ES NT3H2111_2211

NTAG I²C *plus*

Rev. 4.1 — 30 October 2025 **Errata**

1 Product identification

The following errata sheet entries are related to NTAG I²C *plus* NT3H2xxx product family and documents deviations from the data sheet ref.[1].

2 I²C Read command treated as I²C Write command and I²C Read/Write payload data not valid

This chapter is intended to clarify specific situations, which could arise in the NXP, focusing on the NFC tag part - NTAG I²C *plus* (Figure 1). For more details, refer to the data sheet.

This chapter describes:

- the occurrences and possible workarounds for events when I²C and RF communications happen simultaneously. These events lead to potential data corruption during reading or writing to NTAG I²C *plus* EEPROM memory
- general best practices for Host MCU Software design, to achieve a reliable I²C transaction in cases when an RF field interferes at specific timings
- NTAG I²C *plus* I²C follower address recovery mechanism, if NTAG I²C *plus* I²C address gets unintentionally reprogrammed

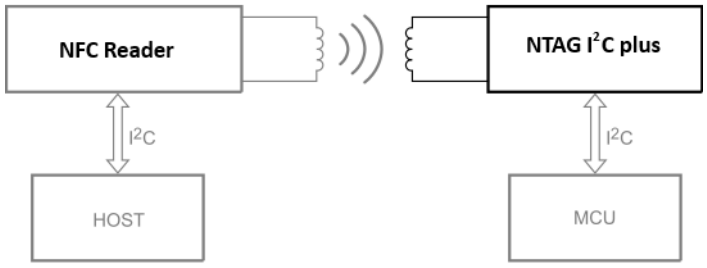

Figure 1. NFC system overview

2.1 Issue description

Table 1. Problems summary table

Scenario ID	Short description	Detailed description
1	I²C Read command treated as I²C Write command	Section 2.1.1
2	I²C Read/Write payload data not valid	Section 2.1.2

2.1.1 I²C Read command treated as I²C Write command

2.1.1.1 Scenario description

If RF field toggling (RF-ON/RF-OFF) occurs during I²C READ operation, there is a low probability that an I²C READ operation can be unintentionally turned into treated as I²C WRITE operation by NTAG I²C *plus*.

2.1.1.2 Scenario impact

EEPROM data may be unintentionally overwritten. All EEPROM memory blocks may be affected, listed ones with possible higher impact on application behavior:

1. NTAG I²C *plus* I²C follower Address (EEPROM Block0)
2. Configuration Registers (NTAG I²C *plus* startup behavior)

2.1.1.3 Recommendations

2.1.1.3.1 I²C START and STOP recommendation

Use the I²C STOP and START symbols, with a wait time of at least 50 µs between STOP and START, instead of using I²C repeated start (no STOP condition).

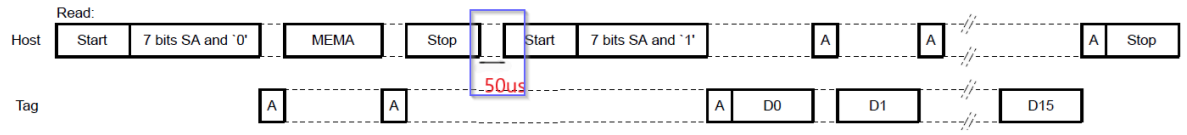

Figure 2. I²C START and STOP conditions timing recommendation

2.1.1.3.2 FD Signal Monitoring

From the MCU Host side, use FD signal to detect whether the RF field has switched ON/OFF during an I²C transaction. If the event is detected, abort and repeat the ongoing I²C transaction.

It is recommendded to check FD state:

- before initiating an I²C frame, with a minimum guard time (t_g) of 20 µs before the start of the I²C frame
- 20 µs after the I²C frame's end

FD signal latency (time between FD pin toggle and real RF ON/OFF) must be considered, more details in chapter Section 2.1.1.3.4. Below Figure 3 gives a visual representation (the timebase is not in scale).

