Mask Set Errata for 2P43B

1. Introduction

This report applies to mask 2P43B (**SILICONREV_ID = 0x000B0002**) for these products:

- MIMXRT595SFFOC
- MIMXRT555SFFOC
- MIMXRT533SFFOC
- MIMXRT595SFFOCR
- MIMXRT555SFFOCR
- MIMXRT533SFFOCR
- MIMXRT533SFAWCR
- MIMXRT555SFAWCR
- MIMXRT595SFAWCR

Table 1 Errata and Information Summary

Erratum ID	Erratum Title
ERR050638	ADC: ADC misses software trigger when there is no ADC clock
ERR011246	CortexM33- 937163C - Floating-point state can be incorrectly cleared on some exception return faults
ERR011247	CortexM33 - 1015127C :Processor might not wake up to a SEVONPEND event when in WIC-based WFE sleep
ERR050458	FlexIO: Shifter Status/Error flag not generated correctly in Logic Mode
ERR011377	FlexSPI: FlexSPI DLL lock status bit not accurate due to timing issue
ERR050610	FlexSPI: TX buffer fill / RX buffer drain by DMA with a single DMA descriptor cannot be performed
ERR050641	GPIO: During initial power-up, a brief pull-up pulse could occur on the port pins
ERR011439	MIPI DSI: Checksum is incorrect for DCS command long packet writes with zero-length data payload
ERR050799	Non-Secure Boot: ROM API initializes unused FlexSPI0 IO pins
ERR050716	Power Management: Leakage path between VDD1V8 and VDDIO_x
ERR050715	USBHSD: The detection handshaking fails when certain full-speed hubs are connected
ERR050739	USBHSD: Isochronous IN endpoint MaxPacketSize of 1024 byte limitation
ERR050742	USBHSH: Transaction limitation for isochronous IN endpoints in High-bandwidth mode

Table 2 Revision History

Revision	Changes
0	Initial Release
1	Added ERR050739 and ERR050742
2	Added ERR050799

2. ERR011246 CortexM33- 937163C - Floating-point state can be incorrectly cleared on some exception return faults

2.1. Description:

The Armv8-M architecture defines integrity checks which are performed before the exception return unstacking occurs.
These check the validity of the EXC_RETURN value and raise a fault if they fail. Because of this erratum it is possible for the floating-point state to be incorrectly cleared when one of these faults occurs.

Conditions
The floating-point state will be incorrectly cleared when all the following conditions are met:

1. One of the following exception return integrity checks fails:
   - SFSR.INVER.
   - UFSR.INVPC (exiting a handler that is not active).
   - UFSR.INVPC (EXC_RETURN[1]!=0).
   - SFSR.LSERR (when attempting to clear because of FPCCR.CLRONRET).
2. The floating-point state would have been unstacked if there had been no fault (that is, EXC_RETURN[4]==0, FPCCR.LSPACT==0 and access is permitted to the FPU).

Implications
The floating-point state can be incorrectly cleared if software causes one of the faults mentioned above. The scenario that could be problematic is when a Secure exception calls a Non-secure function, which in turn attempts to return from the exception. This erratum allows the Non-secure function to clear the Secure floating-point context. Note that doing so will always cause a Secure fault to be raised and no Secure state is ever leaked to Non-secure.

2.2. Workarounds:

This erratum is not expected to require a workaround.

2.3. Proposed solution

No fix scheduled.

3. ERR011247 CortexM33 - 1015127C :Processor might not wake up to a SEVONPEND event when in WIC-based WFE sleep

3.1. Description:

The Armv8-M architecture includes a feature which allows an event to be sent when an interrupt state changes from inactive to pending (SEVONPEND). The Cortex-M33 processor also includes a Wakeup Interrupt Controller (WIC) to enable the processor to enter a low-power state. Because of this erratum, when in WIC-based WFE sleep, it is possible that the processor will fail to wake up as expected because a pended interrupt does not generate the expected event.

Conditions
• WIC-based sleep enabled (SCR.SLEEPDEEP==1, WICENACK==1).
• Only one of the banked SCR.SEVONPEND bits is set.
• The processor enters WFE sleep in the security state where the associated banked SCR.SEVONPEND field is not set.

