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®-M4F
Core Size	32-Bit Single-Core
Speed	120MHz
Connectivity	EBI/EMI, Ethernet, I²C, IrDA, LINbus, MMC/SD, QSPI, SPI, UART/USART, USB
Peripherals	Brown-out Detect/Reset, DMA, I²S, POR, PWM, WDT
Number of I/O	51
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 24x12b; D/A 2x12b
Oscillator Type	Internal
Operating Temperature	-40°C ~ 85°C (TA)
Mounting Type	Surface Mount
Package / Case	64-VFQFN Exposed Pad
Supplier Device Package	64-VQFN (9x9)
Purchase URL	https://www.e-xfl.com/product-detail/microchip-technology/atsame53j20a-mu

17.5.2 Power Management

The RAMECC will continue to operate in any sleep mode where the selected source clock is running. The RAMECC's interrupts can be used to wake up the device from sleep modes. Refer to the Power Manager chapter for details on the different sleep modes.

Related Links

18. PM – Power Manager

17.5.3 Clocks

The RAMECC bus clock is provided by the Main Clock Controller (MCLK) through the AHB-APB B bridge. The clock is enabled and disabled by writing RAMECC bit the in the APB B Mask register (MCLK.APBBMASK.RAMECC). See the register description for the default state of the RAMECC bus clock.

Related Links

15.6.2.6 Peripheral Clock Masking

17.5.4 DMA

Not applicable.

17.5.5 Interrupts

The interrupt request line is connected to the interrupt controller. Using the RAMECC interrupt(s) requires the interrupt controller to be configured first.

Related Links

10.2 Nested Vector Interrupt Controller

17.5.6 Events

Not applicable.

Related Links

31. EVSYS – Event System

17.5.7 Debug Operation

When the CPU is halted in debug mode the RAMECC will correct and log ECC errors based on the table below.

Table 17-1. ECC Debug Operation

DBGCTRL.ECCELOG	DBGCTRL.ECCDIS	Description
0	0	ECC errors from debugger reads are corrected but not logged in INTFLAG.
1	0	ECC errors from debugger reads are corrected and logged in INTFLAG.
X	1	ECC errors from debugger reads are not corrected or logged in INTFLAG.

19.8.11 Backup Input (BKIN) Value

Name: BKIN
Offset: 0x28
Reset: 0x00000000
Property: -

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
Access								
Reset								

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

Bits 1:0 – BKIN[1:0] Backup Input Value
These bits are cleared when the corresponding backup I/O pin detects a logical low level on the input pin or when the backup I/O is not enabled.

These bits are set when the corresponding backup I/O pin detects a logical high level on the input pin when the backup I/O is enabled.

Value	Name	Description
BKIN[0]	OUT[0]	If BKOUT.EN[0]=1, BKIN[0] will give the input value of the OUT[0] pin
BKIN[1]	OUT[1]	If BKOUT.EN[1]=1, BKIN[1] will give the input value of the OUT[1] pin

21.10.4 Interrupt Enable Clear in COUNT16 mode (CTRLA.MODE=1)

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			CMPn[3:0]			
Access	R/W	R/W			R/W	R/W	R/W	R/W
Reset	0	0			0	0	0	0

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

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
Writing a '0' to this bit has no effect. Writing a '1' to this bit will clear the Tamper Interrupt Enable bit, which disables the Tamper interrupt.

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

Bits 11:8 – CMPn[3:0] Compare n Interrupt Enable [n = 3..0]
Writing a '0' to this bit has no effect. Writing a '1' to this bit will clear the Compare n Interrupt Enable bit, which disables the Compare n interrupt.

Value	Description
0	The Compare n interrupt is disabled.
1	The Compare n interrupt is enabled.

Bits 7:0 – PERn[7:0] 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.

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

Name: CLOCK
Offset: 0x18
Reset: 0x00000000
Property: PAC Write-Protection, Write-Synchronized, Read-Synchronized

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 year offset with respect to the reference year (defined in software).

The year is considered a leap year if YEAR[1:0] is zero.

