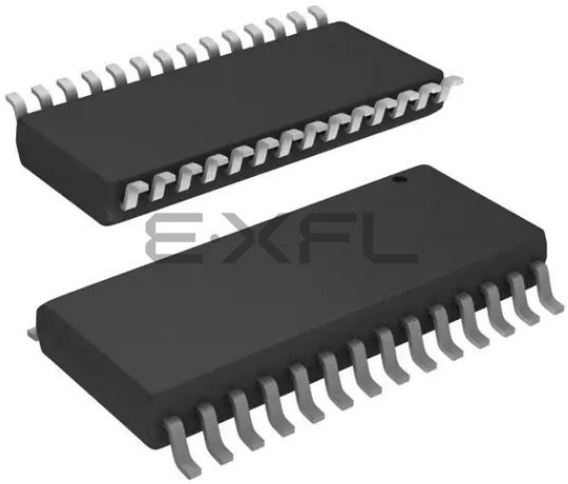


Welcome to E-XFL.COM

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	PIC
Core Size	16-Bit
Speed	32MHz
Connectivity	I²C, IrDA, LINbus, SmartCard, SPI, UART/USART
Peripherals	AES, Brown-out Detect/Reset, DMA, I²S, HLVD, POR, PWM, WDT
Number of I/O	21
Program Memory Size	128KB (43K x 24)
Program Memory Type	FLASH
EEPROM Size	-
RAM Size	8K x 8
Voltage - Supply (Vcc/Vdd)	2V ~ 3.6V
Data Converters	A/D 10x10b/12b
Oscillator Type	Internal
Operating Temperature	-40°C ~ 85°C (TA)
Mounting Type	Surface Mount
Package / Case	28-SOIC (0.295", 7.50mm Width)
Supplier Device Package	28-SOIC
Purchase URL	https://www.e-xfl.com/product-detail/microchip-technology/pic24fj128ga202-i-so

3.0 CPU

Note: This data sheet summarizes the features of this group of PIC24F devices. It is not intended to be a comprehensive reference source. For more information on the CPU, refer to the *"dsPIC33/PIC24 Family Reference Manual"*, **"CPU with Extended Data Space (EDS)"** (DS39732). The information in this data sheet supersedes the information in the FRM.

The PIC24F CPU has a 16-bit (data) modified Harvard architecture with an enhanced instruction set and a 24-bit instruction word with a variable length opcode field. The Program Counter (PC) is 23 bits wide and addresses up to 4M instructions of user program memory space. A single-cycle instruction prefetch mechanism is used to help maintain throughput and provides predictable execution. All instructions execute in a single cycle, with the exception of instructions that change the program flow, the double-word move (`MOV.D`) instruction and the table instructions. Overhead-free program loop constructs are supported using the `REPEAT` instructions, which are interruptible at any point.

PIC24F devices have sixteen, 16-bit Working registers in the programmer's model. Each of the Working registers can act as a Data, Address or Address Offset register. The 16th Working register (W15) operates as a Software Stack Pointer (SSP) for interrupts and calls.

The lower 32 Kbytes of the Data Space (DS) can be accessed linearly. The upper 32 Kbytes of the Data Space are referred to as Extended Data Space to which the extended data RAM, EPMP memory space or program memory can be mapped.

The Instruction Set Architecture (ISA) has been significantly enhanced beyond that of the PIC18, but maintains an acceptable level of backward compatibility. All PIC18 instructions and addressing modes are supported, either directly, or through simple macros. Many of the ISA enhancements have been driven by compiler efficiency needs.

The core supports Inherent (no operand), Relative, Literal and Memory Direct Addressing modes along with three groups of addressing modes. All modes support Register Direct and various Register Indirect modes. Each group offers up to seven addressing modes. Instructions are associated with predefined addressing modes depending upon their functional requirements.

For most instructions, the core is capable of executing a data (or program data) memory read, a Working register (data) read, a data memory write and a program (instruction) memory read per instruction cycle. As a result, three parameter instructions can be supported, allowing trinary operations (that is, A + B = C) to be executed in a single cycle.

A high-speed, 17-bit x 17-bit multiplier has been included to significantly enhance the core arithmetic capability and throughput. The multiplier supports Signed, Unsigned and Mixed mode, 16-bit x 16-bit or 8-bit x 8-bit, integer multiplication. All multiply instructions execute in a single cycle.

The 16-bit ALU has been enhanced with integer divide assist hardware that supports an iterative non-restoring divide algorithm. It operates in conjunction with the `REPEAT` instruction looping mechanism and a selection of iterative divide instructions to support 32-bit (or 16-bit), divided by 16-bit, integer signed and unsigned division. All divide operations require 19 cycles to complete but are interruptible at any cycle boundary.

The PIC24F has a vectored exception scheme with up to 8 sources of non-maskable traps and up to 118 interrupt sources. Each interrupt source can be assigned to one of seven priority levels.

A block diagram of the CPU is shown in Figure 3-1.

3.1 Programmer's Model

The programmer's model for the PIC24F is shown in Figure 3-2. All registers in the programmer's model are memory-mapped and can be manipulated directly by instructions.

A description of each register is provided in Table 3-1. All registers associated with the programmer's model are memory-mapped.

4.1.1 PROGRAM MEMORY ORGANIZATION

The program memory space is organized in word-addressable blocks. Although it is treated as 24 bits wide, it is more appropriate to think of each address of the program memory as a lower and upper word, with the upper byte of the upper word being unimplemented. The lower word always has an even address, while the upper word has an odd address (Figure 4-2).

Program memory addresses are always word-aligned on the lower word and addresses are incremented or decremented by two during code execution. This arrangement also provides compatibility with data memory space addressing and makes it possible to access data in the program memory space.

4.1.2 HARD MEMORY VECTORS

All PIC24F devices reserve the addresses between 000000h and 000200h for hard-coded program execution vectors. A hardware Reset vector is provided to redirect code execution from the default value of the PC on device Reset to the actual start of code. A GOTO instruction is programmed by the user at 000000h with the actual address for the start of code at 000002h.

PIC24F devices also have two Interrupt Vector Tables, (IVTs), located from 000004h to 0000FFh and 000100h to 0001FFh. These vector tables allow each of the many device interrupt sources to be handled by separate ISRs. A more detailed discussion of the Interrupt Vector Tables is provided in **Section 8.1 "Interrupt Vector Table"**.

