LPC55S6x

Errata sheet LPC55S6x

Rev. 2.8 — 19 December 2023 **Errata**

Document information

Information	Content
Keywords	LPC55S69JBD100, LPC55S69JEV98, LPC55S66JBD100, LPC55S66JEV98,LPC55S66JBD64, LPC55S69JBD64
Abstract	LPC55S6x errata.

1 Product identification

The LPC55S6x VFBGA98 package has the following top-side markings:

- First line: LPC55S6x
- Second line: JEV98
- Third line: xxxxxxxx
- Fourth line: zzzyywwxR
  - yyww: Date code with yy = year and ww = week.
  - xR: Device revision 1B

The LPC55S6x HLQFP100 package has the following top-side markings:

- First line: LPC55S6x
- Second line: xxxxxxxx
- Third line: zzzyywwxR
  - yyww: Date code with yy = year and ww = week.
  - xR: Device revision 0A or Device revision 1B

The LPC55S6x HTQFP64 package has the following top-side:

- First line: LPC55S6x marking
- Second line: JBD64
- Third line: xxxx
- Fourth line: xxxx
- Fifth line: zzzyywwxR
  - yyww: Date code with yy = year and ww = week.
  - xR: Device revision 1B

2 Errata overview

Table 1. Functional problems table

Functional problems	Short description	Revision identifier	Detailed description
ROM.1	For PRINCE encrypted region, partial erase cannot be performed.	0A	Section 3.1
ROM.2	For PUF based key provisioning, a reset must be performed.	0A	Section 3.2
ROM.3	Unprotected sub regions in PRINCE defined regions cannot be used.	0A	Section 3.3
ROM.4	Last page of image is erased when simultaneously programming the signed image and CFPA region.	0A	Section 3.4
ROM.5	ROM fails to enter ISP mode when image is corrupted with flash pages in an erased or unprogrammed state.	0A, 1B	Section 3.5
ROM.6	ROM fails to respond to debug session request.	0A	Section 3.7
VDD.1	The minimum operating voltage is 1.85 V.	0A	Section 3.8
CMP.1	The hysteresis on the comparator cannot be enabled.	0A	Section 3.6
USB.1	USB HS host fails when connecting to an LS device (mouse).	0A, 1B	Section 3.9

Table 1. Functional problems table*...continued*

Functional problems	Short description	Revision identifier	Detailed description
USB.2	USB PHY does not auto-power down in suspend mode.	0A	Section 3.10
USB.3	Automatic USB rate adjustment not functional when using multiple hubs.	0A, 1B	Section 3.11
USB.4	For the USB high-speed device controller, the detection handshaking fails when certain full-speed hubs are connected.	0A, 1B	Section 3.12
ADC.1	Async interrupts with resume not supported.	0A, 1B	Section 3.13
ADC.2	Request for offset calibration function bit (CALOFS) is not cleared after completion of offset calibration function.	0A	Section 3.14
ADC.3	Sign-extend calibration results for averaging is not supported.	0A	Section 3.15
GPIO.1	During power-up, an unexpected glitch (low pulse) can occur on port pins (PIO0_28, PIO1_1, PIO1_18, PIO1_30).	0A	Section 3.16
I2S.1	I2S signal sharing is not functional.	0A	Section 3.17
AES.1	AES keys are not available when Cortex-M33 is running a security level less than 3.	0A	Section 3.18
Powerquad.1	Format issue in matrix scale function.	0A	Section 3.19
Powerquad.2	Floating Point to integer converter scaling issue.	0A	Section 3.20
WAKEIO.1	Wake-up I/O cause register identifies the wake-up I/O (WAKEUP pins) source from deep power-down mode.	0A, 1B	Section 3.21
USB.5	In USB high-speed device mode, device writes extra byte(s) to the buffer if the NBytes is not multiple of 8 for OUT transfer.	0A, 1B	Section 3.22
USB.6	In USB high-speed device mode, when device isochronous IN endpoint sends a packet of MaxPacket Size 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.	0A, 1B	Section 3.23
USB.7	In USB high-speed host mode, only one transaction per micro-frame is allowed for isochronous IN endpoints.	0A, 1B	Section 3.24
DM-AP.1	I2C ISP via debug mailbox is not functional.	0A, 1B	Section 3.25
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.	0A, 1B	Section 3.26
ROM.8	ROM API can't be used correctly to update and read monotonic counter in CFPA.VENDOR_USAGE word.	0A, 1B	Section 3.27
ROM.9	ENTER_ISP_MODE mailbox command does not work.	0A, 1B	Section 3.28
PLL.1	PLL LOCK bit is not reliable.	0A, 1B	Section 3.29

