Document identifier: KW45_K32W1_2P43C

Rev. 1.4, 12/2022

KW45_K32W1_2P43C

Mask Set Errata

Mask Set Errata for Mask 2P43C

Revision History

This report applies to mask 2P43C for these products:

- KW45_K32W1
- KW45Z410x3AFxBx
- KW45Z410x2AFxBx
- KW45B41Zx3AFxBx
- KW45B41Zx2AFxBx
- K32W1480VFTBT

Table 1. Revision History

Revision	Date	Significant Changes
1.4	12/2022	Initial Revision

Errata and Information Summary

Table 2. Errata and Information Summary

Erratum ID	Erratum Title
ERR051051	Core: A partially completed VLLDM might leave Secure floating-point data unprotected
ERR050505	Core: Access permission faults are prioritized over unaligned Device memory faults
ERR050501	Core: DFSR.EXTERNAL is not set correctly when waking up from sleep
ERR050502	Core: Execution priority might be wrong for one cycle after AIRCR is changed
ERR050500	Core: Group priority of a Non-secure interrupt might be incorrect when AIRCR.PRIS is set
ERR050503	Core: Non-secure HardFault exception might preempt when disabled by AIRCR.BFHFNMINS
ERR050504	Core: Sorting of pending interrupts might be wrong when high latency IRQs are pending
ERR050810	I3C: t(CPB) & t(CPSr) , t(CASr) parameter different from standard
ERR051120	I3C: The Not Acknowledge Error bit in the Master Errors and Warnings register (MERRWARN[NACK]) is not set when slave does not acknowledge High Data Rate - Double Data Rate (HDR-DDR) read.
ERR050811	I3C: tSU_STO and tSU_STA do not met for I3C legacy mode Fm+
ERR051118	LPI2C: Aborting a multiple byte receive transfer will cause subsequent transfer to hang
ERR051119	LPI2C: NACK Detect Flag can be set when IGNACK=1
ERR051136	Read Stall: flash read/write operation causes error during program/erase
ERR051135	RF RAM Retention increases power consumption in Power Down modes

Known Errata

ERR051135: RF RAM Retention increases power consumption in Power Down modes

Description

When the RF RAM is retained by using the RF_CMC[RAM_PWR] registers in Power Down mode, the power consumption is around 2uA higher than when using Deep Sleep mode.

Workaround

Turn off the RF RAM manually using the RF_CMC[RAM_PWR] registers before entering in Power Down modes.

ERR051119: LPI2C: NACK Detect Flag can be set when IGNACK=1

Description

When MCFG1[IGNACK] is set any received NACK should be ignored, but under some conditions the NACK Detect Flag (NDF) can still be set.

However, the LPI2C will not automatically generate a STOP or Repeated START if the NACK Detect Flag is set when IGNACK=1 and the transfer will continue as if the NDF had not been set.

The LPI2C will continue to block a new START condition if the NDF is set.

Workaround

When IGNACK=1, the NDF must be cleared by software to allow new I2C transfers to start.

ERR050505: Core: Access permission faults are prioritized over unaligned Device memory faults

Description

Cortex-M33 1080541-C :

A load or store which causes an unaligned access to Device memory will result in an UNALIGNED UsageFault exception. However, if the region is not accessible because of the MPU access permissions (as specified in MPU_RBAR.AP), then the resulting MemManage fault will be prioritized over the UsageFault.

Workaround

There is no workaround.

However, it is expected that no existing software is relying on this behavior since it was permitted in Armv7-M.

ERR050503: Core: Non-secure HardFault exception might preempt when disabled by AIRCR.BFHFNMINS

Description

Cortex-M33 1453380-C:

When the processor implements the Security Extension and AIRCR.BFHFNMINS is 1, the Non-secure banked version of SHCSR.HARDFAULTPENDED can be set to 1. This Non-secure pended HardFault might not preempt per architecture because it does not have enough priority (that is, the processor is in HardFault handler mode). If AIRCR.BFHFNMINS is subsequently changed to 0 with the Non-secure HardFault still pending, then the architecture requires that the Nonsecure HardFault should never preempt regardless of execution priority. Because of this erratum, the pended Non-secure HardFault exception preempts when AIRCR.BFHFNMINS is 0 and current execution priority is larger than -1 (Non-secure HardFault having higher priority).

Workaround

There is no workaround for this erratum.

ERR051136: Read Stall: flash read/write operation causes error during program/erase

Description

The Program Flash Controller (PFC) provides access to the flash memory from the AHB bus masters. If a master does a flash memory access to a flash array while that array is busy, the access is terminated with an AHB bus error. The PFC implements an optional "flash read stall" mechanism to avoid this situation. This mechanism is enabled by a control bit in the Secure Miscellaneous System Control Module (SMSCM). If enabled, the flash read stall logic will hold any flash memory access to a flash array while that array is busy. The access will "stall" (be held in its AHB bus data phase) until the target flash array is not busy. Once the busy flag has been negated, the access will be complete.