4.1.3 FLASH CONFIGURATION WORDS

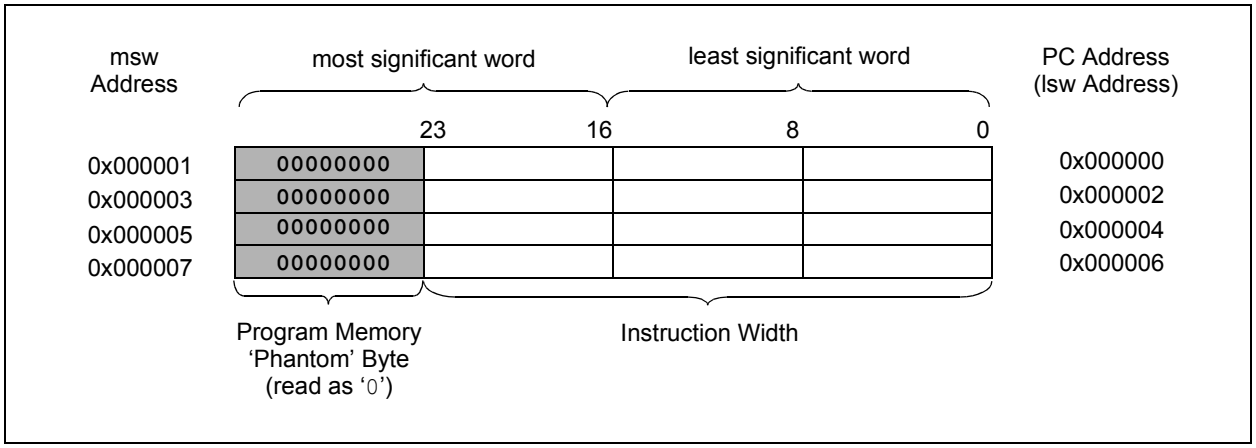
In PIC24FJ128GA204 family devices, the top four words of on-chip program memory are reserved for configuration information. On device Reset, the configuration information is copied into the appropriate Configuration register. The addresses of the Flash Configuration Word for devices in the PIC24FJ128GA204 family are shown in Table 4-1. Their location in the memory map is shown with the other memory vectors in Figure 4-1.

The Configuration Words in program memory are a compact format. The actual Configuration bits are mapped in several different registers in the configuration memory space. Their order in the Flash Configuration Words does not reflect a corresponding arrangement in the configuration space. Additional details on the device Configuration Words are provided in **Section 29.0 "Special Features"**.

TABLE 4-1: FLASH CONFIGURATION WORDS FOR PIC24FJ128GA204 FAMILY DEVICES

Device	Program Memory (Words)	Configuration Word Addresses
PIC24FJ64GA2XX	22,016	00ABF8h:00ABFEh
PIC24FJ128GA2XX	44,032	0157F8h:0157FEh

FIGURE 4-2: PROGRAM MEMORY ORGANIZATION



8.0 INTERRUPT CONTROLLER

Note: This data sheet summarizes the features of this group of PIC24F devices. It is not intended to be a comprehensive reference source. For more information, refer to the *"dsPIC33/PIC24 Family Reference Manual"*, **"Interrupts"** (DS70000600). The information in this data sheet supersedes the information in the FRM.

The PIC24F interrupt controller reduces the numerous peripheral interrupt request signals to a single interrupt request signal to the PIC24F CPU. It has the following features:

- Up to 8 processor exceptions and software traps
- Seven user-selectable priority levels
- Interrupt Vector Table (IVT) with up to 118 vectors
- Unique vector for each interrupt or exception source
- Fixed priority within a specified user priority level
- Alternate Interrupt Vector Table (AIVT) for debug support
- Fixed interrupt entry and return latencies

8.1 Interrupt Vector Table

The Interrupt Vector Table (IVT) is shown in Figure 8-1. The IVT resides in program memory, starting at location, 000004h. The IVT contains 126 vectors, consisting of 8 non-maskable trap vectors, plus up to 118 sources of interrupt. In general, each interrupt source has its own vector. Each interrupt vector contains a 24-bit wide address. The value programmed into each interrupt vector location is the starting address of the associated Interrupt Service Routine (ISR).

Interrupt vectors are prioritized in terms of their natural priority; this is linked to their position in the vector table. All other things being equal, lower addresses have a higher natural priority. For example, the interrupt associated with Vector 0 will take priority over interrupts at any other vector address.

PIC24FJ128GA204 family devices implement non-maskable traps and unique interrupts. These are summarized in Table 8-1 and Table 8-2.

8.1.1 ALTERNATE INTERRUPT VECTOR TABLE

The Alternate Interrupt Vector Table (AIVT) is located after the IVT, as shown in Figure 8-1. The ALTIVT (INTCON2<15>) control bit provides access to the AIVT. If the ALTIVT bit is set, all interrupt and exception processes will use the alternate vectors instead of the default vectors. The alternate vectors are organized in the same manner as the default vectors.

The AIVT supports emulation and debugging efforts by providing a means to switch between an application and a support environment without requiring the interrupt vectors to be reprogrammed. This feature also enables switching between applications for evaluation of different software algorithms at run time. If the AIVT is not needed, the AIVT should be programmed with the same addresses used in the IVT.

8.2 Reset Sequence

A device Reset is not a true exception because the interrupt controller is not involved in the Reset process. The PIC24F devices clear their registers in response to a Reset, which forces the PC to zero. The microcontroller then begins program execution at location, 000000h. The user programs a `GOTO` instruction at the Reset address, which redirects program execution to the appropriate start-up routine.

Note: Any unimplemented or unused vector locations in the IVT and AIVT should be programmed with the address of a default interrupt handler routine that contains a `RESET` instruction.

REGISTER 8-3: INTCON1: INTERRUPT CONTROL REGISTER 1

R/W-0	U-0	U-0	U-0	U-0	U-0	U-0	U-0
NSTDIS	—	—	—	—	—	—	—
bit 15							bit 8

U-0	U-0	U-0	R/W-0	R/W-0	R/W-0	R/W-0	U-0
—	—	—	MATHERR	ADDRERR	STKERR	OSCFAIL	—
bit 7							bit 0

Legend:			
R = Readable bit	W = Writable bit	U = Unimplemented bit, read as '0'	
-n = Value at POR	'1' = Bit is set	'0' = Bit is cleared	x = Bit is unknown

bit 15 **NSTDIS:** Interrupt Nesting Disable bit
1 = Interrupt nesting is disabled
0 = Interrupt nesting is enabled

bit 14-5 **Unimplemented:** Read as '0'

bit 4 **MATHERR:** Arithmetic Error Trap Status bit
1 = Overflow trap has occurred
0 = Overflow trap has not occurred

bit 3 **ADDRERR:** Address Error Trap Status bit
1 = Address error trap has occurred
0 = Address error trap has not occurred

bit 2 **STKERR:** Stack Error Trap Status bit
1 = Stack error trap has occurred
0 = Stack error trap has not occurred

bit 1 **OSCFAIL:** Oscillator Failure Trap Status bit
1 = Oscillator failure trap has occurred
0 = Oscillator failure trap has not occurred

bit 0 **Unimplemented:** Read as '0'

REGISTER 8-15: IEC2: INTERRUPT ENABLE CONTROL REGISTER 2

U-0	R/W-0	R/W-0	U-0	U-0	R/W-0	R/W-0	R/W-0
—	DMA4IE	PMPIE	—	—	OC6IE	OC5IE	IC6IE
bit 15							bit 8

R/W-0	R/W-0	R/W-0	R/W-0	R/W-0	R/W-0	R/W-0	R/W-0
IC5IE	IC4IE	IC3IE	DMA3IE	CRYROLLIE	CRYFREEIE	SPI2TXIE	SPI2IE
bit 7							bit 0

