

# UZ2400

## Low Power 2.4 GHz Transceiver for IEEE 802.15.4 Standard

### Errata

### ER-2400-01

The content of this technical document is subject to change without notice. Please contact UBEC for further information.

Version: 0.3  
Released Date: 2008/8/15

All rights are strictly reserved. Any portion of this paper shall not be reproduced, copied, or transformed to any other forms without permission from Uniband Electronic Corp.

**UZ2400**

Low Power 2.4 GHz Transceiver for IEEE 802.15.4 Standard

## 1. Unable to keep MISO default output high impedance

### *Description*

For the applications of multiple SPI buses, the output pin of MISO (master in, slave out) generally needs to be at high impedance state when it's disabled. While in UZ2400, the default state of MISO disable is at "low" state.

### *Workaround*

If multiple SPI buses are used, a tri-state buffer IC such as 74HC244 can be used at MISO output of UZ2400. The enabling signal of 74HC244 should be connected to the chip enable signal of slave SPI. A block diagram is shown in Figure 1. Multiple SPI slave connection.

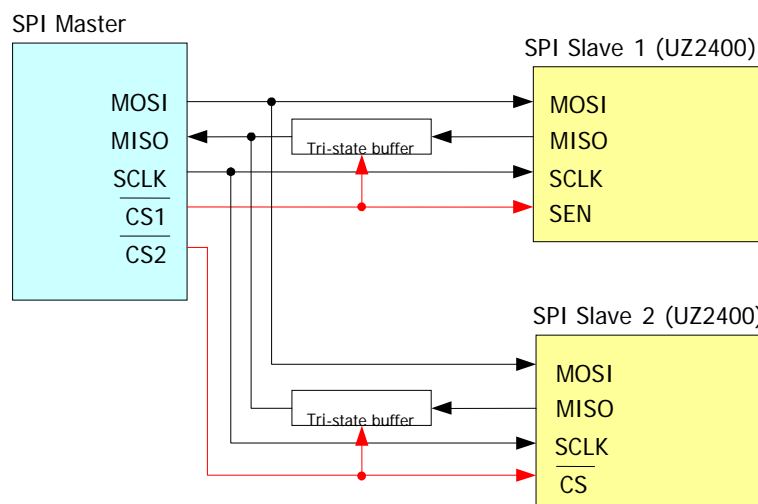


Figure 1. Multiple SPI slave connection

## **2. RXFIFO data corruption due to premature reception of the next data packet**

### ***Description***

When a packet is received and qualified, an RX interrupt is issued for the event. The data packet which is stored and locked in the RXFIFO may be corrupted if the next data packet comes in before the received data has been flushed or completely read. This is because when the user starts reading the data, the RXFIFO will begin to be unlocked.

### ***Workaround***

To prevent this from happening, one first disables the receiving path for the new incoming data in the RX-baseband by setting the RX decode bit (SReg39[2]) to inversion state "1" before reading the existing RXFIFO data.

## **3. Potential security key FIFO data change due to excessive continuous reading**

### ***Description***

There is a possibility of read error for the FIFO data when the user continuously reads (around every 100,000 times) the security key FIFO without writing any information to it in the meantime. This potential risk exists because the security key FIFO is not required to be updated for most of the applications.

### ***Workaround***

Be sure to update the security key every time, even if the key has not been changed. This will greatly reduce the likelihood for this problem to happen.

## **4. Potential read error due to SPI signal glitches**

### ***Description***

There is a remote chance (around once per million read accesses) that a read error on RXFIFO may occur due to the glitches contained in the SPI signals.

### ***Workaround***

- Observe sound layout practices (especially those for SEN and SCLK) for the SPI pin layout to minimize the

possibility of glitch occurrence to begin with.

- ❑ Adopt a payload checking code in the upper layer protocol.

## 5. Limitation of UZ2400's header length

### *Description*

Using hardware security engine of UZ2400, the header length including the auxiliary header information is limited to 31 bytes, meaning the header length field is limited to 5 bits. It was designed hardware-wise to conform to the IEEE802.15.4-2003 specification, but is too short to meet the newer IEEE802.15.4-2006 specification.

### *Workaround*

- ❑ Recommend the user not to use header length longer than 31 bytes.
- ❑ Use software encryption/decryption algorithm to overcome the 5-bit limitation of UZ2400.

