STM32WB09xE device errata

Applicability

This document applies to the part numbers of STM32WB09xE devices and the device variants as stated in this page.

It gives a summary and a description of the device errata, with respect to the device datasheet and reference manual RM0505.

Deviation of the real device behavior from the intended device behavior is considered to be a device limitation. Deviation of the description in the reference manual or the datasheet from the intended device behavior is considered to be a documentation erratum. The term *"errata"* applies both to limitations and documentation errata.

Table 1. Device summary

Reference	Part numbers
STM32WB09xE	STM32WB09KE, STM32WB09TE

Table 2. Device variants

Reference	Silicon revision codes	
	Device marking(1)	DIE_ID(2)
STM32WB09KEVx	Z	0x0110
STM32WB09TEFx		

1. *Refer to the device datasheet for how to identify this code on different types of package.*
2. *Register system controller (SYSCFG) - DIE_ID register.*

1 Summary of device errata

The following table gives a quick reference to the STM32WB09xE device limitations and their status:

A = limitation present, workaround available

N = limitation present, no workaround available

P = limitation present, partial workaround available

"-" = limitation absent

Applicability of a workaround may depend on specific conditions of target application. Adoption of a workaround may cause restrictions to target application. Workaround for a limitation is deemed partial if it only reduces the rate of occurrence and/or consequences of the limitation, or if it is fully effective for only a subset of instances on the device or in only a subset of operating modes, of the function concerned.

Table 3. Summary of device limitations

Function	Section	Limitation	Status
			Rev. Z
Radio system	2.2.1	Possible RX lock when receiving connectionless AoA/AoD packet	P
GPIO	2.3.1	Activity on some GPIOs may affect the RF performance	P
RTC	2.4.1	RTC alarm is not able internally to wakeup the device from Deepstop mode	A
	2.4.2	RTC interrupt not triggered in Run mode	P

2 Description of device errata

The following sections describe the errata of the applicable devices with Arm® core and provide workarounds if available. They are grouped by device functions.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

2.1 Core

Reference manual and errata notice for the Arm® Cortex®-M0+ core revision r0p1 is available from http://infocenter.arm.com.

2.2 Radio system

2.2.1 Possible RX lock when receiving connectionless AoA/AoD packet

Description

In some specific conditions, when it is receiving an advertising packet with CTE extension, the digital radio can be stuck in the RX state. Typically, an extended advertising packet including a CTE extension includes at least 3 bytes of payload.If the packet is malformed or corrupted over the air, and if it is understood by the digital radio with a payload length of either 1 or 2 bytes, it locks the de-framing process of the digital radio, which stays in RX state.

The digital radio stays in the RX state and never reports any interrupt to the software about the completion of the reception. This occurs using either LE_1M or LE_2M phy.

Workaround

When the software is preparing to receive an extended advertising packet with CTE (setting TxRxPack.CTEAndSamplingEnable = 1 and TxRxPack.Advertise = 1), it must assume that the radio can be locked, and never terminate the operation autonomously.

It may set a parallel timer watchdog with a duration of the maximum expected payload and CTE information. If the watchdog timer expires without receiving any interruption, it must abort the current receive operation.

2.3 GPIO

2.3.1 Activity on some GPIOs may affect the RF performance

Description

RF performance can be degraded in the presence of one of the following conditions:

- VFQFPN32 package only: toggling activity on PB14 and PB15 during RF communication
- VFQFPN32 and WLCSP36 packages: GPIOs tracks are routed close to OSCIN/OSCOUT pins and toggling activity on those GPIOs during RF communications.

The user might experience a high packet error rate during RF communications.

Workaround

- VFQFPN32 package only: avoid toggling PB14/15 (input or output) during RF communications.
- VFQFPN32 and WLCSP36 packages: avoid routing GPIO tracks close to OSCIN/OSCOUT tracks, if they are toggling during RF communications.

2.4 RTC

2.4.1 RTC alarm is not able internally to wakeup the device from Deepstop mode

Description

The RTC is able to run in Deepstop mode but it cannot generate an internal RTC alarm wake-up event.

An RTC alarm cannot be used as an internal wakeup source when the device is in Deepstop mode.

Workaround

In software, output an RTC alarm on PA8 and use this as the wakeup pin from Deepstop mode.

2.4.2 RTC interrupt not triggered in Run mode

Description

The RTC interrupts might get lost in Run mode when the selected RTC clock source is LSI or LSE. The problem does not occur when the RTC clock source is CLK_16MHz/512.

RTC interrupts cannot be reliably used for real-time control functions, since some occurrences of RTC interrupts could be missed.

Note: Wakeup from Deepstop mode is not affected and RTC interrupt is always reliable in Deepstop mode.

Workaround

While in Run mode, do not use RTC interrupts, but instead use polling on the RTC_ISR register. Another possible option is to output the RTC alarm or wakeup on PA8 or PA9, and use one of these pins as an I/O interrupt pin.

Important security notice

The STMicroelectronics group of companies (ST) places a high value on product security, which is why the ST product(s) identified in this documentation may be certified by various security certification bodies and/or may implement our own security measures as set forth herein. However, no level of security certification and/or built-in security measures can guarantee that ST products are resistant to all forms of attacks. As such, it is the responsibility of each of ST's customers to determine if the level of security provided in an ST product meets the customer needs both in relation to the ST product alone, as well as when combined with other components and/or software for the customer end product or application. In particular, take note that:

- ST products may have been certified by one or more security certification bodies, such as Platform Security Architecture (www.psacertified.org) and/or Security Evaluation standard for IoT Platforms (www.trustcb.com). For details concerning whether the ST product(s) referenced herein have received security certification along with the level and current status of such certification, either visit the relevant certification standards website or go to the relevant product page on www.st.com for the most up to date information. As the status and/or level of security certification for an ST product can change from time to time, customers should re-check security certification status/level as needed. If an ST product is not shown to be certified under a particular security standard, customers should not assume it is certified.
- Certification bodies have the right to evaluate, grant and revoke security certification in relation to ST products. These certification bodies are therefore independently responsible for granting or revoking security certification for an ST product, and ST does not take any responsibility for mistakes, evaluations, assessments, testing, or other activity carried out by the certification body with respect to any ST product.
- Industry-based cryptographic algorithms (such as AES, DES, or MD5) and other open standard technologies which may be used in conjunction with an ST product are based on standards which were not developed by ST. ST does not take responsibility for any flaws in such cryptographic algorithms or open technologies or for any methods which have been or may be developed to bypass, decrypt or crack such algorithms or technologies.
- While robust security testing may be done, no level of certification can absolutely guarantee protections against all attacks, including, for example, against advanced attacks which have not been tested for, against new or unidentified forms of attack, or against any form of attack when using an ST product outside of its specification or intended use, or in conjunction with other components or software which are used by customer to create their end product or application. ST is not responsible for resistance against such attacks. As such, regardless of the incorporated security features and/or any information or support that may be provided by ST, each customer is solely responsible for determining if the level of attacks tested for meets their needs, both in relation to the ST product alone and when incorporated into a customer end product or application.
- All security features of ST products (inclusive of any hardware, software, documentation, and the like), including but not limited to any enhanced security features added by ST, are provided on an "AS IS" BASIS. AS SUCH, TO THE EXTENT PERMITTED BY APPLICABLE LAW, ST DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, unless the applicable written and signed contract terms specifically provide otherwise.

Revision history

Table 4. **Document revision history**

Date	Version	Changes
21-Sep-2023	1	Initial release.

Contents