Legend:			
R = Readable bit	W = Writable bit	U = Unimplemented bit, read as '0'	
-n = Value at POR	'1' = Bit is set	'0' = Bit is cleared	x = Bit is unknown

bit 15 **Unimplemented:** Read as '0'

bit 14 **DMA4IE:** DMA Channel 4 Interrupt Enable bit
1 = Interrupt request is enabled
0 = Interrupt request is not enabled

bit 13 **PMPIE:** Parallel Master Port Interrupt Enable bit
1 = Interrupt request is enabled
0 = Interrupt request is not enabled

bit 12-11 **Unimplemented:** Read as '0'

bit 10 **OC6IE:** Output Compare Channel 6 Interrupt Enable bit
1 = Interrupt request is enabled
0 = Interrupt request is not enabled

bit 9 **OC5IE:** Output Compare Channel 5 Interrupt Enable bit
1 = Interrupt request is enabled
0 = Interrupt request is not enabled

bit 8 **IC6IE:** Input Capture Channel 6 Interrupt Enable bit
1 = Interrupt request is enabled
0 = Interrupt request is not enabled

bit 7 **IC5IE:** Input Capture Channel 5 Interrupt Enable bit
1 = Interrupt request is enabled
0 = Interrupt request is not enabled

bit 6 **IC4IE:** Input Capture Channel 4 Interrupt Enable bit
1 = Interrupt request is enabled
0 = Interrupt request is not enabled

bit 5 **IC3IE:** Input Capture Channel 3 Interrupt Enable bit
1 = Interrupt request is enabled
0 = Interrupt request is not enabled

bit 4 **DMA3IE:** DMA Channel 3 Interrupt Enable bit
1 = Interrupt request is enabled
0 = Interrupt request is not enabled

bit 3 **CRYROLLIE:** Cryptographic Rollover Interrupt Enable bit
1 = Interrupt request is enabled
0 = Interrupt request is not enabled

bit 2 **CRYFREEIE:** Cryptographic Buffer Free Interrupt Enable bit
1 = Interrupt request is enabled
0 = Interrupt request is not enabled

REGISTER 8-35: IPC14: INTERRUPT PRIORITY CONTROL REGISTER 14

U-0	R/W-1	R/W-0	R/W-0	U-0	R/W-1	R/W-0	R/W-0
—	SPI2RXIP2	SPI2RXIP1	SPI2RXIPO	—	SPI1RXIP2	SPI1RXIP1	SPI1RXIPO
bit 15							bit 8

U-0	U-0	U-0	U-0	U-0	R/W-1	R/W-0	R/W-0
—	—	—	—	—	KEYSTRIP2	KEYSTRIP1	KEYSTRIP0
bit 7							bit 0

Legend:			
R = Readable bit	W = Writable bit	U = Unimplemented bit, read as '0'	
-n = Value at POR	'1' = Bit is set	'0' = Bit is cleared	x = Bit is unknown

bit 15 **Unimplemented:** Read as '0'

bit 14-12 **SPI2RXIP<2:0>:** SPI2 Receive Interrupt Priority bits
111 = Interrupt is Priority 7 (highest priority interrupt)
•
•
•
001 = Interrupt is Priority 1
000 = Interrupt source is disabled

bit 11 **Unimplemented:** Read as '0'

bit 10-8 **SPI1RXIP<2:0>:** SPI1 Receive Interrupt Priority bits
111 = Interrupt is Priority 7 (highest priority interrupt)
•
•
•
001 = Interrupt is Priority 1
000 = Interrupt source is disabled

bit 7-3 **Unimplemented:** Read as '0'

bit 2-0 **KEYSTRIP<2:0>:** Cryptographic Key Store Program Done Interrupt Priority bits
111 = Interrupt is Priority 7 (highest priority interrupt)
•
•
•
001 = Interrupt is Priority 1
000 = Interrupt source is disabled

REGISTER 11-6: RPINR2: PERIPHERAL PIN SELECT INPUT REGISTER 2

U-0	U-0	R/W-1	R/W-1	R/W-1	R/W-1	R/W-1	R/W-1
—	—	OCTRIG2R5	OCTRIG2R4	OCTRIG2R3	OCTRIG2R2	OCTRIG2R1	OCTRIG2R0
bit 15							bit 8

U-0	U-0	R/W-1	R/W-1	R/W-1	R/W-1	R/W-1	R/W-1
—	—	INT4R5	INT4R4	INT4R3	INT4R2	INT4R1	INT4R0
bit 7							bit 0

Legend:			
R = Readable bit	W = Writable bit	U = Unimplemented bit, read as ‘0’	
-n = Value at POR	‘1’ = Bit is set	‘0’ = Bit is cleared	x = Bit is unknown

bit 15-14 **Unimplemented:** Read as ‘0’

bit 13-8 **OCTRIG2R<5:0>:** Assign Output Compare Trigger 2 to Corresponding RPn or RPIn Pin bits

bit 7-6 **Unimplemented:** Read as ‘0’

bit 5-0 **INT4R<5:0>:** Assign External Interrupt 4 (INT4) to Corresponding RPn or RPIn Pin bits

REGISTER 11-7: RPINR7: PERIPHERAL PIN SELECT INPUT REGISTER 7

U-0	U-0	R/W-1	R/W-1	R/W-1	R/W-1	R/W-1	R/W-1
—	—	IC2R5	IC2R4	IC2R3	IC2R2	IC2R1	IC2R0
bit 15							bit 8

U-0	U-0	R/W-1	R/W-1	R/W-1	R/W-1	R/W-1	R/W-1
—	—	IC1R5	IC1R4	IC1R3	IC1R2	IC1R1	IC1R0
bit 7							bit 0

Legend:			
R = Readable bit	W = Writable bit	U = Unimplemented bit, read as ‘0’	
-n = Value at POR	‘1’ = Bit is set	‘0’ = Bit is cleared	x = Bit is unknown

