

#### 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 "<u>Embedded -</u> <u>Microcontrollers</u>"

#### Details

E·XFI

Product Status	Active
Core Processor	ARM® Cortex®-M4F
Core Size	32-Bit Single-Core
Speed	120MHz
Connectivity	EBI/EMI, Ethernet, I <sup>2</sup> C, IrDA, LINbus, MMC/SD, QSPI, SPI, UART/USART, USB
Peripherals	Brown-out Detect/Reset, DMA, I <sup>2</sup> S, POR, PWM, WDT
Number of I/O	81
Program Memory Size	1MB (1M x 8)
Program Memory Type	FLASH
EEPROM Size	-
RAM Size	256K x 8
Voltage - Supply (Vcc/Vdd)	1.71V ~ 3.63V
Data Converters	A/D 28x12b; D/A 2x12b
Oscillator Type	Internal
Operating Temperature	-40°C ~ 85°C (TA)
Mounting Type	Surface Mount
Package / Case	100-TQFP
Supplier Device Package	100-TQFP (14x14)
Purchase URL	https://www.e-xfl.com/product-detail/microchip-technology/atsame53n20a-au

Email: info@E-XFL.COM

Address: Room A, 16/F, Full Win Commercial Centre, 573 Nathan Road, Mongkok, Hong Kong

## **GCLK - Generic Clock Controller**

#### Table 14-7. Generator Selection

Value	Description
0x0	Generic Clock Generator 0
0x1	Generic Clock Generator 1
0x2	Generic Clock Generator 2
0x3	Generic Clock Generator 3
0x4	Generic Clock Generator 4
0x5	Generic Clock Generator 5
0x6	Generic Clock Generator 6
0x7	Generic Clock Generator 7
0xA	Generic Clock Generator 10
0xB	Generic Clock Generator 11

#### Table 14-8. Reset Value after a User Reset or a Power Reset

Reset	PCHCTRLm.GEN	PCHCTRLm.CHEN	PCHCTRLm.WRTLOCK
Power Reset	0x0	0x0	0x0
User Reset	If WRTLOCK = 0 : 0x0	If WRTLOCK = 0 : 0x0	No change
	If WRTLOCK = 1: no change	If WRTLOCK = 1: no change	

A Power Reset will reset all the PCHCTRLm registers.

A User Reset will reset a PCHCTRL if WRTLOCK=0, or else, the content of that PCHCTRL remains unchanged.

PCHCTRL register Reset values are shown in the table PCHCTRLm Mapping.

Table 14-9. PCHCTRLm Mapping

index(m)	Name	Description
0	GCLK_OSCCTRL_DFLL48	DFLL48 input clock source
1	GCLK_OSCCTRL_FDPLL0	Reference clock for FDPLL0
2	GCLK_OSCCTRL_FDPLL1	Reference clock for FDPLL1
3	GCLK_OSCCTRL_FDPLL0_32K GCLK_OSCCTRL_FDPLL1_32K GCLK_SDHC0_SLOW GCLK_SDHC1_SLOW GCLK_SERCOM[07]_SLOW	FDPLL0 32KHz clock for internal lock timer FDPLL1 32KHz clock for internal lock timer SDHC0 Slow SDHC1 Slow SERCOM[07] Slow
4	GCLK_EIC	EIC
5	GCLK_FREQM_MSR	FREQM Measure

#### 15.8.1 Control A

Name:CTRLAOffset:0x00Reset:0x00Property:PAC Write-Protection

All bits in this register are reserved.

Bit	7	6	5	4	3	2	1	0
Access		•	*	•			•	

Reset

#### 21.12.11 Alarm n Value in Clock/Calendar mode (CTRLA.MODE=2)

 Name:
 ALARM

 Offset:
 0x20 + n\*0x08 [n=0..1]

 Reset:
 0x00000000

 Property:
 PAC Write-Protection, Write-Synchronized

The 32-bit value of ALARMn is continuously compared with the 32-bit CLOCK value, based on the masking set by MASKn.SEL. When a match occurs, the Alarm n interrupt flag in the Interrupt Flag Status and Clear register (INTFLAG.ALARMn) 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	
Γ			YEAF	R[5:0]			MON	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	
Dit	22	22	01	20	10	10	17	16	
	23	22	21	20	19	10	17	10	
	MON	TH[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	
		HOU	R[3:0]						
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W	
Reset	0	0	0	0	0	0	0	0	
Bit	7	6	5	4	3	2	1	0	
Γ	MINU	TE[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 MASKn.SEL is 6

#### Bits 25:22 - MONTH[3:0] Month

The alarm month. Months are matched only if MASKn.SEL is greater than 4.

