MCP2517FD

MCP2517FD Silicon Errata and Data Sheet Clarification

The functionality of the MCP2517FD device is described in the device Data Sheet (DS20005688**B**), except for the anomalies described below.

1. Module: SPI Module

TX MAB underflow/RX MAB overflow due to long delays between SPI bytes

The SPI interface may block the CAN FD Controller module from accessing RAM in-between SPI bytes and between the last byte and the rising edge of the nCS line during an SPI `READ` or SPI `READ_CRC` instruction while accessing RAM.

If the CAN FD Controller module is blocked for more than TSPIMAXDLY, a TX MAB underflow or an RX MAB overflow may occur.

Fix/Work Around

Keep the delay between two SPI bytes and between the last SPI byte and the rising edge of nCS shorter than TSPIMAXDLY; see Figure 1.

The maximum allowed delay between two bytes depends on which CAN message frame is transmitted and on the selected Nominal Bit Time (NBT) and Data Bit Time (DBT). Table 1 lists TSPIMAXDLY for the worst-case scenarios.

For example: TSPIMAXDLY is 8.5 µs for a CAN FD frame at 500 kbps/2 Mbps. In comparison, an SPI byte takes 0.67 µs at 12 MHz SCK. A delay of ten times the duration of one SPI byte could cause a TX MAB underflow. It is highly unlikely for an MCU application to introduce such a long delay, but this error could occur when running an operation system, such as Linux® on a slower MPU.

In case of a TX MAB underflow, the device will notify the application by setting SERRIF and MODIF and by transitioning to Restricted Operation or Listen Only mode (depending on CiCON.SERR2LOM). After the application requests Normal mode, the CAN FD Controller module will automatically attempt to retransmit the message that caused the TX MAB underflow. It is not necessary to reset the device.

In case of an RX MAB overflow, the device will notify the application by setting SERRIF. The device will remain in Normal mode. The message that caused the RX MAB overflow will be discarded.

FIGURE 1: MAXIMUM DELAY BETWEEN SPI BYTES

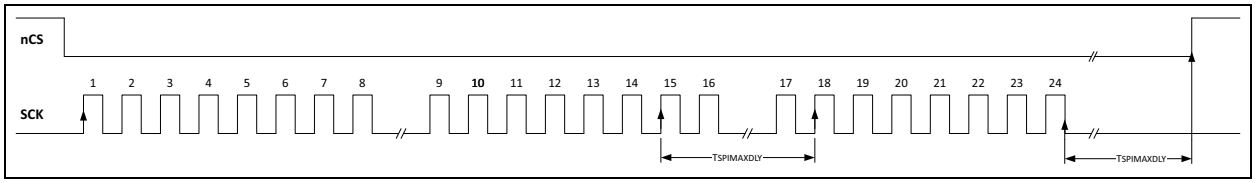

TABLE 1: WORST-CASE SCENARIOS

Scenario	Frame Format	TSPIMAXDLY
1	CAN Base Frame	5 NBT
2	CAN FD Control Field	3 NBT + 5 DBT
3	CAN FD Data Phase	32 DBT

2. Module: SPI Module

Incorrect CRC for certain READ_CRC commands

It is possible that there is a mismatch between the transmitted CRC and the actual CRC for the transmitted data when data are updated at a specific time during the SPI READ_CRC command. In these cases, the transmitted CRC is wrong. The data transmitted are correct.

Fix/Work Around:

If a CRC mismatch occurs, reissue the READ_CRC command.

Only bits 7/15/23/31 of the following registers may be affected:

- CiTXIF
- CiRXIF
- CiCON
- CiTBC
- CiINT
- CiRXOVIF
- CiTXATIF
- CiTXREQ
- CiTREC
- CiBDIAG0
- CiBDIAG1
- CiTXQSTA
- CiFIFOSTAm

The occurrence can be minimized by not using FIFOs 7/15/23/31. In these cases, the registers CiTXIF, CiRXIF, CiRXOVIF, CiTXATIF and CiTXREQ are not affected.

Bit 31 of RAM reads with CRC could also be affected. This can be avoided by reading from a received FIFO only after the message has been loaded into the FIFO, indicated by the receive flags. This is the recommended procedure independent of the issue described here.