Bits 25:22 – MONTH[3:0] Month
1 – January

2 – February

...

12 – December

Bits 21:17 – DAY[4:0] Day
Day starts at 1 and ends at 28, 29, 30, or 31, depending on the month and year.

Bits 16:12 – HOUR[4:0] Hour
When CTRLA.CLKREP=0, the Hour bit group is in 24-hour format, with values 0-23. When CTRLA.CLKREP=1, HOUR[3:0] has values 1-12, and HOUR[4] represents AM (0) or PM (1).

Bits 11:6 – MINUTE[5:0] Minute
0 – 59

23.4 Signal Description

Signal Name	Type	Description
EXTINT[15..0]	Digital Input	External interrupt pin
NMI	Digital Input	Non-maskable interrupt pin

One signal may be available on several pins.

23.5 Product Dependencies

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

23.5.1 I/O Lines

Using the EIC's I/O lines requires the I/O pins to be configured.

Related Links

32. PORT - I/O Pin Controller

23.5.2 Power Management

All interrupts are available down to STANDBY sleep mode, but the EIC can be configured to automatically mask some interrupts in order to prevent device wake-up.

The EIC will continue to operate in any sleep mode where the selected source clock is running. The EIC's 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.

Related Links

18. PM – Power Manager

23.5.3 Clocks

The EIC bus clock (CLK_EIC_APB) can be enabled and disabled by the Main Clock Controller, the default state of CLK_EIC_APB can be found in the Peripheral Clock Masking section.

Some optional functions need a peripheral clock, which can either be a generic clock (GCLK_EIC, for wider frequency selection) or a Ultra Low Power 32KHz clock (CLK_ULP32K, for highest power efficiency). One of the clock sources must be configured and enabled before using the peripheral:

GCLK_EIC is configured and enabled in the Generic Clock Controller.

CLK_ULP32K is provided by the internal ultra-low-power (OSCULP32K) oscillator in the OSC32KCTRL module.

Both GCLK_EIC and CLK_ULP32K are asynchronous to the user interface clock (CLK_EIC_APB). Due to this asynchronicity, writes to certain registers will require synchronization between the clock domains. Refer to Synchronization for further details.

Related Links

15. MCLK – Main Clock

15.6.2.6 Peripheral Clock Masking

14. GCLK - Generic Clock Controller

29. OSC32KCTRL – 32KHz Oscillators Controller

Offset	Name	Bit Pos.								
0x01E0	EFTSL	7:0	RUD[7:0]							
		15:8	RUD[15:8]							
		23:16	RUD[23:16]							
		31:24	RUD[31:24]							
0x01E4	EFTN	7:0	RUD[7:0]							
		15:8	RUD[15:8]							
		23:16	RUD[23:16]							
		31:24			RUD[29:24]					
0x01E8	EFRSL	7:0	RUD[7:0]							
		15:8	RUD[15:8]							
		23:16	RUD[23:16]							
		31:24	RUD[31:24]							
0x01EC	EFRN	7:0	RUD[7:0]							
		15:8	RUD[15:8]							
		23:16	RUD[23:16]							
		31:24			RUD[29:24]					
0x01F0	PEFTSL	7:0	RUD[7:0]							
		15:8	RUD[15:8]							
		23:16	RUD[23:16]							
		31:24	RUD[31:24]							
0x01F4	PEFTN	7:0	RUD[7:0]							
		15:8	RUD[15:8]							
		23:16	RUD[23:16]							
		31:24			RUD[29:24]					
0x01F8	PEFRSL	7:0	RUD[7:0]							
		15:8	RUD[15:8]							
		23:16	RUD[23:16]							
		31:24	RUD[31:24]							
0x01FC	PEFRN	7:0	RUD[7:0]							
		15:8	RUD[15:8]							
		23:16	RUD[23:16]							
		31:24			RUD[29:24]					
0x0200 ... 0x026F	Reserved									
0x0270	RLPITR	7:0	RLPITR[7:0]							
		15:8	RLPITR[15:8]							
		23:16								
		31:24								
0x0274	RLPITI	7:0	RLPITI[7:0]							
		15:8	RLPITI[15:8]							
		23:16	RLPITI[23:16]							
		31:24								
0x0278	TLPITR	7:0	TLPITR[7:0]							
		15:8	TLPITR[15:8]							
		23:16								