#### Bits 21:17 - DAY[4:0] Day

The alarm day. Days are matched only if MASKn.SEL is greater than 3.

#### Bits 16:12 - HOUR[4:0] Hour

The alarm hour. Hours are matched only if MASKn.SEL is greater than 2.

#### Bits 11:6 - MINUTE[5:0] Minute

The alarm minute. Minutes are matched only if MASKn.SEL is greater than 1.

#### Bits 5:0 - SECOND[5:0] Second

The alarm second. Seconds are matched only if MASKn.SEL is greater than 0.

© 2018 Microchip Technology Inc.

## NVMCTRL – Nonvolatile Memory Controller

Value	Name	Description
0x2	Dual	At Least One Dual Error Detected Since Last Read
0x3		Reserved

#### Bits 23:0 - ADDR[23:0] Error Address

Indicates the Byte address of the last detected error.

stored in the DFLL Multiplication Ratio Difference bit group (DFLLVAL.DIFF) in the DFLL Value register. The relative error on CLK\_DFLL48M compared to the target frequency is calculated as follows:

 $\text{ERROR} = \frac{\text{DIFF}}{\text{MUL}}$ 

#### **Drift Compensation**

If the Stable DFLL Frequency bit (DFLLCTRLB.STABLE) in the DFLL Control register is zero, the frequency tuner will automatically compensate for drift in the CLK\_DFLL48M without losing either of the locks. This means that DFLLVAL.FINE can change after every measurement of CLK\_DFLL48M. If the DFLLVAL.FINE value overflows or underflows due to large drift in temperature and/or voltage, the DFLL Out Of Bounds bit (STATUS.DFLLOOB) in the Status register will be set. After an Out of Bounds error condition, the user must rewrite DFLLMUL.MUL to ensure correct CLK\_DFLL48M frequency. An interrupt is generated on a zero-to-one transition on STATUS.DFLLOOB if the DFLL Out Of Bounds bit (INTENSET.DFLLOOB) in the Interrupt Enable Set register is set. This interrupt will also be set if the tuner is not able to lock on the correct Coarse value. If the Stable DFLL Frequency bit (DFLLCTRLB.STABLE) in the DFLL Control register is one, the DFLLVAL.COARSE and DFLLVAL.FINE values will stay constant after the lock. The user can check for a possible drift by reading the frequency error in the DFLL Multiplication Ratio Difference bit group (DFLLVAL.DIFF).

#### **Reference Clock Stop Detection**

If CLK\_DFLL48M\_REF stops or is running at a very low frequency (slower than CLK\_DFLL48M/(2 \* MULMAX)), the DFLL Reference Clock Stopped bit (STATUS.DFLLRCS) in the Status register will be set. Detecting a stopped reference clock can take a long time, on the order of 2<sup>17</sup> CLK\_DFLL48M cycles. When the reference clock is stopped, the DFLL48M will operate as if in open-loop mode. Closed-loop mode operation will automatically resume if the CLK\_DFLL48M\_REF is restarted. An interrupt is generated on a zero-to-one transition on STATUS.DFLLRCS if the DFLL Reference Clock Stopped bit (INTENSET.DFLLRCS) in the Interrupt Enable Set register is set.

#### **Related Links**

9.4 NVM User Page Mapping14. GCLK - Generic Clock Controller

#### 28.6.4.2 Additional Features

#### Dealing with Delay in the DFLL in Closed-Loop Mode

The time from selecting a new CLK\_DFLL48M frequency until this frequency is output by the DFLL48M can be up to several microseconds. If the value in DFLLMUL.MUL is small, this can lead to instability in the DFLL48M locking mechanism, which can prevent the DFLL48M from achieving locks. To avoid this, a chill cycle, during which the CLK\_DFLL48M frequency is not measured, can be enabled. The chill cycle is enabled by default, but can be disabled by writing a one to the DFLL Chill Cycle Disable bit (DFLLCTRLB.CCDIS) in the DFLL Control register. Enabling chill cycles might double the lock time.

