OVERVIEW

In various mid-range microcontroller data sheets there is a caution statement in reference to the interrupt-on-change function. It reads something like this:

Note: If a change on the I/O pin should occur when the read operation is being executed (start of the Q2 cycle), then the RAIF interrupt flag may not get set.

This technical brief will describe in detail how the IOC interrupt may be missed depending on when the change event takes place in relation to the clock cycle.

Note: The condition described does not affect the enhanced mid-range series of microcontrollers.

INTERRUPT-ON-CHANGE OPERATION

The following is a discussion on how the interrupt-on-change operates both when interrupt-on-change occurs when the port is idle and when change occurs when the port is being read/written to.

Description of Problem

The microcontroller does not detect an interrupt-on-change (IOC) on an I/O pin if the IOC occurs when a READ or WRITE instruction on the port is executed.

Root Cause

A READ/WRITE instruction resets the mismatch latch when the change in level occurs between Q2 and Q3. If there is no READ/WRITE instruction during the change in level, then the interrupt is set as intended.

Figure 1 is a simplified schematic of the input and change capture.
Normal Operation (No Read/Write to Port)

The interrupt detection is done as follows in terms of Q cycles:

a) If pin changes level during Q1 cycle:
   - Q1 will read the current state of the pin.
   - Since pin level is different from the change latch output, the input to the interrupt latch is now '1' and the interrupt flag is set.
   - Change latch will not enable since there is no READ/WRITE instruction.
   - During the Interrupt Service Routine a READ instruction on PORTB will enable the change latch and clear the interrupt flag.

b) If pin changes during Q2, Q3 or Q4 cycles:
   - The state of the pin will be read until the next Q1 cycle and the process described in a) above will follow.

FIGURE 2: NORMAL OPERATION
Problem Operation (When change in level occurs during a READ/WRITE instruction)

If the interrupt is occurring during the execution of a READ or WRITE instruction to the port, then there is a risk of not detecting said interrupt:

a) If pin changes level during Q1 cycle:
   - Q1 will read the current state of the pin.
   - Since pin level is different from the change latch output, the input to the interrupt latch is now ‘1’ and the interrupt flag is set at Q1.

b) If pin changes level during Q2 cycle:
   - New level is at change latch input.

c) If pin changes level during Q3 cycle:
   - The same sequence of events as in b) above occurs.

b) If pin changes level during Q4 cycle:
   - Pin will be read on the following Q1 cycle.
   - The sequence of events as in a) will follow.

From the above discussion, we can see that the best possible action is to not execute a READ or WRITE instruction to the port when an IOC event is expected.
Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip’s Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as “unbreakable.”

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip’s code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.