24.9.29 GMAC Specific Address 1 Mask Bottom

Name: SAMB1
Offset: 0x0C8
Reset: 0x00000000
Property: -

Bit	31	30	29	28	27	26	25	24
	ADDR[31:24]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

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

Bit	15	14	13	12	11	10	9	8
	ADDR[15:8]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

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

Bits 31:0 – ADDR[31:0] Specific Address 1 Mask
Setting a bit to '1' masks the corresponding bit in the Specific Address 1 Bottom register (SAB1).

24.9.30 GMAC Specific Address Mask 1 Top

Name: SAMT1
Offset: 0x0CC
Reset: 0x00000000
Property: -

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
	ADDR[15:8]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

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

Bits 15:0 – ADDR[15:0] Specific Address 1 Mask
Setting a bit to '1' masks the corresponding bit in the Specific Address 1 register SAT1.

26.6.3.1.4 Region Next Address Structure Member

Name: RNEXT
Offset: 0x0C + n*0x0C [n=0..3]
Reset: 0x00000000
Property: Read/Write

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
Access								
Reset								

Bit	7	6	5	4	3	2	1	0
Access								
Reset								

26.6.4 Using ICM as an SHA Engine

The ICM can be configured to only calculate a SHA1, SHA224, SHA256 digest value.

26.6.4.1 Settings for Simple SHA Calculation

The start address of the system memory containing the data to hash must be configured in the transfer descriptor of the DMA embedded in the ICM.

The transfer descriptor is a system memory area integer multiple of 4 x 32-bit word and the start address of the descriptor must be configured in DSCR (the start address must be aligned on 64-bytes; six LSB must be cleared). If the data to hash is already padded according to SHA standards, only a single descriptor is required, and the EOM bit of RCFGn must be written to 1. If the data to hash does not contain a padding area, it is possible to define the padding area in another system memory location, the ICM can be configured to automatically jump from a memory area to another one by writing the descriptor register RNEXT with a value that differs from 0. Writing the RNEXT register with the start address of the padding area forces the ICM to concatenate both areas, thus providing the SHA result from the start address of the hash area configured in HASH.

Whether the system memory is configured as a single or multiple data block area, the bits CDWBN and WRAP must be cleared in the region descriptor structure member RCFGn. The bits WBDIS, EOMDIS, SLBDIS must be cleared in CFG.

Write the bits RHIEN and ECIEN in the Region Configuration Structure Member (RCFGn) to ‘0’:

Condition	Request		
	DMA	Interrupt	Event
Receive Break (RXBRK)	NA	Yes	
Error (ERROR)	NA	Yes	

34.6.4.1 DMA Operation

The USART generates the following DMA requests:

- Data received (RX): The request is set when data is available in the receive FIFO. The request is cleared when DATA is read.
- Data transmit (TX): The request is set when the transmit buffer (TX DATA) is empty. The request is cleared when DATA is written.

34.6.4.2 Interrupts

The USART has the following interrupt sources. These are asynchronous interrupts, and can wake up the device from any sleep mode:

- Data Register Empty (DRE)
- Receive Complete (RXC)
- Transmit Complete (TXC)
- Receive Start (RXS)
- Clear to Send Input Change (CTSIC)
- Received Break (RXBRK)
- Error (ERROR)

Each interrupt source has its own interrupt flag. The interrupt flag in the Interrupt Flag Status and Clear register (INTFLAG) will be set when the interrupt condition is met. Each interrupt can be individually enabled by writing '1' to the corresponding bit in the Interrupt Enable Set register (INTENSET), and disabled by writing '1' to the corresponding bit in the Interrupt Enable Clear register (INTENCLR).