Another solution to this problem consists of using less strict lock requirements. This is called Quick Lock (QL), which is also enabled by default, but it can be disabled by writing a one to the Quick Lock Disable bit (DFLLCTRLB.QLDIS) in the DFLL Control register. The Quick Lock might lead to a larger spread in the output frequency than chill cycles, but the average output frequency is the same.

#### 32.9.4 Data Direction Toggle

Name:DIRTGLOffset:0x0CReset:0x0000000Property:PAC Write-Protection

This register allows the user to toggle the direction of one or more I/O pins, without doing a read-modifywrite operation. Changes in this register will also be reflected in the Data Direction (DIR), Data Direction Set (DIRSET) 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	
Γ	DIRTGL[31:24]								
Access	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	
				DIRTG	L[23:16]				
Access	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	
Γ				DIRTG	iL[15:8]				
Access	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	
Γ				DIRTO	GL[7:0]				
Access	RW	RW	RW	RW	RW	RW	RW	RW	
Reset	0	0	0	0	0	0	0	0	

#### Bits 31:0 - DIRTGL[31:0] Port Data Direction Toggle

Writing '0' to a bit has no effect.

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.

#### 32.9.7 Data Output Value Set

Name:OUTSETOffset:0x18Reset:0x00000000Property:PAC Write-Protection

This register allows the user to set one or more output I/O pin drive levels high, without doing a readmodify-write operation. Changes in this register will also be reflected in the Data Output Value (OUT), Data Output Value Toggle (OUTTGL) and Data Output Value Clear (OUTCLR) 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	
Γ	OUTSET[31:24]								
Access	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	
Γ				OUTSE	T[23:16]				
Access	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	
				OUTSE	T[15:8]				
Access	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	
				OUTS	ET[7:0]				
Access	RW	RW	RW	RW	RW	RW	RW	RW	
Reset	0	0	0	0	0	0	0	0	

#### Bits 31:0 - OUTSET[31:0] PORT Data Output Value Set

Writing '0' to a bit has no effect.

Writing '1' to a bit will set the corresponding bit in the OUT register, which sets the output drive level high for I/O pins configured as outputs via the Data Direction register (DIR). For pins configured as inputs via Data Direction register (DIR) with pull enabled via the Pull Enable register (PULLEN), these bits will set the input pull direction to an internal pull-up.

#### 39.8.11 Timeout Counter Configuration

Name:	TOCC
Offset:	0x28
Reset:	0xFFFF0000
Property:	Write-restricted

This register is write-restricted and only writable if bit fields CCCR.CCE = 1 and CCCR.INIT = 1.

Bit	31	30	29	28	27	26	25	24		
	TOP[15:8]									
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W		
Reset	1	1	1	1	1	1	1	1		
Bit	23	22	21	20	19	18	17	16		
				TOF	P[7:0]					
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W		
Reset	1	1	1	1	1	1	1	1		
Bit	15	14	13	12	11	10	9	8		
Access										
Reset										
Bit	7	6	5	4	3	2	1	0		
						TOS	6[1:0]	ETOC		
Access						R/W	R/W	R/W		
Reset						0	0	0		

#### Bits 31:16 - TOP[15:0] Timeout Period

Start value of the Timeout Counter (down-counter). Configures the Timeout Period.

#### Bits 2:1 - TOS[1:0] Timeout Select

When operating in Continuous mode, a write to TOCV presets the counter to the value configured by TOCC.TOP and continues down-counting. When the Timeout Counter is controlled by one of the FIFOs, an empty FIFO presets the counter to the value configured by TOCC.TOP. Down-counting is started when the first FIFO element is stored.

Value	Name	Description
0x0	CONT	Continuous operation.
0x1	TXEF	Timeout controlled by TX Event FIFO.
0x2	RXF0	Timeout controlled by Rx FIFO 0.
0x3	RXF1	Timeout controlled by Rx FIFO 1.

#### Bit 0 – ETOC Enable Timeout Counter

Value	Description
0	Timeout Counter disabled.
1	Timeout Counter enabled.