Table 1. Functional problems table*...continued*

Functional problems	Short description	Revision identifier	Detailed description
ROM.13	Invalid TrustZone preset data structure can prevent ROM from applying specified debug settings.	0A, 1B	Section 3.30

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
ISP.1	Devices with date code 2101 (yyww) onward, contain ROM Bootloader version T1.1.5 or higher with run Bootloader API to enter into ISP mode.	0A, 1B	Section 5.1run Bootloader API to enter ISP mode does not work".
ROM.7	Stack pointer for application code cannot be located in the SRAM area when shared with PowerQuad RAM and USB RAM.	0A, 1B	Section 5.2Stack pointer for application code cannot be located in SRAM area when shared with PowerQuad and USB RAM
ROM.10	Devices with date code 2222 (yyww) and onwards contain ROM Target version T1.1.0 (or higher). On these devices, the get-property command is not functional and as a result, bootloader properties like target version cannot be read.	1B	Section 5.3ROM get-property is not functional"
ROM.11	Devices with date code between 2219 (yyww) and 2227 (yyww) contain ROM Target version T1.1.8. On these devices, accessing reserved region (RAM3) in ISP mode results in hard fault and does not return k StatusMemoryRangeInvalid error code to the host.	1B	Section 5.4On devices with total SRAM size of 256 KB, accessing reserved region RAM3 will result in hard fault
ROM.12	Devices with date code between 2219 (yyww) and 2227 (yyww) contain ROM Target version T1.1.8. On these devices, accessing reserved regions (RAM3 and RAM4) in ISP mode results in hard fault and does not return kStatusMemoryRangeInvalid error code to the host.	1B	Section 5.5On devices with total SRAM size of 144 KB, accessing reserved regions RAM3 and RAM4 will result in hard fault

3 Functional problems detail

3.1 ROM.1: For PRINCE encrypted regions, partial erase cannot be performed

Introduction

The LPC55S6x devices support real-time encryption and decryption for on-chip flash using the PRINCE encryption algorithm. The PRINCE module supports three flash memory regions for real-time encryption and

decryption, referred to as crypto regions. Each crypto region resides at a 256 KB address boundary within the flash and are divided into 8 KB sub-regions, which can be individually enabled.

Problem

For the LPC55S6x, when an erase operation is performed with a size less than 8 KB for a PRINCE encrypted region, a return error is returned and subsequent ISP commands do not respond.

Work-around

When a region is marked as a PRINCE encrypted region, a full erase of the PRINCE encrypted region must be performed.

This issue is fixed on device revision 1B.

3.2 ROM.2: For PUF based key provisioning, a reset must be performed

Introduction

On the LPC55S6x, the Key Management module supports storing three 128-bit PRINCE Keys (KEY1, KEY2, and KEY3) used for the decryption process.

Problem

After PUF based key provisioning, the PRINCE module cannot perform the decryption process without performing a reset.

Work-around

Perform a reset via the external reset pin or power cycle the device for a successful decryption process when using a PUF key.

This issue is fixed on device revision 1B.

3.3 ROM.3: Unprotected sub regions in PRINCE defined regions cannot be used

Introduction

The LPC55S6x devices support real-time encryption and decryption for on-chip flash using the PRINCE encryption algorithm. The PRINCE module supports three flash memory regions for real-time encryption and decryption, referred to as crypto regions. Each crypto region resides at a 256 KB address boundary within the flash and is divided into 8 KB sub-regions, which can be individually enabled.

Problem

Unprotected (non PRINCE encrypted) sub flash in PRINCE defined regions cannot be written after an erase operation. Any non PRINCE encrypted sub regions in the PRINCE defined regions cannot be used.

Work-around

There is no work-around.

This issue is fixed on device revision 1B.