## 6. Unexpected packets receiving at the 20MHz-spaced alternative channels

### *Description*

Under certain condition such as channel scanning, the UZ2400 receiver may receive unexpected packets at the 20MHz-spaced alternative channels if there are interfering sources whose intensities are sufficiently strong and whose locations are too close to the receiver. For instance, if the receiver is tuned to the 2425MHz channel, one could detect spurious signals at the 2405MHz, 2445MHz and 2465MHz alternative channels.

### *Workaround*

To prevent the system degradation due to the reception of unexpected packets caused by nearby sources, it is recommended that the user adds a "Channel ID" to the "Frame Payload" of the MAC layer (details of MAC layer structure please refer to Figure 2. Packet format for PHY and MAC or UZ2400 Datasheet DS-2400-02 V1.2 Section 3.2.1) Then the application software can filter out the unexpected packets and thus eliminate their impact to the system performance.

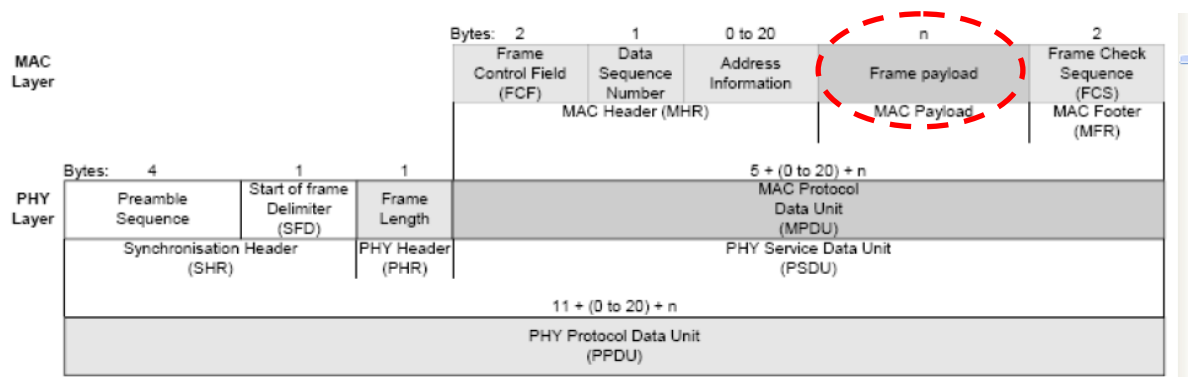


Figure 2. Packet format for PHY and MAC

## Revision History

Revision	Date	Description of Change
0.1	2008/3/26	Initial version.
0.2	2008/7/2	1. Restructure document format 2. Update V 0.1 errors to DS-2400-02 v1_1 3. Duplicate DN-2400-01 v0_1 to ER-2400-01 v0_2 and cancel DN-2400-01 v0_1
0.3	2008/8/15	Add 6. Unexpected packets receiving at the 20MHz-spaced alternative channels

## Contact UBEC:

### *Headquarters*

Address: 7F-1, No. 192, Dongguang Rd., Hsinchu, 300 Taiwan

Tel: +886-3-5729898

Fax: +886-3-5718599

Website: <http://www.ubec.com.tw>

### *Sales Services*

Tel: +886-3-5729898

Fax: +886-3-5718599

E-mail: [sales@ubec.com.tw](mailto:sales@ubec.com.tw)

### *FAE Services*

Tel: +886-3-5729898

Fax: +886-3-5718599

E-mail: [fae@ubec.com.tw](mailto:fae@ubec.com.tw)

## DISCLAIMER

ALTHOUGH TO THE BEST KNOWLEDGE OF THE UNIBAND ELECTRONIC CORPORATION (UBEC) THIS DOCUMENT IS ADEQUATE FOR ITS INTENDED PURPOSES, UBEC MAKES NO WARRANTY OF ANY KIND WITH REGARD TO ITS COMPLETENESS AND ACCURACY. UBEC EXPRESSLY DISCLAIMS ANY AND ALL OTHER WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY INCLUDING WITHOUT LIMITATION WARRANTIES OF TITLE, MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE, WHETHER ARISING IN LAW, CUSTOM, CONDUCT OR OTHERWISE.