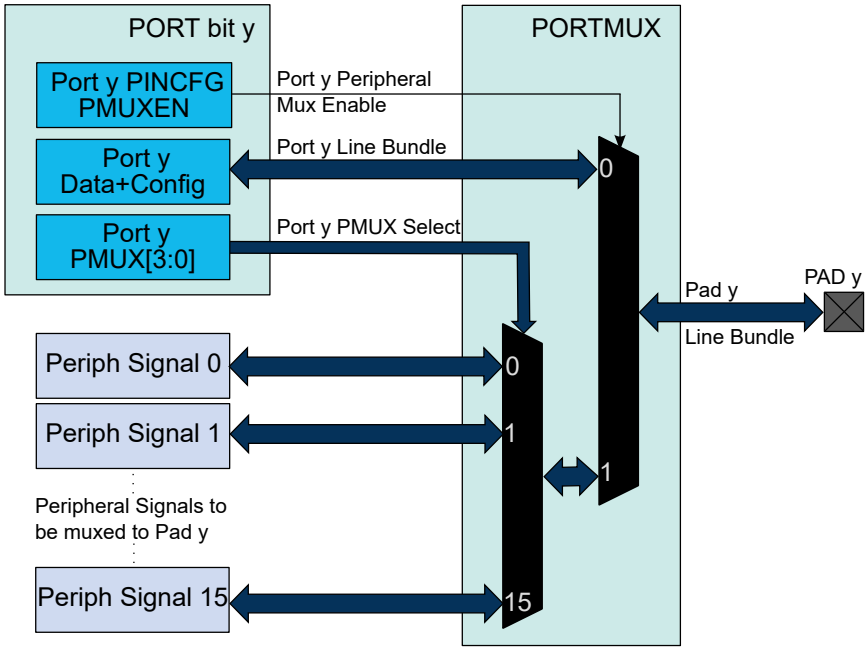
The periodic events can also wake up the CPU through the interrupt function of the Event System. In this case, the event must be enabled and connected to an event channel with its interrupt enabled. See *EVSYS – Event System* for more information.

31.6.5 Synchronization

Due to the asynchronicity between event sources and CLK_TRAM_APB some registers must be synchronized when accessed. A register can require:

- Synchronization when written

Figure 32-3. Overview of the peripheral functions multiplexing



The I/O pins of the device are controlled by PORT peripheral registers. Each port pin has a corresponding bit in the Data Direction (DIR) and Data Output Value (OUT) registers to enable that pin as an output and to define the output state.

The direction of each pin in a PORT group is configured by the DIR register. If a bit in DIR is set to '1', the corresponding pin is configured as an output pin. If a bit in DIR is set to '0', the corresponding pin is configured as an input pin.

When the direction is set as output, the corresponding bit in the OUT register will set the level of the pin. If bit y in OUT is written to '1', pin y is driven HIGH. If bit y in OUT is written to '0', pin y is driven LOW. Pin configuration can be set by Pin Configuration (PINCFGy) registers, with y=00, 01, ..31 representing the bit position.

The Data Input Value (IN) is set as the input value of a port pin with resynchronization to the PORT clock. To reduce power consumption, these input synchronizers are clocked only when system requires reading the input value. The value of the pin can always be read, whether the pin is configured as input or output. If the Input Enable bit in the Pin Configuration registers (PINCFGy.INEN) is '0', the input value will not be sampled.

In PORT, the Peripheral Multiplexer Enable bit in the PINCFGy register (PINCFGy.PMUXEN) can be written to '1' to enable the connection between peripheral functions and individual I/O pins. The Peripheral Multiplexing n (PMUXn) registers select the peripheral function for the corresponding pin. This will override the connection between the PORT and that I/O pin, and connect the selected peripheral signal to the particular I/O pin instead of the PORT line bundle.

The security attribution of each pin in a PORT group is configured by the NONSEC register. If a bit in the NONSEC register is set to '0', the corresponding pin is configured as a secured pin and can only be handled by secure accesses. If a bit in the NONSEC register is set to '1', the corresponding pin is configured as a non-secured pin. Only secure accesses are allowed to write to the NONSEC register.

Writing '1' to a bit will toggle the corresponding bit in the DIR register, which reverses the direction of the I/O pin.

Value	Description
0	The corresponding I/O pin in the PORT group will keep its configuration.
1	The direction of the corresponding I/O pin is toggled.

38.7.1.4 Event Control

Name: EVCTRL
Offset: 0x06
Reset: 0x0000
Property: PAC Write-Protection, Enable-Protected

Bit	15	14	13	12	11	10	9	8
			MCEOx	MCEOx				OVFEO
Access			R/W	R/W				R/W
Reset			0	0				0

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

Bits 13,12 – MCEOx Match or Capture Channel x Event Output Enable [x = 1..0]
These bits enable the generation of an event for every match or capture on channel x.