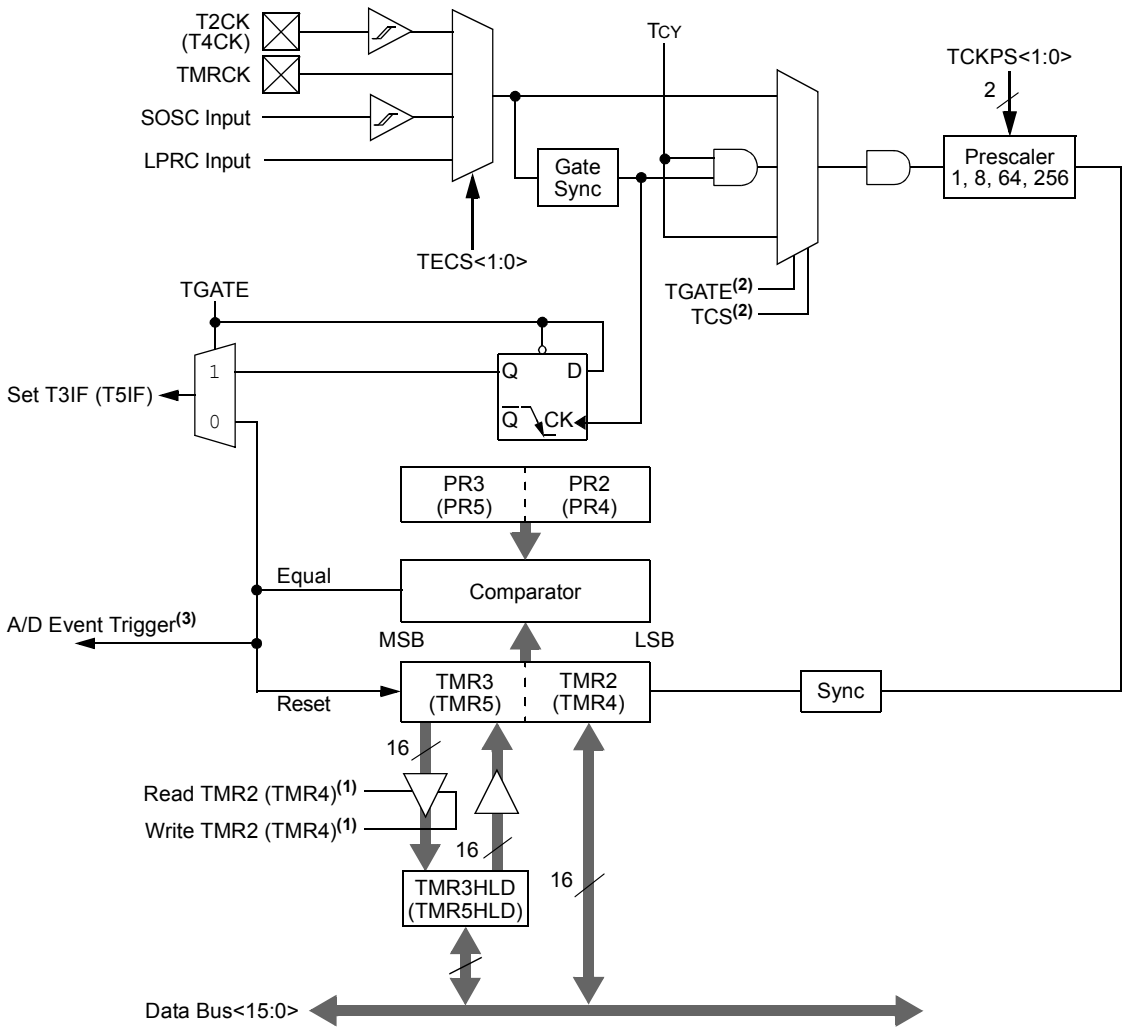
bit 15-14 **Unimplemented:** Read as ‘0’

bit 13-8 **IC2R<5:0>:** Assign Input Capture 2 (IC2) to Corresponding RPn or RPIn Pin bits

bit 7-6 **Unimplemented:** Read as ‘0’

bit 5-0 **IC1R<5:0>:** Assign Input Capture 1 (IC1) to Corresponding RPn or RPIn Pin bits

FIGURE 13-1: TIMER2/3 AND TIMER4/5 (32-BIT) BLOCK DIAGRAM



Note 1: The 32-Bit Timer Configuration bit, T32, must be set for 32-bit timer/counter operation. All control bits are respective to the T2CON and T4CON registers.

2: The timer clock input must be assigned to an available RPn/RPIn pin before use. See **Section 11.4 "Peripheral Pin Select (PPS)"** for more information.

3: The A/D Event Trigger is available only on Timer2/3 in 32-bit mode and Timer3 in 16-bit mode.

REGISTER 15-1: OCxCON1: OUTPUT COMPARE x CONTROL REGISTER 1 (CONTINUED)

bit 4 **OCFLT0:** Output Compare x PWM Fault 0 (OCFA pin) Condition Status bit(2,4)
1 = PWM Fault 0 has occurred
0 = No PWM Fault 0 has occurred

bit 3 **TRIGMODE:** Trigger Status Mode Select bit
1 = TRIGSTAT (OCxCON2<6>) is cleared when OCxRS = OCxTMR or in software
0 = TRIGSTAT is only cleared by software

bit 2-0 **OCM<2:0>:** Output Compare x Mode Select bits(1)
111 = Center-Aligned PWM mode on OCx(2)
110 = Edge-Aligned PWM mode on OCx(2)
101 = Double Compare Continuous Pulse mode: Initializes the OCx pin low; toggles the OCx state continuously on alternate matches of OCxR and OCxRS
100 = Double Compare Single-Shot mode: Initializes the OCx pin low; toggles the OCx state on matches of OCxR and OCxRS for one cycle
011 = Single Compare Continuous Pulse mode: Compare events continuously toggle the OCx pin
010 = Single Compare Single-Shot mode: Initializes OCx pin high; compare event forces the OCx pin low
001 = Single Compare Single-Shot mode: Initializes OCx pin low; compare event forces the OCx pin high
000 = Output compare channel is disabled

Note 1: The OCx output must also be configured to an available RPn pin. For more information, see **Section 11.4 "Peripheral Pin Select (PPS)"**.

2: The Fault input enable and Fault status bits are valid when OCM<2:0> = 111 or 110.

3: The Comparator 1 output controls the OC1-OC2 channels; Comparator 2 output controls the OC3-OC4 channels; Comparator 3 output controls the OC5-OC6 channels.

4: The OCFA/OCFB Fault input must also be configured to an available RPn/RPIn pin. For more information, see **Section 11.4 "Peripheral Pin Select (PPS)"**.

REGISTER 21-3: ALCFGRPT: ALARM CONFIGURATION REGISTER

R/W-0	R/W-0	R/W-0	R/W-0	R/W-0	R/W-0	R/W-0	R/W-0
ALRMEN	CHIME	AMASK3	AMASK2	AMASK1	AMASK0	ALRMPTR1	ALRMPTR0
bit 15							bit 8

R/W-0	R/W-0	R/W-0	R/W-0	R/W-0	R/W-0	R/W-0	R/W-0
ARPT7	ARPT6	ARPT5	ARPT4	ARPT3	ARPT2	ARPT1	ARPT0
bit 7							bit 0

Legend:			
R = Readable bit	W = Writable bit	U = Unimplemented bit, read as '0'	
-n = Value at POR	'1' = Bit is set	'0' = Bit is cleared	x = Bit is unknown

bit 15 **ALRMEN:** Alarm Enable bit
1 = Alarm is enabled (cleared automatically after an alarm event whenever ARPT<7:0> = 00h and CHIME = 0)
0 = Alarm is disabled

bit 14 **CHIME:** Chime Enable bit
1 = Chime is enabled; ARPT<7:0> bits are allowed to roll over from 00h to FFh
0 = Chime is disabled; ARPT<7:0> bits stop once they reach 00h

bit 13-10 **AMASK<3:0>:** Alarm Mask Configuration bits
0000 = Every half second
0001 = Every second
0010 = Every 10 seconds
0011 = Every minute
0100 = Every 10 minutes
0101 = Every hour
0110 = Once a day
0111 = Once a week
1000 = Once a month
1001 = Once a year (except when configured for February 29th, once every 4 years)
101x = Reserved – do not use
11xx = Reserved – do not use

bit 9-8 **ALRMPTR<1:0>:** Alarm Value Register Window Pointer bits
Points to the corresponding Alarm Value registers when reading the ALRMVALH and ALRMVALL registers. The ALRMPTR<1:0> value decrements on every read or write of ALRMVALH until it reaches '00'.
ALRMVAL<15:8>:
00 = ALRMMIN
01 = ALRMWD
10 = ALRMMNTH
11 = PWCSTAB
ALRMVAL<7:0>:
00 = ALRMSEC
01 = ALRMHR
10 = ALRMDAY
11 = PWCSAMP

bit 7-0 **ARPT<7:0>:** Alarm Repeat Counter Value bits
11111111 = Alarm will repeat 255 more times
•
•
•
00000000 = Alarm will not repeat
The counter decrements on any alarm event; it is prevented from rolling over from 00h to FFh unless CHIME = 1.