An interrupt request is generated when the interrupt flag is set and if the corresponding interrupt is enabled. The interrupt request remains active until either the interrupt flag is cleared, the interrupt is disabled, or the USART is reset. For details on clearing interrupt flags, refer to the INTFLAG register description.

The value of INTFLAG indicates which interrupt is executed. Note that interrupts must be globally enabled for interrupt requests. Refer to *Nested Vector Interrupt Controller* for details.

Related Links

10.2 Nested Vector Interrupt Controller

34.6.4.3 Events

Not applicable.

34.6.5 Sleep Mode Operation

The behavior in sleep mode is depending on the clock source and the Run In Standby bit in the Control A register (CTRLA.RUNSTDBY):

- Internal clocking, CTRLA.RUNSTDBY=1: GCLK_SERCOMx_CORE can be enabled in all sleep modes. Any interrupt can wake up the device.

37.8.2 Control B

Name: CTRLB
Offset: 0x04
Reset: 0x00000000
Property: PAC Write-Protection

Control B

Bit	31	30	29	28	27	26	25	24
	DLYCS[7:0]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bit	23	22	21	20	19	18	17	16
	DLYBCT[7:0]							
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bit	15	14	13	12	11	10	9	8
					DATALEN[3:0]			
Access					R/W	R/W	R/W	R/W
Reset					0	0	0	0

Bit	7	6	5	4	3	2	1	0
			CSMODE[1:0]		SMEMREG	WDRBT	LOOPEN	MODE
Access			R/W	R/W	R/W	R/W	R/W	R/W
Reset			0	0	0	0	0	0

Bits 31:24 – DLYCS[7:0] Minimum Inactive CS Delay
This bit field defines the minimum delay between the inactivation and the activation of CS. The DLYCS time guarantees the slave minimum deselect time.

If DLYCS is 0x00, one CLK_QSPI_AHB period will be inserted by default.

Otherwise, the following equation determines the delay:

Bits 23:16 – DLYBCT[7:0] Delay Between Consecutive Transfers
This field defines the delay between two consecutive transfers with the same peripheral without removing the chip select. The delay is always inserted after each transfer and before removing the chip select if needed.

When DLYBCT=0x00, no delay between consecutive transfers is inserted and the clock keeps its duty cycle over the character transfers. In Serial Memory mode (MODE=1), DLYBCT is ignored and no delay is inserted. Otherwise, the following equation determines the delay:

Bits 11:8 – DATALEN[3:0] Data Length
The DATALEN field determines the number of data bits transferred. Reserved values should not be used.

2. Auto CMD23: when the ACMDEN field is set to 2, the peripheral issues a CMD23 automatically before issuing a command specified in CR.

The following conditions are required to use Auto CMD23:

- A memory card that supports CMD23 (SCR[33] = 1)
- If DMA is used, it must be ADMA (SDMA not supported).
- Only CMD18 or CMD25 is issued.

Note: The peripheral does not check the command index.

Auto CMD23 can be used with or without ADMA. By writing CR, the peripheral issues a CMD23 first and then issues a command specified by the CR.CMDIDX field. If CMD23 response errors are detected, the second command is not issued. A CMD23 error is indicated in ACESR. The CMD23 argument (32-bit block count value) is defined in SSAR.

This field determines the use of auto command functions.

Value	Name	Description
0	DISABLED	Auto Command Disabled
1	CMD12	Auto CMD12 Enabled
2	CMD23	Auto CMD23 Enabled
3	Reserved	Reserved

Bit 1 – BCEN Block Count Enable
This bit is used to enable BCR, which is only relevant for multiple block transfers. When this bit is 0, BCR is disabled, which is useful when executing an infinite transfer (refer to Table 1-4). If an ADMA2 transfer is more than 65535 blocks, this bit is set to 0 and the data transfer length is designated by the Descriptor Table.

Value	Name	Description
0	DISABLED	Block count is disabled
1	ENABLED	Block count is enabled

Bit 0 – DMAEN DMA Enable
This bit enables the DMA functionality described in section “Supporting DMA” in “SD Host Controller Simplified Specification V3.00” . DMA can be enabled only if it is supported as indicated by the bit CA0R.ADMA2SUP. One of the DMA modes can be selected using the field HC1R.DMASEL. If DMA is not supported, this bit is meaningless and then always reads 0. When this bit is set to 1, a DMA operation begins when the user writes to the upper byte of CR.

