Communicating With the RFID Base Station

Stefan Recknagel

ABSTRACT

This document describes the USB RFID base station that is delivered with the eZ430-TMS37157 demo tool. It does not describe the GUI that is delivered with the tool [for a description of the GUI and other information about the tool, see the *eZ430-TMS37157 Development Tool User's Guide* (SLAU281)]. This application report helps the reader design a custom Windows GUI to control the RFID base station. The RFID base station is capable of communicating with all Digital Signature Transponder (DST) compliant Texas Instruments transponders.

Contents

List of Figures

List of Tables

1 Introduction

The base station implements a USB to serial converter that emulates a COM port in Windows. Figure 1 shows the COM port settings that are necessary for communication with the base station.

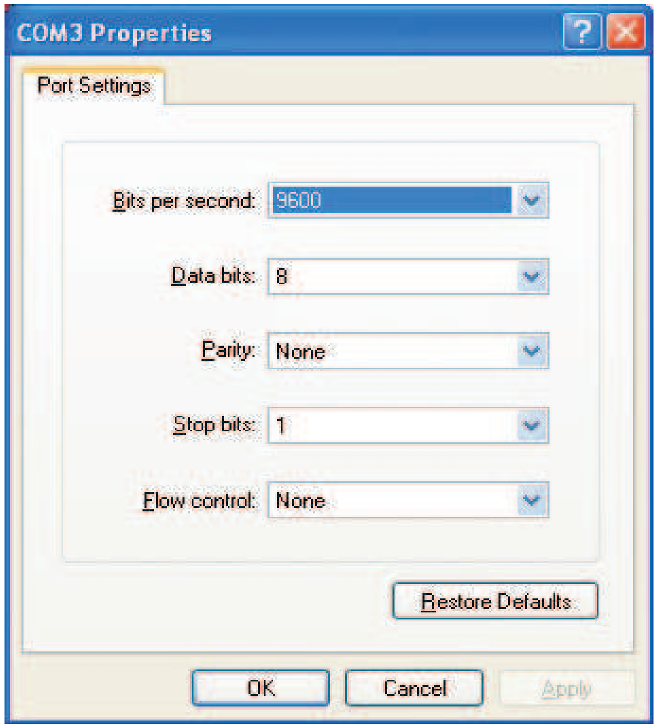

Figure 1. Com Port Settings for the USB Base Station

Upon receipt of a transponder command, the base station sends the command to an RFID transponder and also receives the answer if a transponder is in range. The downlink modulation [Pulse Width Modulation (PWM) or Pulse Position Modulation (PPM)] and the decoding of the transponder response [frequency shift keying (FSK) modulated] are handled in the base station.

The base station is capable of using PWM or PPM for the downlink protocol; the timings are predefined in the base station and cannot be changed (see Table 1 and Table 2). The user does not need to know these timings for communication with the base station; these are provided for information only.

Table 1. PWM Timings for Downlink Protocol

SYMBOL	TIME	NODE
Toff low bit	170 µs	Transmitter off time for a low bit
Ton low bit	330 µs	Transmitter on time for a low bit
Toff high bit	480 µs	Transmitter off time for a high bit
Ton high	520 µs	Transmitter on time for a high bit

Table 2. PPM Timings for Downlink Protocol

SYMBOL	TIME	NODE
Toff low bit	170 µs	Transmitter off time for a low bit
Ton low bit	230 µs	Transmitter on time for a low bit
Toff high bit	170 µs	Transmitter off time for a high bit
Ton high	350 µs	Transmitter on time for a high bit

2 Communication Protocol Between Host PC and Base Station

2.1 Downlink Protocol from Host PC to Base station

The downlink protocol to initiate a transponder command is shown in Figure 2. The base station immediately sends the corresponding command to the RFID transponder and sends a response back to the host PC, regardless of whether or not a transponder was in range.

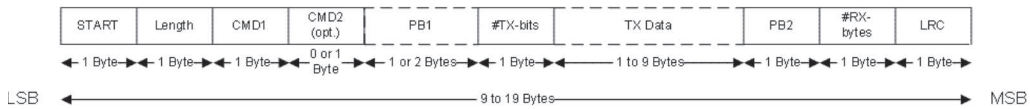

Figure 2. Downlink Protocol Structure

Table 3. Downlink Protocol Bytes

BYTE	NODE
Start	Start byte indicating a new command = 0x01
Length	Length of the whole command (bytes) excluding start byte, length and LRC
CMD1	Command byte 1
CMD2	Command byte 2 (optional)
PB1	Length of power burst 1 in ms – charge time to charge the VCL capacitor, can be extended to 2 bytes
#TX-bits	Number of bits transmitted to the transponder
TX Data	Data transmitted to the transponder
PB2	Length of power burst 2 in ms, needed for a programming or MSP access command
#RX-bytes	Number of bytes which the transponder will send back, usually 0x0A – 10 bytes (TMS37157)
LRC	Redundancy check over the data sent to the base station, excluding start byte

The structure of command byte 1 is shown in Figure 3, and its bits are explained in Table 4.