Value	Description
0	Match/Capture event on channel x is disabled and will not be generated.
1	Match/Capture event on channel x is enabled and will be generated for every compare/capture.

Bit 8 – OVFEO Overflow/Underflow Event Output Enable
This bit enables the Overflow/Underflow event. When enabled, an event will be generated when the counter overflows/underflows.

Value	Description
0	Overflow/Underflow event is disabled and will not be generated.
1	Overflow/Underflow event is enabled and will be generated for every counter overflow/underflow.

Bit 5 – TCEI TC Event Enable
This bit is used to enable asynchronous input events to the TC.

Value	Description
0	Incoming events are disabled.
1	Incoming events are enabled.

Bit 4 – TCINV TC Inverted Event Input Polarity
This bit inverts the asynchronous input event source.

Value	Description
0	Input event source is not inverted.
1	Input event source is inverted.

Bits 2:0 – EVACT[2:0] Event Action
These bits define the event action the TC will perform on an event.

Figure 40-2. Truth Table Output Value Selection

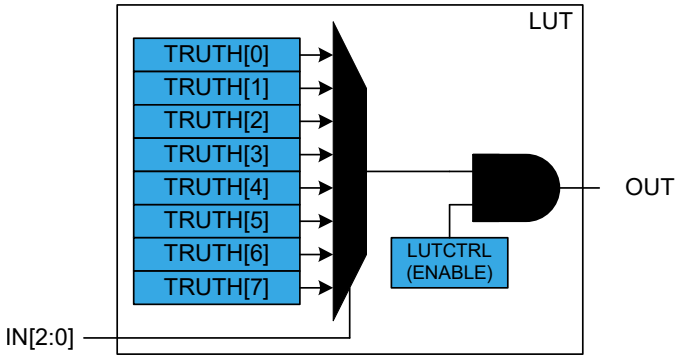


Table 40-1. Truth Table of LUT

IN[2]	IN[1]	IN[0]	OUT
0	0	0	TRUTH[0]
0	0	1	TRUTH[1]
0	1	0	TRUTH[2]
0	1	1	TRUTH[3]
1	0	0	TRUTH[4]
1	0	1	TRUTH[5]
1	1	0	TRUTH[6]
1	1	1	TRUTH[7]

40.6.2.4 Truth Table Inputs Selection

Input Overview

The inputs can be individually:

- Masked
- Driven by peripherals:
  - Analog comparator output (AC)
  - Timer/Counters waveform outputs (TC)
  - Serial Communication output transmit interface (SERCOM)
- Driven by internal events from Event System
- Driven by other CCL sub-modules

The Input Selection for each input y of LUT x is configured by writing the Input y Source Selection bit in the LUT x Control register (LUTCTRLx.INSELy).

Masked Inputs (MASK)

When a LUT input is masked (LUTCTRLx.INSELy=MASK), the corresponding TRUTH input (IN) is internally tied to zero, as shown in this figure:

41.8.11 Average Control

Name: AVGCTRL
Offset: 0x0C
Reset: 0x00
Property: PAC Write-Protection, Write-Synchronized

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

Bits 6:4 – ADJRES[2:0] Adjusting Result / Division Coefficient
These bits define the division coefficient in 2n steps.