22.1 Data Register Spaces

There are four register spaces used for cryptographic data and key storage:

- CRYTXTA
- CRYTXTB
- CRYTXTC
- CRYKEY

Although mapped into the SFR space, all of these Data Spaces are actually implemented as 128-bit or 256-bit wide arrays, rather than groups of 16-bit wide Data registers. Reads and writes to and from these arrays are automatically handled as if they were any other register in the SFR space.

CRYTXTA through CRYTXTC are 128-bit wide spaces; they are used for writing data to and reading from the Cryptographic Engine. Additionally, they are also used for storing intermediate results of the encryption/decryption operation. None of these registers may be written to when the module is performing an operation (CRYGO = 1).

CRYTXTA and CRYTXTB normally serve as inputs to the encryption/decryption process.

CRYTXTA usually contains the initial plaintext or ciphertext to be encrypted or decrypted. Depending on the mode of operation, CRYTXTB may contain the ciphertext output or intermediate cipher data. It may also function as a programmable length counter in certain operations.

CRYTXTC is primarily used to store the final output of an encryption/decryption operation. It is also used as the input register for data to be programmed to the secure OTP array.

CRYKEY is a 256-bit wide space, used to store cryptographic keys for the selected operation; it is writable from both the SFR space and the secure OTP array. Although mapped into the SFR space, it is a write-only memory area; any data placed here, regardless of its source, cannot be read back by any run-time operations. This feature helps to ensure the security of any key data.

22.2 Modes of Operation

The Cryptographic Engine supports the following modes of operation, determined by the OPMOD<3:0> bits:

- Block Encryption
- Block Decryption
- AES Decryption Key Expansion
- Random Number Generation
- Session Key Generation
- Session Key Encryption
- Session Key Loading

The OPMOD<3:0> bits may be changed while CRYON is set. They should only be changed when a cryptographic operation is not being done (CRYGO = 0).

Once the encryption operation, and the appropriate and valid key configuration is selected, the operation is performed by setting the CRYGO bit. This bit is automatically cleared by hardware when the operation is complete. The CRYGO bit can also be manually cleared by software; this causes any operation in progress to terminate immediately. Clearing this bit in software also sets the CRYABRT bit (CRYSTAT<5>).

For most operations, CRYGO can only be set when an OTP operation is not being performed and there are no other error conditions. CRYREAD, CRYWR, CRYABRT, ROLLOVR, MODFAIL and KEYFAIL must all be '0'.

Setting CRYWR and CRYGO simultaneously will not initiate an OTP programming operation or any other operation. Setting CRYGO when the module is disabled (CRYON = 0) also has no effect.

22.3 Enabling the Engine

The Cryptographic Engine is enabled by setting the CRYON bit. Clearing this bit disables both the DES and AES engines, as well as causing the following register bits to be held in Reset:

- CRYGO (CRYCONL<8>)
- TXTABSY (CRYSTAT<6>)
- CRYWR (CRYOTP<0>)

All other register bits and registers may be read and written while CRYON = 0.

22.4 Operation During Sleep and Idle Modes

22.4.1 OPERATION DURING SLEEP MODES

Whenever the device enters any Sleep or Deep Sleep mode, all operation engine state machines are reset. This feature helps to preserve the integrity, or any data being encrypted or decrypted, by discarding any intermediate text that might be used to break the key.

Any OTP programming operations under way when a Sleep mode is entered are also halted. Depending on what is being programmed, this may result in permanent loss of a memory location or potentially the use of the entire secure OTP array. Users are advised to perform OTP programming only when entry into power-saving modes is disabled.

Note:	OTP programming errors, regardless of the source, are not recoverable errors. Users should ensure that all foreseeable interruptions to the programming operation, including device interrupts and entry into power-saving modes, are disabled.

22.8 Encrypting a Session Key

Note: ECB and CBC modes are restricted to 128-bit session keys only.

1. If not already set, set the CRYON bit.
2. If not already programmed, program the SKEYEN bit to '1'.

Note: Setting SKEYEN permanently makes Key #1 available as a Key Encryption Key only. It cannot be used for other encryption or decryption operations after that.

3. Set OPMOD<3:0> to '1110'.
4. Configure the CPHRSEL, CPHRMOD<2:0> and KEYMOD<1:0> register bit fields as desired, set SKEYSEL to '0'.
5. Read the KEYFAIL status bit. If this bit is '1', an illegal configuration has been selected and the encrypt operation will not be performed.
6. Write the software generated session key into the CRYKEY register or generate a random key into the CRYKEY register. It is only necessary to write the lowest *n* bits of CRYKEY for a key length of *n*, as all unused key bits are ignored.
7. Set the CRYGO bit. Poll the bit until it is cleared by hardware; alternatively, set the DONEIE bit (CRYCONL<11>) to generate an interrupt when the encryption is done.
8. Read the encrypted session key out of the appropriate CRYTXT register.
9. For total key lengths of more than 128 bits, set SKEYSEL to '1' and repeat Steps 6 and 7.
10. Set KEYSRC<3:0> to '0000' to use the session key to encrypt data.

22.9 Receiving a Session Key

Note: ECB and CBC modes are restricted to 128-bit session keys only.

1. If not already set, set the CRYON bit.
2. If not already programmed, program the SKEYEN bit to '1'.

Note: Setting SKEYEN permanently makes Key #1 available as a Key Encryption Key only. It cannot be used for other encryption or decryption operations after that. It also permanently disables the ability of software to decrypt the session key into the CRYTXTA register, thereby breaking programmatic security (i.e., software can read the unencrypted key).

3. Set OPMOD<3:0> to '1111'.
4. Configure the CPHRSEL, CPHRMOD<2:0> and KEYMOD<1:0> register bit fields as desired, set SKEYSEL to '0'.
5. Read the KEYFAIL status bit. If this bit is '1', an illegal configuration has been selected and the encrypt operation will NOT be performed.
6. Write the encrypted session key received into the appropriate CRYTXT register.
7. Set the CRYGO bit. Poll the bit until it is cleared by hardware; alternatively, set the DONEIE bit (CRYCONL<11>) to generate an interrupt when the process is done.
8. For total key lengths of more than 128 bits, set SKEYSEL to '1' and repeat Steps 6 and 7.
9. Set KEYSRC<3:0> to '0000' to use the newly generated session key to encrypt and decrypt data.