Value	Name	Description
0	DISABLED	DMA functionality is disabled
1	ENABLED	DMA functionality is enabled

Note:

1. The nu1 Workspace2 must be a multiple of 256.

43.3.4.13.7 Options

The option is set by the u2Options input parameter that must take one of the values listed in the following table. Please note that the values, OPTION_RNG_SEED and OPTION_RNG_GETSEED, are reserved for future use.

Table 43-41. RNG Service Options

Option	Purpose	Required Parameters
PUKCL_RNG_SEED	Reserved	Reserved
PUKCL_RNG_GET	Generation of a random number from the RNG	nu1RBase, u2RLength
PUKCL_RNG_X931_GET	Generation of a random number from the Deterministic RNG	nu1XKeyBase, nu1Workspace, nu1XSeedBase, u2XKeyLength, nu1QBase, nu1RBase
PUKCL_RNG_GETSEED	Reserved	Reserved

43.3.4.13.8 Code Example

```
PUKCL_PARAM PUKCLParam;
PPUKCL_PARAM pvPUKCLParam = &PUKCLParam;

// ! The Random Number Generator must be initialized and started
// ! following the directives given for the RNG on the chip

PUKCL(u2Option) =...;

// Initializing parameters
PUKCL_Rng(nu1RBase) = <Base of the ram location to store the rng>;
PUKCL_Rng(u2RLength) = <Length of the rng to get>;

// vPUKCL_Process() is a macro command, which populates the service name
// and then calls the library...
vPUKCL_Process(Rng,pvPUKCLParam);
if (PUKCL(u2Status) == PUKCL_OK)
            {
            // The RNG generation has been executed correctly
            ...
            }
else // Manage the error
```

43.3.4.13.9 Constraints

Random Number Generation

The following conditions must be avoided to ensure that the service works correctly:

- {nu1RBase,u2RLength} not in RAM
- {nu1RBase,u2RLength} not accessible or authorized for writing

Deterministic Random Number Generation

The length of the parameter nu1XSeedbase is: XSeedLength = max(2*u2XKeyLength, 44 bytes) The `max()` macro takes a maximum of two values.

The following conditions must be avoided to ensure that the service works correctly:

- nu1XKeyBase,nu1Workspace, nu1Workspace2, nu1XSeedBase, nu1QBase, nu1RBase are not aligned on 32-bit boundaries

```
// vPUKCL_Process() is a macro command, which populates the service name
// and then calls the library...
vPUKCL_Process(GF2NEcDsaGenerateFast, pvPUKCLParam);
if (PUKCL (u2Status) == PUKCL_OK)
            {
            ...
            }
else // Manage the error
```

43.3.7.9.6 Constraints

No overlapping between either input and output are allowed. The following conditions must be avoided to ensure the service works correctly:

- nu1ModBase, nu1CnsBase, nu1PointABase, nu1PrivateKey, nu1ScalarNumber, nu1OrderPointBase,nu1ABase, nu1Workspace or nu1HashBase are not aligned on 32-bit boundaries
- {nu1ModBase, u2ModLength + 4}, {nu1CnsBase, u2ModLength + 8}, {nu1PointABase, 3*u2ModLength+ 12},{nu1PrivateKey, u2ScalarLength + 4},{nu1ScalarNumber, u2ScalarLength + 4},{nu1OrderPointBase, u2ScalarLength + 4}, {nu1ABase, u2ModLength + 4}, {nu1Workspace, <WorkspaceLength>} or {nu1HashBase, u2ScalarLength + 4} are not in Crypto RAM
- u2ModLength is either: < 12, > 0xffc or not a 32-bit length
- All overlapping between {nu1ModBase, u2ModLength + 4}, {nu1CnsBase, u2ModLength +8}, {nu1PointABase, 3*u2ModLength + 12}, {nu1PrivateKey, u2ScalarLength + 4}, {nu1ScalarNumber, u2ScalarLength + 4}, {nu1OrderPointBase, u2ScalarLength + 4}, {nu1ABase, u2ModLength + 4}, {nu1Workspace, <WorkspaceLength>} and {nu1HashBase, u2ScalarLength + 4}