## **CAN - Control Area Network**

#### Bit 18 – TOO Timeout Occurred

Value	Description
0	No timeout.
1	Timeout reached.

Bit 17 – MRAF Message RAM Access Failure

The flag is set, when the Rx Handler

- has not completed acceptance filtering or storage of an accepted message until the arbitration field of the following message has been received. In this case acceptance filtering or message storage is aborted and the Rx Handler starts processing of the following message.
- was not able to write a message to the Message RAM. In this case message storage is aborted.

In both cases the FIFO put index is not updated resp. the New Data flag for a dedicated Rx Buffer is not set, a partly stored message is overwritten when the next message is stored to this location.

The flag is also set when the Tx Handler was not able to read a message from the Message RAM in time. In this case message transmission is aborted. In case of a Tx Handler access failure the CAN is switched into Restricted Operation Mode. To leave Restricted Operation Mode, the Host CPU has to reset CCCR.ASM.

Value	Description
0	No Message RAM access failure occurred.
1	Message RAM access failure occurred.

#### Bit 16 - TSW Timestamp Wraparound

Value	Description
0	No timestamp counter wrap-around.
1	Timestamp counter wrapped around.

#### Bit 15 - TEFL Tx Event FIFO Element Lost

Value	Description
0	No Tx Event FIFO element lost.
1	Tx Event FIFO element lost, also set after write attempt to Tx Event FIFO of size zero.

#### Bit 14 – TEFF Tx Event FIFO Full

Value	Description
0	Tx Event FIFO not full.
1	Tx Event FIFO full.

#### Bit 13 – TEFW Tx Event FIFO Watermark Reached

Value	Description
0	Tx Event FIFO fill level below watermark.
1	Tx Event FIFO fill level reached watermark.

Bit 12 - TEFN Tx Event FIFO New Entry

## **CAN - Control Area Network**

#### Bits 15:0 - F1SA[15:0] Rx FIFO 1 Start Address

Start address of Rx FIFO 1 in Message RAM. When the CAN module addresses the Message RAM it addresses 32-bit words, not single bytes. The configurable start addresses are 32-bit word addresses, i.e. only bits 15 to 2 are evaluated, the two least significant bits are ignored. Bits 1 to 0 will always be read back as "00".

### Public Key Cryptography Controller (PUKCC)

```
// Clear contents of PUKCLParam
    memset(&PUKCLParam, 0, sizeof(PUKCL PARAM));
   pvPUKCLParam = &PUKCLParam;
   vPUKCL_Process(SelfTest, pvPUKCLParam);
    // In case of error, loop here
   while (PUKCL(u2Status) != PUKCL OK) {
    while (pvPUKCLParam->P.PUKCL SelfTest.u4Version != PUKCL VERSION) {
    :
    while (pvPUKCLParam->P.PUKCL SelfTest.u4CheckNum1 != 0x6E70DDD2) {
    while (pvPUKCLParam->P.PUKCL SelfTest.u4CheckNum2 != 0x25C8D64F) {
}
int main (void)
    /* Initializes MCU, drivers and middleware */
   atmel start init();
    // Wait for Crypto RAM clear process
    while ((PUKCCSR & BIT PUKCCSR CLRRAM BUSY) != 0);
    // Initialize PUKCC and perform self test
   PUKCC self test();
    while (1)
}
```

**Note:** It may also be necessary to initialize the Random Number Generator (RNG) on the microcontroller, as some services in the library use the peripheral. Before calling such services, be sure to follow the directives given for random number generation on the selected microcontroller (particularly initialization and seeding) and compulsorily start the RNG. For details refer to each service.

#### 43.3.3.2 Accessing Different Library Services

All cryptographic services in the library are accessed by the macro vPUKCL\_Process. All of these services use the same process for receiving and returning parameters. PUKCL receives two arguments: the requested service and a pointer to a structure called the parameter block. The parameter block contains two structures, a common parameter structure for all commands and specific parameter structure for each service. A specific service is accessed with vPUKCL\_Process by passing the service name as the first argument. For example, to perform SelfTest, use vPUKCL\_Process(SelfTest, pvPUKCLParam).