3.4 ROM.4: Last page of the image is erased when simultaneously programming the signed image and CFPA region

Introduction

On the LPC55S6x, the protected flash region (PFR) supports a Customer Field Programmable Area (CFPA) which can be used for Monotonic counters, Key revocation, and PRINCE IV codes. Also, the ROM supports secure boot using a signed image.

Problem

When simultaneously programming the signed image and the CFPA via the Secure Binary (SB2 file) image format, the last page of the image is erased.

Work-around

The signed image and the CFPA need to be programmed at a time to prevent the last page of the image from being erased.

This issue is fixed on device revision 1B.

3.5 ROM.5: ROM fails to enter ISP mode when the image is corrupted with flash pages in an erased or unprogrammed state

Introduction

On the LPC55S6x, 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.

This issue occurs on device revisions 0A and 1B.

3.6 CMP.1: The hysteresis on the comparator cannot be enabled

Introduction

On the LPC55S6x, the analog comparator control register (COMP) provides an option to enable and disable the hysteresis.

Problem

On the LPC55S6x, the hysteresis feature of the comparator cannot be enabled.

Work-around

There is no work-around.

This issue will be fixed in the next silicon revision 1B.

3.7 ROM.6: ROM fails to respond to debug session request on version 0A parts

Introduction

Debugging is supported through Arm's Serial Wire Debug (SWD) interface, enabling debugging with a range of debug probes and tools from NXP and other ecosystem partners. Debug access by a remote host is controlled by the LPC55S6x ROM and is only enabled when permitted through the device configuration and when the correct protocol is followed to initiate a debug session. The Boot ROM implements a debug mailbox protocol to interact with host debug systems over the SWD interface. For LPC55S6x, if the device has been configured for debug authentication, then a debug session must be initiated following the correct authentication sequence.

Problem

For the LPC55S6x, a new method of initiating a debug session was introduced, as documented in the current user manual. However, when used on 0A parts, a debug system attempting to connect could become stuck in an endless loop because the ROM in that silicon revision fails to issue a corresponding response to the new debug session request.

Work-around

It is possible to determine whether the cause of the hang during a debug session request is related to the part revision by detecting whether an overrun condition is reported via the debug mailbox, which is only generated by the newer parts and not by the older 0A version. The pseudo code below is a modified version to replace that shown in Chapter 51.6.1 of the user manual, implementing a check for silicon revision when connecting to LPC55S6x parts:

```
// Read AP ID register to identify DM AP at index 2
WriteDP 2 0x020000F0
// The returned AP ID should be 0x002A0000
value = ReadAP 3
print "AP ID: ", value
// Select DM AP index 2
// Select CSW register [BJS]
WriteDP 2 0x02000000
// Write DM RESYNC_REQ + CHIP_RESET_REQ
WriteAP 0 0x21
// Poll CSW register (0) a offset 0x00 for zero return, indicating success
value = -1
```

```
while value != 0 {
value = ReadAP 0
}
print "RESYNC_REQUEST + CHIP_RESET_REQUEST: ", value
// detecting 0A vs 1B silicon.
// Write START_DM-AP command (CMD_1) the response of this command is 0x0
// returned through RETURN register 2
WriteAP 1 1
// Write DM START_DBG_SESSION (CMD_7) to REQUEST register (1) at offset 0x04.
// If the command is successful the return value is 0x80000000.
// However, 0A version silicon doesn't return a success code.
WriteAP 1 7
wait(10ms)
// Check CSW register (0) at offset 0x0 for any errors
// Since we have issued two command in sequence without reading
// the RETURN register in between, on 1B silicon an overrun condition would //
 occur.
value = ReadAP 0
// If the value return is 0x00000008 (AHB or ERR) then it is 1B silicon,
// else it is 0A silicon.
// For 1B silicon, reset the chip by writing 0x21 to register 0 to
// clear the error before continuing
If (value == 0x00000008)  {
// Repeat connection sequence to clear overrun
WriteAP 0 0x21
value = -1
while value != 0 {
value = ReadAP 0
}
// Write DM START_DBG_SESSION to REQUEST register (1)
WriteAP 1 7
value = ReadAP 2
}
```

As a simpler fix, a delay can be introduced (around 100ms is suggested) to allow the ROM code to reach its idle loop after preparing for the debug session; to do this, insert the 100ms delay just before the "detecting 0A vs 1B silicon" comment and omit the rest of the steps.