Implications
The WIC will not wake up to an event generated by a pending interrupt targeting the alternate security state where the associated SCR.SEVONPEND bit is 1. However, it is expected that a system will not be affected by this behavior since software cannot depend on a wake-up event controlled by the alternate security state.

3.2. Workarounds:

This erratum is not expected to require a workaround.

3.3. Proposed solution

No fix scheduled.

4. ERR011439 MIPI DSI: Checksum is incorrect for DCS command long packet writes with zero-length data payload

4.1. Description:

According to the MIPI DSI specification, long packets are comprised of a Packet Header and a payload of 0 to 2^16-1 bytes. For the special case of a zero-length payload, the specification requires the checksum must be set to 0xFFFF.

The MIPI DSI controller produces an incorrect checksum for DCS commands issued via long packets with zero length payloads in LP (DSI Low-Power mode). There is no such issue for similar commands issued in HP (DSI High-Power mode).

This issue should not affect normal application operation because packets with zero data length would normally be sent using the short packet format. However, since the MIPI DSI spec specifically states this behavior, MIPI DSI certification would fail on this issue.

4.2. Workarounds:

Use short packet format to send DCS commands with zero length data payloads.

4.3. Proposed solution

No fix scheduled.

5. ERR011377 FlexSPI: FlexSPI DLL lock status bit not accurate due to timing issue

5.1. Description:

After configuring DLL and the lock status bit is set, the data may be wrong if read/write immediately from FLEXSPI based external flash due to timing issue.

5.2. Workarounds:

Add delay time (100 NOP) again after the DLL lock status is set.

5.3. Proposed solution

No fix scheduled.

6. ERR050458 FlexIO: Shifter Status/Error flag not generated correctly in Logic Mode

6.1. Description:

Some shifters will not generate status or error flags correctly when configured for logic mode (SHIFTCTLn[SMOD] = 0b111). Shifters 0, 1, 2, and 3 behave correctly. All other shifters are affected.

6.2. Workaround:

In logic mode, if the Status/Error flags are required, use shifter 0, 1, 2, or 3. If the Status/Error flag is not required, then any shifter could be used in logic mode.

6.3. Proposed solution

No fix scheduled.

7. ERR050610 FlexSPI: TX buffer fill / RX buffer drain by DMA with a single DMA descriptor cannot be performed

7.1. Description:

Using FlexSPI register interface, you cannot perform TX buffer fill / RX buffer drain by DMA with a single DMA descriptor if the transfer size exceeds the FIFO watermark level.

7.2. Workaround:

The erratum requires a software workaround for maintaining a linked DMA descriptor array. The link array consumes about 2K RAM consumption to support the FLEXSPI TX watermark starting from 8 bytes.

7.3. Proposed solution

No fix scheduled.

8. ERR050638 ADC: ADC misses software trigger when there is no ADC clock

8.1. Description:

ADC command execution can be initiated from up to 16 trigger sources. Those triggers can be generated via either software or hardware. However, when using software triggers, the ADC will not properly capture this event when no ADC clock is present.

The following conditions will cause this behavior:

- System enters low power state (both bus and functional clocks get disabled)
- System receives a temporary wake up and the ADC bus clock starts process to start running
- ADC receives a software trigger before the functional ADC clock completed start up and misses the event

8.2. Workaround:

When no ADC clock is present, use only the hardware trigger functionality.

8.3. Proposed solution

No fix scheduled.

9. ERR050641 GPIO: During initial power-up, a brief pull-up pulse could occur on the port pins

9.1. Description:

By default (reset state), the GPIO pins are in the high Z state and typically stays high Z until the application code changes its state. The internal pull-up and internal pull-down resistors are disabled by default.

During VDDIO_x power-up, the internal pull-up resistor may not initialize during the early part of the VDDIO_x ramp-up, resulting in a brief pull-up current pulse on some port pins that drops to zero before the VDDIO_x supplies reach the minimum operating voltage. Except for GPIO with the high speed pads, all fail safe GPIOs are affected by this issue.

