

Introduction

For the correct management of a MODBUS network the master must know how to query each slave, that which communication protocol, which function codes and which addresses for the slaves and their parameters. This document provides all the information required for the master configuration: details about the physical layer (RTU, baud rate, etc), implemented Modbus function codes, and exchange parameters address map.

Electrical characteristics

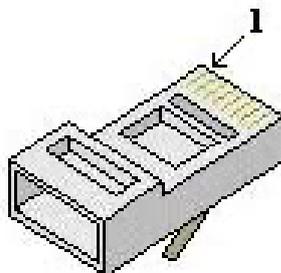
The unit is a **SLAVE** in a MODBUS network. The slave units are compliant to the following specifications:

- | | |
|--------------------------|---|
| 1. Transmission mode: | MODBUS RTU |
| 2. Electrical Interface: | RS485 half-duplex serial line |
| 3. Baud rate: | 4800 / 9600 / 19200 / 38400 (default) bps |
| 4. Data format: | 8 data bits |
| 5. Parity: | even (default) / odd / none |
| 6. Stop bits: | 1 (parity odd or even) / 1 or 2 selectable (parity none) |
| 7. Slave address: | configurable in the range 1 (default) to 247 |
| 8. Connector type: | RJ45 |
| 9. Cable: | shielded twisted pair, 8-wire RJ-45 plug |

According to the device size, as specified in the user manual, the following differences apply:

	Size 3	Size 4
Connector name	AUX2	AUX2 – AUX3
Terminator	120Ω fixed	none (dipswitch off) or 120Ω (dipswitch on)
Bias	560Ω fixed resistor between A and +5V 560Ω fixed resistor between B and GND	FAILSAFE A: none (dipswitch off) or 560Ω resistor between A and +5V (dipswitch on) FAILSAFE B: none (dipswitch off) or 560Ω resistor between B and GND (dipswitch on)
Pinout (fig. below)	A = pin 2, B = pin 1, Common = pin 3	A = pin 5, B = pin 4, Common = pin 3

RJ-45 connector



Functional characteristics

The slave waits for a request from the master, and checks the received packet before performing the action requested in it. In case of errors in the request (e.g. illegal function, illegal address, etc.), the master is notified with an error packet. If no errors are found, the requested action is performed and a reply is sent to the master. All the parameters are 16 bit Holding Registers (HR), with address range 40001-40114.

As far as the Modbus communications is concerned, the device can be operated in **monitoring mode** or in **configuration mode**. For the setting of the monitoring and configuration mode refer to the product user manual.

The **configuration mode** is activated engaging the relevant dipswitch or jumper in conjunction with a battery chemistry selected by means of the device hardware controls at powerup. The configuration mode allows customizing the charging curve of the selected chemistry and storing the modified values in the device internal non-volatile memory. In the configuration mode, the device ignores the front panel controls and uses the parameter values recalled from the device non-volatile memory. However, if during the configuration mode the chemistry is changed with respect to the chemistry referred to by the stored parameters, the newly selected chemistry defaults are stored and the previously customized parameters are lost. The holding register 40027 provides information on whether the configuration mode is enabled (value = 1) or not (value = 0). The configuration mode can be enabled or disabled as described when the battery is not connected to the device.

When the configuration mode is not enabled the device uses the front panel controls. The corresponding configuration holding registers become read-only and mirror the relevant configuration value set using the front panel controls (e.g. the holding register 40072 displays the charge current limit currently set by the front panel potentiometer; the holding register 40104 displays the buffering time in units of seconds corresponding to the front panel time buffering control). Such operating mode is called the **monitoring mode**.

The following hardware controls are always used in both the configuration and the monitoring mode and have no writable configuration holding register counterpart:

- The battery chemistry selection dipswitches or jumpers, which are read at powerup only
- The configuration mode enable dipswitch or jumper, which is read when no battery is connected.
- The "Selection out voltage" jumper, read at powerup only, and used to select the device rated output voltage (size 4 only – refer to the device user manual)

The following holding registers can always be written both in the configuration and the monitoring mode:

- Holding register 40001 (Address of slave unit)
- Holding register 40065 (History clear all: write the value 1 to clear all the histories)
- The history holding registers (only the value 0 to clear the respective history is accepted)

The alarms that are mapped as bitmask in holding registers are active when the bit value is 1.

Note that valid values written to writable holding registers are automatically stored in the device non-volatile memory.

In configuration mode, in size 3 products, turn the front panel potentiometer completely clockwise to be able to perform the current limitation set in the holding register 40072.

The following Modbus functions for HR management are supported: function code 3 (read holding registers), function code 6 (preset single register), function code 16 (preset multiple registers). A summary of the implemented function codes follows.

In all cases, the slave address must be within 1 and 247; the data addresses are computed subtracting 40001 from the holding register number, e.g. to access holding register 40092 the value $(40092 - 40001) = 91 = 0x5B$ must be entered. The CRC at the end of each frame is

computed as detailed in the “Modbus over serial line specification and implementation guide V1.02” document, available for free from www.modbus.org.