43.3.7.9.7 Status Returned Values

Table 43-109. GF2NEcDsaGenerate Fast Service Return Codes

Returned Status	Importance	Meaning
PUKCL_OK	–	The computation passed without problem.
PUKCL_WRONG_SELECTNUMBER	Warning	The given value for nu1ScalarNumber is not good to perform this signature generation.

43.3.7.10 Verifying an ECDSA Signature (Compliant with FIPS 186-2)

43.3.7.10.1 Purpose

This service is used to verify an ECDSA signature following the FIPS 186-2. It performs the second step of the Signature Verification.

A hash value (HashVal) must be provided as input, it has to be previously computed from the message to be signed using a secure hash algorithm.

As second significant input, the Signature is provided to be checked. This service checks the signature and fills the status accordingly.

43.3.7.10.2 How to Use the Service

43.3.7.10.3 Description

The operation performed is:

Verify = *EcDsaVerifySignature*(Pt_A, *HashVal*, *Signature*, *CurveParameters*, *PublicKey*)

The points used for this operation are represented in different coordinate systems. In this computation, the following parameters need to be provided:

46.8.9 Debug Control

Name: DBGCTRL
Offset: 0x09
Reset: 0x00
Property: PAC Write-Protection

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

Bit 0 – DBGRUN Debug 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 AC is halted when the CPU is halted by an external debugger. Any on-going comparison will complete.
1	The AC continues normal operation when the CPU is halted by an external debugger.

Value	Name	Description
0x0	OFF	No filtering
0x1	MAJ3	3-bit majority function (2 of 3)
0x2	MAJ5	5-bit majority function (3 of 5)
0x3-0x7	N/A	Reserved

Bits 21:20 – HYST[1:0] Hysteresis Level
These bits indicate the hysteresis level of comparator n when hysteresis is enabled (COMPCTRLn.HYSTEN=1). Hysteresis is available only for continuous mode (COMPCTRLn.SINGLE=0). COMPCTRLn.HYST can be written only while COMPCTRLn.ENABLE is zero.

These bits are not synchronized.

Value	Name	Description
0x0	HYST50	50mV
0x1	HYST100	100mV
0x2	HYST150	150mV
0x3	N/A	Reserved

Bit 19 – HYSTEN Hysteresis Enable
This bit indicates the hysteresis mode of comparator n. Hysteresis is available only for continuous mode (COMPCTRLn.SINGLE=0).

This bit is not synchronized.

Value	Description
0	Hysteresis is disabled.
1	Hysteresis is enabled.

Bits 17:16 – SPEED[1:0] Speed Selection
This bit must be written to 0x3 for each comparator n. COMPCTRLn.SPEED can be written only while COMPCTRLn.ENABLE is zero.

These bits are not synchronized.

Value	Name	Description
0x3	HIGH	High speed
Other	-	Reserved

Bit 15 – SWAP Swap Inputs and Invert
This bit swaps the positive and negative inputs to COMPn and inverts the output. This function can be used for offset cancellation. COMPCTRLn.SWAP can be written only while COMPCTRLn.ENABLE is zero.

These bits are not synchronized.

Value	Description
0	The output of MUXPOS connects to the positive input, and the output of MUXNEG connects to the negative input.
1	The output of MUXNEG connects to the positive input, and the output of MUXPOS connects to the negative input.

47.8.3 Event Control

Name: EVCTRL
Offset: 0x02
Reset: 0x00
Property: PAC Write-Protection

Bit	7	6	5	4	3	2	1	0
	RESRDYEO1	RESRDYEO0	INVEI1	INVEI0	EMPTYEO1	EMPTYEO0	STARTEI1	STARTEI0
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 – RESRDYEO1 Enable Result Ready of Filter 1 output event
This bit controls whether the RESRDY1 Event is enabled when the interpolated data is ready.

