LPC55S0x/LPC550x

Errata sheet LPC55S0x/LPC550x

Rev. 1.7 — 19 December 2023 **Errata**

Document information

Information	Content
Keywords	LPC55S06JBD64. LPC55S06JHI48, LPC55S04JBD64, LPC55S04JHI48, LPC5506JBD64, LPC5506JHI48, LPC5504JBD64, LPC5504JHI48, LPC5502JBD64, LPC5502JHI48
Abstract	LPC55S0x/LPC550x errata

1 Product identification

The LPC55S0x/LPC550x HTQFP64 package has the following top-side marking:

- First line: LPC55S0x/LPC550x
- Second line: JBD64
- Third line: xxxx
- Fourth line: xxxx
- Fifth line: zzzyywwxR
  - yyww: Date code with yy = year and ww = week.
  - xR: Device revision A

The LPC55S0x/LPC550x HVQFN48 package has the following top-side marking:

- First line: LPC55S0x/LPC550x
- Second line: JHI48
- Third line: xxxxxxxx
- Fourth line: xxxx
- Fifth line: zzzyywwxR
  - yyww: Date code with yy = year and ww = week.
  - xR: Device revision A

2 Errata overview

Table 1. Functional problems table

Functional problems	Short description	Revision identifier	Detailed description
ROM.1	ROM fails to enter ISP mode when image is corrupted with flash pages in an erased or unprogrammed state.	A	Section 3.1
VBAT_DCDC.1	The minimum rise time of the power supply must be 2.6 ms or slower for Tamb = -40 C, and 0.5 ms or slower for Tamb = 0 C to +105 C.	A	Section 3.2
CAN-FD.1	Bus transaction abort could occur when CAN-FD peripheral is using secure alias.	A	Section 3.3.
ROM.2	ROM API can't be used correctly to update and read monotonic counter in CFPA.VENDOR_USAGE word.	A	Section 3.4
PUF SRAM.1	PUF SRAM needs to be reset during the startup of application to prevent high deep-sleep current consumption.	A	Section 3.5
PLL.1	PLL LOCK bit is not reliable.	A	Section 3.6
ROM.3	Invalid TrustZone preset data structure can prevent ROM from applying specified debug settings.	A	Section 3.7

Table 2. AC/DC deviations table

AC/DC deviations	Short description	Product version(s)	Detailed description
n/a	n/a	n/a	n/a

Table 3. Errata notes

Errata notes	Short description	Revision identifier	Detailed description
n/a	n/a	n/a	n/a

3 Functional problems detail

3.1 ROM.1: ROM fails to enter ISP mode when image is corrupted with flash pages in an erased or unprogrammed state

Introduction

On the LPC55S0x/LPC550x, if the image is corrupted with flash pages in an erased or unprogrammed state, the ROM may fail to automatically enter ISP mode.

Problem

When secure boot is enabled in CMPA, and the flash memory contains an erased or unprogrammed memory page inside the memory region specified by the image size field in the image header, the device does not automatically enter into ISP mode using the fallback mechanism, as in the case of a failed boot for an invalid image. This problem occurs when the application image is only partially written or erased but a valid image header is still present in memory.

Work-around

Perform a mass-erase to remove the incomplete and corrupted image using one of the following methods:

- Execute the erase command using Debug Mailbox. The device will enter directly into ISP mode after exiting the mailbox.
- Enter into ISP mode using the Debug Mailbox command and use the flash-erase command.
- Reset the device and enter into ISP mode using the ISP pin. Use the flash-erase command to erase the corrupted (incomplete) image.

3.2 VBAT_DCDC.1: The minimum rise time of the power supply must be 2.6 ms or slower for Tamb = -40 C, and 0.5 ms or slower for Tamb = 0 C to +105 C

Introduction

The datasheet specifies no power-up requirements for the power supply on the VBAT_DCDC pin.

Problem

The device might not always start-up if the minimum rise time of the power supply ramp is 2.6 ms or faster for Tamb = -40 C, and 0.5 ms or faster for Tamb = 0 C to +105 C.

Work-around

None.

