PCN Number:	20100910003	**PCN Date:**	
Title:	MSP430F54xxA and MSP430F55xx Device Derivatives: Flash Read Error Susceptibility		
Customer Contact:	PCN Manager	**Phone:** +1(214) 480-6037	**Dept:** Quality Services
Proposed 1st Ship Date:		**Estimated Sample Availability:**	

Change Type:

☐	Assembly Site	☐	Assembly Process	☐	Assembly Materials
☒	Design	☐	Electrical Specification	☐	Mechanical Specification
☐	Test Site	☐	Packing/Shipping/Labeling	☐	Test Process
☐	Wafer Bump Site	☐	Wafer Bump Material	☐	Wafer Bump Process
☐	Wafer Fab Site	☐	Wafer Fab Materials	☐	Wafer Fab Process

PCN Details

Description of Change:

Dear Customer,

Texas Instruments strives to provide its customers with the highest quality products and to remain in compliance with our strict quality standards. This is formal notification that we have identified a Flash Read error susceptibility in the MSP430F54xxA and MSP430F55xx device derivatives listed in the Affected Product section (up to and including silicon Revision D). The root cause of the issue is understood and implementation of a fix within the Flash array has been completed. Devices incorporating this fix are currently in process. In the meantime, we have stopped shipping the Affected Products and are initiating a voluntary Selected Inventory Exchange Process (SIEP). If you determine that this issue negatively affects your application or if you would like to return any affected material from your stock, please work with TI customer service on an RMR for this material. If you determine, after reviewing the attached Technical Documents (see Appendix A and B), that the application for which you are using these devices is not likely to be affected by this issue, we are implementing a waiver option to enable you to continue receiving affected devices until new material becomes available.

Texas Instruments appreciates your business and apologizes for any inconvenience this may cause. We stand ready to work with you to minimize any problems and address any concerns that you may have. Feel free to contact us at the contacts listed below, or your field sales representative, if you need more information.

Section Content

- **Flash read error susceptibility description**
- **Customer Options**

- **Texas Instruments response and recommendation**
- **Device Fix**

Flash read error susceptibility description:

A Flash Read may return invalid data under certain conditions. This occurs even though the content of the Flash remains correct. The Flash Read error susceptibility is caused by cross-talk influences and is modulated by certain application conditions such as read mode setting, idle time between reads, voltage, and temperature. Normal lot-to-lot process variation can also influence susceptibility.

The Flash read error susceptibility is described in more detail in Appendix A and B.

Appendix A: MSP430F54xxA Device Derivatives.
Appendix B: MSP430F55xx Device Derivatives

Customer options:

Option 1:

Line/Field Risk is deemed unacceptable by customer or customer desires to return affected devices and receive fixed replacement devices.

- Return existing inventory
- Work with customer service to RMR this material
- **Selected Inventory Exchange Process (SIEP) with new material available in December 2010**

Option 2:

Customer determines that its application is not likely to be negatively affected by this issue or that Line/Field Risk is acceptable. (see Note 1).

- Retain current inventory
- Submit waiver application to continue receiving current material until new material is available
- Current material will be discontinued once new material becomes available

Note 1: Texas Instruments strongly recommends that affected devices not be used for any safety-critical application in which a failure of the device could result in an injury to persons or property.

Texas Instruments response and recommendation:

Texas Instruments has stopped production and shipment of all current MSP430F54xxA and MSP430F55xx device derivatives, which are susceptible to Flash Read error. Texas Instruments recommends that you discontinue use of any material that you have in stock and that you return that material to Texas Instruments. Texas Instruments will provide fixed replacement devices, when available. However, if you determine, after reviewing the attached Technical Document (see Appendix A and/or B), that the application for which you are using these devices is not likely to be affected by this issue, Texas Instruments is willing to work with you to supply affected devices until new material becomes available. Texas Instruments strongly recommends that affected devices not be used for any safety-critical application in which a failure of the device could result in an injury to persons or property.

Device Fix:

Texas Instruments is in the process of implementing a fix to remove this issue. The change is to eliminate device susceptibility to Flash Read error; it does not change designed device functionality or require datasheet changes. The estimated time line is as follows:

Fix implementation and design validation: September 2010
Production material available: December 2010

Product Affected:

Table 1. MSP430F54xxA device derivatives. For all listed part numbers, affected silicon revisions are up to and including Revision "D."

MSP430F5418AIPN	MSP430F5435AIPNR	MSP430F5438ACY	MSP430BT5190IPZ
MSP430F5418AIPNR	MSP430F5436AIPZ	MSP430F5438ACYS	MSP430BT5190IPZR
MSP430F5419AIPZ	MSP430F5436AIPZR	MSP430F5438AIPZ	MSP430BT5190IZQWR
MSP430F5419AIPZR	MSP430F5436AIZQW	MSP430F5438AIPZR	MSP430BT5190IZQWT
MSP430F5419AIZQW	MSP430F5436AIZQWR	MSP430F5438AIZQW	
MSP430F5419AIZQWR	MSP430F5436AIZQWT	MSP430F5438AIZQWR	
MSP430F5419AIZQWT	MSP430F5437AIPN	MSP430F5438AIZQWT	
MSP430F5435AIPN	MSP430F5437AIPNR	MSP430F5438AGACYS	

Table 2. MSP430F55xx device derivatives. For all listed part numbers, affected silicon revisions are up to and including Revision "D."

MSP430F5513IRGCR	MSP430F5517IPN	MSP430F5524IRGCR	MSP430F5527IPN
MSP430F5513IRGCT	MSP430F5517IPNR	MSP430F5524IRGCT	MSP430F5527IPNR
MSP430F5513IZQE	MSP430F5519IPN	MSP430F5524IZQE	MSP430F5528IRGC
MSP430F5513IZQER	MSP430F5519IPNR	MSP430F5524IZQER	MSP430F5528IRGCR
MSP430F5514IRGC	MSP430F5521IPN	MSP430F5525IPN	MSP430F5528IRGCT
MSP430F5514IRGCR	MSP430F5521IPNR	MSP430F5525IPNR	MSP430F5528IZQE
MSP430F5514IRGCT	MSP430F5522IRGCR	MSP430F5526IRGC	MSP430F5528IZQER
MSP430F5514IZQE	MSP430F5522IRGCT	MSP430F5526IRGCR	MSP430F5529CY
MSP430F5514IZQER	MSP430F5522IZQE	MSP430F5526IRGCT	MSP430F5529IPN
MSP430F5515IPN	MSP430F5522IZQER	MSP430F5526IZQE	MSP430F5529IPNR
MSP430F5515IPNR	MSP430F5524IRGC	MSP430F5526IZQER	

For questions regarding this notice, inquiries should be directed to your local Field Sales Representative (FSE), your Field Application Engineer (FAE) or local Business Development Manager (BDM) or to the PCN contacts given below.

Location	E-Mail
USA	PCNAmericasContact@list.ti.com
Europe	PCNEuropeContact@list.ti.com
Asia Pacific	PCNAsiaContact@list.ti.com
Japan	PCNJapanContact@list.ti.com

Appendix A

MSP430F54xxA Device Derivatives
Technical Assessment: Flash Read Error & Susceptibility

Technical Assessment: Flash Read Error & Susceptibility

1 Overview

This document provides a description of the issue referred to as “Flash Read Error” impacting the current version of the MSP430F54xxA device derivatives. It also provides guidance in assessing whether and the extent to which the issue may affect a given application. Specific actions and customer recommendations are set forth in the accompanying PCN.

