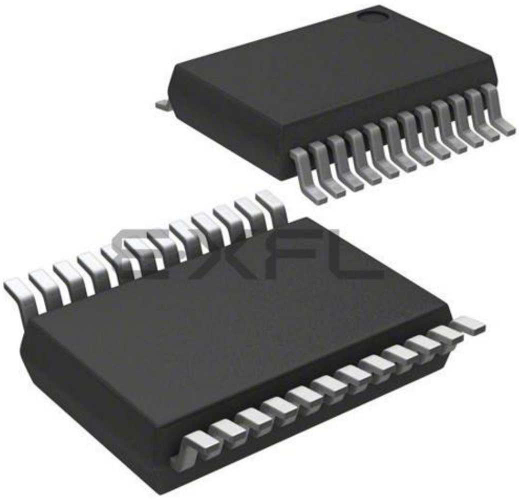
Microchip Technology - ATSAML10D14A-YU Datasheet



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	16KB (16K x 8)
Program Memory Type	FLASH
EEPROM Size	2K x 8
RAM Size	4K 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 ~ 85°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/atsaml10d14a-yu

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:

14.4.5.9 Boot Interactive Mode Commands

Table 14-9. Boot Interactive Mode Commands

Command Name	Description	Command prefix	Command
CMD_INIT	Entering Interactive Mode	0x444247	55
CMD_EXIT	Exit Interactive Mode	0x444247	AA
CMD_RESET	System Reset Request	0x444247	52
CMD_CE0	ChipErase_NS for SAM L11	0x444247	E0
CMD_CE1	ChipErase_S for SAM L11	0x444247	E1
CMD_CE2	ChipErase_ALL for SAM L11	0x444247	E2
CMD_CHIPERASE	ChipErase for SAM L10	0x444247	E3
CMD_CRC	NVM Memory Regions Integrity Checks	0x444247	C0
CMD_DCEK	Random Session Key Generation for SAM L11	0x444247	44
CMD_RAUX	NVM Rows Integrity Checks	0x444247	4C

14.4.5.10 Boot Interactive Mode Status

Table 14-10. Boot Interactive Mode Status

Status Name	Description	Status prefix	Status coding
SIG_NO	No Error	0xEC0000	00
SIG_SAN_FFF	Fresh from factory error	0xEC0000	10
SIG_SAN_UROW	UROW checksum error	0xEC0000	11
SIG_SAN_SECEN	SECEN parameter error	0xEC0000	12
SIG_SAN_BOCOR	BOCOR checksum error	0xEC0000	13
SIG_SAN_BOOTPROT	BOOTPROT parameter error	0xEC0000	14
SIG_SAN_NOSECREG	No secure register parameter error	0xEC0000	15
SIG_COMM	Debugger start communication command	0xEC0000	20
SIG_CMD_SUCCESS	Debugger command success	0xEC0000	21
SIG_CMD_FAIL	Debugger command fail	0xEC0000	22
SIG_CMD_BADKEY	Debugger bad key	0xEC0000	23
SIG_CMD_VALID	Valid command	0xEC0000	24
SIG_CMD_INVALID	Invalid command	0xEC0000	25
SIG_ARG_VALID	Valid argument	0xEC0000	26
SIG_ARG_INVALID	Invalid argument	0xEC0000	27
SIG_CE_CVM	Chip erase error: CVM	0xEC0000	30
SIG_CE_ARRAY_ERASEFAIL	Chip erase error: array erase fail	0xEC0000	31
SIG_CE_ARRAY_NVME	Chip erase error: array NVME	0xEC0000	32
SIG_CE_DATA_ERASEFAIL	Chip erase error: data erase fail	0xEC0000	33
SIG_CE_DATA_NVME	Chip erase error: data NVME	0xEC0000	34
SIG_CE_BCUR	Chip erase error: BOCOR, UROW	0xEC0000	35
SIG_CE_BC	Chip erase error: BC check	0xEC0000	36
SIG_BOOT_OPT	BOOTOPT parameter error	0xEC0000	40

15.7.12 Peripheral Non-Secure Status - Bridge A

Name: NONSECA
Offset: 0x54
Reset: x initially determined from NVM User Row after reset
Property: Write-Secure

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

Reading NONSEC register returns peripheral security attribution status:

Value	Description
0	Peripheral is secured.
1	Peripheral is non-secured.