# Example 43-2. PUKCL Parameter Block

```
typedef struct PUKCL param {
     PUKCL HEADER PUKCL Header;
     union {
     _PUKCL_CLEARFLAGS PUKCL_ClearFlags;
      PUKCL COMP
                             PUKCL Comp;
     _PUKCL_COMP PUKCL_Comp;
_PUKCL_CONDCOPY PUKCL_CondCopy;
     PUKCL_CRT PUKCL_CRT;
PUKCL_DIV PUKCL_Div;
     PUKCL_EXPMOD PUKCL_ExpMod;

PUKCL_FASTCOPY PUKCL_FastCopy;

PUKCL_FILL PUKCL_Fill;

PUKCL_FMULT PUKCL_Fmult:
                            PUKCL Fmult;
     PUKCL FMULT
      PUKCL GCD
                              PUKCL GCD;
     PUKCL PRIMEGEN PUKCL PrimeGen;
     PUKCL REDMOD PUKCL RedMo
PUKCL REDMOD PUKCL RedMo
PUKCL Rng;
                              PUKCL RedMod;
```

- Both PUKCL\_EXPMOD\_REGULARRSA and PUKCL\_EXPMOD\_FASTRSA are specified.
- {nu1PrecompBase,<PrecompLength>} overlaps with either: {nu1NBase, u2NLength + 4}, {nu1CnsBase, u2NLength + 12} {nu1RndBase, u2NLength + 12} or {nu1ExpBase, u2ExpLength + 4}
- {nu1RndBase,3\*u2NLength + 24} overlaps with either: {nu1NBase, u2NLength + 4},{nu1CnsBase, u2NLength + 12} {nu1XBase, u2NLength + 12} or {nu1ExpBase, u2ExpLength + 4}
- {nu1NBase, u2NLength + 4} overlaps {nu1CnsBase, u2NLength +12}

#### 43.3.5.3.9 Status Returned Values

#### Table 43-61. PrimeGen Service Return Codes

Returned Status	Importance	Meaning		
PUKCL_NUMBER_IS_PRIME	Information	The generated or tested number has been detected as probably prime.		
PUKCL_NUMBER_IS_NOT_PRIME	Information	The generated or tested number has been detected as composite.		

#### 43.3.5.4 Modular Exponentiation (With CRT)

#### 43.3.5.4.1 Purpose

The purpose of this service is to perform the Modular Exponentiation with the Chinese Remainders Theorem (CRT). This service processes integers in GF(p) only.

The options available for this service are:

- Fast implementation
- Regular implementation
- Exponent is located in Crypto RAM or not
- Exponent window size

#### 43.3.5.4.2 How to Use the Service

#### 43.3.5.4.3 Description

This service processes a Modular Exponentiation with the Chinese Remainder Theorem:

 $R = X^{D}mod(N)$  with N = P \* Q



**Important:** For this service, be sure to follow the directives given for the RSA implementation on the chip you use.

This service requires that the modulus N is the product of two co-primes P and Q and that the decryption exponents D is co-prime with the product ( $(P-1)^*(Q-1)$ ).

The Input data are P, Q, EP, EQ, Rvalue, and X. P and Q are the co-primes so that N = P\*Q.

X is the number to exponentiate.

EP, EQ and Rval are calculated as follows:

 $EP = Dmod(P - 1) EQ = Dmod(Q - 1) Rval = P^{-1}mod(Q)$ 

In some cases, the decryption exponent D may not be available and the encryption exponent E may be available instead. The possibilities to calculate the parameters are:

 All overlapping between {nu1ModBase, u2ModLength + 4}, {nu1CnsBase, u2ModLength +8}, {nu1PointABase, 3\*u2ModLength + 12}, {nu1ABase, u2ModLength + 4} and {nu1Workspace, 4\*u2ModLength + 28}

#### 43.3.6.4.7 Status Returned Values

Returned Status	Importance	Meaning
PUKCL_OK	_	The computation passed without problem.

#### 43.3.6.5 Fast Multiplying by a Scalar Number of a Point

#### 43.3.6.5.1 Purpose

This service is used to multiply a point by an integral constant K on a given elliptic curve over GF(p).