3.3 CAN-FD.1: Bus transaction abort could occur when CAN-FD peripheral is using secure alias

Introduction

Unlike CM33, for other AHB masters (CAN-FD, USB-FS, DMA), the security level of transaction is fixed based on the level assigned for the master in SEC_AHB->MASTER_SEC_LEVEL register. So, if application needs to restrict the CAN-FD to secure, following steps are required:

- Set the security level of CAN-FD to secure-user (0x2) or secure privilege (0x3) in SEC_AHB->MASTER_SEC_LEVEL register.
- Assign secure-user or secure-privilege level for CAN-FD register space in SEC_AHB-> SEC_CTRL_AHB_PORT8_SLAVE1 Register.
- Assign secure-user or secure-privilege level for message RAM.

Example: If 16KB of SRAM 2 (0x2000_C000) bank is used for CAN message RAM. Then set rules in SEC_AHB-> SEC_CTRL_RAM2_MEM_RULE0 register to secure-user (0x2) or secure privilege (0x3).

Problem

The shared memory used by CAN-FD controller and CPU should be accessible using secure alias with address bit 28 set (example 0x3000_C000). However, when CAN-FD makes a bus transaction using secure alias (address bit 28 set), the transaction is aborted.

Work-around

- When CPU is accessing the CAN-FD register or message RAM it should always use secure alias i.e., 0x3000_C000 for message RAM manipulation. .
- For any structure the CAN-FD peripheral uses to fetch or write, memory should be set to use 0x2000_C000 in order for bus transaction to work. CAN-FD software driver should set "Message RAM base address register (MRBA, offset 0x200)" with physical address of RAM instead of secure alias.

3.4 ROM.2: ROM API can’t be used correctly to update and read monotonic counter in CFPA.VENDOR_USAGE word

Introduction

Customer Field Programmable Area (CFPA) of Protected Flash Region (PFR) contains VENDOR_USAGE word. The lower 16-bits of the VENDOR_USAGE word implements a monotonic counter which should contain current value or higher value when new version of CFPA page is written. Upper 16-bits of the VENDOR_USAGE word should contain inverse value of aforesaid monotonic counter.

Problem

In the ROM, 16-bit monotonic counter is implemented by upper 16-bits of the VENDOR_USAGE word while lower 16-bits contain inverse value of monotonic counter i.e Monotonic Counter and its inverse value are swapped erroneously in the ROM. Due this error, ROM APIs do not access VENDOR_USAGE monotonic counter correctly.

Work-around

User should increment and store Monotonic Counter value in upper 16-bits of VENDOR_USAGE word while inverse value of the monotonic counter should be stored in the lower 16-bits of the VENDOR_USAGE word.

3.5 PUF SRAM.1: PUF SRAM needs to be reset during the startup of application to prevent high deep-sleep current consumption

Introduction

The LPC55S0x family offers SRAM PUF feature where the PUF provides a unique key per device. By default, the SRAM PUF block is disabled on the LPC550x devices.

Problem

The SRAM PUF block is enabled on the LPC550x devices resulting in higher deep-sleep current. The PUF SRAM block needs to be enabled and reset in order to achieve the deep-sleep current specification.

Work-around

On the LPC550x devices, following software workaround must be applied in the SystemInit function (SDK source file - "system_LPC55xx.c") to prevent high deep-sleep mode current consumption:
Enable the PUF Clock to access necessary registers.
Reset the PUF.
Enabled the PUF SRAM.
Disable the PUF clock.

```
/* Following code is to reset PUF to remove over consumption */
/* Enable PUF register clock to access register */
SYSCON->AHBCLKCTRLSET[2] = SYSCON_AHBCLKCTRL2_PUF_MASK;
/* Release PUF reset */
SYSCON->PRESETCTRLCLR[2] = SYSCON_PRESETCTRL2_PUF_RST_MASK ;
/* Enable PUF SRAM */
#define PUF_SRAM_CTRL_CFG (*((volatile uint32_t*)(0x4003B000u + 0x300u)))
#define PUF_SRAM_CTRL_INT_STATUS (*((volatile uint32_t*)(0x4003B000u + 0x3E0u)))
PUF_SRAM_CTRL_CFG |= 0x01 | 0x04 ;
/* Disable PUF register clock. */
// Delaying the line of code below until the PUF State Machine execution is completed:
// Shutting down the clock to early will prevent the state machine from reaching the end.
// => Wait for status bit in PUF Controller Registers before stop PUF clock.
while(!(PUF_SRAM_CTRL_INT_STATUS & 0x1));
SYSCON->AHBCLKCTRLCLR[2] = SYSCON_AHBCLKCTRL2_PUF_MASK;
```