The flash read error results in the possibility that invalid data may be read from the Flash memory by the CPU. The issue is not related to Flash bit (cell) corruption: the Flash is valid as programmed. During Flash access, however, it is possible that data read out of the Flash by the CPU is corrupted. This may be undetected in the application with no ill effects; it could also result in an application error due to incorrect instruction execution or incorrect data fetch.

The root cause of the flash read error is understood and implementation of the fix within the Flash array has been completed. Device revisions incorporating this fix are currently in-process. For more information refer to the PCN.

The remainder of this document is intended to better describe the read error, how it can manifest within an application and recommendations for assessing the effects.

2 Affected devices

The flash read error affects the MSP430F54xxA device derivatives. The table below lists all affected devices by orderable part number and can also be found in the “Product Affected” section of the accompanying PCN.

Table 1. Affected Devices

MSP430F5418AIPN	MSP430F5435AIPNR	MSP430F5438ACY	MSP430BT5190IPZ
MSP430F5418AIPNR	MSP430F5436AIPZ	MSP430F5438ACYS	MSP430BT5190IPZR
MSP430F5419AIPZ	MSP430F5436AIPZR	MSP430F5438AIPZ	MSP430BT5190IZQWR
MSP430F5419AIPZR	MSP430F5436AIZQW	MSP430F5438AIPZR	MSP430BT5190IZQWT
MSP430F5419AIZQW	MSP430F5436AIZQWR	MSP430F5438AIZQW	
MSP430F5419AIZQWR	MSP430F5436AIZQWT	MSP430F5438AIZQWR	
MSP430F5419AIZQWT	MSP430F5437AIPN	MSP430F5438AIZQWT	
MSP430F5435AIPN	MSP430F5437AIPNR	MSP430F5438AGACYS	

Note: For all listed part numbers, affected silicon revisions are up to and including Revision “D”

3 Description

The flash read error is a read out of Flash memory by the CPU of certain data bits as a logic “1” when the actual value stored in the flash memory bit location is a logic “0”.

3.1 Bus architecture

To better describe the flash read error mechanism, it is important to understand the device architecture. The MSP430F54xxA implements a 32-bit cache for memory read operation – e.g. a physical read of the flash memory is performed on 32-bit boundaries; every 4 bytes, which is stored in a cache logic array. These 32-bit values are referred to as “double words”. Memory access by the CPU to individual bytes and words is then done by accessing the cache. This cache architecture is shown in Figure 1.

Note: The addresses used below are for example only and not intended to show specific susceptibility to the flash read error.

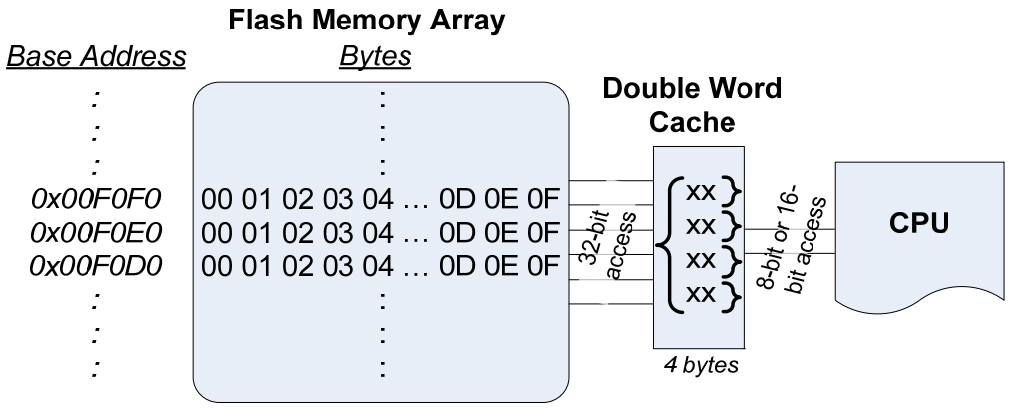

Figure 1. Simplified Cache Architecture and CPU Access

3.2 Affected Bits

The flash read error only affects the read access of the most significant bit (MSB) of each 32-bit Flash access by the cache. No other bit locations are affected. Each 31st bit location - i.e. the MSB of the 4th byte for each double word access, is susceptible to being read as “1” when it should be “0”. Bit locations for an entire 32-bit double word are defined as 0 to 31.

Furthermore, the issue only affects the 32-bit MSB when the flash bit is programmed as a “0”. In cases where the actual value stored is logic “1”, the bit will always read valid as logic “1” and is not susceptible to an invalid read.

Example: This illustration considers 16 bytes of flash data starting at address 0x0F0F0 and all contain the value 0x00. A CPU instruction execution triggers an access of the Flash word (at 0x0F0FE) and saves it to CPU register R5:

Instruction: `mov.w &0x0F0FEh, R5`

Result: Valid: R5= **0**000h
Invalid: R5= **8**000h

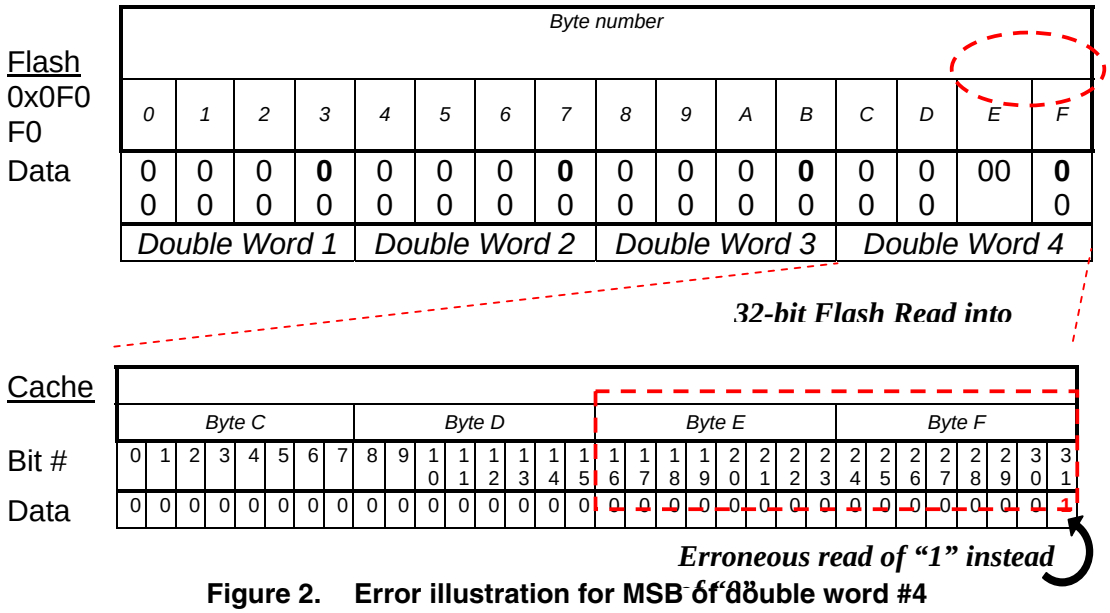

Figure 2. Error illustration for MSB of double word #4

The read operation by the CPU of address 0x0F0FE will actually trigger the reading of double word #4 from flash (data from 0x0F0FC to 0x0F0FF), which is then stored into the 32-bit cache. The uppermost two bytes (0x0F0FE and 0x0F0FF) make up the 16-bit word located at 0x0F0FE. The result of the read in the case of a flash read error is an invalid readout of the MSB for the given double word access. Instead of the expected logic "0", a logic "1" may be erroneously read out and stored in the cache for CPU computation: 0x8000 is erroneously read out and moved to R5 instead of 0x0000. This potential error applies to the MSB for each double word as indicated by the bold "**0**"s in Figure 2 at each 4th byte.

