MCXA156VLL_0P29K

Mask Set Errata

Rev. 2.0 — 24 November 2025 Errata

1 Mask Set Errata for Mask 0P29K

1.1 Revision History

This report applies to mask 0P29K for these products:

- MCXA154VMP
- MCXA156VPJ
- MCXA155VPJ
- MCXA154VPJ
- MCXA146VPJ
- MCXA145VPJ
- MCXA144VPJ
- MCXA146VLL
- MCXA146VMP
- MCXA145VLL
- MCXA145VMP
- MCXA144VLL
- MCXA144VMP
- MCXA156VMP
- MCXA155VLL
- MCXA155VMP
- MCXA154VLL

Table 1. Revision History

Revision	Release Date	Significant Changes
2.0	11/2025	The following errata were removed. • ERR051730 The following errata were added. • ERR053147 • ERR052748 The following errata were revised. • ERR051734
1.0	6/2024	Initial Revision

1.2 Errata and Information Summary

Table 2. Errata and Information Summary

Erratum ID	Erratum Title
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

Table 2. Errata and Information Summary*...continued*

Erratum ID	Erratum Title
ERR051588	LPSPI:Reset transmit FIFO after FIFO underrun by LPSPI Slave.
ERR051605	LPUART: Transmit Complete does not set if TX FIFO is flushed when CTS negated
ERR051727	Arm Errata 2219175: [Cortex-M33] A partially completed VLLDM might leave Secure floating-point data unprotected
ERR051728	Arm Errata 1080541: [Cortex-M33] Access permission faults are prioritized over unaligned Device memory faults
ERR051729	Arm Errata 1113997: [Cortex-M33] Group priority of a Non-secure interrupt might be incorrect when AIRCR.PRIS is set
ERR051731	Arm Errata 1435973: [Cortex-M33] Execution priority might be wrong for one cycle after AIRCR, NVIC_ITNS, NVIC_IPR, NVIC_ISER, or NVIC_ICER is changed
ERR051732	Arm Errata 1453380: [Cortex-M33] Non-secure HardFault exception might preempt when disabled by AIRCR.BFHFNMINS
ERR051733	Arm Errata 1540599: [Cortex-M33] Sorting of pending interrupts might be wrong when high latency IRQs are pending
ERR051734	Core: DWT comparator match on cycle count is not reported to the ETM if there is no instruction executing on the processor
ERR052748	ISP_PIN_ENTRY issue
ERR053147	ISP pin is not on the defined P3_29 during POR on LQFP64 and QFN48 packages

2 Known Errata

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.

ERR051588: LPSPI:Reset transmit FIFO after FIFO underrun by LPSPI Slave.

Description

Transmit FIFO pointers are corrupted when a transmit FIFO underrun occurs (SR[TEF]) in slave mode.

Workaround

When clearing the transmit error flag (SR[TEF] = 0b1) following a transmit FIFO underrun, reset the transmit FIFO (CR[RTF] = 0b1) before writing any new data to the transmit FIFO.

ERR051605: LPUART: Transmit Complete does not set if TX FIFO is flushed when CTS negated

Description

If TX FIFO is flushed by software when CTS is enabled (MODIR[TXCTSE] field is set) and its value is negated and the transmitter is idle waiting for CTS to assert, but Transmit Complete (STAT[TC]) bit is not set.

Workaround

Do not use TC bit to check the TX status.

ERR051727: Arm Errata 2219175: [Cortex-M33] A partially completed VLLDM might leave Secure floating-point data unprotected

Description

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.

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)

ERR051728: Arm Errata 1080541: [Cortex-M33] Access permission faults are prioritized over unaligned Device memory faults

Description

Affects: Cortex-M33

Fault Type: Programmer Category C

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

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.

ERR051729: Arm Errata 1113997: [Cortex-M33] Group priority of a Non-secure interrupt might be incorrect when AIRCR.PRIS is set

Description

Affects: Cortex-M33

Fault Type: Programmer Category C

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

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.