Function code 3 (0x03): Read Holding Register

Request (Master to Slave)

Field name ->	Slave address	Function code	Start address	Number of registers (N)	CRC
Field bytes ->	1 byte	1 byte	2 bytes	2 bytes	2 bytes
Range ->	0x01 – 0xF7	0x03	0x0000 – 0x0071	0x0001 – 0x0072	see text

Example 1 - reading the first holding register (i.e. the slave address) of a CBI280W having slave address 1 (factory default):

01 03 00 00 01 84 0A

Example 2 - reading all the 114 holding registers of a CBI280W having slave address 1 (factory default).

01 03 00 00 00 72 C5 EF

Response (Slave to Master)

Field name ->	Slave address	Function code	Number of data bytes to follow	Registers data	CRC
Field bytes ->	1 byte	1 byte	1 byte	N * 2 bytes	2 bytes
Range ->	0x01 – 0xF7 (same as the request)	0x03	2 * N	actual data read	see text

Example: response of a CBI280W having slave address 1 (factory default) to a read request of the first holding register (i.e. its own slave address):

01 03 02 00 01 79 84

Error (Slave to Master)

Field name ->	Slave address	Function code	Exception code	CRC
Field bytes ->	1 byte	1 byte	1 byte	2 bytes
Range ->	0x01 – 0xF7 (same as the request)	0x83	0x01 - 0x02	see text

Function code 6 (0x06): Write Single Register

Request (Master to Slave)

Field name ->	Slave address	Function code	Data address of the register	Value to write	CRC
Field bytes ->	1 byte	1 byte	2 bytes	2 bytes	2 bytes
Range ->	0x01 – 0xF7	0x06	0x0000 – 0x0071	0x0000 to 0xFFFF	see text

Response (Slave to Master)

Field name ->	Slave address	Function code	Data address of the register	Value written	CRC
Field bytes ->	1 byte	1 byte	2 bytes	2 bytes	2 bytes
Range ->	0x01 – 0xF7 (same as the request)	0x06	0x0000 – 0x0071 (same as the request)	0x0001 – 0xFFFF (same as the request)	see text

Error (Slave to Master)

Field name ->	Slave address	Function code	Exception code	CRC
Field bytes ->	1 byte	1 byte	1 byte	2 bytes
Range ->	0x01 – 0xF7 (same as the request)	0x86	0x01 - 0x02	see text

Function code 16 (0x10): Write Multiple Register

Request (Master to Slave)

Field name ->	Slave address	Function code	Data address of the first register (addr)	Number of registers to write (N)	No. of data bytes to follow	Values to write	CRC
Field bytes ->	1 byte	1 byte	2 bytes	2 bytes	1 byte	N * 2 bytes	2 bytes
Range ->	0x01 – 0xF7	0x10	0x0000 – 0x0071	0x0000 to 0x0072	2 * N	data @addr, data @(addr+1) etc.	see text

Response (Slave to Master)

Field name ->	Slave address	Function code	Data address of the first register	Number of registers written	CRC
Field bytes ->	1 byte	1 byte	2 bytes	2 bytes	2 bytes
Range ->	0x01 – 0xF7 (same as the request)	0x10	0x0000 – 0x0071 (same as the request)	N	see text

Error (Slave to Master)

Field name ->	Slave address	Function code	Exception code	CRC
Field bytes ->	1 byte	1 byte	1 byte	2 bytes
Range ->	0x01 – 0xF7 (same as the request)	0x90	0x01 - 0x02	see text

Communications parameters settings

Devices are configured for communications at **38400bps** with **even parity (1 stop bit)** by default. The permissible slave address range is 1-247. Such address must be unique for every slave present in the same Modbus network and it is stored in HR 40001. Its default value is 1. Similarly it is possible to modify the serial communication default settings (baud rate and parity), that are stored at the holding registers 40002 and 40003. **After any of them are modified, the master must query the slave using such modified settings.** Holding register 40003 sets the parity value for the serial communications and also the number of the expected stop bits. Note that irrespective of the device configuration (monitoring or configuration mode), it always uses the communications parameter (HR40001 thru HR40003) values stored in the internal user non-volatile memory.

Restoring communications parameters to factory settings

To restore the communication parameter values (slave address, baud rate, parity):

1. switch off the device disconnecting both the AC mains and the battery;
2. turn the "TIME BUFFERING" selector to position 7;
3. turn the "BATTERY CHARGING LEVEL" trimmer fully counterclockwise to position MIN;
4. press the "BATTERY START" button and then switch on the device connecting the AC mains;
5. keep pressed the "BATTERY START" button for 10 seconds; during these 10 seconds the 3 LEDs stay steady ON; at the end of these 10 seconds all 3 LEDs (together with the 2 relays) will toggle 3 times, and then the unit starts up with default communication settings restored;
6. henceforth, the "TIME BUFFERING" selector and the "BATTERY CHARGING LEVEL" trimmer are available again for their standard function;

NOTE – If during the 10 seconds the "BATTERY START" button is released or the "TIME BUFFERING" selector or the "BATTERY CHARGING LEVEL" are changed, the unit starts up immediately (without the 3 LEDs triple blinking) and the communication settings remain the previous ones; the factory ones are NOT restored.

Restoring configuration parameters to factory settings

Whatever the current set of values of parameters be, writing the value 1 to Holding Register 40066 restores the default charging algorithm (i.e. the Open Lead one) and its respective default values. Writing to holding register 40066 is only possible when the device is set for the configuration mode and the battery is not connected.