Typically, for a 20 ms power-up ramp, the pulse width of the glitch is approximately 8 ms and the amplitude is about 1.2V.

9.2. Workaround:

A pulldown resistor (~10K) can be added to the GPIO pin(s) to minimize the peak voltage where the application is sensitive to potential pulses.

9.3. Proposed solution

No fix scheduled.

10. ERR050715 USBHSD: The detection handshaking fails when certain full-speed hubs are connected

10.1. Description:

As a high-speed device, when certain full-speed hubs are connected, the USB device does not detect the HOST KJ sequence correctly and, as a result, does not recognize the speed of the connected host. In this case, the USB device can act erratically due to the wrong speed detection.

10.2. Workaround:

There are two workarounds:

1. The software workaround below can be implemented in usb_dev_hid_mouse where API is called "USB_DeviceHsPhyChirpIssueWorkaround()". In event handler in USB_DeviceCallback(),

– On "kUSB_DeviceEventBusReset" event, USB_DeviceHsPhyChirpIssueWorkaround() should be called to identify the speed of the host connected to. If full-speed host is connected or

"isConnectedToFsHostFlag" is set, FORCE_FS (bit 21) of DEVCMDSTAT register should be set to force the device operating in full-speed mode.

– On "kUSB_DeviceEventDetach" event, FORCE_FS (bit 21) of DEVCMDSTAT register should be cleared.

2. The software workaround below is available in tech note (TN00071) In event handler in USB_DeviceCallback(),

– On "kUSB_DeviceEventAttach" event, set PHY_RX register trip-level voltage to

the highest. USBPHY->RX &= ~(USBPHY_RX_ENVADJ_MASK);USBPHY->RX |= 2;.

– On "kUSB_DeviceEventBusReset" event, check the DEVCMDSTAT[SPEED] to determine the connected bus speed. (SPEED are bits 22 and 23). If DEVCMDSTAT[SPEED]=FS, FORCE_FS (bit 21) of DEVCMDSTAT should be set to force the device operating in full-speed mode.

– On "kUSB_DeviceEventGetDeviceDescriptor" event, or first SETUP packet has arrived, Set the USBPHY_RX[ENVADJ] field back to default 0. Otherwise, USBPHY_RX[ENVADJ] field will remain as 2 unless a disconnect event occurs.

– On "kUSB_DeviceEventDetach" event, Clear FORCE_FS (bit 21) of DEVCMDSTAT register to zero. Reset USBPHY_RX[ENVADJ] field back to default 0.

10.3. Proposed solution

No fix scheduled.

11. ERR050716 Power Management: Leakage path between VDD1V8 and VDDIO_x

11.1. Description:

The power sequencing specification in the datasheet mentions that the VDDIO_x rail can be optionally powered after the VDD1V8 and the delta voltage between VDDIO_x and VDD1V8 must be 1.89 V or less.

Before the VDDIO_x is powered, there is a leakage path between the VDD1V8 and VDDIO_x domain. The leakage is approximately 1.5 mA (VDD1V8 - VDDIO / 800 ohm). This leakage does not cause any reliability issues. There is no leakage once the VDDIO_x rail is above VDD1V8 - 0.4 V.

11.2. Workaround:

In order to avoid the leakage path, the VDDIO_x rail should not be powered after the VDD1V8.

11.3. Proposed solution

No fix scheduled.

12. ERR050739 USBHSD: Isochronous IN endpoint MaxPacketSize of 1024 byte limitation

12.1. Description:

The RT500 device family include a USB high-speed interface (USB1) that can operate in device mode at high-speed. The isochronous IN endpoint supports a MaxPacketSize of 1024 bytes.

When device isochronous IN endpoint sends a packet of MaxPacketSize of 1024 bytes in response to IN token from host, the isochronous IN endpoint interrupt is not set and the endpoint command/status list entry for the isochronous IN endpoint is not updated.

12.2. Workaround:

Restrict the isochronous IN endpoint MaxPacketSize to 1023 bytes in device descriptor.

12.3. Proposed solution

No fix scheduled.