Bit	31	30	29	28	27	26	25	24
Access								
Reset								

Bit	23	22	21	20	19	18	17	16
Access								
Reset								

Bit	15	14	13	12	11	10	9	8
			AC	PORT	FREQM	EIC	RTC	WDT
Access			R/R/R	R/R/R	R/R/R	R/R/R	R/R/R	R/R/R
Reset			x	x	x	x	x	x

Bit	7	6	5	4	3	2	1	0
	GCLK	SUPC	OSC32KCTRL	OSCCTRL	RSTC	MCLK	PM	PAC
Access	R/R/R	R/R/R	R/R/R	R/R/R	R/R/R	R/R/R	R/R/R	R/R/R
Reset	x	x	x	x	x	x	x	0

Bit 13 – AC Peripheral AC Non-Secure

Bit 12 – PORT Peripheral PORT Non-Secure

Bit 11 – FREQM Peripheral FREQM Non-Secure

Bit 10 – EIC Peripheral EIC Non-Secure

Bit 9 – RTC Peripheral RTC Non-Secure

Related Links

22. PM – Power Manager

16.5.3 Clocks

The DSU bus clocks (CLK_DSU_APB and CLK_DSU_AHB) can be enabled and disabled by the Main Clock Controller.

Related Links

22. PM – Power Manager
19. MCLK – Main Clock
19.6.2.6 Peripheral Clock Masking

16.5.4 DMA

The DMA request lines are connected to the DMA Controller (DMAC). To use DMA requests with this peripheral, the DMAC must be configured first. Refer to 28. DMAC – Direct Memory Access Controller for details. The CFG.DCCDMALEVEL bitfield must be configured depending on the DMA channels access modes (read or write for DCC0 and DCC1).

16.5.5 Interrupts

Not applicable.

16.5.6 Events

Not applicable.

16.5.7 Register Access Protection

Registers with write-access can be optionally write-protected by the Peripheral Access Controller (PAC), except for the following:

- Debug Communication Channel 0 register (DCC0)
- Debug Communication Channel 1 register (DCC1)
- Boot Communication Channel 0 register (BCC0)
- Boot Communication Channel 1 register (BCC1)

Note: Optional write-protection is indicated by the "PAC Write-Protection" property in the register description.

Write-protection does not apply for accesses through an external debugger.

Related Links

15. PAC - Peripheral Access Controller

16.5.8 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

19.5.7 Debug Operation

When the CPU is halted in debug mode, the MCLK continues normal operation. In sleep mode, the clocks generated from the MCLK are kept running to allow the debugger accessing any module. As a consequence, power measurements are incorrect in debug mode.

19.5.8 Register Access Protection

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

- Interrupt Flag register (INTFLAG)

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

PAC write-protection does not apply to accesses through an external debugger.

Related Links

15. PAC - Peripheral Access Controller

19.5.9 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.

19.5.10 Analog Connections

Not applicable.

19.6 Functional Description

19.6.1 Principle of Operation

The CLK_MAIN clock signal from the GCLK module or the DFLLULP is the source for the main clock, which in turn is the common root for the synchronous clocks for the CPU, APBx, and AHBx modules. The CLK_MAIN is divided by an 8-bit prescaler. Each of the derived clocks can run from any divided or undivided main clock, ensuring synchronous clock sources for each clock domain. The clock domain (CPU) can be changed on the fly to respond to variable load in the application. The clocks for each module in a clock domain can be masked individually to avoid power consumption in inactive modules. Depending on the sleep mode, some clock domains can be turned off.

19.6.2 Basic Operation

19.6.2.1 Initialization

After a Reset, the default clock source of the CLK_MAIN clock (GCLK_MAIN) is started and calibrated before the CPU starts running. The GCLK_MAIN clock is selected as the main clock without any prescaler division.

By default, only the necessary clocks are enabled.

19.8.2 Interrupt Enable Clear

Name: INTENCLR
Offset: 0x01
Reset: 0x00
Property: PAC Write-Protection

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

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

Bit 0 – CKRDY Clock Ready Interrupt Enable
Writing a '0' to this bit has no effect.

