**ZB-BOOTLOADER-MODBUS Specification**

*Rev 0.1*

*Last Updated, Sep/30/2019*

*Scanjet Macron*

*This page is left blank intentionally*.

Table of contents

[1. Objective 4](#_Toc15544698)

[2. Introduction 4](#_Toc15544699)

[3. Communication Parameters 4](#_Toc15544700)

[4. MODBUS RTU Slave Address 4](#_Toc15544701)

[5. MODBUS Registers 5](#_Toc15544702)

[5.2. Firmware Page Buffer Register 7](#_Toc15544703)

[5.3. Running Mode Register 8](#_Toc15544704)

[5.4. Command Register 8](#_Toc15544705)

[5.5. Bootloader Version 8](#_Toc15544706)

[5.6. Recommended Firmware Flashing Procedure 9](#_Toc15544707)

1. Objective

This document aims at describing MODBUS protocol used by bootloader of ZB boards.

1. Introduction

ZB-BOOTLOADER-MODBUS acts as MODBUS RTU slave. ZB-BOOTLOADER-MODBUS accepts requests from MODBUS RTU master and responds appropriately as specified in MODBUS RTU standard literatures and this document.

1. Communication Parameters

ZB-BOOTLOADER-MODBUS board provides industry standard RS485 interface to communicate with MODBUS RTU masters. The communication parameters used by ZBANA-MODBUS are as follows.

|  |  |  |
| --- | --- | --- |
| Parameter | Value | Note |
| Baud Rate | 38400 BPS | - |
| Parity | No parity | - |
| Stop Bit | 1 stop bit | - |
| Data | 8 bit | - |

1. MODBUS RTU Slave Address

MODBUS RTU Slave address is set by adjusting address selector rotary switch on the board. MODBUS RTU Address is decided using the following formula.

***MODBUS RTU Address = 10 + Rotary Switch Value***

For example, if you set the rotary switch to 5, the MODBUS RTU address becomes 15.

***Rotary Switch Address 15, that is, MODBUS address 25, isn’t available for normal use. The rotary switch position is used to force the board to enter bootloader mode so that the board can be recovered from corrupted application firmware.***

1. MODBUS Registers

|  |  |  |
| --- | --- | --- |
| Register Type | Address | Description |
| Holding | 30000 | Firmware Page Address Register |
| Holding | 31000 ~ 31127 | Firmware Page Buffer Register |
| Holding | 32000 | Running Mode Register |
| Holding | 33000 | Command Register |
| Holding | 34000 | Bootloader Version |

**All the 16 bit registers are in big-endian format unless specified otherwise, that is, high byte comes first.**

* 1. Firmware Page Address Register

ATMEGA flash memory is organized as a group of pages and programming the flash should be performed on page basis. **Page size is 256 bytes and Firmware Page Address Register contains page number** in the flash for actions (read/write) to be performed.

Before any read or write action, this page address register should be set appropriately.

Page Number is calculated using the following simple formula.

***Page number = address / 256***

* 1. Firmware Page Buffer Register

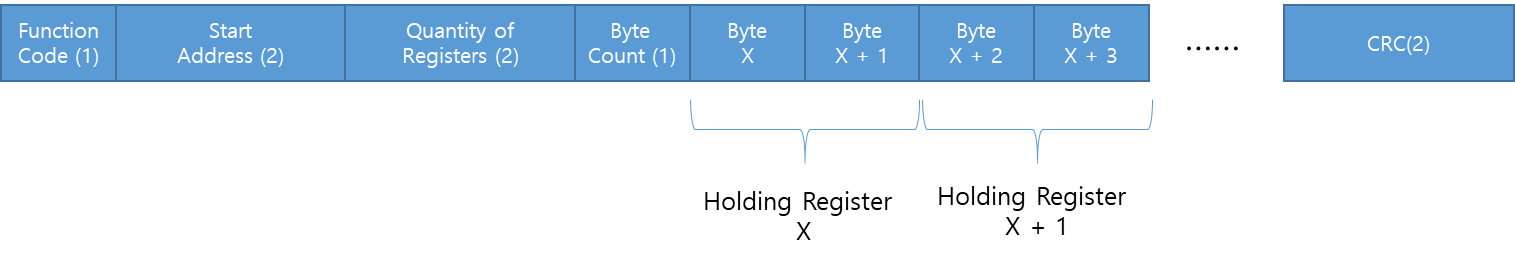
Flash programming and reading are performed on page basis. Firmware Page Buffer Register contains either

1. 256 byte of firmware data to be programmed or
2. 256 bytes of firmware data read from flash

Before programming a page, the whole 256 byte of these registers should be written, and the whole 256 byte of these registers are filled with data read from flash after read command.

For a program operation, if the target page of the firmware image has less than 256 bytes of data, then the remaining bytes should be filled with 0xff.

***Lower byte of page occupies MSB of this 16 bit register and higher byte of page occupies LSB of this 16 bit register assuming that 16 bit holding register is in big endian format. In MODBUS RTU frame, the firmware data should be carried over MODBUS RTU frame as shown below.***



* 1. Running Mode Register

Running Mode Register is used to exit from bootloader.

Value 0 in this register indicates that the board is running in bootloader mode.

Value 1 in this register indicates that the board is running in application mode.

Writing 1 to this register causes the bootloader to exit and run into application mode.

* 1. Command Register

Command Register is used to initiate program or read actions. The following commands are defined.

|  |  |
| --- | --- |
| Commands | Description |
| 1 (Program) | Program data in ***Firmware Page Buffer Register*** into flash page specified in ***Firmware Page Address Register*** |
| 2 (Read) | Read flash page specified in ***Firmware Page Address Register*** into ***Firmware Page Buffer Register*** |

* 1. Bootloader Version

This register holds bootloader program version. Writing to this register has no effect.

* 1. Recommended Firmware Flashing Procedure

