Document identifier: iMX7ULP_2N54W
Rev. 1, 5/2023

iMX7ULP_2N54W

Mask Set Errata

Mask Set Errata for Mask 2N54W

Revision History

This report applies to mask 2N54W for these products:

- MCIMX7U3CVP06SD
- MCIMX7U3DVK07SD
- MCIMX7U5CVP06SD
- MCIMX7U5DVK07SD
- MCIMX7U5DVP07SD

Table 1. Revision History

Revision	Date	Significant Changes
1	5/2023	Initial Revision

Errata and Information Summary

Table 2. Errata and Information Summary

Erratum ID	Erratum Title
ERR010469	ARM A7: A7 core reset as a source for the M4 core
ERR010472	MSMC: Reset delay on A7 domain when interrupt is enabled for Core0 reset sources
ERR010473	uSDHC: Data Timeout Counter Value may be insufficient for HS400 mode
ERR010740	QuadSPI: Insufficient read data may be received in the RX Data Buffer register
ERR011097	LPSPI: Command word not loaded correctly when TXMSK=1
ERR011372	Power: High leakage current on VDD18_IOREF when VDD supplies for PORT segments are turned off in VLLS modes
ERR011403	CA7: LLS/VLPS wakeup time is longer when PMC1_CTRL[LDOOKDIS]=0
ERR011432	SNVS: TAMPER pin does not retain pull-up/down configuration in VBAT mode
ERR011433	DAC: Transfer error generated when accessing offset addresses 0x19-0x1B
ERR011439	MIPI DSI: Checksum is incorrect for DCS command long packet writes with zero-length data payload
ERR050134	GPIO: GPIO pull-ups/pull-downs may become enabled during reset
ERR050138	PMC: PMC0 PM_STAT[PMC0CURRPM] stuck at VLPR after reset in VLPS/LLS/VLLS modes
ERR051560	SNVS: State machine stuck in CHECK after resume from VLLS

Known Errata

ERR010469: ARM A7: A7 core reset as a source for the M4 core

Description

The i.MX 7ULP provides the following reset options between the two ARM cores:

1) M4 core reset of A7 core: There is hardware capability on the SoC for the M4 core to reset the A7 core directly.

2) A7 core reset of M4 core: There is no hardware capability for the A7 to reset the M4 directly. This is achieved through the Messaging Unit (MU). The MU A-side Control Register field MUA_CR[RAIE] provides a software mechanism for the M4 to detect that the A7 has been reset.

Workaround

The A7 reset is mapped as an interrupt to the M4 core so anytime the A7 is reset, an interrupt is triggered to the M4 core. The M4 core can then reset as required using an ISR.

ERR010472: MSMC: Reset delay on A7 domain when interrupt is enabled for Core0 reset sources

Description

The Multicore System Mode Controller (MSMC) System Reset Interrupt Enable (SRIE) feature allows that some reset sources can be delayed to service an interrupt request.

For the A7 domain, this feature can be enabled for Core 0 (M4) reset sources. This can cause potential issues because when the M4 resets, the A7 domain will lose its clock references from the PLLs and will not be able to service the interrupt. Even when the M4 returns from reset, it is not guaranteed that the PLLs will relock without reconfiguration.

Workaround

Do not use the Core 0 reset interrupt function available to the A7 domain.

ERR010473: uSDHC: Data Timeout Counter Value may be insufficient for HS400 mode

Description

When the Data Timeout Counter Value programmed in SYS_CTRL[DTOCV] is set to the maximum value (0xF), the maximum busy timeout is [2^29 * 2.5 ns] = 1.34 s because the root clock is 400 MHz for HS400 mode. For other speed modes, the maximum busy timeout time is longer because the root clock is slower.

Some eMMC datasheets show maximum busy timeout specifications of 1.6 s, so the programmable timeout in the uSDHC will not be long enough for HS400 mode.

This issue only affects HS400 mode with a 200 MHz SD clock. If the SD clock is reduced to 150 MHz, the timing requirements for 1.6 s can be met.

Workaround

1) Reduce the SD clock to 150 MHz

2) Disable hardware timeout and use a software timeout mechanism to generate a 1.6 s timeout

ERR010740: QuadSPI: Insufficient read data may be received in the RX Data Buffer register

Description

Data read from flash through QuadSPI using Peripheral Bus Interface (IPS) may return insufficient data in the RX Buffer Data register (QuadSPI_RBDRn) when the read data size of a flash transaction is programmed to be greater than 32 bytes.

Workaround

For data size greater than 32 bytes, program the IP data transfer size in the IP configuration register (QuadSPI_IPCR[IDATSZ]) to be in multiples of 8 bytes.

ERR011097: LPSPI: Command word not loaded correctly when TXMSK=1

Description

When the Transmit Command Register is written with TCR[TXMSK]=1 and the next write to the TX FIFO is another command, then the first command may not load correctly.

Workaround

When writing the Transmit Command Register with TCR[TXMSK]=1, wait for the TX FIFO to go empty (FSR[TXCOUNT] = 0) before writing another command to the Transmit Command Register.

ERR011372: Power: High leakage current on VDD18_IOREF when VDD supplies for PORT segments are turned off in VLLS modes

Description

Excessive current around 370uA on VDD18_IOREF is observed when both the M4 and A7 cores are in VLLS mode and VDD_PTA, VDD_PTC or VDD_PTE are turned off.

Workaround

VDD_PTA, VDD_PTC and VDD_PTE should remain powered when the M4 and A7 are both in VLLS mode. The expected leakage current for keeping these supplies powered is approximately 2 uA at 3.3V.