Writing a '1' to this bit will clear the Clock Ready Interrupt Enable bit and the corresponding interrupt request.

Value	Description
0	The Clock Ready interrupt is enabled and will generate an interrupt request when the Clock Ready Interrupt Flag is set.
1	The Clock Ready interrupt is disabled.

Bit 7 – DMAEN DMA Enable
The RTC can trigger a DMA request when the timestamp is ready in the TIMESTAMP register.

Value	Description
0	Tamper DMA request is disabled. Reading TIMESTAMP has no effect on INTFLAG.TAMPER.
1	Tamper DMA request is enabled. Reading TIMESTAMP will clear INTFLAG.TAMPER.

Bit 6 – RTCOUT RTC Output Enable

Value	Description
0	The RTC active layer output is disabled.
1	The RTC active layer output is enabled.

Bit 5 – DEBASYNC Debouncer Asynchronous Enable

Value	Description
0	The tamper input debouncers operate synchronously.
1	The tamper input debouncers operate asynchronously.

Bit 4 – DEBMAJ Debouncer Majority Enable

Value	Description
0	The tamper input debouncers match three equal values.
1	The tamper input debouncers match majority two of three values.

Bit 0 – GP0EN General Purpose 0 Enable

Value	Description
0	COMP0 compare function enabled. GP0/GP1 disabled.
1	COMP0 compare function disabled. GP0/GP1 enabled.

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

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

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

Bit	15	14	13	12	11	10	9	8
	OVF	TAMPER						ALARM0
Access	R/W	R/W						R/W
Reset	0	0						0

Bit	7	6	5	4	3	2	1	0
	PER7	PER6	PER5	PER4	PER3	PER2	PER1	PER0
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

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

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

Bit 14 – TAMPER Tamper Interrupt Enable

Bit 8 – ALARM0 Alarm 0 Interrupt Enable
Writing a '0' to this bit has no effect. Writing a '1' to this bit will clear the Alarm 0 Interrupt Enable bit, which disables the Alarm interrupt.

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

Bits 0, 1, 2, 3, 4, 5, 6, 7 – PERn Periodic Interval n Interrupt Enable [n = 7..0]
Writing a '0' to this bit has no effect. Writing a '1' to this bit will clear the Periodic Interval n Interrupt Enable bit, which disables the Periodic Interval n interrupt.

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

27.12.11 Alarm Value in Clock/Calendar mode (CTRLA.MODE=2)

Name: ALARM
Offset: 0x20
Reset: 0x00000000
Property: PAC Write-Protection, Write-Synchronized

The 32-bit value of ALARM is continuously compared with the 32-bit CLOCK value, based on the masking set by MASK.SEL. When a match occurs, the Alarm n interrupt flag in the Interrupt Flag Status and Clear register (INTFLAG.ALARM) is set on the next counter cycle, and the counter is cleared if CTRLA.MATCHCLR is '1'.

Bit	31	30	29	28	27	26	25	24
	YEAR[5:0]						MONTH[3:2]	
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
	MONTH[1:0]		DAY[4:0]					HOUR[4:4]
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
	HOUR[3:0]				MINUTE[5:2]			
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
	MINUTE[1:0]		SECOND[5:0]					
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 31:26 – YEAR[5:0] Year
The alarm year. Years are only matched if MASK.SEL is 6

Bits 25:22 – MONTH[3:0] Month
The alarm month. Months are matched only if MASK.SEL is greater than 4.

Bits 21:17 – DAY[4:0] Day
The alarm day. Days are matched only if MASK.SEL is greater than 3.

Bits 16:12 – HOUR[4:0] Hour
The alarm hour. Hours are matched only if MASK.SEL is greater than 2.

Bits 11:6 – MINUTE[5:0] Minute
The alarm minute. Minutes are matched only if MASK.SEL is greater than 1.

Bits 5:0 – SECOND[5:0] Second
The alarm second. Seconds are matched only if MASK.SEL is greater than 0.