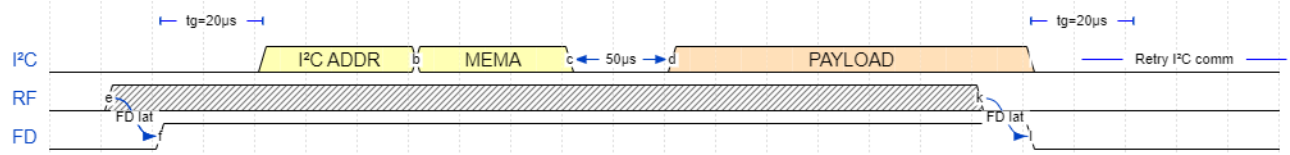

Figure 3. FD signal monitoring

2.1.1.3.3 Flow diagram of reliable I²C communication with FD pin monitoring from Host Controller

Flowchart in Figure 4 is describing the steps to ensure reliable I²C communication, while monitoring RF field status using the FD pin from the Host MCU:

1. MCU Host initially configures and enables the FD GPIO IRQ for RF-ON and RF-OFF
2. MCU Host clears the FD GPIO IRQ
3. MCU Host waits for 20 µs and FD pin latency
4. Perform I²C transaction
5. MCU Host waits for 20 µs and FD pin latency
6. MCU Host disables and reads FD GPIO IRQ
7. Based on FD GPIO IRQ read, MCU Host takes a decision to finish or continue with the I²C transaction