Value	Description
0	Interpolated Data Ready Event is disabled
1	Interpolated Data Ready Event is enabled

Bit 6 – RESRDYEO0 Enable Result Ready of Filter 0 output event
This bit controls whether the RESRDY0 Event is enabled when the interpolated data is ready.

Value	Description
0	Interpolated Data Ready Event is disabled
1	Interpolated Data Ready Event is enabled

Bit 5 – INVEI1 Enable Inversion of DAC1 Start Conversion Input Event
This bit defines the detection of the input event for DAC1 START.

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

Bit 4 – INVEI0 Enable Inversion of DAC0 Start Conversion Input Event
This bit defines the detection of the input event for DAC0 START.

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

Bit 3 – EMPTYEO1 Data Buffer Empty Event Output DAC1
This bit indicates if the Data Buffer Empty Event output for DAC1 is enabled.

Value	Description
0	Data Buffer Empty event is disabled.
1	Data Buffer Empty event is enabled.

Bit 2 – EMPTYEO0 Data Buffer Empty Event Output DAC0
This bit indicates if the Data Buffer Empty Event output for DAC0 is enabled.

48.7.1.2 Control B Clear

Name: CTRLBCLR
Offset: 0x04
Reset: 0x00
Property: PAC Write-Protection, Read-Synchronized, Write-Synchronized

This register allows the user to clear bits in the CTRLB register without doing a read-modify-write operation. Changes in this register will also be reflected in the Control B Set register (CTRLBSET).

Bit	7	6	5	4	3	2	1	0
	CMD[2:0]					ONESHOT	LUPD	DIR
Access	R/W	R/W	R/W			R/W	R/W	R/W
Reset	0	0	0			0	0	0

Bits 7:5 – CMD[2:0] Command
These bits are used for software control of the TC. The commands are executed on the next prescaled GCLK_TC clock cycle. When a command has been executed, the CMD bit group will be read back as zero.

Writing 0x0 to these bits has no effect.

Writing a '1' to any of these bits will clear the pending command.

Bit 2 – ONESHOT One-Shot on Counter
This bit controls one-shot operation of the TC.

Writing a '0' to this bit has no effect

Writing a '1' to this bit will disable one-shot operation.

Value	Description
0	The TC will wrap around and continue counting on an overflow/underflow condition.
1	The TC will wrap around and stop on the next underflow/overflow condition.

Bit 1 – LUPD Lock Update
This bit controls the update operation of the TC buffered registers.

When CTRLB.LUPD is set, no any update of the registers with value of its buffered register is performed on hardware UPDATE condition. Locking the update ensures that all buffer registers are valid before an hardware update is performed. After all the buffer registers are loaded correctly, the buffered registers can be unlocked.

This bit has no effect when input capture operation is enabled.

Writing a '0' to this bit has no effect.

Writing a '1' to this bit will clear the LUPD bit.

Value	Description
0	The CCBUFx and PERBUF buffer registers value are copied into CCx and PER registers on hardware update condition.
1	The CCBUFx and PERBUF buffer registers value are not copied into CCx and PER registers on hardware update condition.

49.8.13 Status

Name: STATUS
Offset: 0x30
Reset: 0x00000001
Property: -

Bit	31	30	29	28	27	26	25	24
			CMPx	CMPx	CMPx	CMPx	CMPx	CMPx
Access			R	R	R	R	R	R
Reset			0	0	0	0	0	0

Bit	23	22	21	20	19	18	17	16
			CCBUFVx	CCBUFVx	CCBUFVx	CCBUFVx	CCBUFVx	CCBUFVx
Access			R/W	R/W	R/W	R/W	R/W	R/W
Reset			0	0	0	0	0	0

Bit	15	14	13	12	11	10	9	8
	FAULTx	FAULTx	FAULTB	FAULTA	FAULT1IN	FAULT0IN	FAULTBIN	FAULTAIN
Access	R/W	R/W	R/W	R/W	R	R	R	R
Reset	0	0	0	0	0	0	0	0

Bit	7	6	5	4	3	2	1	0
	PERBUFV		PATTBUFV	SLAVE	DFS		IDX	STOP
Access	R/W		R/W	R	R/W		R	R
Reset	0		0	0	0		0	1

Bits 29,28,27,26,25,24 – CMPx Channel x Compare Value
This bit reflects the channel x output compare value.