3.8 VDD.1: The minimum operating voltage is 1.85 V

Introduction

The LPC55S6x operating voltage range specification is from 1.80 V to 3.6 V.

Problem

On the LPC55S6x rev 0A, the minimum operating range is 1.85 V.

Work-around

There is no work-around.

This issue is fixed on device revision 1B.

3.9 USB.1: HS host fails when connecting with the LS device (mouse)

Introduction

The USB1 high-speed controller is available on select LPC55S6x devices and provides a plug-and-play connection of peripheral devices to a host with three different data speeds:

- high-speed with a data rate of 480 Mbps.
- full-speed with a data rate of 12 Mbps.
- low-speed with a data rate of 1.5 Mbps.

Many portable devices can benefit from the ability to communicate with each other over the USB interface without the intervention of a host PC.

Problem

USB HS host fails when connecting with an LS device (mouse).

Work-around

To support Full-Speed and Low-Speed applications, it is recommended to use the USB0 Full-Speed port and the USB1 High-speed port for Device or Host. In addition, should an application require support of Low-Speed USB devices with a USB High-Speed Host, this can be accomplished by inserting a USB Hub between the USB1 High-speed port and external USB devices.

3.10 USB.2: PHY does not auto-power down in suspend mode

Introduction

The USB1 High-Speed Physical Layer (PHY) is available on LPC55S6x devices that include USB high-speed controllers.

A device goes into the L2 suspend state, if there is no activity on the USB bus for more than three ms.

The USB protocol requires power management by the USB device.

Problem

The device does not auto-power down properly in suspend states, which impacts power consumption in the PHY.

Work-around

This issue is fixed on device revision 1B.

3.11 USB.3: Automatic USB rate adjustment is not functional when using multiple hubs

Introduction:

Full-speed and low-speed signaling uses bit stuffing throughout the packet without exception. If the receiver sees seven consecutive ones anywhere in the packet, then a bit stuffing error has occurred, and the packet should be ignored.

The time interval just before an End of Packet (EOP) is a special case. The last data bit before the EOP can become stretched by hub switching skews. This is known as dribble and can lead to a situation where dribble introduces a sixth bit that does not require a bit stuff. Therefore, the receiver must accept a packet where there are up to six full bit times at the port with no transitions prior to the EOP.

Problem:

The LPC55S6x device use the start of an EOP for frequency measurements. This is not functional when going through multiple hubs that introduce a dribble bit because of hub switching skews. For this reason, the start of the EOP cannot be used for frequency measurements for automatic USB rate adjustment (by setting USBCLKADJ in the FRO192M_CTRL register). The problem does not occur when a single hub is used.

Work-around:

Use the FRO calibration library provided in technical note TN00063. This library allows the application to have a crystal-less USB device operation in full-speed mode.

3.12 USB.4: For the USB high-speed device controller, the detection handshaking fails when certain full-speed hubs are connected

Introduction

See the USB2.0 specification for details regarding the USB High-speed Detection Handshake protocol.

Problem

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.

Work-around

There are two workarounds:

1. The software work-around 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 remains 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.

3.13 ADC.1: Async interrupts with resume not supported

Introduction

The ADC controller is available on all LPC55S6x devices. Trigger detect with up to 16 trigger sources is supported with priority level configuration. A software or hardware trigger option is provided for each.

Problem

The following problems are all related to the restart after interrupt feature:

- Low priority trigger executes twice when resumed.
- Trigger can't restart when it is configured to do so.
- Incorrect trigger resumed after exception.

Work-around

There is no work-around.

The async interrupts with resume is not supported on device revisions 0A and 1B.