Remark: The SRAM PUF block should not be used on the LPC550x devices and is not guaranteed to function. This feature is only available on the LPC55S0x devices.

3.6 PLL.1: PLL LOCK bit is not reliable

Introduction

On the LPC55S0x/LPC550x devices, PLLxSTAT register of PLLs contains a LOCK detector status bit (bit 0 of PLLxSTAT register).

When the LOCK detector status bit is set to 1, the PLL is considered to be locked and stable.

The PLL LOCK signal is specified to work for Fref range from 100 kHz to 20 MHz. When the Fref is below 100 kHz or above 20 MHz, software should use a 6 ms time interval to insure the PLL will be stable.

Problem

On the LPC55S0x/LPC550x, the PLL status LOCK bit is not always reliable in the ranges specified and as a result, the PLL doesn´t initialize correctly.

Work-around

For Fref ≥ 20 MHz:

Software must wait at least (500us + 400/Fref) (Fref in Hz result in s) to ensure the PLL is stable.

For Fref < 20 MHz:

- If the PLL lock detector status bit is 1 before the wait time duration ((500us + 400/Fref)) is completed, the PLL is stable.
- If the PLL lock detector status bit is 0 but the wait time duration ((500us + 400/Fref)) is completed, the PLL is stable.

Software workaround is implemented in SDK 2.14 clock driver version 2.3.7.

Remark: This errata does not apply for spread spectrum mode.

3.7 ROM.3: Invalid TrustZone preset data structure can prevent ROM from applying specified debug settings

Introduction

On LPC55S0x devices, secure firmware images can optionally include TrustZone preset data that allows the core to configure TrustZone related registers while executing ROM code before jumping to the application code.

Problem

If the TrustZone preset data is invalid, in some cases this can prevent the ROM execution from proceeding further. Consequently, the application will not boot, and the ROM will not apply debug configurations (DBGEN, NIDEN, SPIDEN, etc.) settings.

Work-around

All application firmware images in this device should use secure boot. Also, the TrustZone preset data should be included within the authentication area to prevent the ROM from attempting to apply corrupted and/or maliciously modified TrustZone preset data settings.

4 AC/DC deviations detail

No known errata.

5 Errata notes detail

No known errata.

6 Revision history

Table 4. Revision history

Rev	Date	Description
1.7	20231219	Corrected Revision identifier field for PLL.1 in Table 1. Added Section 3.7 "ROM:3 Invalid TrustZone preset data structure can prevent ROM from applying specified debug settings"
1.6	20230524	Added Section 3.6 "PLL.1: PLL LOCK bit is not reliable"
1.5	20221219	Added Section 3.5 "PUF SRAM.1: PUF SRAM needs to be reset during the startup of application to prevent high deep-sleep current consumption"
1.4	20220513	Added ROM.2: Section 3.4 "ROM.2: ROM API can't be used correctly to update and read monotonic counter in CFPA.VENDOR_USAGE word"
1.3	20211110	Added CAN-FD.1 note in Section 3.3 "CAN-FD.1: Bus transaction abort could occur when CAN-FD peripheral is using secure alias"
1.2	20210810	Added VBAT_DCDC.1: Section 3.2 "VBAT_DCDC.1: The minimum rise time of the power supply must be 2.6 ms or slower for Tamb = -40 C, and 0.5 ms or slower for Tamb = 0 C to +105 C"
1.1	20201006	Second version.
1.0	20200814	Initial version.

7 Legal information

7.1 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.

7.2 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.

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.

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.

7.3 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

For more information, please visit: http://www.nxp.com

Date of release: 19 December 2023
Document identifier: ES_LPC55S0x/LPC550x