ERR011403: CA7: LLS/VLPS wakeup time is longer when PMC1_CTRL[LDOOKDIS]=0

Description

The CA7 wakeup time from LLS/VLPS is significantly longer when PMC1_CTRL[LDOOKDIS]=0. This bitfield selects whether the PMC will check the regulated output from the LDO Regulator during a mode transition.

Approximate wakeup time from LLS when PMC1_CTRL[LDOOKDIS]=1: 41.5 us

Approximate wakeup time from LLS when PMC1_CTRL[LDOOKDIS]=0: 80 us

Approximate wakeup time from VLPS when PMC1_CTRL[LDOOKDIS]=1: 23 us

Approximate wakeup time from VLPS when PMC1_CTRL[LDOOKDIS]=0: 46 us

This issue does not affect systems designed for CA7 LDO Bypass Mode.

Workaround

Set PMC1_CTRL[LDOOKDIS]=1 before entering LLS/VLPS modes. This setting keeps the register asserted when returning to RUN mode. After RUN mode is reached, the register may be de-asserted.

PMC1_CTRL[LDOOKDIS]=0 reduces the response time of the LDO voltage adjustments in RUN mode, while PMC1_CTRL[LDOOKDIS]=1 sets a fixed timing internal for any voltage adjustment. When moving to LLS or VLPS modes, there are no side effects if PMC1_CTRL[LDOOKDIS]=1 is used.

In CA7 LDO Bypass Mode, always set PMC1_CTRL[LDOOKDIS]=1.

ERR011432: SNVS: TAMPER pin does not retain pull-up/down configuration in VBAT mode

Description

The TAMPER pin has the capability to enable an internal pull-up or pull-down resistor. The internal pull-up / pull-down configuration is not retained when the SoC enters VBAT mode.

Workaround

Use an external pull-up or pull-down resistor if the TAMPER function is desired during VBAT mode.

ERR011433: DAC: Transfer error generated when accessing offset addresses 0x19-0x1B

Description

The DAC generates a transfer error for both read and write accesses to offset addresses 0x19-0x1B. These offsets are part of the ITRM register which is 32 bits and starts at offset address 0x18. Accesses to offset address 0x18 work properly.

Workaround

Use only 32-bit accesses to offset address 0x18 to read/write the IRTM register.

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

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 DSI Low-Power mode (LP). There is no issue for similar commands issued in DSI High-Power mode (HP).

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

Workaround

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

ERR050134: GPIO: GPIO pull-ups/pull-downs may become enabled during reset

Description

During reset, the failsafe GPIOs (Ports A, B, C, E, and F) are supposed to be in the input/H-Z state. Due to a reset issue, the GPIO buffers may come up as Hi-Z with an internal pull-up or pull-down being enabled. The issue persists until the associated internal core supply is on (VDD_DIG0 for Ports A and B; VDD_DIG1 for Ports C, E, and F). After the internal core supply is present, the issue is cleared and the GPIOs will behave as expected.

Ports A and B are susceptible to this issue, however it will only occur until VDD_DIG0 is on. In this case, the GPIO issue will clear before RESET0_b is released.

On Ports C, E, and F, the issue will persist until VDD_DIG1 is turned on internally by the M4. Therefore, the issue will persist after RESET0_b is released until the boot ROM process enables VDD_DIG1 to the A7 domain.

This issue occurs only on power-on reset (POR). After the core supplies have been turned on, the issue will not occur on subsequent resets (including when the A7 exits VLLS mode).

Port D GPIOs are not affected.

Workaround

1) For critical signals that must be controlled during reset, choose GPIOs on ports A, B, or D.

2) For critical signals on ports C, E, and F, include a strong enough pull-up or pull-down on the board to overdrive the internal pull-up or pull-down if it occurs. The internal pull-up/pull-downs may be as strong as approximately 20k ohms.

ERR050138: PMC: PMC0 PM_STAT[PMC0CURRPM] stuck at VLPR after reset in VLPS/LLS/VLLS modes

Description

The Real-Time Domain PMC0 Current Power Mode status bits (PMC0 PM_STAT[PMC0CURRPM]) become stuck indicating VLPR mode (0x3) if a reset occurs when the Real-Time Domain is in VLPS, LLS, or VLLS mode and those power modes were reached from VLPR mode (i.e. RUN -> VLPR -> VLPS/LLS/VLLS). Notice that VLLS wake-up always includes a reset regardless of the wakeup source (RESET0_B, GPIO, NMI, etc.) so this issue is always seen after a wake-up via GPIO/NMI pin events.

Workaround

If PMC0 PM_STAT[PMC0CURRPM] is not used, no action is required.

If the Real-Time Domain needs to go from VLPR to one of the affected modes (i.e. VLPS/LLS/VLLS), go from VLPR to RUN first, and then go to the target mode (VLPS, LLS, or VLLS).

ERR051560: SNVS: State machine stuck in CHECK after resume from VLLS

Description

SNVS state machine stays in CHECK state after M4 core resumes from VLLS low power modes when silicon lifecycle is OPEN/RETURN. In CHECK state, you cannot write the SNVS registers except HPCOMR. This impacts the operations to RTC and others.

Workaround

Set the SSM_ST bit in HPCOMR to start state machine transition, and then reset the SNVS LP by set LP_SWR in HPCOMR. This workaround makes SNVS state machine transit from CHECK to TRUSTED state.

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.

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

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

Date of release: 5/2023
Document identifier: iMX7ULP_2N54W