#### 43.3.6.5.2 How to Use the Service

#### 43.3.6.5.3 Description

These two services process the Multiplying by a scalar number:

$$Pt_C = K \times Pt_A$$

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

- A the input point is filled in projective coordinates (X,Y,Z) (pointed by {nu1PointABase, 3\*u2ModLength + 12}). This point can be the Infinite Point.
- Cns the Fast Modular Constant filled (pointed by {nu1CnsBase,u2ModLength +8})
- P the modulus filled (pointed by {nu1ModBase,u2ModLength +4})
- The workspace not initialized (pointed by {nu1WorkSpace, 8\*u2ModLength +44}
- The a parameter relative to the elliptic curve (pointed by {nu1ABase,u2ModLength +4})
- K the scalar number (pointed by {nu1ScalarNumber,u2ScalarLength +4})

The resulting C point is represented in projective coordinates (X,Y,Z) and is stored at the very same place than the input point A. This point can be the Infinite Point.

The service name for this operation is  ${\tt ZpEccMulFast}$ . This service uses Fast mode and Fast Modular Reduction for computations.

**Note:** Before using this service, ensure that the constant Cns has been calculated with the setup of the Fast Modular Reduction service.

#### 43.3.6.5.4 Parameters Definition

Table 43-73. ZpEccMulFast Service Parameters

Parameter	Туре	Direction	Location	Data Length	Before Executing the Service	After Executing the Service
nu1ModBase	nu1	I	Crypto RAM	u2ModLength + 4	Base of modulus P	Base of modulus P
nu1CnsBase	nu1	I	Crypto RAM	u2ModLength + 8	Base of Cns	Base of Cns
u2ModLength	u2	1	—	-	Length of modulus P	Length of modulus P

## DAC – Digital-to-Analog Converter

### 47.8.15 Debug Control

Name: Offset: Reset: Property:		DBGCTRL 0x18 0x00 PAC Write-Pr	otection					
Bit	7	6	5	4	3	2	1	0
								DBGRUN
Access								
Reset								0
	Bit 0 – DBC	GRUN Debug I	Run					

This bit is not reset by a software reset.

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

Value	Description
0	The DAC is halted when the CPU is halted by an external debugger. Any ongoing conversion
	will complete.
1	The DAC continues normal operation when the CPU is halted by an external debugger.

#### 48.7.3.1 Control A

Name:	CTRLA
Offset:	0x00
Reset:	0x0000000
Property:	PAC Write-Protection, Write-Synchronized, Enable-Protected

Bit	31	30	29	28	27	26	25	24
				CAPTMODE1[1:0]			CAPTMC	DE0[1:0]
Access				R/W	R/W		R/W	R/W
Reset				0	0		0	0
<b>D</b> :4	00	22	04	20	10	40	47	40
BIL	23	22	21	20	19	18	17	10
			COPEN1	COPEN0			CAPTEN1	CAPTEN0
Access			R/W	R/W			R/W	R/W
Reset			0	0			0	0
Bit	15	14	13	12	11	10	9	8
	DMAOS				ALOCK	F	PRESCALER[2:0	)]
Access	R/W			•	R/W	R/W	R/W	R/W
Reset	0				0	0	0	0
Bit	7	6	5	4	3	2	1	0
	ONDEMAND	RUNSTDBY	PRESCS	SYNC[1:0]	MOD	E[1:0]	ENABLE	SWRST
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	W
Reset	0	0	0	0	0	0	0	0

## Bits 28:27 - CAPTMODE1[1:0] Capture mode Channel 1

These bits select the channel 1 capture mode.

Value	Name	Description
0x0	DEFAULT	Default capture
0x1	CAPTMIN	Minimum capture
0x2	CAPTMAX	Maximum capture
0x3		Reserved

#### Bits 25:24 - CAPTMODE0[1:0] Capture mode Channel 0 These bits select the channel 0 capture mode.

Value	Name	Description
0x0	DEFAULT	Default capture
0x1	CAPTMIN	Minimum capture
0x2	CAPTMAX	Maximum capture
0x3		Reserved

#### Bits 20, 21 – COPENx Capture On Pin x Enable

Bit x of COPEN[1:0] selects the trigger source for capture operation, either events or I/O pin input.

### Bit 0 – STOP Stop

This bit is set when the TCC is disabled either on a STOP command or on an UPDATE condition when One-Shot operation mode is enabled (CTRLBSET.ONESHOT=1).