3.3 Affected memory locations

This flash read error is limited to specific memory locations for affected devices. MSP430F54xxA device derivative flash memory organization is based on 4 banks. Each bank can be up to 64KB in size and are combined to create the different device memory configurations. Table 2 sets forth each device's memory configuration and affected banks.

Table 2. Affected Flash memory locations for MSP430F54xxA device derivatives

		MSP430F5419A ***MSP430F5418A***	***MSP430F5436A*** ***MSP430F5435A***	***MSP430F5438A*** ***MSP430F5437A*** ***MSP430BT5190***
Memory (flash)	*Total Size*	*128 KB*	*192 KB*	*256 KB*
Main: code memory	*Flash range*	*025BFFh-005C00h*	*035BFFh-005C00h*	*045BFFh-005C00h*
Main: code memory	Bank 3	N/A	23 KB 035BFFh-030000h	64 KB 03FFFFh-030000h
	Bank 2	**23 KB** **025BFFh-020000h**	**64 KB** **02FFFFh-020000h**	**64 KB** **02FFFFh-020000h**

Bank 1	64 KB 01FFFFh-010000h	64 KB 01FFFFh-010000h	64 KB 01FFFFh-010000h
Bank 0	**41 KB 00FFFFh- 005C00h**	**41 KB 00FFFFh- 005C00h**	**64 KB 045BFFh-040000h 00FFFFh- 005C00h**

	affected
	not affected

Only banks 0 and 2 are susceptible to the flash read error as highlighted. Within these banks, the MSB locations for each double word can read out incorrectly when programmed as "0". Flash program and data stored within banks 1 and 3, independent of the value, will always be accessed correctly and are not susceptible to this issue.

3.4 Affected Flash IDLE time

Further narrowing the scope of this issue, this flash read error only affects the first flash access that occurs after some period of time during which no flash accesses have occurred. This time of no flash access prior to the first flash read is referred to as the "IDLE" time. Double word reads from flash following the first read after a defined IDLE time are not subject to the flash read error and will be accessed correctly by the cache when the CPU clock is running at a frequency above 10kHz.

Testing has shown that when the device is operating at 30°C the IDLE time, beyond which the read error may occur, is typically 15 msec. Any read of an affected bit after an IDLE time that exceeds 15 msec at 30°C is potentially susceptible to this issue. This IDLE time reduces to 0.5 msec typical at 85°C. When flash access has been inactive for longer than this IDLE time the issue can occur on the first double word read upon resuming access to the flash.

4 Application effects

The way in which a given application may be affected if the flash read error occurs is dependent upon what the corrupted data accessed is intended to be used for. This section outlines the basic ways in which the read error can manifest into improper device functionality.

The first instance at which the flash read error may occur is at device power-up. Flash will be accessed by the CPU at the location containing the factory programmed bootcode. The bootcode is always executed after a BOR and loads factory stored calibration values and assesses the BSL configuration. If the flash read error occurs at this point, the access to start the bootcode is invalid and the device will enter a LPM4-like state without beginning user code execution, requiring reset or power cycle to restart.

Resetting the device via the RST pin can also be affected by the flash read error. When RST is asserted flash access will stop. When the assertion time of the RST signal is longer than the IDLE time discussed in section 3.4, the first flash access after RST is released can be affected. In this case, because a reset assertion triggers execution of the bootcode, the result is identical to that stated for the power-up scenario- if the flash read error occurs the access to start the bootcode is invalid and the device will enter a LPM4-like state without beginning user code execution, requiring reset or power cycle to restart.

After the device has properly powered up, the flash read error can occur during flash access through CPU instruction execution – e.g. active mode operation. This typically occurs only after flash access has been IDLE for a time greater than the IDLE time discussed in section 3.4. Operation usage for this to occur in-application can be illustrated into four use-cases: (i) entering and exiting LPMx modes from Flash, (ii) switching between active operation from RAM and Flash, (iii) using while(1) and (iv) using the DMA.

4.1 Low Power Mode (LPMx) Use

A commonly used feature of the MSP430 that results in periods of flash access inactivity is the low power mode operation of the CPU. When using any of the LPMx modes built into the MSP430 architecture flash access is halted until the CPU is awakened via interrupt. Waking on any interrupt resumes active mode operation and consequently flash access for program execution.

When any low power mode is entered for a time that exceeds the IDLE time discussed in section 3.4, the first flash access made after that time can be affected by the read error. This will occur through the servicing of any enabled interrupt source. The first flash access made when an interrupt occurs is the access to fetch the 16-bit address pointer stored at the given ISR (interrupt service routine) vector location in flash. Table 3 shows the ISR vector location for each interrupt source in the affected device derivatives and highlights potentially affected ISR vector locations.

Table 3. MSP430F54xxA Device Derivative Interrupt Vector Addresses

INTERRUPT SOURCE	WORD ADDRESS	Lower Byte	Upper Byte	
System Reset *(e.g. Power-Up, RST, WDT Timeout)*	0FFFEh	0FFFEh	***0FFFFh***	*32-bit Double Word*
System NMI *(e.g. PMM, Vacant Memory Access)*	0FFFCh	0FFFCh	0FFFDh	
User NMI *(e.g. OSC Fault, Flash Access Violation)*	0FFFAh	0FFFAh	***0FFFBh***	*32-bit Double Word*
TB0	0FFF8h	0FFF8h	0FFF9h	
TB0 Watchdog Timer *(Interval Mode)*	0FFF6h 0FFF4h	0FFF6h 0FFF4h	***0FFF7h*** 0FFF5h	*32-bit Double Word*
USCI_A0 Receive/Transmit	0FFF2h	0FFF2h	***0FFF3h***	*32-bit Double*

USCI_B0 Receive/Transmit	0FFF0h	0FFF0h	0FFF1h	*Word*
ADC12_A	0FFEEh	0FFEEh	***0FFEFh***	*32-bit Double*
TA0	0FFECh	0FFECh	0FFEDh	*Word*
TA0	0FFEAh	0FFEAh	***0FFEBh***	*32-bit Double*
USCI_A2 Receive/Transmit	0FFE8h	0FFE8h	0FFE9h	*Word*
USCI_B2 Receive/Transmit	0FFE6h	0FFE6h	***0FFE7h***	*32-bit Double*
DMA	0FFE4h	0FFE4h	0FFE5h	*Word*
TA1	0FFE2h	0FFE2h	***0FFE3h***	*32-bit Double*
TA1	0FFE0h	0FFE0h	0FFE1h	*Word*
I/O Port P1	0FFDEh	0FFDEh	***0FFDFh***	*32-bit Double*
USCI_A1 Receive/Transmit	0FFDCh	0FFDCh	0FFDDh	*Word*
USCI_B1 Receive/Transmit	0FFDAh	0FFDAh	***0FFDBh***	*32-bit Double*
USCI_A3 Receive/Transmit	0FFD8h	0FFD8h	0FFD9h	*Word*
USCI_B3 Receive/Transmit	0FFD6h	0FFD6h	***0FFD7h***	*32-bit Double*
I/O Port P2	0FFD4h	0FFD4h	0FFD5h	*Word*
RTC_A	0FFD2h	0FFD2h	***0FFD3h***	*32-bit Double*
Reserved	0FFD0h	0FFD0h	0FFD1h	*Word*

0FFxxh *– Susceptible address*

Interrupt vector addresses highlighted in Table 3 are susceptible to the flash read error. When the CPU wakes to service a susceptible ISR after the IDLE time discussed in section 3.4 has been exceeded in any LPMx mode, the MSB of the upper affected byte may be corrupted as a “1”. If this occurs the CPU will vector to a location that is not the valid start address for the given ISR and potentially execute code erroneously.