13. ERR050742 USBHSH: Transaction limitation for isochronous IN endpoints in High-bandwidth mode

13.1. Description:

The RT500 device family includes a USB high-speed interface which can operate in host mode. Up to three high-speed transactions are allowed in a single micro-frame to support high-bandwidth endpoints. This mode is enabled by setting the MULT (Multiple) field in the Proprietary Transfer Descriptor (PTD) and is used to indicate to the host controller the number of transactions that should be executed per

micro-frame. The allowed bit settings are:

- 00b Reserved. A zero in this field yields undefined results.
- 01b One transaction to be issued for this endpoint per micro-frame
- 10b Two transactions to be issued for this endpoint per micro-frame
- 11b Three transactions to be issued for this endpoint per micro-frame

However, for High-bandwidth mode, using multiple packets (MULT = 10b or 11b) in a frame causes unreliable operation. Only one transaction (MULT = 01b) can be issued per micro-frame.

13.2. Workaround:

For isochronous IN endpoints, transactions should be limited to only one transaction (MULT = 01b) per micro-frame.

13.3. Proposed solution

No fix scheduled.

14. ERR050799 Non-Secure Boot: ROM API initializes unused FlexSPI0 IO pins

14.1. Description:

Each port IO pin has a dedicated control register in the IOPCTL module that allows control of various functions and characteristics. By default, the port IO pins have their input buffer disabled. This keeps pins that may be left floating from causing excess current leakage.

During the FlexSPI boot flow, the ROM API IAP_FlexspiNorAutoConfig() is called, for initialization of the FlexSPI module before accessing the Flash memory. The ROM configures the FLEXSPI0 pins (PIO1_18 - PIO1_28) enabling the input buffers for those respective pins regardless of what memory device is used.

14.2. Workaround:

If the application does not use these FlexSPI0 pins as inputs, it should disable the input buffers for these pins in the IOPCTL registers via bit 6 (IBENA).

14.3. Proposed solution

No fix scheduled.

How To Reach Us

Home Page:

nxp.com

Web Support:

nxp.com/support

Limited warranty and liability — Information in this document is provided solely to enable system and software implementers to use NXP products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document. NXP reserves the right to make changes without further notice to any products herein.

NXP makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does NXP assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters that may be provided in NXP data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including “typicals,” must be validated for each customer application by customer's technical experts. NXP does not convey any license under its patent rights nor the rights of others. NXP sells products pursuant to standard terms and conditions of sale, which can be found at the following address: nxp.com/SalesTermsandConditions.

Right to make changes - NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Security — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer’s applications and products. Customer’s responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer’s applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP, the NXP logo, NXP SECURE CONNECTIONS FOR A SMARTER WORLD, COOLFLUX,EMBRACE, GREENCHIP, HITAG, ICODE, JCOP, LIFE, VIBES, MIFARE, MIFARE CLASSIC, MIFARE DESFire, MIFARE PLUS, MIFARE FLEX, MANTIS, MIFARE ULTRALIGHT, MIFARE4MOBILE, MIGLO, NTAG, ROADLINK, SMARTLX, SMARTMX, STARPLUG, TOPFET, TRENCHMOS, UCODE, Freescale, the Freescale logo, AltiVec, CodeWarrior, ColdFire, ColdFire+, the Energy Efficient Solutions logo, Kinetis, Layerscape, MagniV, mobileGT, PEG, PowerQUICC, Processor Expert, QorIQ, QorIQ Qonverge, SafeAssure, the SafeAssure logo, StarCore, Symphony, VortiQa, Vybrid, Airfast, BeeKit, BeeStack, CoreNet, Flexis, MXC, Platform in a Package, QUICC Engine, Tower, TurboLink, EdgeScale, EdgeLock, eIQ, and Immersive3D are trademarks of NXP B.V. All other product or service names are the property of their respective owners. AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, µVision, Versatile are trademarks or registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. The Power Architecture and Power.org word marks and the Power and Power.org logos and related marks are trademarks

Table continues on the next page...

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 4/2021
Document identifier: RT500_2P43B