Value	Description
0	Channel compare output value is 0.
1	Channel compare output value is 1.

Bits 21,20,19,18,17,16 – CCBUFVx Channel x Compare or Capture Buffer Valid
For a compare channel, this bit is set when a new value is written to the corresponding CCBUFx register. The bit is cleared either by writing a '1' to the corresponding location when CTRLB.LUPD is set, or automatically on an UPDATE condition.

For a capture channel, the bit is set when a valid capture value is stored in the CCBUFx register. The bit is automatically cleared when the CCx register is read.

Bits 15,14 – FAULTx Non-recoverable Fault x State
This bit is set by hardware as soon as non-recoverable Fault x condition occurs.

This bit is cleared by writing a one to this bit and when the corresponding FAULTxIN status bit is low.

Once this bit is clear, the timer/counter will restart from the last COUNT value. To restart the timer/counter from BOTTOM, the timer/counter restart command must be executed before clearing the corresponding

Table 54-2. General Operating Conditions

Symbol	Description	Min.	Typ.	Max.	Units
V_{DDIO}	IO Supply Voltage	1.71 (see **Note 1**)	3.3	3.63	V
V_{DDIOB}	IOB Supply Voltage	1.71 (see **Note 1**)	3.3	3.63	V
V_{DDANA}	Analog supply voltage	1.71 (see **Note 1**)	3.3	3.63	V
T_A	Temperature range	-40	25	85	°C
T_J	Junction temperature	-	-	105	°C

Note:

1. With BOD33 disabled.
2. The same voltage must be applied to V_{DDIO} and V_{DDANA}. V_{DDIOB} should be lower or equal to V_{DDIO} / V_{DDANA}. The common voltage is referred to as V_{DD} in the data sheet.
3. When I/O pads in the V_{DDIOB} cluster are multiplexed as analog pads, V_{DDANA} is used to power the I/O. Using this configuration may result in an electrical conflict if the V_{DDIOB} voltage is different from that of V_{DDIO} / V_{DDANA}. If the application has such requirements, it is required to power V_{DDIOB}, V_{DDIO} and V_{DDANA} from the same supply source to ensure that they are always at the same voltage.

54.4 Injection Current

Stresses beyond those listed in the table below may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

Table 54-3. Injection Current(1, 2)

Symbol	Description	min	max	Unit
I_{INJ1}(3)	IO pin injection current	-1	+1	mA
I_{INJ2}(4)	IO pin injection current	-15	+15	mA
$I_{INJtotal}$	Sum of IO pins injection current	-45	+45	mA

Note:

1. Injecting current may have an effect on the accuracy of Analog blocks.
2. Injecting current on Backup I/Os is not allowed.
3. Conditions for V_{PIN}: V_{PIN} < GND - 0.6V or 3.6V < V_{PIN} ≤ 4.2V. Conditions for V_{DD}: 3V < V_{DD} ≤ 3.6V. If V_{PIN} is lower than GND-0.6V, a current limiting resistor is required. The negative DC injection current limiting resistor is calculated as R = |(GND - 0.6V – V_{PIN}) / Inj1|. If V_{PIN} is greater than V_{DD} + 0.6V, a current limiting resistor is required. The positive DC injection current limiting resistor is calculated as R = (V_{PIN} - (V_{DD} + 0.6)) / Inj1.
4. Conditions for V_{PIN}: GND - 0.6V < V_{PIN} < GND or V_{PIN} ≤ 3.6V. Conditions for V_{DD}: V_{DD} ≤ 3V. If V_{PIN} is lower than GND-0.6V, a current limiting resistor is required. The negative DC injection current