4.2 CPU code execution from RAM and Flash

In applications where the CPU is redirected in user code to execute from RAM instead of flash, the read error can occur upon resumption of flash access; either program or data access within the flash memory range. Code executed from RAM that does not make any flash accesses for a time exceeding the IDLE time discussed in section 3.4 can be subject to the flash read error once flash access resumes, causing an invalid data or instruction fetch to occur. In cases where interrupts are also active while code is executed from RAM, the same scenarios may apply as outlined in section 4.1.

4.3 while(1) use (also JMP$ in assembly)

Use of while(1) in C (which corresponds to the assembly equivalent `JMP$`; e.g. “jump to self”) can result in flash IDLE times even though the CPU is active. This is due to the manner in which the CPU and cache operate and the placement of the JMP$ instruction within flash.

Such operation may be affected by the flash read error depending on memory position of the JMP$ instruction. The read error is possible when the JMP$ instruction resides in the lower word of a double word fetch from flash allowing execution to happen completely from cache turning off flash access. In this case, when the execution of the JMP$ exceeds the IDLE time discussed in section 3.4 prior to servicing an interrupt, the device is susceptible to the flash read error with the next ISR service and the same scenarios outline in section 4.1 may apply.

Figure 3 shows the relationship of the JMP$ instruction position in memory and the behavior of the Flash access. On the right, the JMP$ is at the lower word of the double word fetched from flash. This placement results in the CPU being able to execute entirely from the cached double word containing the JMP$ instruction which stops flash access activity. Execution of the JMP$ in such a memory alignment for a time exceeding the IDLE time discussed in section 3.4 can result in a read error on the next flash access – e.g. servicing an active ISR.

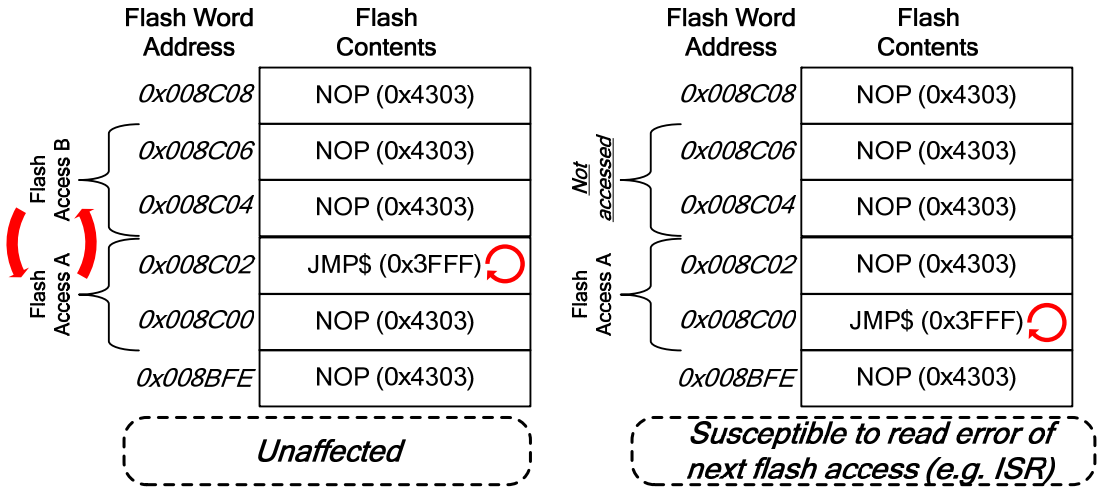

Figure 3. JMP$ alignment and read error behavior

However, when the `JMP$` instruction resides in the upper word of the double word memory fetch, as shown in the left portion of Figure 3, the cache continuously alternates between flash accesses A and B which keeps the flash access constant and unaffected by the read error on a subsequent ISR service fetch.

4.4 DMA Use

The DMA can be used to read data from flash without any CPU activity and accesses the cache in the same way to make Flash accesses. DMA access can be configured to read flash and is triggered independently of any interrupt activity (e.g. Timers, ADC, USCI). When the DMA is configured to read from flash upon receiving a given trigger, the first read of flash may be affected by the read error when the IDLE time discussed in section 3.4 is exceeded.

5 Influencing factors

There are numerous factors that influence the likelihood of the flash read error occurring during application operation. One factor is the operating temperature of the device and IDLE time of the flash as discussed in section 3.4. Table 4 summarizes the typical IDLE time durations beyond which the flash read error becomes more likely to occur.

Table 4. Flash IDLE time (t_IDLE) variation with temperature

Temperature [°C]	Idle Time Typical [ms]
25	15
85	0.5

APPENDIX A

External supply voltage (DVcc. AVcc) and internal core voltage (Vcore) also have an influence on likelihood of whether the flash read error may occur. Figure 5 shows Vcc vs System (CPU) clock vs Vcore valid operating conditions per the device datasheet.

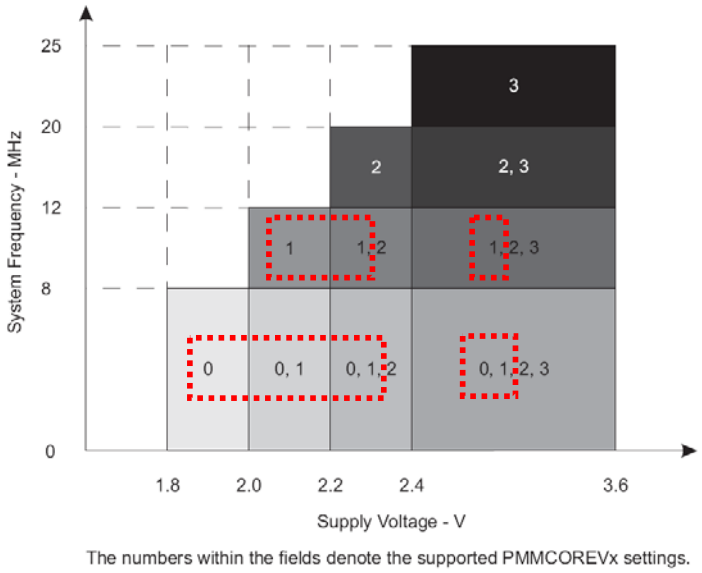

Figure 4. Core voltage settings with reduced susceptibility

The Vcore settings 0 and 1 and corresponding operating ranges are highlighted in the figure. These Vcore level settings result in reduced susceptibility to the flash read issue vs levels 2 and 3.

While all Vcore settings when used under the proper Vcc and clock frequency ranges are valid for device operation, usage of Vcore level 2 and 3 settings are twice as likely to result in flash read errors at susceptible bit locations compared to levels 0 and 1.

An additional influence on the likelihood of the flash read error occurring is process variation during fabrication of the devices. These variations are not detectable directly by the user but can result in variation of flash read error failure rates seen in production and the field.

6 Application analysis

The following checklist highlights specific areas to assess within a given application to determine if the conditions previously outlined are present. It is not intended to be a complete list and sound judgment should be used in analyzing any specific application. All items should be considered independently.

☐ Is the longest time the CPU spends in any LPM mode (CPUOFF) or executing code from RAM > the applicable t_IDLE at the expected operating temperature of the device (see Table 4 and section 3.4)?