22.10 Generating a Pseudorandom Number (PRN)

For operations that require a Pseudorandom Number (PRN), the method outlined in NIST SP800-90 can be adapted for efficient use with the Cryptographic Engine. This method uses the AES algorithm in CTR mode to create PRNs with minimal CPU overhead. PRNs generated in this manner can be used for cryptographic purposes or any other purpose that the host application may require.

The random numbers used as initial seeds can be taken from any source convenient to the user's application. If possible, a non-deterministic random number source should be used.

Note:	PRN generation is not available when software keys are disabled (SWKYDIS = 1).

To perform the initial reseeding operation, and subsequent reseedings after the reseeding interval has expired:

1. Store a random number (128 bits) in CRYTXTA.
2. For the initial generation ONLY, use a key value of 0h (128 bits) and a counter value of 0h.
3. Configure the engine for AES encryption, CTR mode (OPMOD<3:0> = 0000, CPHRSEL = 1, CPHMOD<2:0> = 100).
4. Perform an encrypt operation by setting CRYGO.
5. Move the results in CRYTXTC to RAM. This is the new key value (NEW_KEY).
6. Store another random number (128 bits) in CRYTXTA.
7. Configure the module for encryption as in Step 3.
8. Perform an encrypt operation by setting CRYGO.
9. Store this value in RAM. This is the new counter value (NEW_CTR).
10. For subsequent reseeding operations, use NEW_KEY and NEW_CTR for the starting key and counter values.

To generate the pseudorandom number:

1. Load NEW_KEY value from RAM into CRYKEY.
2. Load NEW_CTR value from RAM into CRYTXTB.
3. Load CRYTXTA with 0h (128 bits).
4. Configure the engine for AES encryption, CTR mode (OPMOD<3:0> = 0000, CPHRSEL = 1, CPHMOD<2:0> = 100).
5. Perform an encrypt operation by setting CRYGO.
6. Copy the generated PRN in CRYTXTC (PRNG_VALUE) to RAM.
7. Repeat the encrypt operation.
8. Store the value of CRYTXTC from this round as the new value of NEW_KEY.
9. Repeat the encrypt operation.
10. Store the value of CRYTXTC from this round as the new value of NEW_CTR.

Subsequent PRNs can be generated by repeating this procedure until the reseeding interval has expired. At that point, the reseeding operation is performed using the stored values of NEW_KEY and NEW_CTR.

22.11 Generating a Random Number

1. Enable the Cryptographic mode (CRYON (CRYCONL<0>) = 1).
2. Set the OPMOD<3:0> bits to '1010'.
3. Start the request by setting the CRYGO bit (CRYCONL<8>) to '1'.
4. Wait for the CRYGO bit to be cleared to '0' by the hardware.
5. Read the random number from the CRYTXTA registers.

22.12 Testing the Key Source Configuration

The validity of the key source configuration can always be tested by writing the appropriate register bits and then reading the KEYFAIL register bit. No operation needs to be started to perform this check; the module does not even need to be enabled.

REGISTER 24-2: AD1CON2: A/D CONTROL REGISTER 2 (CONTINUED)

bit 6-2 **SMPI<4:0>:** Interrupt Sample/DMA Increment Rate Select bits

When DMAEN = 1:

11111 = Increments the DMA address after completion of the 32nd sample/conversion operation
11110 = Increments the DMA address after completion of the 31st sample/conversion operation
•
•
•
00001 = Increments the DMA address after completion of the 2nd sample/conversion operation
00000 = Increments the DMA address after completion of each sample/conversion operation

When DMAEN = 0:

11111 = Interrupts at the completion of the conversion for each 32nd sample
11110 = Interrupts at the completion of the conversion for each 31st sample
•
•
•
00001 = Interrupts at the completion of the conversion for every other sample
00000 = Interrupts at the completion of the conversion for each sample

bit 1 **BUFM:** Buffer Fill Mode Select bit(1)

1 = Starts buffer filling at ADC1BUF0 on first interrupt and ADC1BUF8 on next interrupt
0 = Always starts filling buffer at ADC1BUF0

bit 0 **ALTS:** Alternate Input Sample Mode Select bit

1 = Uses channel input selects for Sample A on first sample and Sample B on next sample
0 = Always uses channel input selects for Sample A

Note 1: These bits are only applicable when the buffer is used in FIFO mode (BUFREGEN = 0). In addition, BUFS is only used when BUFM = 1.

26.0 COMPARATOR VOLTAGE REFERENCE

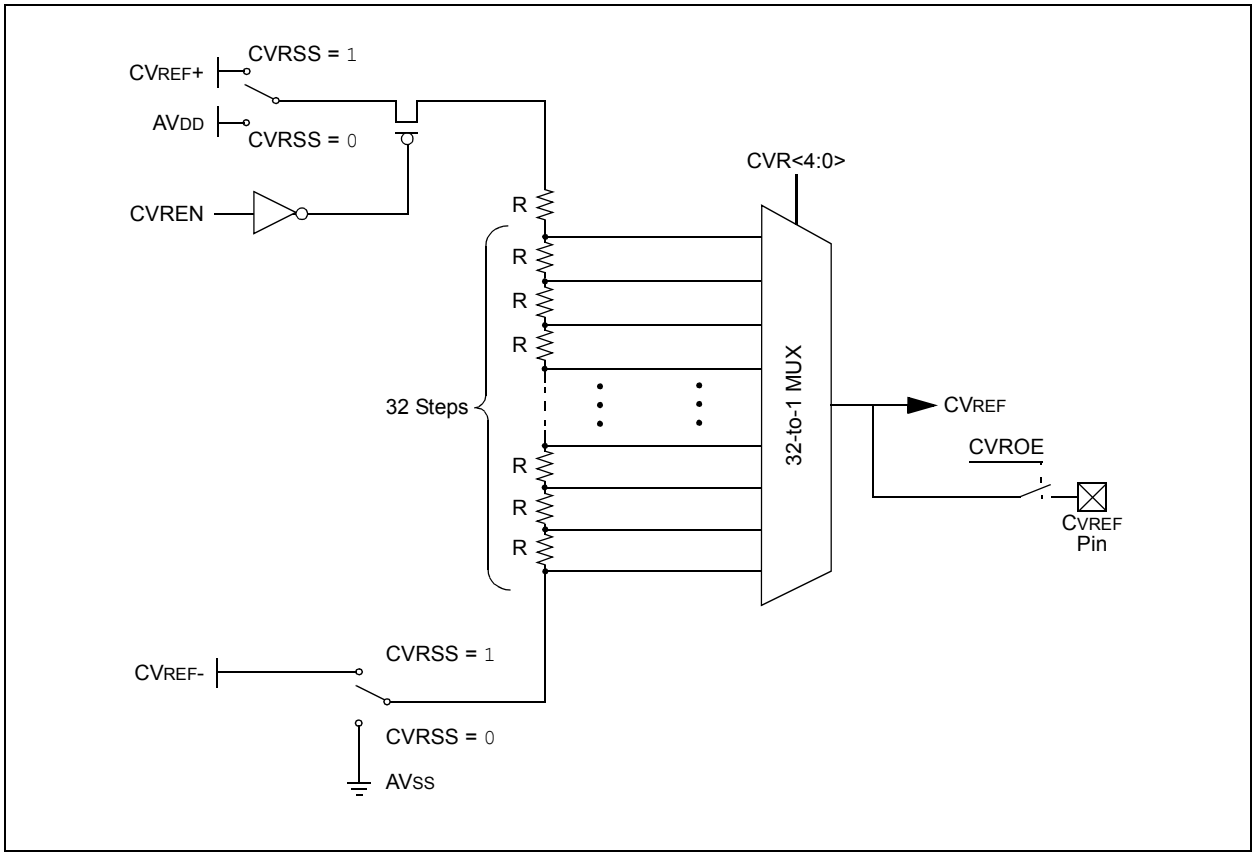
Note: This data sheet summarizes the features of this group of PIC24F devices. It is not intended to be a comprehensive reference source. For more information, refer to the *"dsPIC33/PIC24 Family Reference Manual"*, **"Comparator Voltage Reference Module"** (DS39709). The information in this data sheet supersedes the information in the FRM.