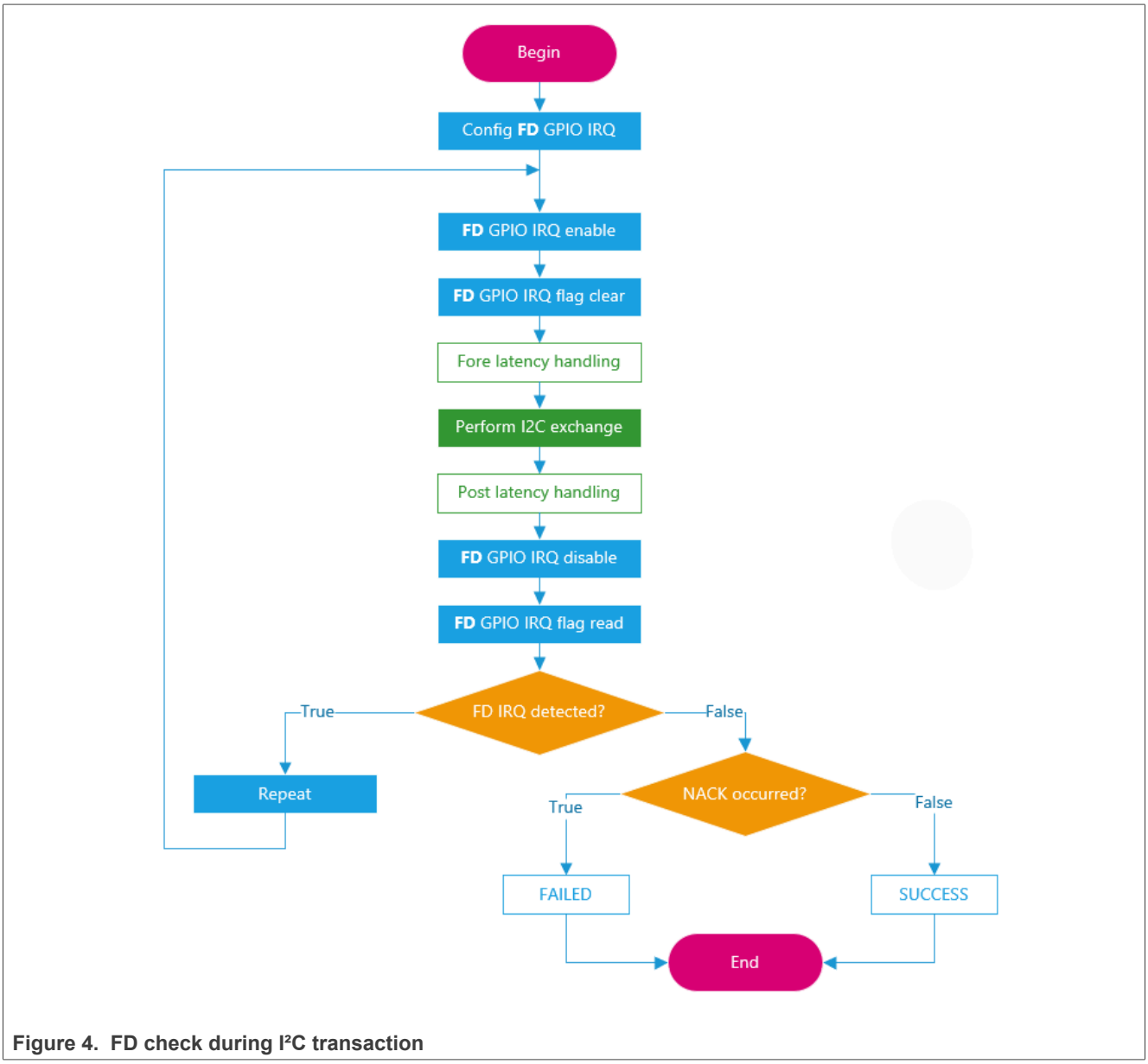

Figure 4. FD check during I²C transaction

2.1.1.3.4 FD Pin and latency explanation

FD pin can be used to monitor NFC RF field presence.

On Figure 5 it is shown:

- Typical connection of FD pin to MCU (incl. voltage level conversion)
- FD toggling latency depends on the component values used

For more information about Field Detection Pin, refer to the data sheet.

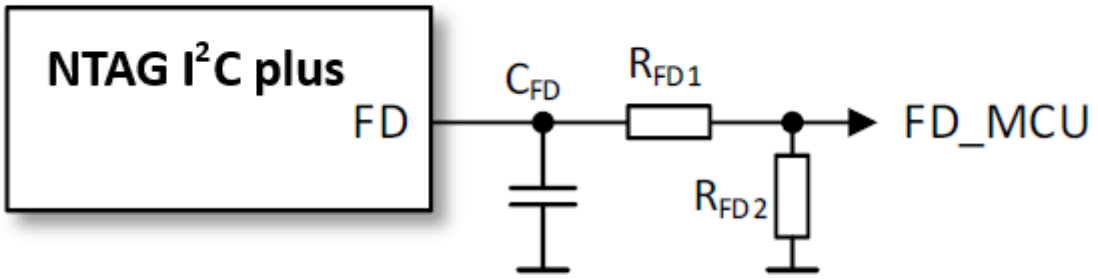

Figure 5. Typical connection of FD to MCU

2.1.2 I²C Read/Write payload data not valid

2.1.2.1 Scenario description

NTAG I²C *plus* cannot send valid data to MCU Host or can skip I²C Write, when the RF-ON/RF-OFF event occurs during I²C Read and Write transactions.

This scenario can occur due to below points mentioned in Figure 6. It is a visual representation, without precise timings.

1. RF state change (RF-ON) occurs within a 20 µs window before the I²C transaction starts.
2. RF state change (RF-OFF) happens during an I²C transaction.
3. RF state change (RF-ON) happens during an I²C transaction.
4. RF state change (RF-OFF) happens within a 20 µs window after the I²C transaction concludes.

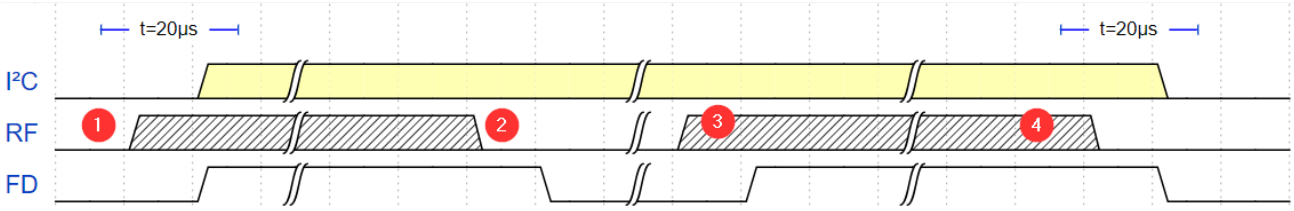

Figure 6. Scenario trigger points

Note: The latency of FD pin at points 1, 2, 3, 4 depends on the decoupling capacitor value.

2.1.2.2 Scenario impact

EEPROM data coming from an I²C READ transaction (from NTAG I²C *plus*) may not be valid.