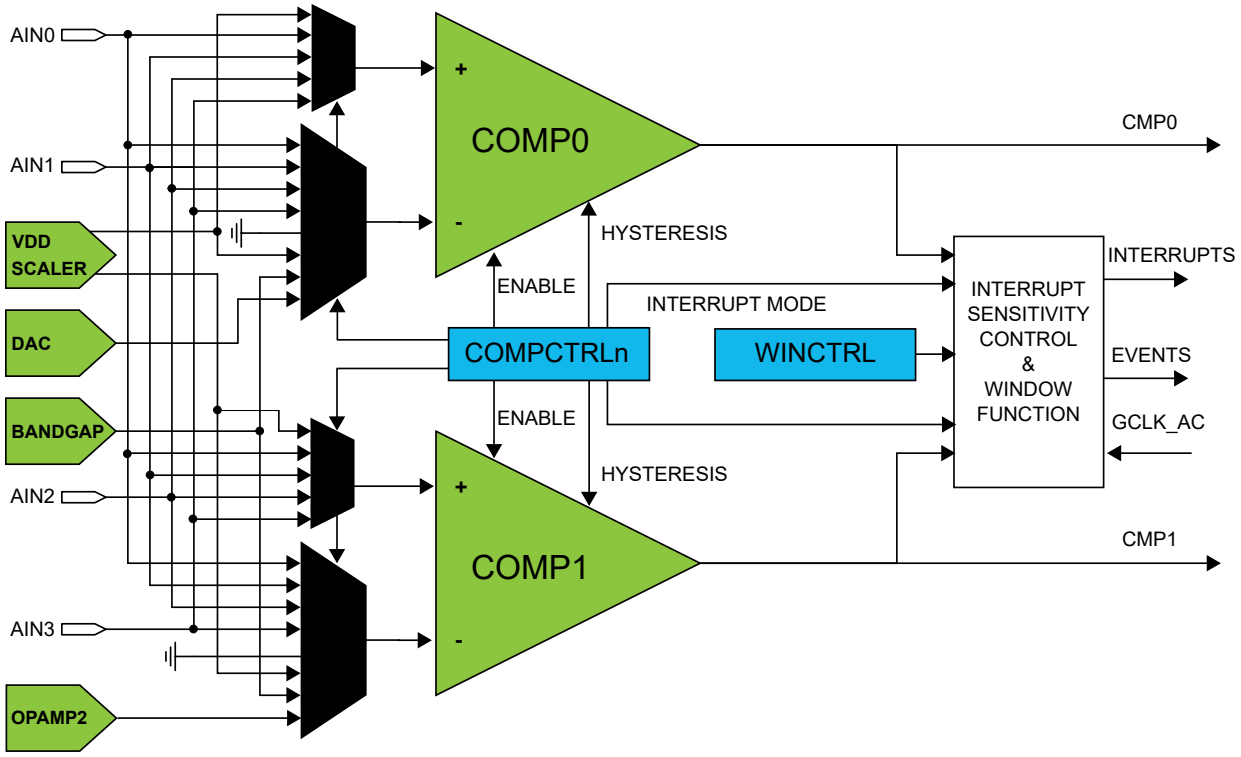
Bits 3:0 – SAMPLENUM[3:0] Number of Samples to be Collected
These bits define how many samples are added together. The result will be available in the Result register (RESULT). Note: if the result width increases, CTRLC.RESSEL must be changed.

Value	Description
0x0	1 sample
0x1	2 samples
0x2	4 samples
0x3	8 samples
0x4	16 samples
0x5	32 samples
0x6	64 samples
0x7	128 samples
0x8	256 samples
0x9	512 samples
0xA	1024 samples
0xB - 0xF	Reserved

- Optional digital filter on comparator output

42.3 Block Diagram

Figure 42-1. Analog Comparator Block Diagram



42.4 Signal Description

Signal	Description	Type
AIN[3..0]	Analog input	Comparator inputs
CMP[1..0]	Digital output	Comparator outputs

Refer to *I/O Multiplexing and Considerations* for details on the pin mapping for this peripheral. One signal can be mapped on several pins.

42.5 Product Dependencies

In order to use this peripheral, other parts of the system must be configured correctly, as described below.

42.5.1 I/O Lines

Using the AC's I/O lines requires the I/O pins to be configured. Refer to *PORT - I/O Pin Controller* for details.

Related Links

32. PORT - I/O Pin Controller

Related Links

15. PAC - Peripheral Access Controller

42.5.9 SAM L11 TrustZone Specific 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.

42.5.10 Analog Connections

Each comparator has up to four I/O pins that can be used as analog inputs. Each pair of comparators shares the same four pins. These pins must be configured for analog operation before using them as comparator inputs.

Any internal reference source, such as a bandgap voltage reference, OPAMP2,or DAC must be configured and enabled prior to its use as a comparator input.

The analog signals of AC, ADC, DAC and OPAMP can be interconnected. The AC and ADC peripheral can request the OPAMP using an analog ONDEMAND functionality.

See *Analog Connections of Peripherals* for details.

42.6 Functional Description

42.6.1 Principle of Operation

Each comparator has one positive input and one negative input. Each positive input may be chosen from a selection of analog input pins. Each negative input may be chosen from a selection of both analog input pins and internal inputs, such as a bandgap voltage reference.

The digital output from the comparator is '1' when the difference between the positive and the negative input voltage is positive, and '0' otherwise.

The individual comparators can be used independently (normal mode) or paired to form a window comparison (window mode).

42.6.2 Basic Operation

42.6.2.1 Initialization

Some registers are enable-protected, meaning they can only be written when the module is disabled.

The following register is enable-protected:

- Event Control register (EVCTRL)

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

42.6.2.2 Enabling, Disabling and Resetting

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

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.