26.1 Configuring the Comparator Voltage Reference

The comparator voltage reference module is controlled through the CVRCON register (Register 26-1). The comparator voltage reference provides a range of output voltages with 32 distinct levels. The comparator reference supply voltage can come from either VDD and VSS or the external CVREF+ and CVREF- pins. The voltage source is selected by the CVRSS bit (CVRCON<5>).

The settling time of the comparator voltage reference must be considered when changing the CVREF output.

FIGURE 26-1: COMPARATOR VOLTAGE REFERENCE BLOCK DIAGRAM



30.11 Demonstration/Development Boards, Evaluation Kits and Starter Kits

A wide variety of demonstration, development and evaluation boards for various PIC MCUs and dsPIC DSCs allows quick application development on fully functional systems. Most boards include prototyping areas for adding custom circuitry and provide application firmware and source code for examination and modification.

The boards support a variety of features, including LEDs, temperature sensors, switches, speakers, RS-232 interfaces, LCD displays, potentiometers and additional EEPROM memory.

The demonstration and development boards can be used in teaching environments, for prototyping custom circuits and for learning about various microcontroller applications.

In addition to the PICDEM™ and dsPICDEM™ demonstration/development board series of circuits, Microchip has a line of evaluation kits and demonstration software for analog filter design, KEELOQ® security ICs, CAN, IrDA®, PowerSmart battery management, SEEVAL® evaluation system, Sigma-Delta ADC, flow rate sensing, plus many more.

Also available are starter kits that contain everything needed to experience the specified device. This usually includes a single application and debug capability, all on one board.

Check the Microchip web page (www.microchip.com) for the complete list of demonstration, development and evaluation kits.

30.12 Third-Party Development Tools

Microchip also offers a great collection of tools from third-party vendors. These tools are carefully selected to offer good value and unique functionality.

- Device Programmers and Gang Programmers from companies, such as SoftLog and CCS
- Software Tools from companies, such as Gimpel and Trace Systems
- Protocol Analyzers from companies, such as Saleae and Total Phase
- Demonstration Boards from companies, such as MikroElektronika, Digilent® and Olimex
- Embedded Ethernet Solutions from companies, such as EZ Web Lynx, WIZnet and IPLogika®

FIGURE 32-3: EXTERNAL CLOCK TIMING

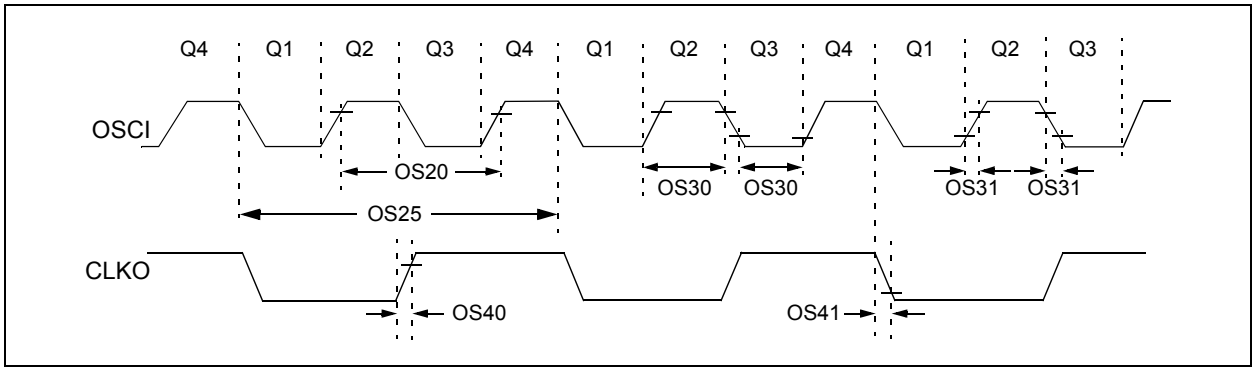


TABLE 32-19: EXTERNAL CLOCK TIMING REQUIREMENTS

AC CHARACTERISTICS			Standard Operating Conditions: 2.0V to 3.6V (unless otherwise stated) Operating temperature -40°C ≤ TA ≤ +85°C for Industrial -40°C ≤ TA ≤ +125°C for Extended				
Param No.	**Symbol**	**Characteristic**	**Min**	**Typ(1)**	**Max**	**Units**	**Conditions**
OS10	FOSC	External CLKI Frequency (External clocks allowed only in EC mode)	DC 4	— —	32 48	MHz MHz	EC ECPLL **(Note 2)**
		Oscillator Frequency	3.5 4 10 12 31	— — — — —	10 8 32 32 33	MHz MHz MHz MHz kHz	XT XTPLL HS HSPLL SOSC
OS20	TOSC	TOSC = 1/FOSC	—	—	—	—	See Parameter OS10 for FOSC value
OS25	TCY	Instruction Cycle Time(3)	62.5	—	DC	ns	
OS30	TosL, TosH	External Clock in (OSCI) High or Low Time	0.45 x TOSC	—	—	ns	EC
OS31	TosR, TosF	External Clock in (OSCI) Rise or Fall Time	—	—	20	ns	EC
OS40	TckR	CLKO Rise Time(4)	—	6	10	ns	
OS41	TckF	CLKO Fall Time(4)	—	6	10	ns	

Note 1: Data in the "Typ" column is at 3.3V, +25°C unless otherwise stated. Parameters are for design guidance only and are not tested.

2: Represents input to the system clock prescaler. PLL dividers and postscalers must still be configured so that the system clock frequency does not exceed the maximum frequency shown in Figure 32-1.