I²C write access might be skipped and still acknowledged.

2.1.2.3 Recommendations

Refer to Section 2.3.7. In general all recommendations from Section 2.1.1.3 shall be considered.

2.2 NTAG I²C *plus* I²C address recovery mechanism

If NTAG I²C *plus* I²C follower address is corrupted, the following can be applied to recover the NTAG I²C *plus* I²C follower address.

2.2.1 NTAG I²C *plus* I²C address recovery procedure to any address between 0x00 to 0x7F

1. Scan for the address starting from 0x00 to 0x7F
2. Read a Block of NTAG I²C *plus* and verify for the status
3. Success shows the address of the device
4. With the obtained address, write back the original address of NTAG I²C *plus* in the Byte 0 of memory block 0x00
5. With the original address, perform the Read operation of the block for confirming the default address is written back properly

2.3 Best practices for Host MCU SW

2.3.1 Verify the EEPROM_WR_BUSY Flag in EEPROM Write

1. Once EEPROM Write started, the Application software shall use a HW timer for time counting, set up for 5 ms.
2. While the timer is running, the Application software checks for the EEPROM_WR_BUSY flag in the NS_REG.
3. If it's cleared before the timer expired, the EEPROM write operation is finished, exit the loop.
4. In the case of timeout – the Application software WRITE function returns an error flag, the Application software takes appropriate actions.
5. If the loop is exited before timeout (and the ERR flag isn't set), the WRITE operation completed successfully.

2.3.2 Use SESSION_REG to control and adjust NTAG I²C *plus* runtime settings

1. Content of CONFIG_REG copied into SESSION_REG at first RF_ON.
2. Content of CONFIG_REG is checked once per boot and modified if there are any wrong parameters (Can be Skipped if Configuration Register is LOCKED).
3. The Application software controls SESSION_REG for runtime settings of NTAG I²C *plus* [the Application software/application does not verify contents of SESSION_REG at boot].

2.3.3 Reset the I²C Arbitration Flag

1. Clear the I2C_LOCKED bit in the NS_REG after the common Application software functions where I²C communication is used.
2. Although the I2C_LOCKED flag will be released by WDT, the Application software does it manually to get back into the defined state and increase the speed of data flow.

2.3.4 Verify I²C communication timing parameters for 400kbits/s Fast Mode: SCL high and low time

1. SCL high time for fast mode must be greater than 950 ns.
2. SCL low time for fast mode must be greater than 1.3 µs.

2.3.5 Lock CONFIG_REG

It is recommended to set the REG_LOCK byte to 0x03 as the last step of personalization.

Table 2. Configuration bytes

Bit	Field	Access via NFC	Access via I²C	Default values	Description
Configuration register: REG_LOCK					
7-2	RFU	R&W	R&W	000000b	RFU - all 6-bits SHALL be 0b
1	REG_LOCK_I2C[1]	R&W	R&W	0b	I²C Configuration Lock Bit 0b: Configuration bytes may be changed via I²C 1b: Configuration bytes cannot be changed via I²C Once set to 1b, it cannot be reset to 0b anymore.
0	REG_LOCK_NFC[1]	R&W	R&W	0b	NFC Configuration Lock Bit 0b: Configuration bytes may be changed via NFC 1b… Configuration bytes cannot be changed via NFC Once set to 1b, it cannot be reset to 0b anymore.

[1] Setting both bits REG_LOCK_I2C and REG_LOCK_NFC to 1b, permanently locks write-access to register default values (as no write is allowed anymore). As long as one bit is still 0b, the corresponding interface can still access and change the register lock bytes.

2.3.6 Data programming/writing verification

Verify if the data was programmed correctly in the following order:

1. I²C READ the data
2. store this data for later comparison
3. I²C WRITE new data
4. I²C READ newly programmed data
5. compare 2 fetched data sets and confirm the success of I²C WRITE operation

2.3.7 Data read verification

Verify if the data read has the correct values, comparing it to known values (for example, Configuration registers) in the following order:

1. I²C READ the data
2. Compare the data
3. if compared data has not match with expected values redo I²C Read once more

3 SCL and SDA glitch

3.1 Issue description

When powering NTAG I²C *plus* via V_{CC}, I²C lines are pulled low for a specific duration during startup only.