28.6.2 Basic Operation

28.6.2.1 Initialization

The following DMAC registers are enable-protected, meaning that they can only be written when the DMAC is disabled (CTRL.DMAENABLE=0):

- Descriptor Base Memory Address register (BASEADDR)
- Write-Back Memory Base Address register (WRBADDR)

The following DMAC bit is enable-protected, meaning that it can only be written when both the DMAC and CRC are disabled (CTRL.DMAENABLE=0 and CTRL.CRCENABLE=0):

- Software Reset bit in Control register (CTRL.SWRST)

The following DMA channel register is enable-protected, meaning that it can only be written when the corresponding DMA channel is disabled (CHCTRLA.ENABLE=0):

- Channel Control B (CHCTRLB) register, except the Command bit (CHCTRLB.CMD) and the Channel Arbitration Level bit (CHCTRLB.LVL)

The following DMA channel bit is enable-protected, meaning that it can only be written when the corresponding DMA channel is disabled:

- Channel Software Reset bit in Channel Control A register (CHCTRLA.SWRST)

The following CRC registers are enable-protected, meaning that they can only be written when the CRC is disabled (CTRL.CRCENABLE=0):

- CRC Control register (CRCCTRL)
- CRC Checksum register (CRCCHKSUM)

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

Before the DMAC is enabled it must be configured, as outlined by the following steps:

- The SRAM address of where the descriptor memory section is located must be written to the Description Base Address (BASEADDR) register
- The SRAM address of where the write-back section should be located must be written to the Write-Back Memory Base Address (WRBADDR) register
- Priority level x of the arbiter can be enabled by setting the Priority Level x Enable bit in the Control register (CTRL.LVLENx=1)

Before a DMA channel is enabled, the DMA channel and the corresponding first transfer descriptor must be configured, as outlined by the following steps:

- DMA channel configurations
  - The channel number of the DMA channel to configure must be written to the Channel ID (CHID) register
  - Trigger action must be selected by writing the Trigger Action bit group in the Channel Control B register (CHCTRLB.TRIGACT)
  - Trigger source must be selected by writing the Trigger Source bit group in the Channel Control B register (CHCTRLB.TRIGSRC)
- Transfer Descriptor
  - The size of each access of the data transfer bus must be selected by writing the Beat Size bit group in the Block Transfer Control register (BTCTRL.BEATSIZE)

28.10.3 Block Transfer Source Address

Name: SRCADDR
Offset: 0x04
Property: -

The SRCADDR register offset is relative to (BASEADDR or WRBADDR) + Channel Number * 0x10

Bit	31	30	29	28	27	26	25	24
	SRCADDR[31:24]							
Access								
Reset								

Bit	23	22	21	20	19	18	17	16
	SRCADDR[23:16]							
Access								
Reset								

Bit	15	14	13	12	11	10	9	8
	SRCADDR[15:8]							
Access								
Reset								

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

Bits 31:0 – SRCADDR[31:0] Transfer Source Address
This bit group holds the source address corresponding to the last beat transfer address in the block transfer.

32.7 Register Summary

Important:
For SAM L11, the PORT register map is automatically duplicated in a Secure and Non-Secure alias:

- The Non-Secure alias is at the peripheral base address
- The Secure alias is located at the peripheral base address + 0x200

Refer to *Mix-Secure Peripherals* for more information on register access rights

Offset	Name	Bit Pos.								
0x00	DIR	7:0	DIR[7:0]							
		15:8	DIR[15:8]							
		23:16	DIR[23:16]							
		31:24	DIR[31:24]							
0x04	DIRCLR	7:0	DIRCLR[7:0]							
		15:8	DIRCLR[15:8]							
		23:16	DIRCLR[23:16]							
		31:24	DIRCLR[31:24]							
0x08	DIRSET	7:0	DIRSET[7:0]							
		15:8	DIRSET[15:8]							
		23:16	DIRSET[23:16]							
		31:24	DIRSET[31:24]							
0x0C	DIRTGL	7:0	DIRTGL[7:0]							
		15:8	DIRTGL[15:8]							
		23:16	DIRTGL[23:16]							
		31:24	DIRTGL[31:24]							
0x10	OUT	7:0	OUT[7:0]							
		15:8	OUT[15:8]							
		23:16	OUT[23:16]							
		31:24	OUT[31:24]							
0x14	OUTCLR	7:0	OUTCLR[7:0]							
		15:8	OUTCLR[15:8]							
		23:16	OUTCLR[23:16]							
		31:24	OUTCLR[31:24]							
0x18	OUTSET	7:0	OUTSET[7:0]							
		15:8	OUTSET[15:8]							
		23:16	OUTSET[23:16]							
		31:24	OUTSET[31:24]							
0x1C	OUTTGL	7:0	OUTTGL[7:0]							
		15:8	OUTTGL[15:8]							
		23:16	OUTTGL[23:16]							
		31:24	OUTTGL[31:24]							
0x20	IN	7:0	IN[7:0]							
		15:8	IN[15:8]							
		23:16	IN[23:16]							