This device has a PFC for the primary flash attached to the main processor and a PFC for the flash in the radio subsystem. The primary flash and the radio subsystem flash each have three flash arrays - a main program flash array, an IFR flash array, and an IFR1 flash array. Each PFC can access the three flash arrays of its attached flash. The flash read stall should work for access to any of these arrays. Due to a logic error, the flash read stall mechanism only works correctly for accesses to a busy program flash array. Even when the flash read stall mechanism is enabled, access to busy IFR or IFR1 flash arrays is not stalled and terminates with an AHB bus error.

Workaround

Do not access IFR or IFR1 flash arrays when they may be busy due to a flash erase or program operation. When performing Flash erase/program operations, execute from SRAM or ROM.

ERR050501: Core: DFSR.EXTERNAL is not set correctly when waking up from sleep

Description

Cortex-M33 1367266-C:

An external debug event which causes the processor to enter Debug state or the debug monitor should set DFSR.EXTERNAL. It has been found that this field is not set if the event occurs while the processor is asleep.

Workaround

There is no workaround.

ERR050502: Core: Execution priority might be wrong for one cycle after AIRCR is changed

Description

Cortex-M33 1435973-C:

AIRCR is used in the NVIC active tree to calculate the execution priority, which in turn is used to determine fault escalation, exception preemption, and other NVIC-related behaviors. When the active tree is pipelined and there are high latency IRQs active, there might be a glitch in the active tree output for one cycle after AIRCR is changed. The glitch results in NVIC producing wrong execution priority that is neither based on the old AIRCR value nor the new one.

Workaround

There is no workaround for this erratum.

ERR051120: I3C: The Not Acknowledge Error bit in the Master Errors and Warnings register (MERRWARN[NACK]) is not set when slave does not acknowledge High Data Rate - Double Data Rate (HDR-DDR) read.

Description

I3C: The Master Errors and Warnings register (MERRWARN) is used to debug I3C/I2C errors and warnings in Master mode. The MERRWARN[NACK] bit does not set when slave does not accept read while HDR-DDR mode is used. This bit is set to 1 in Single Data Rate (SDR) mode when slave does not acknowledge.

Workaround

If a slave does not accept HDR-DDR read and master side is not able to debug, the slave availability/readiness can be checked by sending SDR read request. The MERRWARN[NACK] will reflect the slave response.

ERR050810: I3C: t(CPB) & t(CPSr) , t(CASr) parameter different from standard

Description

1. tCBP parameter defines the minimum timing for clock before stop Tcbp (I3C Spec V1.1.1 Table 122) in I3C push-pull mode and may not meet the value in the standard 17.2ns .

The value observed for FCLK 160MHz is 6.26ns and for 120MHz is 8.34ns respectively .

IMPACT : No Functional Impact .The actual I3C devices are not expected to have any issues at all, as the behavior around STOP is only verifying SCL is High when SDA rises, so plenty of setup time (tSU_OD (I3C Spec V1.1.1 Table 122) - 3ns) .

2. tCBSr parameter defines the minimum timing for clock before repeated start TCBSr(I3C Spec V1.1.1 Table 123) in I3C push-pull mode and may not meet the value in the standard 17.2ns .

The value observed for FCLK 160MHz is 9.39ns and for120Mhz is 12.51 ns respectively .

IMPACT : No Functional Impact .For Repeated start The actual behavior of Targets will be to detect that SDA is low on the following SCL Falling edge , for which there is plenty of setup (tSU_OD (I3C Spec V1.1.1 Table 122) - 3ns) . Even if a Target has an SDA rise detector which checks if SCL is High, there is plenty of setup time (tSU_OD (I3C Spec V1.1.1 Table 122) - 3ns).

3. tCASr parameter defines the minimum timing for clock after repeated start (tCASr) (I3C Spec V1.1.1 Table 123) in I3C push-pull mode and may not meet the value in the standard 17.2ns .

The value observed for FCLK 48MHz is 10.42 ns .

IMPACT : No Functional Impact .For Repeated start The actual behavior of Targets will be to detect that SDA is low on the following SCL Falling edge , for which there is plenty of setup (tSU_OD (I3C Spec V1.1.1 Table 122) - 3ns) . Even if a Target has an SDA rise detector which checks if SCL is High, there is plenty of setup time (tSU_OD (I3C Spec V1.1.1 Table 122) - 3ns).

Workaround

User needs to skip conformance timing checks for tCBP , tCBSr , tCASr

ERR050811: I3C: tSU_STO and tSU_STA do not met for I3C legacy mode Fm+

Description

Minimum timing for clock before stop tSU_STO (I3C Spec V1.1.1 Table 121) is not met in I3C legacy Fm+ mode . Standard expected minimum 260ns .

For Different FCLKs tSU_STO observed is in range of (94ns - 125ns)

This conformance violation will not cause functional issue as the behavior around STOP is only verifying SCL is High when SDA rises, so plenty of setup time (tSU_DAT (I3C Spec V1.1.1 Table 121) - 50ns) .

