BlueNRG-LPS device limitations

Silicon identification

This errata sheet applies to the following STMicroelectronics BlueNRG-LPS devices:

Table 1. Ordering information

Order code	Package	Identification information of the device(1)	Device cut
BlueNRG-332A	QFN32	0x120	2.0
BlueNRG-332A	QFN32	0x121	2.1
BlueNRG-332A	QFN32	0x121	2.2(2)
BlueNRG-332V	WLCSP36	0x120	2.0
BlueNRG-332V	WLCSP36	0x121	2.1
BlueNRG-332V	WLCSP36	0x121	2.2(2)

1. *Value as read from the register system controller (SYSCFG) - DIE_ID register (0x40000000).*
2. *Cut 2.2 and cut 2.1 have the same identification information from register read, they can be distinguished through the marking information printed on the package.*

Note: For each device limitation the following information is provided:

- *Part number affected: which part number and cut is affected by the limitation (the part numbers and cuts not reported are not affected by the limitation)*
- *Description: limitation description*
- *Impact: limitation impact*
- *Workaround: possible workaround if any*

1 Limitations

The following sections describe the errata of the applicable devices with Arm® core and provide workarounds if available.

arm

Note: Arm and Cortex are registered trademarks of Arm Limited (or its subsidiaries or affiliates) in the US and/or elsewhere.

The Arm word and logo are trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved.

1.1 RTC alarm is not able to internally wake up the device from DEEPSTOP

Part numbers affected: BlueNRG-332A cut 2.0, BlueNRG-332A cut 2.1, BlueNRG-332A cut 2.2, BlueNRG-332V cut 2.0, BlueNRG-332V cut 2.1 and BlueNRG-332V cut 2.2.

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

Impact: RTC alarm cannot be used as an internal wake-up source when the device is in DEEPSTOP.
Workaround: A software workaround consists of outputting the RTC alarm on PA8 and using this pin as a wake-up pin from DEEPSTOP.

1.2 RTC interrupt not triggered in RUN mode

Part numbers affected: BlueNRG-332A cut 2.0, BlueNRG-332A cut 2.1, BlueNRG-332A cut 2.2, BlueNRG-332V cut 2.0, BlueNRG-332V cut 2.1 and BlueNRG-332V cut 2.2.

Description: The RTC interrupts could 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.

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

Workaround: While in RUN mode, don't use RTC interrupts and use polling on RTC_ISR register. Other possible options consist of outputting the RTC alarm or wakeup on PA8 or PA9 and using one of these pins as I/O interrupt pin.

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

1.3 Activity on some GPIOs may affect the RF performance

Part numbers affected: BlueNRG-332A cut 2.0, BlueNRG-332A cut 2.1, BlueNRG-332A cut 2.2, BlueNRG-332V cut 2.0, BlueNRG-332V cut 2.1 and BlueNRG-332V cut 2.2.

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

- QFN32 package only: toggling activity on PB14 and PB15 during RF communication
- QFN32 and WLCSP36 packages: GPIOs tracks are routed close to OSCIN/OSCOUT pins and toggling activity on those GPIOs during RF communications.

Impact: The users can experience high packet error rate during RF communications.

Workaround:

- QFN32 package only: avoid toggling PB14/15 (input or output) during RF communications
- QFN32 and WLCSP36 packages: avoid routing GPIO tracks close to OSCIN/OSCOUT tracks, if they are toggling during RF communications.

1.4 Possible RX lock when receiving connectionless AoA/AoD packet

Part numbers affected: BlueNRG-332A cut 2.0, BlueNRG-332A cut 2.1, BlueNRG-332A cut 2.2, BlueNRG-332V cut 2.0, BlueNRG-332V cut 2.1 and BlueNRG-332V cut 2.2.

Description:

In some specific conditions, when it is receiving an advertising packet with CTE extension, the digital radio can become 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 byte(s), it locks the de-framing process of the digital radio, which stays in RX state.

Impact:

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 the LE_1M or the 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 should abort the current receive operation.

1.5 I/Os are wrongly stated as 5 V tolerant

Description

Some datasheet revisions may wrongly state that the I/Os are 5 V tolerant, by indicating *“FT”* in the *“I/O structure”* column of the *“Pin description”* table.

Some reference manual revisions show the figures *“Basic structure of a mixed analog/digital five-volt tolerant I/O port bit”* and *“Basic structure of a digital only five-volt tolerant I/O port bit”*. However, these figures are not applicable.

These errors have been corrected in DS13819 revision 8, in RM0491 revision 2, and all the later documents revisions.

Workaround

No application workaround is applicable.

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 2. **Document revision history**

Date	Version	Changes
14-Apr-2022	1	Initial release.
23-Aug-2022	2	Updated Table 1. Ordering information. Added Section 1.3 Activity on some GPIOs may affect the RF performance and the affected part numbers on the limitation description.
16-Dec-2022	3	Added Section 1.4 Possible RX lock when receiving connectionless AoA/AoD packet.
27-Feb-2023	4	Updated: • Table 1. Ordering information • Part numbers affected in Section 1 Limitations..
12-Aug-2026	5	Added I/Os are wrongly stated as 5 V tolerant

IMPORTANT NOTICE – READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgment.

The purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of the purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

If the purchasers identify an ST product that meets their functional and performance requirements but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2026 STMicroelectronics – All rights reserved