This bit is clear on the next incoming counter increment or decrement.

Value	Description
0	Counter is running.
1	Counter is stopped.

#### 53.6.4 Interrupts

The PDEC has the following interrupt sources:

- Overflow/Underflow: OVF
- Compare Channels: COMPx
- Error: ERR
- Velocity: VLC. This interrupt is available only in QDEC and HALL operation modes.
- Direction: DIR. This interrupt is available only in QDEC and HALL operation modes.

Each interrupt source has an interrupt flag associated with it. The interrupt flag in the Interrupt Flag Status and Clear register (INTFLAG) is set when the interrupt condition occurs. Each interrupt can be individually enabled by writing a '1' to the corresponding bit in the Interrupt Enable Set register (INTENSET), and disabled by writing a '1' to the corresponding bit in the Interrupt Enable Clear register (INTENCLR).

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 PDEC is reset. See the INTFLAG register description for details on how to clear interrupt flags.

The user must read the INTFLAG register to determine which interrupt condition is present. **Note:** Interrupts must be globally enabled for interrupt requests to be generated.

#### 53.6.5 Events

The PDEC can generate the following output events:

- Overflow/Underflow: OVF
- Channel x Compare Match: MCx
- Error: ERR
- Velocity: VLC. This interrupt is available only in QDEC and HALL operation modes.
- Direction: DIR. This interrupt is available only in QDEC and HALL operation modes.

Writing a '1' to an Event Output bit in the Event Control register (EVCTRL.MCEO) enables the corresponding output event. Writing a '0' to this bit disables the corresponding output event.

#### **Related Links**

31. EVSYS – Event System

#### 53.6.6 Sleep Mode Operation

The PDEC can be configured to operate in any sleep mode. To be able to run in standby, the RUNSTDBY bit in the Control A register (CTRLA.RUNSTDBY) must be written to '1'. The PDEC can wake up the device using interrupts from any sleep mode or perform actions through the Event System.

#### 53.6.7 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 the Control A register (CTRLA.SWRST)
- Enable bit in the Control A register (CTRLA.ENABLE)

The following registers need synchronization when written:

**Electrical Characteristics at 85°C** 

Symbol	Parameters	Conditions (see Notes 3, 4)	Min	Тур	Мах	Unit
VBOD+ (see Note 2)	BOD33 threshold level Hysteresis	LEVEL[7:0] = 0x00 (min)	1.426	1.522	1.611	
	ON at power voltage rising	LEVEL[7:0]= 0x19 (recommended value)	1.564	1.672	1.773	
		LEVEL[7:0] = 0x1C (fuse value)	1.582	1.690	1.791	
		LEVEL[7:0] = 0xFF (max)	2.848	3.045	3.230	
Level_Step	DC threshold step	-	-	6.00	-	mV
Tstart	Startup time (see <b>Note 6</b> )	Time from enable to RDY	-	27	-	μs

#### Note:

- 1. VBOD = VBOD- = 1.5 + LEVEL[7:0) \* Level\_Step LEVEL[7:0] is calibration setting bus of threshold level.
- 2. VBOD+ = VBOD- + N \* HYST\_STEP N = 0 to 15 according to HYST[3:0] value HYST\_STEP = Level\_Step.
- 3. Hysteresis OFF mode, HYST[3:0] = 0x0.
- 4. Hysteresis ON mode, HYST[3:0] = 0x1 to 0xf; Min/Typ/Max values given for 0x2.
- At the upper side of LEVEL[7:0] values depending on the Hysteresis value chosen with HYST[3:0], the VBOD+ level reaches an overflow, e.g., for HYST[3:0] = 0d2 the hysteresis is 2 x Level\_Step = 12 mV up to position 253 and position 254 to 255 above must not be used.
- 6. These are based on design simulation. They are not covered by production test limits or characterization.