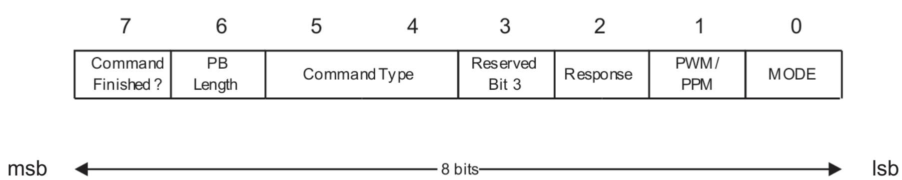

Figure 3. Command Byte 1

Table 4. Command Byte 1 Description

COMMAND FINISHED?	Bit 7	Indicates if one additional command byte is following 0 No command byte is following 1 Command byte is following
PB LENGTH	Bit 6	Length of PB1 is one or two bytes 0 PB1 is one byte 1 PB1 is two bytes
COMMAND TYPE	Bits 5 - 4	Low-frequency command type 00 Standard transponder commands (default) 01 Reserved 10 Reserved 11 Reserved
RESERVED	Bit 3	Reserved 0 Default

Table 4. Command Byte 1 Description (continued)

RESPONSE	Bit 2	Determines which response can be expected 0 Reserved 1 LF response (default)
PWM/PPM	Bit 1	Chooses which modulation is used for LF downlink protocol 0 PWM modulation is used 1 PPM modulation is used
MODE	Bit 0	Chooses between transponder mode or setup mode 0 Transponder mode (default) 1 Reserved

If bit 7 of command byte 1 is set, command byte 2 must follow. The majority of bits in command byte 2 are reserved. Command byte 2 is needed only for a battery charge command, if the magnetic field must stay on after power burst 2 and no response is expected. The structure of command byte 2 is shown in Figure 4 and its bits are explained in Table 5.

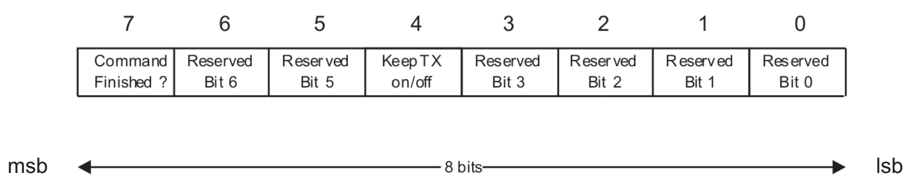

Figure 4. Command Byte 2

Table 5. Command Byte 2 Description

COMMAND FINISHED?	Bit 7	Indicates if one additional command byte follows 0 No command byte follows (default) 1 Command byte follows
RESERVED	Bit 6 - 5	Reserved 00 Default
KEEP TX ON/OFF	Bit 4	Chooses if the magnetic field (TX) should stay on after PB2 (for battery charge) 0 Turn TX off after PB2 1 Keep TX on after PB2 (no response)
RESERVED	Bits 3 - 0	Reserved 0000 Default

2.2 *Uplink Protocol from Base Station to Host PC*

The uplink protocol for the communication from the base station to the host PC is similar to the downlink protocol. The transponder answer is usually 12 bytes (TMS37157), the base station automatically deletes the 2-byte pre-bit phase; the first transponder data is then the start byte (0x7E for the TMS37157). This results in a length of 10 bytes for transponder data. The length of the uplink protocol is always 14 bytes for standard transponder commands. Figure 5 shows the structure of the uplink protocol, and its bytes are described in Table 6.

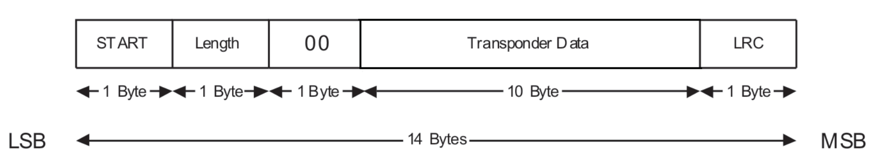

Figure 5. Uplink Protocol Structure

Table 6. Uplink Protocol Bytes

BYTE	NODE
Start	Start byte indicating an new command 0x01 (by default)
Length	Length of the whole command (bytes) excluding start byte, length and LRC, usually 0x0B – 11 bytes (TMS37157)
00	Reserved. 0x00 (default).
Transponder data	Response of the transponder begins usually with 0x7E (TMS37157)
LRC	Redundancy check over the data sent to the base station, excluding Start byte

If no transponder is in range or a battery charge command was performed, the base station responds by setting the whole transponder data (10 bytes) to 0x0.

2.3 How to Calculate the Longitudinal Redundancy Check (LRC)

The base station calculates the LRC over all bytes of the incoming and outgoing data excluding the start byte. The LRC byte is calculated by performing a XOR over the bytes. The user has to calculate the LRC over the data he sends to the base station and add it to the send string. The LRC is always the last byte of the outgoing or incoming data. The user can calculate the LRC over the received data and compare it with the received LRC for error detection.

The source code below shows a calculation routine for the LRC. It returns the LRC as a byte value.

```
public byte LRC_calc(byte[] bytes, int length)
{
    int lrc;

    lrc = bytes[0];

    for (int i = 1; i < length; i++)
    {
        lrc = lrc ^ bytes[i];
    }

    return (byte)(lrc);
}
```

3 Summary

This application report provides the user of the RFID base station the possibility of writing a custom GUI for communicating with the RFID base station. In conjunction with the TMS37157 PaLFI data sheet, the user can create custom transponder commands that extend the capabilities of the RFID demo software delivered with the eZ430-TMS37157 demo tool.

4 References

1. *TMS37157 Passive Low-Frequency Interface (PaLFI) Device With EEPROM and 134.2-kHz Transponder* data sheet (SWRS083)
2. *eZ430-TMS37157 Development Tool User's Guide* (SLAU281)
3. *Low-Frequency RFID in a Nutshell* (SWRA284)