32.8.3 Data Direction Set

Name: DIRSET
Offset: 0x08
Reset: 0x00000000
Property: PAC Write-Protection, Mix-Secure

Important: For **SAM L11 Non-Secure** accesses, read and write accesses (RW*) are allowed only if the security attribution for the corresponding I/O pin is set as Non-Secured in the NONSEC register.

This register allows the user to set one or more I/O pins as an output, without doing a read-modify-write operation. Changes in this register will also be reflected in the Data Direction (DIR), Data Direction Toggle (DIRTGL) and Data Direction Clear (DIRCLR) registers.

Tip: The I/O pins are assembled in pin groups (”PORT groups”) with up to 32 pins. Group 0 consists of the PA pins, group 1 is for the PB pins, etc. Each pin group has its own PORT registers, with a 0x80 address spacing. For example, the register address offset for the Data Direction (DIR) register for group 0 (PA00 to PA31) is 0x00, and the register address offset for the DIR register for group 1 (PB00 to PB31) is 0x80.

Bit	31	30	29	28	27	26	25	24
	DIRSET[31:24]							
Access	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW
Reset	0	0	0	0	0	0	0	0

Bit	23	22	21	20	19	18	17	16
	DIRSET[23:16]							
Access	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW
Reset	0	0	0	0	0	0	0	0

Bit	15	14	13	12	11	10	9	8
	DIRSET[15:8]							
Access	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW
Reset	0	0	0	0	0	0	0	0

Bit	7	6	5	4	3	2	1	0
	DIRSET[7:0]							
Access	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW	RW/RW*/RW
Reset	0	0	0	0	0	0	0	0

Bits 31:0 – DIRSET[31:0] Port Data Direction Set
Writing '0' to a bit has no effect.

Protocol T=0

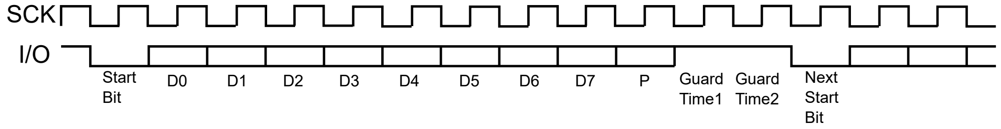
In T=0 protocol, a character is made up of:

- one start bit,
- eight data bits,
- one parity bit
- and one guard time, which lasts two bit times.

The transfer is synchronous (CTRLA.CMODE=1). The transmitter shifts out the bits and does not drive the I/O line during the guard time. Additional guard time can be added by programming the Guard Time (CTRLC.GTIME).

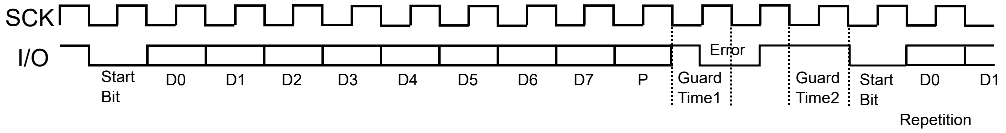
If no parity error is detected, the I/O line remains during the guard time and the transmitter can continue with the transmission of the next character, as shown in the figure below.

Figure 35-16. T=0 Protocol without Parity Error



If a parity error is detected by the receiver, it drives the I/O line to 0 during the guard time, as shown in the next figure. This error bit is also named NACK, for Non Acknowledge. In this case, the character lasts 1 bit time more, as the guard time length is the same and is added to the error bit time, which lasts 1 bit time.