Figure 7. Startup behavior

3.2 Issue impact

This glitch may be interpreted by other I²C targets on the same I²C bus as an I²C start condition. Ongoing I²C communication with other I²C targets may be disturbed.

3.3 Issue workaround

It is recommended to power up NTAG I²C *plus* as the first I²C target or simultaneously with other I²C targets.

Alternatively, there should be no communication with other I²C targets during NTAG I²C *plus* startup and any pulses shall be ignored for 1 ms.

4 I²C target address NAK-ed

4.1 Issue description

- NTAG does not respond on its I²C address Figure 8
- or NAKs I²C address on read part Figure 9

if RF field turns ON in the time range between ~22 µs to 16 µs before I²C start condition as depicted below in yellow:

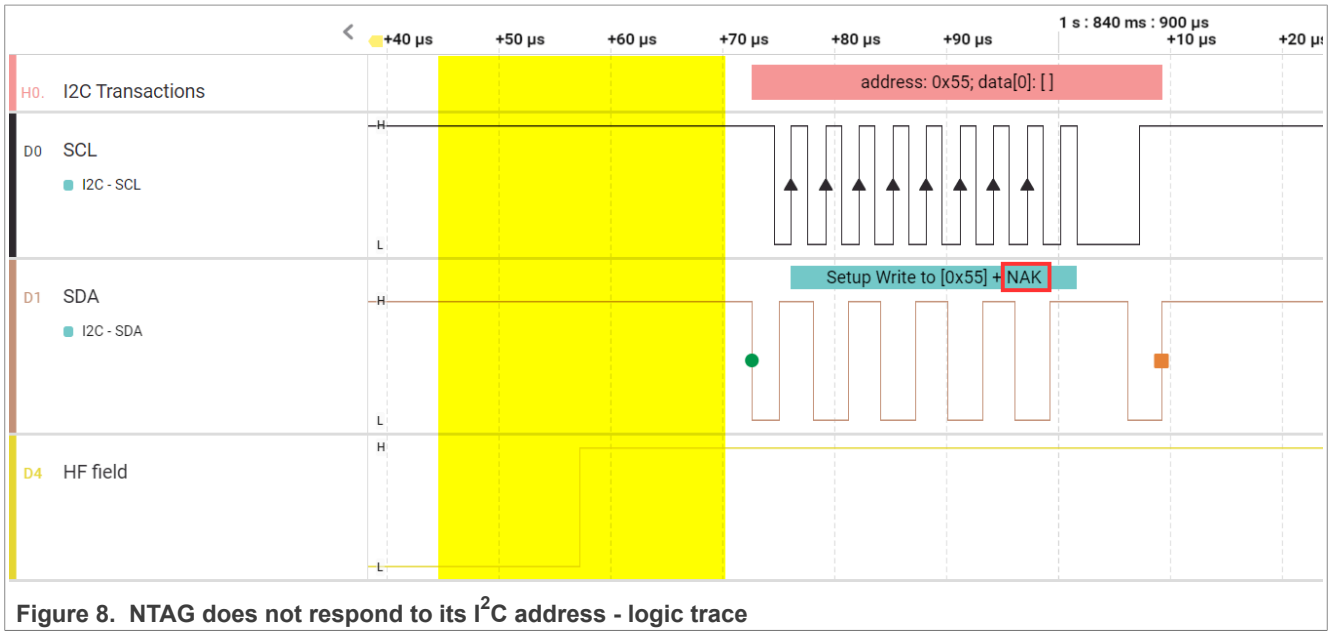

Figure 8. NTAG does not respond to its I²C address - logic trace

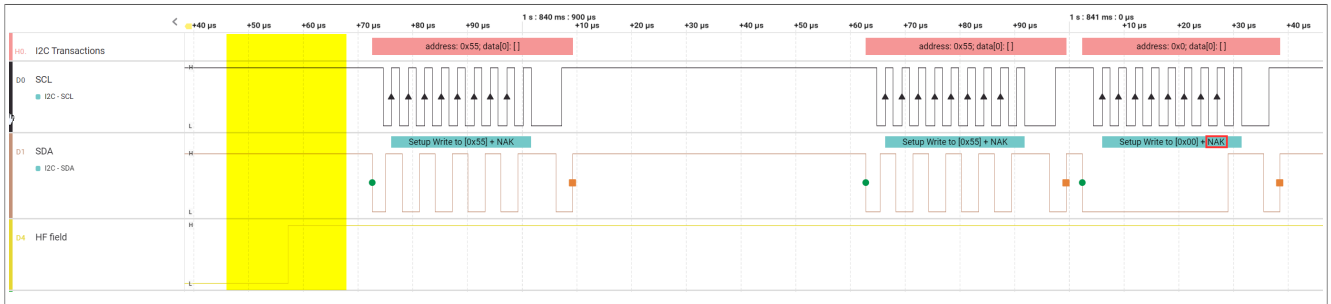

Figure 9. NAK on READ part of I²C Read frame - logic trace

4.2 Issue impact

In applications, where the I²C controller device randomly accesses NTAG's user memory (EEPROM), NTAG may not respond to its I²C address anymore. I²C command retry, VCC reset, or RF reset is needed. The issue occurs at the time when RF goes ON within the exact time-window and the I²C command frame starts (START&STOP, no repeated start).

4.3 Issue workaround

1. Retry of I²C command frame

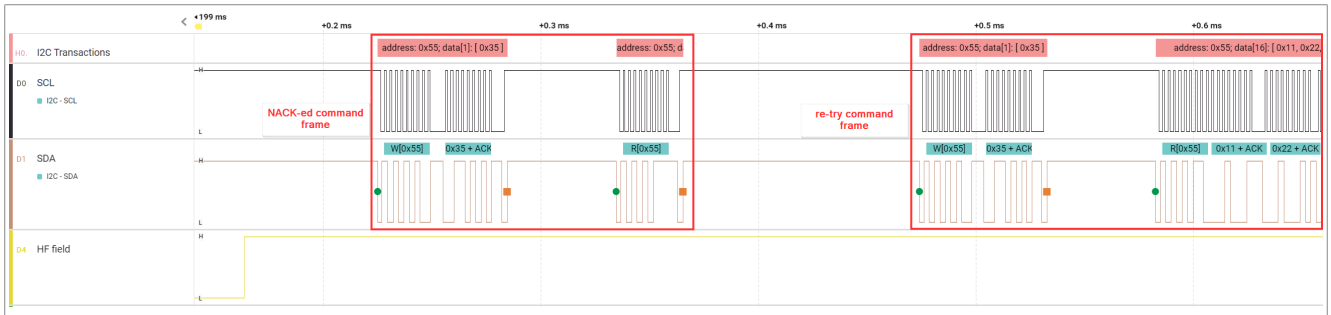

Figure 10. Retry of I²C command frame

2. VCC reset
3. RF reset