3. Module: ECC Module

ECC Single Error Correction does not work in all cases

Fix/Work Around:

Enable Single Error Correction (SEC) and Double Error Detection (DED) interrupts by setting SECIE and DEDIE. Handle SECIF as a detection interrupt and do not rely on the error correction. Instead, handle both interrupts as a notification that the RAM word at ERRADDR was corrupted.

4. Module: SPI Module

SFR address rollover does not work

The SFR address rollover, from 0x3FF to 0x000 and from 0xFFF to 0xE00, does not work. Instead, the address changes from 0x3FF to 0x400 and from 0xFFF to 0x000.

The address rollover for the RAM works as described.

Fix/Work Around:

None.

5. Module: SPI/RAM Module

The SPI may read corrupted data from the RAM at fast SPI speeds

Simultaneous activity on the CAN bus while reading data from the RAM via the SPI interface, with a high SCK frequency, may lead to corrupted data being read from the RAM.

Fix/Work Around:

Ensure that FSCK is less than or equal to 0.85 * (FSYSCLK/2).

6. Module: SPI/GPIO Module

Writing multiple bytes to the IOCON register using one SPI WRITE instruction may overwrite LAT0 and LAT1

Writing Byte 2 and Byte 3 of the IOCON register using one SPI WRITE instruction clears LAT0 and LAT1.

Fix/Work Around:

When setting LAT0 or LAT1, do not use a multi-data byte SPI WRITE instruction. Instead, write the bit fields in the IOCON register using single data byte SFR WRITE instructions.

7. Module: SPI Module

The reading of the FIFOCI bits in the FIFOSTA register may be corrupted:

The reading of the FIFOCI bits in the FIFOSTA register for an RX FIFO may be corrupted if a certain timing is met with regards to a frame on the CAN bus. The generated CRC matches the false data. A subsequent READ will return the correct FIFOCI.

Fix/Work Around:

Perform multiple read-outs to detect unexpected data.

8. Module: SPI/Device

Failed wake up when clearing OSCDIS:

When waking up the device by clearing the OSCDIS bit, it is possible to hit a timing window where the wake up will fail. The device will wake up briefly and go back to sleep again.

Fix/Work Around:

1. Prolong the TSCK2NCS/Byte2Byte timing to at least 50 TSYSCLK cycles depending on whether regular Write commands or CRC/Write-safe commands are used. The delay needs to be after the byte containing the OSCDIS bit.
2. When polling OSCRDY to determine whether the device woke up already, ensure that two back-to-back reads of the bit show it as '1' to qualify for a successful wake up. If the second read returns a '0', repeat the wake-up sequence by writing OSCDIS to '0' again.

Clarifications/Corrections to the Data Sheet

In the MCP2517FD Data Sheet (DS20005688**B**), the following clarifications and corrections should be noted:

1. Register 3-3: CRC - CRC Register

The bit FERRIF (bit 17) may be set on illegal SPI transactions if the last successful transfer was one of the following commands: READ_CRC, WRITE_CRC or WRITE_SAFE. One example is the CS line going low and going up again without any activity on the SCK line.

This will generate a Format error and needs to be handled by clearing the error bit in the CRC Register.

APPENDIX A: REVISION HISTORY

Revision D (January 2025)

- Clarification of **Register 3-3: CRC - CRC Register** was added to **Section "Clarifications/Corrections to the Data Sheet"**.
- Added **Section 7. Module: "SPI Module"**.
- Added **Section 8. Module: "SPI/Device"**.

Revision C (September 2020)

- Added **Section 3. Module: "ECC Module"**.
- Added **Section 4. Module: "SPI Module"**.
- Added **Section 5. Module: "SPI/RAM Module"**.
- Added **Section 6. Module: "SPI/GPIO Module"**.

Revision B (July 2019)

- Updated **Section 1. Module: "SPI Module"**.
- Updated **Figure 1**.
- Added **Section 2. Module: "SPI Module"**.

Revision A (May 2018)

- Initial release of this document.

Microchip Information

Trademarks

The “Microchip” name and logo, the “M” logo, and other names, logos, and brands are registered and unregistered trademarks of Microchip Technology Incorporated or its affiliates and/or subsidiaries in the United States and/or other countries (“Microchip Trademarks”). Information regarding Microchip Trademarks can be found at https://www.microchip.com/en-us/about/legalinformation/microchip-trademarks.

ISBN: 979-8-3371-0518-5

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is “unbreakable”. Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.