- If no, the read error typically will not affect runtime operation

☐ Is while(1)/`JMP$` being used?

- If yes, does the disassembled `JMP$` (jump to self) instruction reside in the lower word of a 32-bit aligned double word in Flash?
  - If yes, is the time spent executing the while(1) > the applicable t_IDLE at the expected operating temperature of the device?
  - If no applies to any of the above questions, the read error typically will not affect runtime operation

☐ Is the DMA used to access affected flash source addresses as defined in Table 2?

- If no, the DMA susceptibility does not apply

☐ Are the Flash memory banks affected (see Table 2) by read error used in the application (for program or data)?

- If no, the read error will not affect runtime operation

Note: The interrupt vector address fetch locations reside in BANK0 which is affected. See the next checklist item.

☐ Are susceptible ISR vector address locations highlighted in Table 3 serviced after a time > the applicable t_IDLE at the expected operating temperature of the device?

- If no, the read error typically will not affect runtime operation

☐ If used do the 16-bit values at the ISR vector address locations highlighted as susceptible in Table 3 contain a “0” in the MSB?

- If no, the read error will not affect valid interrupt vector fetching of these ISRs
- For applications that exceed the applicable t_IDLE idle time at the expected operating temperature of the device while in LPM modes, RAM execution or while(1) from an affected address AND wake to interrupts:
  - The interrupts that exit the given mode if at the affected addresses in Table 3 and containing an MSB = 1, will not be affected by the flash read error .

7 Application robustness

While it is not possible to completely eliminate the possibility of flash read error occurrence under all application use cases, there are steps that one can take to reduce susceptibility in instances in which changes to application functionality are acceptable.

Operating the device at an internal core voltage level 0 or 1 can reduce the likelihood of flash read error occurrence by as much as 50% versus operation at level 2 and level 3.

APPENDIX A

Reducing IDLE time between flash accesses as low as possible will reduce the likelihood of flash read error occurring. Temperature range of the application should be taken into account given the variation on IDLE time relation to temperature.

Manual placement of interrupt service routines into memory locations above 0x008000 can eliminate the effect on interrupt vector address fetches. When ISR locations cannot be manipulated, limiting interrupt wakeup to peripheral interrupt vectors that are fetched from addresses unaffected by the flash read error can also be leveraged to wake from extended IDLE times between flash accesses properly.

Manual placement of all user code and data into memory locations within banks 1 and/or 3 eliminate the possibility that the flash read error affects this code.

To minimize the potential of encountering the flash read error effects upon reset of the device, issuance of 2 external reset pulses externally to the RST pin where the duration of each low reset pulse and the time between pulses is less than the IDLE time discussed in section 3.4 is an effective methodology.

Production testing at the maximum specified temperature for the given application will provide the worst-case corner for occurrence of the flash read error. In addition, subjecting the application to expected operating conditions resulting in worst-case flash IDLE time duration will also enhance the likelihood of flash read error occurrence. While this exercise will not assure all potentially affected devices will be detected it is the most effective means to increase probability of detection.

8 Summary

The information in this document provides the reader with information that can be applied to assessing the susceptibility of an application to the flash read error described herein. In addition to the information presented here, the performance of the application being assessed should also be considered as an important data point in determining risk. Occurrence or not of failures in the field or at production of a given end equipment serve as an additional indicator of robustness and the likelihood of an application to flash read susceptibility.

APPENDIX A

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and applications using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI products or services with statements different from or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

TI products are not authorized for use in safety-critical applications (such as life support) where a failure of the TI product would reasonably be expected to cause severe personal injury or death, unless officers of the parties have executed an agreement specifically governing such use. Buyers represent that they have all necessary expertise in the safety and regulatory ramifications of their applications, and acknowledge and agree that they are solely responsible for all legal, regulatory and safety-related requirements concerning their products and any use of TI products in such safety-critical applications, notwithstanding any applications-related information or support that may be provided by TI. Further, Buyers must fully indemnify TI and its representatives against any damages arising out of the use of TI products in such safety-critical applications.

TI products are neither designed nor intended for use in military/aerospace applications or environments unless the TI products are specifically designated by TI as military-grade or "enhanced plastic." Only products designated by TI as military-grade meet military specifications. Buyers acknowledge and agree that any such use of TI products which TI has not designated as military-grade is solely at the Buyer's risk, and that they are solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI products are neither designed nor intended for use in automotive applications or environments unless the specific TI products are designated by TI as compliant with ISO/TS 16949 requirements. Buyers acknowledge and agree that, if they use any non-designated products in automotive applications, TI will not be responsible for any failure to meet such requirements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

Products		**Applications**	
Amplifiers	amplifier.ti.com	Audio	www.ti.com/audio
Data Converters	dataconverter.ti.com	Automotive	www.ti.com/automotive
DLP® Products	www.dlp.com	Communications and Telecom	www.ti.com/communications
DSP	dsp.ti.com	Computers and Peripherals	www.ti.com/computers
Clocks and Timers	www.ti.com/clocks	Consumer Electronics	www.ti.com/consumer-apps
Interface	interface.ti.com	Energy	www.ti.com/energy
Logic	logic.ti.com	Industrial	www.ti.com/industrial
Power Mgmt	power.ti.com	Medical	www.ti.com/medical
Microcontrollers	microcontroller.ti.com	Security	www.ti.com/security
RFID	www.ti-rfid.com	Space, Avionics & Defense	www.ti.com/space-avionics-defense
RF/IF and ZigBee® Solutions	www.ti.com/lprf	Video and Imaging	www.ti.com/video
		Wireless	www.ti.com/wireless-apps

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265

APPENDIX A

APPENDIX A

Appendix B

MSP430F55xx Device Derivatives
Technical Assessment: Flash Read Error & Susceptibility

Technical Assessment: Flash Read Error & Susceptibility

1 Overview

This document provides a description of the issue referred to as “Flash Read Error” impacting the current version of the MSP430F55xx device derivatives. It also provides guidance in assessing whether and the extent to which the issue may affect a given application. Specific actions and customer recommendations are set forth in the accompanying PCN.

The flash read error results in the possibility that invalid data may be read from the Flash memory by the CPU. The issue is not related to Flash bit (cell) corruption: the Flash is valid as programmed. During Flash access, however, it is possible that data read out of the Flash by the CPU is corrupted. This may be undetected in the application with no ill effects; it could also result in an application error due to incorrect instruction execution or incorrect data fetch.

The root cause of the flash read error is understood and implementation of the fix within the Flash array has been completed. Device revisions incorporating this fix are currently in-process. For more information refer to the PCN.

The remainder of this document is intended to better describe the read error, how it can manifest within an application and recommendations for assessing the effects.

2 Affected devices

The flash read error affects the MSP430F55xx device derivatives. The table below lists all affected devices by orderable part number and can also be found in the “Product Affected” section of the accompanying PCN.