#### Table 54-23. BOD33 Power Consumption

Symbol	CPU Mode	Conditions	T <sub>A</sub>	Тур.	Мах	Units
I <sub>DD</sub>	Active / Idle	VCC = 1.8V	Max 85°C Typ 25°C	8.52	12.07	μA
		VCC = 3.3V		10.10	14.28	
	Standby with BOD continuous normal mode Standby with BOD continuous low power mode or Hibernate mode	VCC = 1.8V		4.71	6.34	
		VCC = 3.3V		6.01	8.06	
		VCC = 1.8V		0.15	0.22	
		VCC = 3.3V		0.21	0.30	

### **Electrical Characteristics at 85°C**

Symbol	Parameters	Conditions	Min.	Тур.	Max.	Unit
VREF	Reference input	External or Internal variable reference	1.0	-	AVDD-0.4	V
		REFCTRL.REFCOMP=0x3	AVDD			
VIN	Input channel range	-	0	-	VDDANA	V
VCMIN	Input common mode voltage	CTRLC.R2R=1	0	-	VDDANA	V
		CTRLC.R2R=0	See No	te 2		V
CSAMPLE	Input sampling capacitance		2	2.5	3	pF
RSAMPLE	Input sampling on-resistance	For a sampling rate at 1 Msps	-		2000	Ω
R <sub>REF</sub>	Reference source resistance	For a sampling rate at 1 Msps		-	2.5	kΩ

#### Note:

- 1. These values are based on simulation. They are not covered by production test limits or characterization.
- Limit the input common mode voltage using the following equations (where, VCM\_IN is the input channel common mode voltage): When CTRLC.R2R = 0:
  - VCM\_IN < 0.75\*VREF</p>
  - VCM\_IN > Maximum of (0, VREF-VDDANA-0.7, 1.25\*VREF-VDDANA)

#### Figure 54-5. ADC Analog Input AINx



The minimum sampling time  $t_{\text{samplehold}}$  for a given  $R_{\text{source}}$  can be found using a general formula:

 $t_{\text{samplehold}} \ge (R_{\text{sample}} + R_{\text{source}}) \times C_{\text{sample}} \times (n+2) \times \ln(2)$ For 12-bit accuracy, this turns into:

$$t_{\text{samplehold}} \ge (R_{\text{sample}} + R_{\text{source}}) \times C_{\text{sample}} \times 9.7$$
  
where  $t_{\text{samplehold}} \ge \frac{1}{2 \times f_{\text{ADC}}}$ .

#### Table 54-25. Differential Mode

Symbol	Parameter	Conditions		Min.	Тур.	Max.	Unit
ENOB	NOBEffectivefADC = 500 ksps -Number ofR2R disabled		$V_{DDANA} = 3.0V, V_{REF}$ = $V_{DDANA}$	10.7	11.0	11.3	bits
	DIIS		V <sub>DDANA</sub> = 3.0V, V <sub>REF</sub> = 2.0V	9.9	10.6	10.9	
		fADC = 1 Msps - R2R disabled	$V_{DDANA} = 3.0V, V_{REF}$ = $V_{DDANA}$	10.5	10.8	11.2	

## 57. Conventions

### 57.1 Numerical Notation

#### Table 57-1. Numerical Notation

Symbol	Description
165	Decimal number
0b0101	Binary number (example 0b0101 = 5 decimal)
'0101'	Binary numbers are given without prefix if unambiguous
0x3B24	Hexadecimal number
x	Represents an unknown or don't care value
Z	Represents a high-impedance (floating) state for either a signal or a bus

## 57.2 Memory Size and Type

Table 57-2. Memory Size and Bit Rate

Symbol	Description
KB (kbyte)	kilobyte (2 <sup>10</sup> = 1024)
MB (Mbyte)	megabyte (2 <sup>20</sup> = 1024*1024)
GB (Gbyte)	gigabyte (2 <sup>30</sup> = 1024*1024*1024)
b	bit (binary '0' or '1')
В	byte (8 bits)
1kbit/s	1,000 bit/s rate (not 1,024 bit/s)
1Mbit/s	1,000,000 bit/s rate
1Gbit/s	1,000,000,000 bit/s rate
word	32 bit
half-word	16 bit

## 57.3 Frequency and Time

## Table 57-3. Frequency and Time

Symbol	Description
kHz	1 kHz = 10 <sup>3</sup> Hz = 1,000 Hz
KHz	1 KHz = 1,024 Hz, 32 KHz = 32,768 Hz

© 2018 Microchip Technology Inc.