Figure 35-17. T=0 Protocol with Parity Error



When the USART is the receiver and it detects a parity error, the parity error bit in the Status Register (STATUS.PERR) is set and the character is not written to the receive FIFO.

Receive Error Counter

The receiver also records the total number of errors (receiver parity errors and NACKs from the remote transmitter) up to a maximum of 255. This can be read in the Receive Error Count (RXERRCNT) register. RXERRCNT is automatically cleared on read.

Receive NACK Inhibit

The receiver can also be configured to inhibit error generation. This can be achieved by setting the Inhibit Not Acknowledge (CTRLC.INACK) bit. If CTRLC.INACK is 1, no error signal is driven on the I/O line even if a parity error is detected. Moreover, if CTRLC.INACK is set, the erroneous received character is stored in the receive FIFO, and the STATUS.PERR bit is set. Inhibit not acknowledge (CTRLC.INACK) takes priority over disable successive receive NACK (CTRLC.DSNACK).

Transmit Character Repetition

When the USART is transmitting a character and gets a NACK, it can automatically repeat the character before moving on to the next character. Repetition is enabled by writing the Maximum Iterations register (CTRLC.MAXITER) to a non-zero value. The USART repeats the character the number of times specified in CTRLC.MAXITER.

- Status register (STATUS)
- Data register (DATA)

Optional PAC Write-Protection is denoted by the "PAC Write-Protection" property in each individual register description.

Write-protection does not apply to accesses through an external debugger.

Related Links

15. PAC - Peripheral Access Controller

36.5.9 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.

36.5.10 Analog Connections

Not applicable.

36.6 Functional Description

36.6.1 Principle of Operation

The SPI is a high-speed synchronous data transfer interface It allows high-speed communication between the device and peripheral devices.

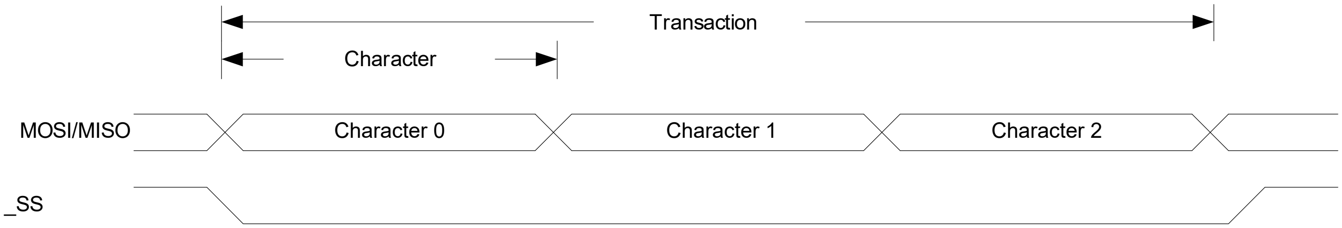
The SPI can operate as master or slave. As master, the SPI initiates and controls all data transactions. The SPI is single buffered for transmitting and double buffered for receiving.

When transmitting data, the Data register can be loaded with the next character to be transmitted during the current transmission.

When receiving, the data is transferred to the two-level or four-level receive buffer, and the receiver is ready for a new character.

The SPI transaction format is shown in SPI Transaction Format. Each transaction can contain one or more characters. The character size is configurable, and can be either 8 or 9 bits.

Figure 36-2. SPI Transaction Format



Value	Description
0	General call address recognition disabled.
1	General call address recognition enabled.

Writing '1' to this bit location will clear the MB flag. The transaction will not continue or be terminated until one of the above actions is performed.

Writing '0' to this bit has no effect.

Value	OPAMPx	Name	Description
0x0	x=0,1,2	OAxPOS	OPAMPx Positive Input
0x1	x=0,1,2	OAxTAP	OPAMPx Resistor Ladder Taps
0x2	x=0,1,2	REFERENCE	REFERENCE[DAC/REFBUF]
0x3	x=0,1,2	GND	Ground
0x4	x=0	Reserved	
	x=1	OA0OUT	OPAMP0 output
	x=2	OA1OUT	OPAMP1 output
0x5	x=0,1	Reserved	
	x=2	OA0POS	OPAMP0 Positive Input
0x6	x=0,1	Reserved	
	x=2	OA1POS	OPAMP1 Positive Input
0x7	x=0,1	Reserved	
	x=2	OA0TAP	OPAMP0 Resistor Ladder Taps
0x8	x=0,1	Reserved	
	x=2	RES3TAP	

Bits 15:13 – POTMUX[2:0] Potentiometer selection
Resistor selection bits control a numeric potentiometer with eight fixed values.