The recovery mechanism shall be done in the above order as it can happen, that a simple I²C command retry will be sufficient.

Recommendation: The frequency of accessing NTAG's EEPROM from the I²C perspective shall be as low as possible. I²C controller device shall wait for events from the RF side and act later, to avoid accessing EEPROM consequently. This would give RF interface higher priority to EEPROM access over RF and would avoid simultaneous accessing.

5 References

[1] Data Sheet – NT3H2111_2211 – NTAG I²C *plus*: NFC Forum T2T with I²C interface, password protection and energy harvesting (link)

6 Revision history

Table 3. Revision history

Document ID	Release date	Description
ES_NT3H2111_2211 v.4.1	30 October 2025	Document security status changed to "public". Editorial changes. Updated the term "NACK" to "NAK" throughout this document. • Section 5 "References": added.
ES_NT3H2111_2211 v.4.0	20 March 2025	Editorial changes. Section 2 "I²C Read command treated as I²C Write command and I²C Read/Write payload data not valid": added.
ES_NT3H2111_2211 v.3.0	3 November 2023	Section 3 "SCL and SDA glitch": added.
ES_NT3H2111_2211 v.2.0	31 October 2019	Section 4 "I2C target address NAK-ed": added.

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://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.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

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.

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.

I2C-bus — logo is a trademark of NXP B.V.

NTAG — is a trademark of NXP B.V.

Tables

Figures

Contents