3.14 ADC.2: Request for offset calibration function bit (CALOFS) is not cleared after completion of offset calibration function

Introduction

The ADC controller is available on all LPC55S6x devices and supports a calibration step where the ADC is configured to perform a calibration operation to determine the value needed in the OFSTRIM register. The CALOFS bit is set to determine the value for the OFSTRIM register which automatically begins a sequence that calculates the value. Once the sequence has completed, the OFSTRIM register is updated with a signed value between -16 and 15. This value is used to minimize offset during normal operation

Problem

The CALOFS bit is written a 1 by software with a bus access to initiate the calibration offset function implemented in hardware. The CALOFS control bit is supposed to be cleared by hardware upon completion of the offset calibration function, but the clock used for the CALOFS bit is only active when the ADC registers are being accessed by software and the hardware clearing mechanism does not work except when an ADC bus access is in progress on the exact cycle that hardware is trying to clear the CALOFS bit. In the failing case where CALOFS does not clear after the offset calibration function, the ADC logic begins the calibration offset function again. This results in an indefinite loop that can only be terminated by a system reset or some form of polling of the ADC registers that coincides with the successful clearance of the CALOFS bit.

Work-around

To clear the OFSTRIM-request, read the register STATUS (poll for the CAL_RDY bit in the STATUS register). The polling for the bit is enough to ensure that the request is cleared.

This issue is fixed on device revision 1B.

3.15 ADC.3: Sign-extend calibration results for averaging is not supported

Introduction

The ADC controller is available on all LPC55S6x devices.

The ADC module includes offset and linearity calibration logic. A request for calibration should be made any time upon reset or power up. Each SAR conversion will utilize calibration data calculated during the auto-calibration routine.

Problem

Sign-extend calibration values for averaging is not supported (averaging of negative numbers in the offset calibration).

Work-around

Software-based averaging can be used as a work-around.

This issue is fixed on device revision 1B.

3.16 GPIO.1: During power-up, an unexpected glitch (low pulse) could occur on port pins (PIO0_28, PIO1_1, PIO1_18, PIO1_30).

Introduction

To wake up from reduced power modes, the wake-up source must be properly configured. Each reduced power mode supports its own wake-up sources and needs to be configured accordingly.

Problem

An unexpected glitch (low pulse for around 200 us) could occur on port pins (PIO0_28, PIO1_1, PIO1_18, PIO1_30) as the VDD supply ramps up. This glitch does not occur when device wakes up from sleep, deep-sleep, power-down, and deep power-down modes.

Work-around

There is no work-around.

This issue is fixed in the silicon revision 1B.

3.17 I2S.1: I2S signal sharing is not functional

Introduction

Signal sharing allows more than one on-chip I2S interface to be connected to a clock, WS, and input data on the same pins without the need for any external board wiring. I2S signal sharing allows the use of multiple I2S that function together in a single TDM stream thus reducing the number of pins that are required for a particular application.

Problem

The I2S signal sharing feature is not functional.

Work-around

There is no work-around.

This issue is fixed in device revision 1B.

3.18 AES.1: Keys are not available when Cortex-M33 is running a security level less than 3

Introduction

The security system on LPC55S6x has a set of hardware blocks and ROM code to

implement the security features provided by the device. The hardware consists of an AES, SHA, and PRINCE engine, a random number generator, and a key storage block that can wrap user provided keys and derive device unique keys from an SRAM based PUF (Physically Unclonable Function). The wrapped keys and derived keys are exported by PUF to firmware in key codes (encrypted data) through the SET_KEY and GEN_KEY commands.

During key code generation, the KEY_INDEX parameter can be specified, which determines the output path of the unwrapped plain key values. Keys wrapped with KEY_INDEX set to 0 are only provided to hardware engines (AES & PRINCE) through a secret bus; these keys are also referred to as secret keys. All other keys with KEY_INDEX set from 1 to 15 are provided through the registers interface. Also, when you choose not to use the TrustZone mechanism, you cannot use the secret keys (KEY_INDEX = 0) with the AES engine. Instead, you have to use the software supplied key.

Problem

Hardware logic makes all secret keys passed from PUF to the AES engine unusable unless firmware running on the Cortex-M33 accesses the HashCrypt engine at secure-privilege level 3. Thus, firmware should be written to make sure the Cortex-M33 uses the appropriate secure-privilege mode before configuring the AES engine to use secret keys. In addition, the TrustZone mechanism must be enabled to use secret keys (KEY_INDEX = 0) with the AES engine.

Work-around

To use secret keys with the AES engine, firmware should make sure that the Cortex-M33 is at secure-privilege level 3 before configuring the AES engine registers.