Value	R1	R2
0x0	14R	2R
0x1	12R	4R
0x2	8R	8R
0x3	6R	10R
0x4	4R	12R
0x5	3R	13R
0x6	2R	14R
0x7	R	15R

Bits 12:10 – RES1MUX[2:0] Resistor 1 Mux
These bits select the connection of R1 resistor of the potentiometer.

Value	OPAMPx	Name	Description
0x0	x=0,1,2	OAxPOS	OPAMPx Positive Input
0x1	x=0,1,2	OAxNEG	OPAMPx Negative Input

Symbol	Parameters	Conditions		Measurements			Unit
				Min	Typ	Max	
			Vref=Vddana=1.6V to 3.6V	-	+/-0.15	+/-0.9	
Offset	Offset Error	without offset compensation	Vref=1V Vddana=1.6V to 3.6V	-	+/-0.13	+/-15.8	mV
			Vref=3V Vddana=1.6V to 3.6V	-	+/-1.82	+/-14.9	
			Bandgap Reference	-	+/-2.07	+/-15.8	
			Vref=Vddana=1.6V to 3.6V	-	+/-1.82	+/-15.3	
SFDR	Spurious Free Dynamic Range	Fs = 1MHz / Fin = 13 kHz / Full range Input signal	Vref=2.0V Vddana=3.0V	58.1	70.5	77.5	dB
SINAD	Signal to Noise and Distortion ratio			56.7	63.4	66.5	
SNR	Signal to Noise ratio			56.5	64.4	67.1	
THD	Total Harmonic Distortion			-74.7	-68.7	-57.7	
	Noise RMS	External Reference voltage	External Reference voltage	-	0.42	-	mV

Note:

1. These are given without any ADC oversampling and decimation features enabled.

Symbol	Parameter	Conditions		Min.	Typ.	Max.	Units
tSCKF	SCK fall time(2)	Master		-	0,25*tSCK	-	
tMIS	MISO setup to SCK	Master, VDD>2,70V		43.8	-	-	
		Master, VDD>1,62V		54.1	-	-	
tMIH	MISO hold after SCK	Master, VDD>2,70V		0	-	-	ns
		Master, VDD>1,62V		0	-	-	
tMOV	MOSI output valid after SCK	Master, VDD>2,70V		-	-	17.5	
		Master, VDD>1,62V		-	-	21.2	
tMOH	MOSI hold after SCK	Master, VDD>2,70V		6.32	-	-	
		Master, VDD>1,62V		6.32	-	-	
tSSCK	Slave SCK Period when tMIS=0 on the master side	Slave	Reception	2*(tSIS +tMASTER_OUT) (5)	-	-	
		Slave	Transmission	2*(tSOV +tMASTER_IN) (6)	-	-	
tSSCKW	SCK high/low width	Slave		-	0,5*tSCK	-	
tSSCKR	SCK rise time(2)	Slave		-	0,25*tSCK	-	
tSSCKF	SCK fall time(2)	Slave		-	0,25*tSCK	-	
tSIS	MOSI setup to SCK	Slave, VDD>2,70V		10.7	-	-	ns
		Slave, VDD>1,62V		11.4	-	-	
tSIH	MOSI hold after SCK	Slave, VDD>2,70V		6.4	-	-	
		Slave, VDD>1,62V		7.1	-	-	
tSSS	SS setup to SCK	Slave	PRELOADEN=1	tSOSS+tEXT_MIS +2*tAPBC (8) (9)	-	-	
			PRELOADEN=0	tSOSS+tEXT_MIS (8)	-	-	
tSSH	SS hold after SCK	Slave		0.5*tSSCK	-	-	
tSOV	MISO output valid after SCK	Slave, VDD>2,70V		-	-	36.1	
		Slave, VDD>1,62V		-	-	46.4	
tSOH	MISO hold after SCK	Slave, VDD>2,70V		13.4	-	-	