Minimum timing for clock before repeated start tSU_STA(I3C Spec V1.1.1 Table 121) is not met in I3C legacy Fm+ mode . Standard expected minimum 260ns

For different FCLKs tSU_STA observed is (92 - 145ns) .

This conformance violation will not cause functional issue as the behavior around Repeated Start is only verifying SCL is High when SDA falls, so plenty of setup time (tSU_DAT (I3C Spec V1.1.1 Table 121) - 50ns) .

Workaround

User needs to skip conformance timing checks for tSU_STA and tSU_STO.

ERR050500: Core: Group priority of a Non-secure interrupt might be incorrect when AIRCR.PRIS is set

Description

Cortex-M33 1113997-C:

When the processor is configured with Security extension and AIRCR.PRIS is 1, the Armv8-M architecture requires that the priorities of Non-secure interrupts are modified to ensure that Secure interrupts are prioritized over Non-secure interrupts. The Armv8-M architecture requires that lower priority numbers take precedence over higher priority numbers. Because of this erratum, a Non-secure interrupt with higher priority number might be handled in the wrong order compared to another Non-secure or Secure interrupt.

Workaround

There is no workaround for this erratum.

ERR051118: LPI2C: Aborting a multiple byte receive transfer will cause subsequent transfer to hang

Description

If the MCFGR0[ABORT] register bit is used to abort a receive transfer that consists of multiple bytes, then the subsequent transfer after the abort completes will hang.

Workaround

If MCFGR0[ABORT] is set by software, first wait for the LPI2C to go idle (MSR[MBF] = 0) and then issue a software reset (MCR[RST] = 1) before initiating the next transfer.

ERR051051: Core: A partially completed VLLDM might leave Secure floating-point data unprotected

Description

Arm errata 2219175

Affects: Cortex-M33

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r0p1, r0p2, r0p3, r0p4, r1p0. Open.

The VLLDM instruction allows Secure software to restore a floating-point context from memory. Due to this erratum, if this instruction is interrupted or it faults before it completes, then Secure data might be left unprotected in the floating point register file, including the FPSCR.

Configurations affected:

This erratum affects all configurations of the Cortex-M33 processor configured with the Armv8-M Security Extension and the Floating-point Extension.

Conditions:

This erratum occurs when all the following conditions are met:

- There is no active floating-point context, (CONTROL.FPCA==0)

- Secure lazy floating-point state preservation is not active, (FPCCR_S.LSPACT==0)

- The floating-point registers are treated as Secure (FPCCR_S.TS==1)

- Secure floating-point state needs to be restored, (CONTROL_S.SFPA == 1)

- Non-secure state is permitted to access to the floating-point registers, (NSACR.CP10 == 1)

- A VLLDM instruction has loaded at least one register from memory and does not complete due to an interrupt or fault

Implications:

If the floating-point registers contain Secure data, a VLSTM instruction is usually executed before calling a Non-secure function to protect the Secure data. This might cause the data to be transferred to memory (either directly by the VLSTM or indirectly by the triggering of a subsequent lazy state preservation operation). If the data has been transferred to memory, it is restored using VLLDM on return to Secure state. If the VLLDM is interrupted or it faults before it completes and enters a Non-secure handler, the partial register state which has been loaded will be accessible to Non-secure state.

Workaround

To avoid this erratum, software can ensure a floating-point context is active before executing the VLLDM instruction by performing the following sequence:

- Read CONTROL_S.SFPA

- If CONTROL_S.SFPA==1 then execute an instruction which has no functional effect apart from causing context creation (such as VMOV S0, S0)

ERR050504: Core: Sorting of pending interrupts might be wrong when high latency IRQs are pending

Description

Cortex-M33 1540599-C:

The NVIC contains a pending tree which sorts all pending and enabled interrupts based on priorities. If DHCSR.C_DEBUGEN and DHCSR.C_MASKINTS are 1, DHCSR.S_SDE is 0 and halting debug is allowed, then Nonsecure PendSV, Non-secure SysTick, and Non-secure IRQs should be masked off and they should not affect the sorting of pending and enabled secure interrupts. If multiple high latency IRQs are pending and enabled with different security targets and priorities, then Non-secure IRQs which should be masked off might cause the pending tree output to be a pending Secure nterrupt without highest priority. This is because of incorrect masking before doing priority comparisons in the tree.

Workaround

There is no workaround for this erratum.

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

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.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Suitability for use in automotive applications — This NXP product has been qualified for use in automotive applications. If this product is used by customer in the development of, or for incorporation into, products or services (a) used in safety critical applications or (b) in which failure could lead to death, personal injury, or severe physical or environmental damage (such products and services hereinafter referred to as "Critical Applications"), then customer makes the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. As such, customer assumes all risk related to use of any products in Critical Applications and NXP and its suppliers shall not be liable for any such use by customer. Accordingly, customer will indemnify and hold NXP harmless from any claims, liabilities, damages and associated costs and expenses (including attorneys' fees) that NXP may incur related to customer's incorporation of any product in a Critical Application.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. 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.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

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