Table 5. Affected Devices

MSP430F5513IRGCR	MSP430F5517IPN	MSP430F5524IRGCR	MSP430F5527IPN
MSP430F5513IRGCT	MSP430F5517IPNR	MSP430F5524IRGCT	MSP430F5527IPNR
MSP430F5513IZQE	MSP430F5519IPN	MSP430F5524IZQE	MSP430F5528IRGC
MSP430F5513IZQER	MSP430F5519IPNR	MSP430F5524IZQER	MSP430F5528IRGCR
MSP430F5514IRGC	MSP430F5521IPN	MSP430F5525IPN	MSP430F5528IRGCT
MSP430F5514IRGCR	MSP430F5521IPNR	MSP430F5525IPNR	MSP430F5528IZQE
MSP430F5514IRGCT	MSP430F5522IRGCR	MSP430F5526IRGC	MSP430F5528IZQER
MSP430F5514IZQE	MSP430F5522IRGCT	MSP430F5526IRGCR	MSP430F5529CY
MSP430F5514IZQER	MSP430F5522IZQE	MSP430F5526IRGCT	MSP430F5529IPN
MSP430F5515IPN	MSP430F5522IZQER	MSP430F5526IZQE	MSP430F5529IPNR
MSP430F5515IPNR	MSP430F5524IRGC	MSP430F5526IZQER	

Note: For all listed part numbers, affected silicon revisions are up to and including Revision “D”

3 Description

The flash read error is a read out of Flash memory by the CPU of certain data bits as a logic “1” when the actual value stored in the flash memory bit location is a logic “0”.

3.1 Bus architecture

To better describe the flash read error mechanism, it is important to understand the device architecture. The MSP430F55xx implements a 32-bit cache for memory read operation – e.g. a physical read of the flash memory is performed on 32-bit boundaries; every 4 bytes, which is stored in a cache logic array. These 32-bit values are referred to as “double words”. Memory access by the CPU to individual bytes and words is then done by accessing the cache. This cache architecture is shown in Figure 1.

Note: The addresses used below are for example only and not intended to show specific susceptibility to the flash read error.

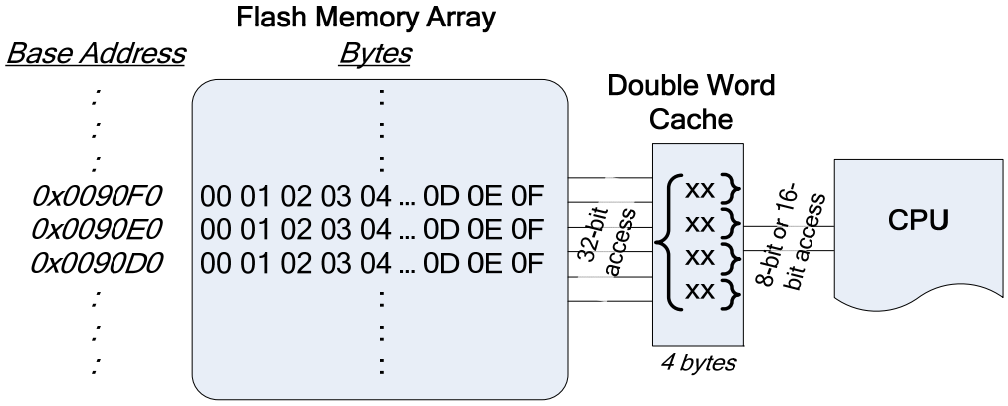

Figure 5. Simplified Cache Architecture and CPU Access

3.2 Affected Bits

The flash read error only affects the read access of the next-to-last most significant bit (MSB-1) of each 32-bit Flash access by the cache. No other bit locations are affected. Each 30th bit location - i.e. the MSB-1 of the 4th byte for each double word access, is susceptible to being read as “1” when it should be “0”. Bit locations for an entire 32-bit double word are defined as 0 to 31.

Furthermore, the issue only affects the 32-bit MSB-1 when the flash bit is programmed as a “0”. In cases where the actual value stored is logic “1”, the bit will always read valid as logic “1” and is not susceptible to an invalid read.

Example: This illustration considers 16 bytes of flash data starting at address 0x090F0 and all contain the value 0x00. A CPU instruction execution triggers an access of the Flash word (at 0x090FE) and saves it to CPU register R5:

Instruction: `mov.w &0x090FEh, R5`

Result: Valid: R5= **0**000h
Invalid: R5= **4**000h

APPENDIX B

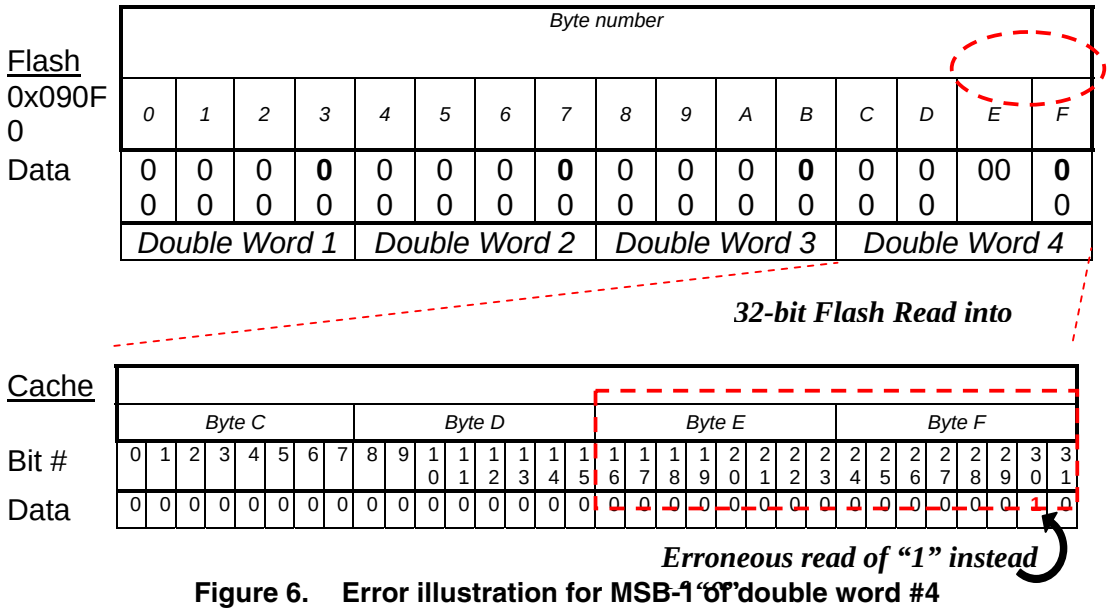

Figure 6. Error illustration for MSB-1 of double word #4

The read operation by the CPU of address 0x090FE will actually trigger the reading of double word #4 from flash (data from 0x090FC to 0x090FF), which is then stored into the 32-bit cache. The uppermost two bytes (0x090FE and 0x090FF) make up the 16-bit word located at 0x090FE. The result of the read in the case of a flash read error is an invalid readout of the MSB-1 for the given double word access. Instead of the expected logic "0", a logic "1" may be erroneously read out and stored in the cache for CPU computation: 0x4000 is erroneously read out and moved to R5 instead of 0x0000. This potential error applies to the MSB-1 for each double word as indicated by the bold "**0**"s in Figure 2 at each 4th byte.

3.3 Affected memory locations

This flash read error is limited to specific memory locations for affected devices. MSP430F55xx device derivative flash memory organization is based on 4 banks. Each bank can be up to 32KB in size and are combined to create the different device memory configurations. Table 2 sets forth each device's memory configuration and affected banks.