User applications which disable the TrustZone mechanism cannot use secret keys.

There is no workaround.

This issue is fixed in device revision 1B.

3.19 Powerquad.1: Format issue in matrix scale function

Introduction

A PowerQuad DSP Coprocessor and Accelerator are available on all LPC55S6x devices.

A matrix operation (Add, Sub, Dot, Prod, Mult, Inverse, Transpose, and Scale) is provided for the DSP.

Problem

When using the matrix scale operation, in floating number to fixed one conversion, every 8th number is wrong.

Work-around

Do not mix fixed and float operands. As long as all operands and results are either fixed or float, then there is no issue.

This issue is fixed in device revision 1B.

3.20 Powerquad.2: Floating point to integer converter scaling issue

Introduction

A PowerQuad DSP Coprocessor and Accelerator is available on all LPC55S6x devices.

For each co-processor output, and for AHB data converter for streaming operations write back, a floating point to fixed point conversion can be performed, while allowing the user to adjust the floating point's numbers exponent value before the conversion. As a result, a scaling by 2^^N of the floating-point value can occur when it gets converted. In the case of co-processor opcodes, this feature is useful in order to 'upscale' by taking numbers which have a fractional component and multiplying them by a power of two to increase the resolution in the resulting integer. In the case of AHB data writeback, it is possible to 'upscale' or 'downscale' the floating-point number.

Problem

When performing a downscale, the result for a floating-point value of 0 is an overflow of the exponent field, resulting in saturation. This is not the appropriate behavior since a 0, whether down-scaled or up-scaled, should result in 0.

When performing an upscale, results are correct, except in the case where a very large number's exponent combined with the up-scaling exceeds 2^^127. In this case, the overflow detection may not work, and saturation may not be correctly engaged due to the overflow in the exponent field. A negative prescaler (2^x prescaler where x is negative) cannot be used.

Work-around

Use floating numbers if fractional numbers are needed.

This issue is fixed in device revision 1B.

3.21 WAKEIO.1: Wake-up I/O register reports incorrect wake-up source

Introduction

On the LPC55S6x, a wake-up I/O cause register is available to identify the wake-up I/O (WAKEUP pins) source from deep power-down mode.

Problem

Before entering DEEP-POWER-DOWN, the following configuration is set for the wake-up sources:

- Wake-up I/O 0 as falling edge.
- Wake up I/O 1 as rising edge.
- Wake up I/O 2 is disabled.
- Wake up I/O 3 as falling edge.

1st case: The first wake up event is a rising edge on wake up I/O 1. PMC->WAKEIOCAUSE will indicate Wake-up I/O 0 trigger (wrong), Wake up I/O 1 trigger (correct) and Wake up I/O 3 trigger (wrong) as wake up I/O cause.

2nd case: The first wake up event is a falling edge on wake up I/O 3. PMC->WAKEIOCAUSE will indicate Wake-up I/O 0 trigger (wrong) and Wake up I/O 3 trigger (correct) as wake up I/O cause.

3rd case: The first wake up event is an RTC. PMC->WAKEIOCAUSE will indicate Wake-up I/O 0 trigger (wrong) and Wake up I/O 3 trigger (wrong) as wake up I/O cause.

Work-around

None. This issue does not occur when the wake I/O is not configured as falling edge.

3.22 USB.5: In USB high-speed device mode, device writes extra byte(s) to the buffer if the NBytes is not multiple of 8 for OUT transfer

Introduction

The LPC55S6x device family include a USB high-speed interface (USB1) that can operate in device mode at high-speed. The NBytes value represents the number of bytes that can be received in the buffer.

Problem

The LPC55S6x USB device controller writes extra bytes to the receive data buffer if the size of the transfer is not a multiple of 8 bytes since the USB device controller always writes 8 bytes. For example, if the transfer length is 1 bytes, 7 extra bytes will be written to the receive data buffer. If the transfer length is 7 bytes, 1 extra bytes will be written to the receive data buffer.

Work-around

Reserve an additional, intermediary buffer along with the buffer used by the application for USB data. After the USB data transfer into the intermediary buffer has been completed, use memcpy to move the data from the intermediary buffer into the application buffer, skipping the extraneous extra byte. This software work-around is implemented on the SDK software platform.