This erratum only affects the processor with Security extension configured and Verilog parameter IRQLVL set to a value less than 8. IRQLVL is the number of priority bits physically implemented within the 8-bit priority value. For IRQLVL less than 8, the least significant bits of the priority field are zeroed.

The erratum can occur if any of the following is true:

The configuration includes an interrupt number of 240 or higher.

The configuration uses the IRQLATENCY parameter to define interrupts of lower and higher interrupt latency.

The Secure software configuration defines some Secure and some Non-secure interrupts.

Workaround

There is no workaround for this erratum.

ERR051731: Arm Errata 1435973: [Cortex-M33] Execution priority might be wrong for one cycle after AIRCR, NVIC_ITNS, NVIC_IPR, NVIC_ISER, or NVIC_ICER is changed

Description

Affects: Cortex-M33

Fault Type: Programmer Category C

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

Programmable registers are used in the Nested Vectored Interrupt Controller (NVIC) to determine execution priority, interrupt priority, and in turn exception pre-emption, fault escalation and other NVIC behavior.

As a result of this erratum, when at least one interrupt is configured as higher-priority and specific programmable register values are changed, there is a one-cycle window where execution and interrupt

priority might be wrong, leading to incorrect NVIC behavior such as exception pre-emption and fault escalation.

Workaround

There is no workaround for this erratum.

Typical applications do not need a workaround for this erratum because registers related to interrupt priority are typically programmed during boot-up and then remain static.

The UFRDY bits in FPCCR might be wrong when the write to the NVIC-related register is followed immediately by a VLSTM instruction.

Instruction stepping, asynchronous debug events, and breakpoints might be incorrectly triggered or missed in the cycle after the write to the NVIC-related register.

ERR051732: Arm Errata 1453380: [Cortex-M33] Non-secure HardFault exception might preempt when disabled by AIRCR.BFHFNMINS

Description

Affects: Cortex-M33

Fault Type: Programmer Category C

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

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 Non-secure 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.

ERR051733: Arm Errata 1540599: [Cortex-M33] Sorting of pending interrupts might be wrong when high latency IRQs are pending

Description

Affects: Cortex-M33

Fault Type: Programmer Category C

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

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 Non-secure 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 interrupt without highest priority. This is because of incorrect masking before doing priority comparisons in the tree.

This erratum affects all processor configurations where the Security Extension is implemented.

Workaround

There is no workaround for this erratum.

ERR051734: Core: DWT comparator match on cycle count is not reported to the ETM if there is no instruction executing on the processor

Description

Cortex-M33 2435965-C

The Cortex-M33 Data Watchpoint and Trace (DWT) unit supports a Cycle count match event which can be used to trigger the Embedded Trace Macrocell (ETM) to generate a trace packet from the processor. Due to this erratum the event signal is only propagated when an instruction is executing in the pipeline and so no event will be transferred to the ETM if the processor is idle.

Workaround

There is no workaround for this erratum, however, non-debug operation of the core is not affected.

ERR052748: ISP_PIN_ENTRY issue

Description

If ISP_PIN_ENTRY in CMPA is set to '01b' (which means ISP entry is disabled) and the ISPMODE_n pin is pulled down during reset, the MCU will be stuck in ISP and doesn't support any ISP command, also will not jump to user application.

Workaround

No workaround.

ERR053147: ISP pin is not on the defined P3_29 during POR on LQFP64 and QFN48 packages

Description

ISP pin is not on the defined P3_29 during POR on small packages like LQFP64, QFN48 and QFN32 packages.

1. On POR (Power On Reset), the ISP pin is P0_6. If P0_6 is low on POR , MCU enters in ISP mode. Else if P0_6 is high on POR, MCU enters normal boot. P3_29 doesn't act as ISP pin on POR.

2. On warm reset (e.g. by reset pin), the ISP pin is P3_29 as defined in the pinout table, P0_6 doesn't act as ISP pin on warm reset.

Workaround

P3_29 can be the ISP pin if a warm rest is started at the beginning of the user code right after POR.

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.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://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.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

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.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

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.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell 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.

Contents