3: Instruction cycle period (TCY) equals two times the input oscillator time base period. All specified values are based on characterization data for that particular oscillator type, under standard operating conditions, with the device executing code. Exceeding these specified limits may result in an unstable oscillator operation and/or higher than expected current consumption. All devices are tested to operate at "Min" values with an external clock applied to the OSCI/CLKI pin. When an external clock input is used, the "Max" cycle time limit is "DC" (no clock) for all devices.

4: Measurements are taken in EC mode. The CLKO signal is measured on the OSCO pin. CLKO is low for the Q1-Q2 period (1/2 TCY) and high for the Q3-Q4 period (1/2 TCY).

TABLE 32-39: A/D MODULE SPECIFICATIONS

AC CHARACTERISTICS			Standard Operating Conditions: 2.0V to 3.6V (unless otherwise stated) Operating temperature -40°C ≤ TA ≤ +85°C for Industrial -40°C ≤ TA ≤ +125°C for Extended				
Param No.	**Symbol**	**Characteristic**	**Min.**	**Typ**	**Max.**	**Units**	**Conditions**
Device Supply							
AD01	AVDD	Module VDD Supply	Greater of: VDD – 0.3 or 2.2	—	Lesser of: VDD + 0.3 or 3.6	V	
AD02	AVSS	Module VSS Supply	VSS – 0.3	—	VSS + 0.3	V	
Reference Inputs							
AD05	VREFH	Reference Voltage High	AVSS + 1.7	—	AVDD	V	
AD06	VREFL	Reference Voltage Low	AVSS	—	AVDD – 1.7	V	
AD07	VREF	Absolute Reference Voltage	AVSS – 0.3	—	AVDD + 0.3	V	
Analog Inputs							
AD10	VINH-VINL	Full-Scale Input Span	VREFL	—	VREFH	V	(Note 2)
AD11	VIN	Absolute Input Voltage	AVSS – 0.3	—	AVDD + 0.3	V	
AD12	VINL	Absolute VINL Input Voltage	AVSS – 0.3	—	AVDD/3	V	
AD13		Leakage Current	—	±1.0	±610	nA	VINL = AVSS = VREFL = 0V, AVDD = VREFH = 3V, Source Impedance = 2.5 kΩ
AD17	RIN	Recommended Impedance of Analog Voltage Source	—	—	2.5K	Ω	10-bit
A/D Accuracy							
AD20B	Nr	Resolution	—	12	—	bits	
AD21B	INL	Integral Nonlinearity	—	±1	<±2	LSb	VINL = AVSS = VREFL = 0V, AVDD = VREFH = 3V
AD22B	DNL	Differential Nonlinearity	—	—	<±1	LSb	VINL = AVSS = VREFL = 0V, AVDD = VREFH = 3V
AD23B	GERR	Gain Error	—	±1	±3	LSb	VINL = AVSS = VREFL = 0V, AVDD = VREFH = 3V
AD24B	EOFF	Offset Error	—	±1	±2	LSb	VINL = AVSS = VREFL = 0V, AVDD = VREFH = 3V
AD25B		Monotonicity(1)	—	—	—	—	Guaranteed

Note 1: The A/D conversion result never decreases with an increase in the input voltage and has no missing codes.

2: Measurements are taken with the external VREF+ and VREF- used as the A/D voltage reference.

NOTES:

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/support
Web Address:
www.microchip.com

Atlanta
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

Austin, TX
Tel: 512-257-3370

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Cleveland
Independence, OH
Tel: 216-447-0464
Fax: 216-447-0643

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Novi, MI
Tel: 248-848-4000

Houston, TX
Tel: 281-894-5983

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608

New York, NY
Tel: 631-435-6000

San Jose, CA
Tel: 408-735-9110

Canada - Toronto
Tel: 905-673-0699
Fax: 905-673-6509

ASIA/PACIFIC

Asia Pacific Office
Suites 3707-14, 37th Floor
Tower 6, The Gateway
Harbour City, Kowloon
Hong Kong
Tel: 852-2943-5100
Fax: 852-2401-3431

Australia - Sydney
Tel: 61-2-9868-6733
Fax: 61-2-9868-6755

China - Beijing
Tel: 86-10-8569-7000
Fax: 86-10-8528-2104

China - Chengdu
Tel: 86-28-8665-5511
Fax: 86-28-8665-7889

China - Chongqing
Tel: 86-23-8980-9588
Fax: 86-23-8980-9500

China - Dongguan
Tel: 86-769-8702-9880

China - Hangzhou
Tel: 86-571-8792-8115
Fax: 86-571-8792-8116

China - Hong Kong SAR
Tel: 852-2943-5100
Fax: 852-2401-3431

China - Nanjing
Tel: 86-25-8473-2460
Fax: 86-25-8473-2470

China - Qingdao
Tel: 86-532-8502-7355
Fax: 86-532-8502-7205

China - Shanghai
Tel: 86-21-5407-5533
Fax: 86-21-5407-5066

China - Shenyang
Tel: 86-24-2334-2829
Fax: 86-24-2334-2393

China - Shenzhen
Tel: 86-755-8864-2200
Fax: 86-755-8203-1760

China - Wuhan
Tel: 86-27-5980-5300
Fax: 86-27-5980-5118

China - Xian
Tel: 86-29-8833-7252
Fax: 86-29-8833-7256

ASIA/PACIFIC

China - Xiamen
Tel: 86-592-2388138
Fax: 86-592-2388130

China - Zhuhai
Tel: 86-756-3210040
Fax: 86-756-3210049

India - Bangalore
Tel: 91-80-3090-4444
Fax: 91-80-3090-4123

India - New Delhi
Tel: 91-11-4160-8631
Fax: 91-11-4160-8632

India - Pune
Tel: 91-20-3019-1500

Japan - Osaka
Tel: 81-6-6152-7160
Fax: 81-6-6152-9310

Japan - Tokyo
Tel: 81-3-6880- 3770
Fax: 81-3-6880-3771

Korea - Daegu
Tel: 82-53-744-4301
Fax: 82-53-744-4302

Korea - Seoul
Tel: 82-2-554-7200
Fax: 82-2-558-5932 or
82-2-558-5934

Malaysia - Kuala Lumpur
Tel: 60-3-6201-9857
Fax: 60-3-6201-9859

Malaysia - Penang
Tel: 60-4-227-8870
Fax: 60-4-227-4068

Philippines - Manila
Tel: 63-2-634-9065
Fax: 63-2-634-9069

Singapore
Tel: 65-6334-8870
Fax: 65-6334-8850

Taiwan - Hsin Chu
Tel: 886-3-5778-366
Fax: 886-3-5770-955

Taiwan - Kaohsiung
Tel: 886-7-213-7828

Taiwan - Taipei
Tel: 886-2-2508-8600
Fax: 886-2-2508-0102

Thailand - Bangkok
Tel: 66-2-694-1351
Fax: 66-2-694-1350

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Dusseldorf
Tel: 49-2129-3766400

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Germany - Pforzheim
Tel: 49-7231-424750

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Italy - Venice
Tel: 39-049-7625286

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Poland - Warsaw
Tel: 48-22-3325737

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

Sweden - Stockholm
Tel: 46-8-5090-4654

UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820

01/27/15