3.23 USB.6: In USB high-speed device mode, 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

Introduction

The LPC55S6x 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.

Problem

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.

Work-around

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

3.24 USB.7: In USB high-speed host mode, only one transaction per micro-frame is allowed for isochronous IN endpoints

Introduction

The LPC55S6x device family include 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.

Problem

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.

Work-around

There is no software workaround. Only one transaction can be issued per micro-frame.

3.25 DM-AP.1: I2C ISP via debug mailbox is not functional

Introduction

The LPC55S6x supports I2C ISP mode via debug mailbox. By default, ISP mode entry is determined by the state of the ISP boot selection pins at reset time. Usually this functionality is disabled through PFR configuration prior to field deployment or when ISP boot selection pins are used for some other board function. In this situation, the DM_AP command "Enter ISP mode" can be used to enter one of the ISP modes (UART, SPI, I2C, USB-HID). Parameter value of 0x2 can be used to enter I2C ISP mode.

Problem

I2C ISP via debug mailbox cannot be entered and is not functional.

Work-around

There is no software workaround.

3.26 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.

3.27 ROM.8: 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 implement 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.

3.28 ROM.9: ENTER_ISP_MODE mailbox command does not work

Introduction

The Debug Mailbox is used to communicate with code executing in the ROM by sending mailbox commands. ENTER_ISP_MODE mailbox command is used to put device in the ISP mode.

Problem

ENTER_ISP_MODE mailbox command does not work in the devices with boot ROM version T1.1.3 or lower.

Work-around

There is no work around. This issue is fixed in the ROM Bootloader versions T1.1.4 or higher, i.e. date code 1935 (yyww) onward.

3.29 PLL.1: PLL LOCK bit is not reliable

Introduction

On the LPC55S6x 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 LPC55S6x, 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.

3.30 ROM.13: Invalid TrustZone preset data structure can prevent ROM from applying specified debug settings

Introduction

On LPC55S6x 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

5.1 ISP.1: ROM runBootloader API to enter ISP mode does not work

Introduction

Devices with date code 2101 (yyww) onward, contain ROM Bootloader version T1.1.5 or higher with runBootloader API to enter into ISP mode.

Problem

RunBootloader API does not work as described in the user manual.

Work-around

User should use below code in their application to invoke auto ISP mode instead of runBootloader API.

```
PMC->AOREG1 |=(0X0A <<16);
NVIC_SystemReset();
```

5.2 ROM.7: Stack pointer for application code cannot be located in SRAM area when shared with PowerQuad and USB RAM

Introduction

Stack pointer for application code cannot be located in the SRAM area when shared with PowerQuad RAM and USB RAM.

Problem

ROM fails to check image if image stack address is >= 0x20040000 and will enter ISP mode.

Work-around

Workaround is to modify the Startup.s and assign the stack pointer to an address < 0x20040000. SDK examples have been modified to handle this scenario.

5.3 ROM.10: ROM get-property is not functional

Introduction

ROM provides get-property command feature to provide bootloader properties.

Problem

Devices with date code 2228 (yyww) and onwards contain ROM Target version T1.1.0 (or higher). On these devices, the get-property command is not functional and as a result, bootloader properties like target version cannot be read. On devices with date code before 2228 (yyww), get-property command is functional.

Work-around

None.

5.4 ROM.11: On devices with a total SRAM size of 256 KB, accessing the reserved region RAM3 will result in hard fault

Introduction

In ISP mode, boot ROM returns the kStatusMemoryRangeInvalid error code to the host when accessing a reserved region.

Problem

Devices with date code between 2219 (yyww) and 2227 (yyww) contain ROM target version T1.1.8. On these devices, accessing the reserved region (RAM3) in ISP mode results in a hard fault and does not return the kStatusMemoryRangeInvalid error code to the host.

Devices with date code between 2228 (yyww) and onwards contains ROM target version T1.1.0. On these devices, accessing the reserved region (RAM3) in ISP mode returns the kStatusMemoryRangeInvalid error code to the host.

Work-around

None.

5.5 ROM.12: On devices with total SRAM size of 144 KB, accessing reserved regions RAM3 and RAM4 will result in hard fault

Introduction

In ISP mode, boot ROM returns kStatusMemoryRangeInvalid error code to the host when accessing reserved region.