Table 6. Affected Flash memory locations for MSP430F55xx device derivatives

		MSP430F5522 MSP430F5521 MSP430F5513	***MSP430F5525 MSP430F5524 MSP430F5515 MSP430F5514***	***MSP430F5527 MSP430F5526 MSP430F5517***	***MSP430F5529 MSP430F5528 MSP430F5519***
Memory (flash)	*Total Size*	*32 KB*	*64 KB*	*96 KB*	*128 KB*
Main: code memory	*Flash Range*	*00FFFFh-008000h*	*0143FFh-004400h*	*01C3FFh-004400h*	*0243FFh-004400h*
Main: code memory	Bank 3	N/A	N/A	N/A	32 KB 0243FFh-01C400h
	Bank 2	**N/A**	**N/A**	**32 KB 01C3FFh-014400h**	**32 KB 01C3FFh-014400h**
	Bank 1	15 KB 00FFFFh-00C400h	32 KB 0143FFh-00C400h	32 KB 0143FFh-00C400h	32 KB 0143FFh-00C400h
	Bank 0	**17 KB 00C3FFh-008000h**	**32 KB 00C3FFh-004400h**	**32 KB 00C3FFh-004400h**	**32 KB 00C3FFh-004400h**

	affected
	not affected

Only banks 0 and 2 are susceptible to the flash read error as highlighted. Within these banks, the MSB-1 locations for each double word can read out incorrectly when programmed as “0”. Flash program and data stored within banks 1 and 3, independent of the value, will always be accessed correctly and are not susceptible to this issue.

3.4 Affected Flash IDLE time

Further narrowing the scope of this issue, this flash read error only affects the first flash access that occurs after some period of time during which no flash accesses have occurred. This time of no flash access prior to the first flash read is referred to as the “IDLE” time. Double word reads from flash following the first read after a defined IDLE time are not subject to the flash read error and will be accessed correctly by the cache when the CPU clock is running at a frequency above 10kHz.

Testing has shown that when the device is operating at 30°C the IDLE time, beyond which the read error may occur, is typically 15 msec. Any read of an affected bit after an IDLE time that exceeds 15 msec at 30°C is potentially susceptible to this issue. This IDLE time reduces to 0.5 msec typical at 85°C. When flash access has been inactive for longer than this IDLE time the issue can occur on the first double word read upon resuming access to the flash.

4 Application effects

The way in which a given application may be affected if the flash read error occurs is dependent upon what the corrupted data accessed is intended to be used for. This section outlines the basic ways in which the read error can manifest into improper device functionality.

The first instance at which the flash read error may occur is at device power-up. Flash will be accessed by the CPU at the location containing the factory programmed bootcode. The bootcode is always executed after a BOR and loads factory stored calibration values and assesses the BSL configuration. If the flash read error occurs at this point, the access to start the bootcode is invalid and the device will enter a LPM4-like state without beginning user code execution, requiring reset or power cycle to restart.

Resetting the device via the RST pin can also be affected by the flash read error. When RST is asserted flash access will stop. When the assertion time of the RST signal is longer than the IDLE time discussed in section 3.4, the first flash access after RST is released can be affected. In this case, because a reset assertion triggers execution of the bootcode, the result is identical to that stated for the power-up scenario- if the flash read error occurs the access to start the bootcode is invalid and the device will enter a LPM4-like state without beginning user code execution, requiring reset or power cycle to restart.

After the device has properly powered up, the flash read error can occur during flash access through CPU instruction execution – e.g. active mode operation. This typically occurs only after flash access has been IDLE for a time greater than the IDLE time discussed in section 3.4. Operation usage for this to occur in-application can be illustrated into four use-cases: (i) entering and exiting LPMx modes from Flash, (ii) switching between active operation from RAM and Flash, (iii) using while(1) and (iv) using the DMA.

4.1 Low Power Mode (LPMx) Use

A commonly used feature of the MSP430 that results in periods of flash access inactivity is the low power mode operation of the CPU. When using any of the LPMx modes built into the MSP430 architecture flash access is halted until the CPU is awakened via interrupt. Waking on any interrupt resumes active mode operation and consequently flash access for program execution.

Important to highlight is that all interrupt vector addresses for the MSP430F55xx device derivatives exist in the address range 0x0FF80 to 0x0FFFE. These flash locations are in bank 1 of flash as shown in Table 2 and are therefore not affected by the flash read error.

The first flash access made when an interrupt occurs is the access to fetch the 16-bit address pointer stored at the given ISR (interrupt service routine) vector location in flash. Given that these locations are in bank 1 and unaffected, servicing of the ISR and subsequent code execution by the CPU will not be affected by the flash read error, independent of the IDLE time of the flash prior to the ISR service.

4.2 CPU code execution from RAM and Flash

In applications where the CPU is redirected in user code to execute from RAM instead of flash, the read error can occur upon resumption of flash access; either program or data access within the flash memory range. Code executed from RAM that does not make any flash accesses for a time exceeding the IDLE time discussed in section 3.4 can be subject to the flash read error once flash access resumes, causing an invalid data or instruction fetch to occur. In cases where interrupts are also active while code is executed from RAM, flash access through servicing as the given ISR is not affected as outlined in section 4.1.

4.3 while(1) use (also JMP$ in assembly)

Use of while(1) in C (which corresponds to the assembly equivalent `JMP$`; e.g. “jump to self”) can result in flash IDLE times even though the CPU is active. This is due to the manner in which the CPU and cache operate and the placement of the JMP$ instruction within flash.

Figure 3 shows the relationship of the `JMP$` instruction position in memory and the behavior of the Flash access. On the right, the `JMP$` is at the lower word of the double word fetched from flash. This placement results in the CPU being able to execute entirely from the cached double word containing the `JMP$` instruction which stops flash access activity.

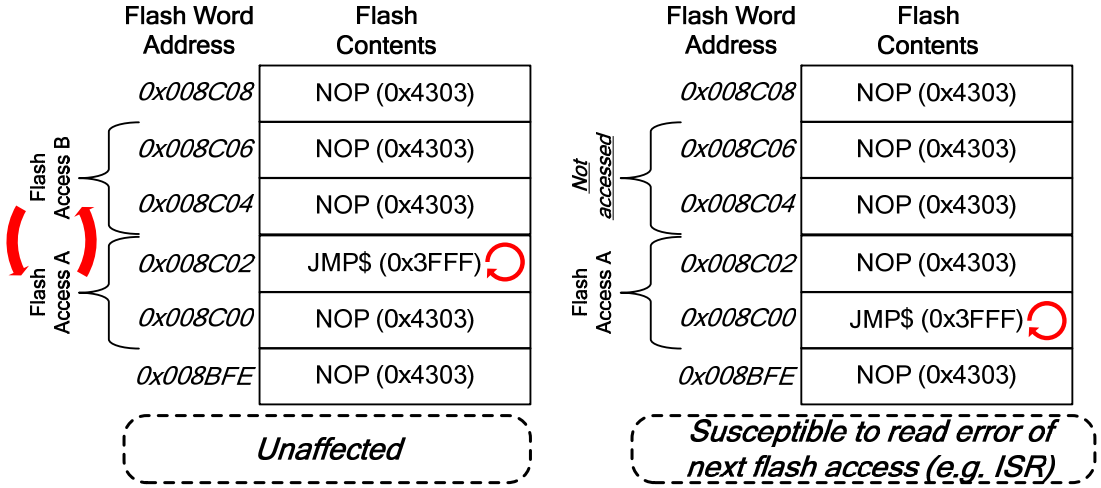

Figure 7. JMP$ alignment and read error behavior

When the `JMP$` instruction resides in the upper word of the double word memory fetch, as shown in the left portion of Figure 3, the cache continuously alternates between flash accesses A and B which keeps the flash access constant.

It is assumed that when using a while(1) program flow, interrupts are active. Given that the interrupt vector address locations are in bank 1 and unaffected, servicing of the ISR and subsequent code execution by the CPU will not be affected by the flash read error. This results in usage of while(1) being unaffected by the flash read error.