Problem

Devices with date code between 2219 (yyww) and 2227 (yyww) contain ROM Target version T1.1.8. On these devices, accessing reserved regions (RAM3 and RAM4) in ISP mode results in hard fault and does not return kStatusMemoryRangeInvalid error code to the host.

Devices with date code between 2228 (yyww) and onwards contains ROM Target version T1.1.0. On these devices, accessing reserved regions (RAM3 and RAM4) in ISP mode returns kStatusMemoryRangeInvalid error code to the host.

Work-around

None.

6 Revision history

Table 4. Revision history

Rev	Date	Description
2.8	20231219	• Updated date code in Section 5.3 "ROM.10:ROM get-property is not functional" • Added Section 5.4 "ROM.11: On devices with a total SRAM size of 256 KB, accessing the reserved region RAM3 will result in hard fault" • Section 5.5 "ROM.12: On devices with total SRAM size of 144 KB, accessing reserved regions RAM3 and RAM4 will result in hard fault" • Section 3.30 "ROM.13: Invalid TrustZone preset data structure can prevent ROM from applying specified debug settings"
2.7	20230524	• Added Section 3.29 "PLL.1: PLL LOCK bit is not reliable"
2.6	20230119	• Updated Table 3 "Errata notes" • Added Section 5.3 "ROM.9: ROM get-property is not functional"
2.5	20220620	• Added Section 3.27 "ROM.8: ROM API can't be used correctly to update and read monotonic counter in CFPA.VENDOR_USAGE word" • Added Section 3.28
2.4	20220228	Updated Section 5.1 "ISP.1: ROM runBootloader API to enter ISP mode does not work" and short description of ISP.1 in Table 3 "Errata notes"
2.3	20211111	Added Section 5.2 "ROM.7: Stack pointer for application code cannot be located in the SRAM area when shared with PowerQuad RAM and USB RAM" in Section 5 "Errata notes detail"
2.2	20210810	Added VBAT_DCDC.1: Section 3.26 "VBAT_DCDC.1: The minimum rise time of the powersupply must be 2.6 ms or slower for Tamb = -40 C, and 0.5 ms or slower for Tamb = 0 C to +105 C"
2.1	20210423	Added USB.6 errata, Section 3.23 "USB.6: In USB high-speed device mode, 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"
		Added USB.7 errata, Section 3.24 "USB.7: In USB high-speed host mode, only one transaction per micro-frame is allowed for isochronous IN endpoints"
		Added DM-AP.1 errata, Section 3.25 "DM-AP.1: I2C ISP via debug mailbox is not functional"
2.0	20210225	Added USB.5 errata, Section 3.22 "USB.5: In USB high-speed device mode, device writes extra byte(s) to the buffer if the NBytes is not multiple of 8 for OUT transfer"
		Updated date code in Section 5.
1.9	20201214	Includes Section 3.12 "USB.4: For the USB high-speed device controller, the detection handshaking fails when certain full-speed hubs are connected"
1.8	20201027	Adds Section 3.21 "WAKEIO.1: Wake-up I/O register reports incorrect wake-up source"
1.7	20200825	Adds Section 5.1 "ISP.1: ROM runBootloader API to enter ISP mode does not work"

Table 4. Revision history...*continued*

Rev	Date	Description
1.6	20191204	Updates ROM.5 workaround.
1.5	20191101	Describes ROM failure to respond to debug session request.
1.4	20191021	Add new product identification for LPC55S6x HTQFP64 package and USB.3 errata.
1.3	20190912	Describes ROM failure to enter ISP mode when an image is corrupted with flash pages in an erased or unprogrammed state.
1.2	20190710	Added USB.1, USB.2, ADC.1, ADC.2, ADC.3, GPIO.1, I2S.1, AES.1, Powerquad.1, Powerquad.2
1.1	20190221	Updated device markings.
1.0	20181204	Initial version.

7 Note about the source code in the document

Example code shown in this document has the following copyright and BSD-3-Clause license:

Copyright 2023 NXP Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials must be provided with the distribution.
3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8 Legal information

8.1 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.

8.2 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.

8.3 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_LPC55S6x