4.4 DMA Use

The DMA can be used to read data from flash without any CPU activity and accesses the cache in the same way to make Flash accesses. DMA access can be configured to read flash and is triggered independently of any interrupt activity (e.g. Timers, USB, ADC, USCI). When the DMA is configured to read from flash upon receiving a given trigger, the first read of flash may be affected by the read error when the IDLE time discussed in section 3.4 is exceeded.

5 Influencing factors

There are numerous factors that influence the likelihood of the flash read error occurring during application operation. One factor is the operating temperature of the device and IDLE time of the flash as discussed in section 3.4. Table 3 summarizes the typical IDLE time durations beyond which the flash read error becomes more likely to occur.

Table 7. Flash IDLE time (t_IDLE) variation with temperature

Temperature [°C]	Idle Time Typical [ms]
25	15
85	0.5

External supply voltage (DVcc. AVcc) and internal core voltage (Vcore) also have an influence on likelihood of whether the flash read error may occur. Figure 5 shows Vcc vs System (CPU) clock vs Vcore valid operating conditions per the device datasheet.

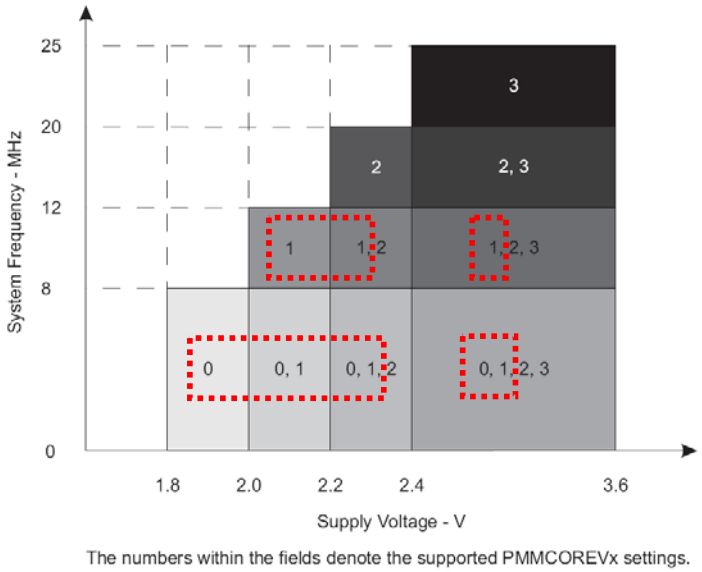

Figure 8. Core voltage settings with reduced susceptibility

The Vcore settings 0 and 1 and corresponding operating ranges are highlighted in the figure. These Vcore level settings result in reduced susceptibility to the flash read issue vs levels 2 and 3.

While all Vcore settings when used under the proper Vcc and clock frequency ranges are valid for device operation, usage of Vcore level 2 and 3 settings are twice as likely to result in flash read errors at susceptible bit locations compared to levels 0 and 1.

An additional influence on the likelihood of the flash read error occurring is process variation during fabrication of the devices. These variations are not detectable directly by the user but can result in variation of flash read error failure rates seen in production and the field.

6 Application analysis

The following checklist highlights specific areas to assess within a given application in order to determine if the conditions previously outlined are present. It is not intended to be a complete list and sound judgment should be used for analyzing a specific application based on the information provided in this document. All items below should be considered independently.

- ☐ Is the longest time the CPU spends executing code from RAM > the applicable t_IDLE at the expected operating temperature of the device (see Table 3 and section 3.4)?
  - o If no, the read error typically will not affect runtime operation
- ☐ Are the Flash memory banks affected (see Table 2) by read error used in the application (for program or data)?
  - o If no, the read error will not affect runtime operation
- ☐ Is the DMA used to access affected flash source addresses as defined in Table 2?
  - o If no, the DMA susceptibility does not apply

7 Application robustness

While it is not possible to completely eliminate the possibility of flash read error occurrence under all application use cases, there are steps that one can take to reduce susceptibility in instances in which changes to application functionality are acceptable.

Operating the device at an internal core voltage level 0 or 1 can reduce the possibility of flash read error occurrence by as much as 50% versus operation at level 2 and level 3.

Reducing IDLE time between flash accesses as low as possible will reduce the likelihood of flash read error occurring. Temperature range of the application should be taken into account given the variation on IDLE time relation to temperature.

Manual placement of all user code and data into memory locations within banks 1 and/or 3 eliminate the possibility that the flash read error affects this code.

To minimize the potential of encountering flash read error effects upon reset of the device, issuance of 2 external reset pulses externally to the RST pin where the duration of each low reset pulse and the time between pulses is less than the IDLE time discussed in section 3.4 is an effective methodology.

Production testing at the maximum specified temperature for the given application will provide the worst-case corner for occurrence of the flash read error. In addition, subjecting the application to expected operating conditions resulting in worst-case flash IDLE time duration will also enhance the likelihood of flash read error occurrence. While this exercise will not assure all potentially affected devices will be detected it is the most effective means to increase probability of detection.

8 Summary

The information in this document provides the reader with information that can be applied to assessing the susceptibility of an application to the flash read error described herein. In addition to the information presented here, the performance of the application being assessed should also be considered as an important data point in determining risk. Occurrence or not of failures in the field or at production of a given end equipment serve as an additional indicator of robustness and the likelihood of an application to flash read error susceptibility.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and applications using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI products or services with statements different from or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

TI products are not authorized for use in safety-critical applications (such as life support) where a failure of the TI product would reasonably be expected to cause severe personal injury or death, unless officers of the parties have executed an agreement specifically governing such use. Buyers represent that they have all necessary expertise in the safety and regulatory ramifications of their applications, and acknowledge and agree that they are solely responsible for all legal, regulatory and safety-related requirements concerning their products and any use of TI products in such safety-critical applications, notwithstanding any applications-related information or support that may be provided by TI. Further, Buyers must fully indemnify TI and its representatives against any damages arising out of the use of TI products in such safety-critical applications.

TI products are neither designed nor intended for use in military/aerospace applications or environments unless the TI products are specifically designated by TI as military-grade or "enhanced plastic." Only products designated by TI as military-grade meet military specifications. Buyers acknowledge and agree that any such use of TI products which TI has not designated as military-grade is solely at the Buyer's risk, and that they are solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI products are neither designed nor intended for use in automotive applications or environments unless the specific TI products are designated by TI as compliant with ISO/TS 16949 requirements. Buyers acknowledge and agree that, if they use any non-designated products in automotive applications, TI will not be responsible for any failure to meet such requirements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

Products		**Applications**	
Amplifiers	amplifier.ti.com	Audio	www.ti.com/audio
Data Converters	dataconverter.ti.com	Automotive	www.ti.com/automotive
DLP® Products	www.dlp.com	Communications and Telecom	www.ti.com/communications
DSP	dsp.ti.com	Computers and Peripherals	www.ti.com/computers
Clocks and Timers	www.ti.com/clocks	Consumer Electronics	www.ti.com/consumer-apps
Interface	interface.ti.com	Energy	www.ti.com/energy
Logic	logic.ti.com	Industrial	www.ti.com/industrial
Power Mgmt	power.ti.com	Medical	www.ti.com/medical
Microcontrollers	microcontroller.ti.com	Security	www.ti.com/security
RFID	www.ti-rfid.com	Space, Avionics & Defense	www.ti.com/space-avionics-defense
RF/IF and ZigBee® Solutions	www.ti.com/lprf	Video and Imaging	www.ti.com/video
		Wireless	www.ti.com/wireless-apps

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265