Modbus Protocol

Technical description

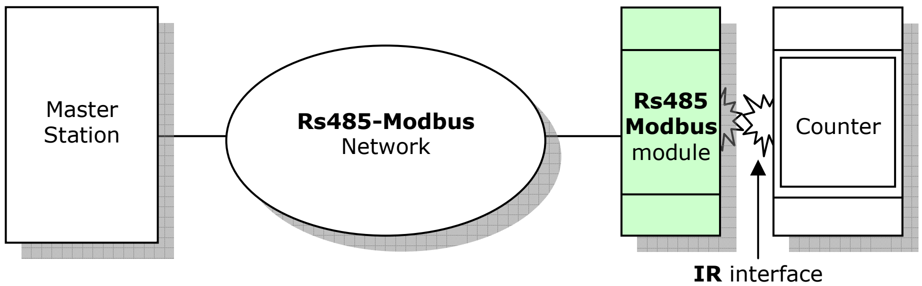
Version 1.0

1. Index

2. Preface

2.1. Overview

The present guide describes the implementation of the Mobus Protocol on the Modbus communication interface.
The interface can be connected to a RS485 Modbus network and can be controlled by a Mobus master station over this network.



The interface supports both the RTU and the ASCII communication protocols modes and it is configurable for what concern to the transmission parameters (speed, parity, stop bits).
Every parameter is controlled by a Modbus register so you can configure the interface by a sequence of writings into the internal interface registers.

2.2. Default settings

These are the factory default settings:

- Protocol: Modbus RTU
- Modbus Address: 001
- Baud rate: 19200 bit/s
- Parity: None
- Stop bits: 1

3. Modbus commands

The interface supports only two type of commands, one for reading the register values, one for writing the configuration registers. The reading is only possible for a block of registers (the command for a single register reading is not supported).

3.1. Read holding registers (function code 03)

This function code is used to read the contents of a contiguous block of holding registers in a remote device. The Request frame specifies the starting register address and the number of registers.
The register data in the response message are packed as two bytes per register, with the binary contents left justified within each byte. For each register, the first byte contains the low order bits and the second contains the high order bits; note that the interface BE (Basic and Full) configured with register 4117=0 (value format 32 bit floating point) is an exception to this rule: for each register, the first byte contains the high order bits and the second contains the low order bits. In many cases more than one register is used to represent the same quantity to allow a correct representation of the quantity value (for example, the active energy is represented using 4 registers – 8 bytes -) Please refer to the chapter "Internal registers" for details.

Warning!
Because of the limited size of a Modbus frame, not all the internal registers can be sent on a single reading request. This means that a complete snapshot can only be acquired performing more (three) read holding registers calls with different starting address.
Example:
poll nr. 1 start 4099 nr. of registers 100
poll nr. 2 start 4197 nr. of registers 100
poll nr. 3 start 4297 nr. of registers 10

3.1.1. Frame layout

ADR	03	STh	STl	NRh	NRl	CRCh	CRCl

ADR	Modbus Address
03	Read holding register function code (fixed)
STh	Starting address register (high order bits)
STl	Starting address register (low order bits)
NRh	Number of registers (high order bits)
NRl	Number of registers (low order bits)
CRCh	Modbus Checksum (high order bits)
CRCl	Modbus Checksum (low order bits)

3.2. Write single register (function code 06)

This function code is used to write a single holding register in a remote device. The Request specifies the address of the register to be written. The normal response is an echo of the request, returned after the register contents have been written.

3.2.1. Frame layout

ADR	06	RAh	RAl	RVh	RVl	CRCh	CRCl

ADR	Modbus Address
06	Write single register function code (fixed)
RAh	Register address (high order bits)
RAl	Register address (low order bits)
RVh	Register value (high order bits)
RVl	Register value (low order bits)
CRCh	Modbus Checksum (high order bits)
CRCl	Modbus Checksum (low order bits)

4. Internal registers

This is the complete list of the internal registers.

Register Address	Designation	Interface & counter types DRM-**-3P	DRM-**-1P	SA	SE	Notes
4099	Device type	x	x	x	x	General reading registers
4100	Firmware version	x	x	x	x	
4101	Range overflow alarm	x	x	x	x	
4102	Running tariff	x	x	x	x	
4104	PID (Product Identification) bytes 1 and 2	x	x	x	x	
4105	PID – bytes 3 and 4	x	x	x	x	
4106	PID – bytes 5 and 6	x	x	x	x	
4107	PID – bytes 7 and 8	x	x	x	x	
4108	PID – bytes 9 and 10	x	x	x	x	
4109	PID – bytes 11 and 12	x	x	x	x	
4110	PID – bytes 13 and 14	x	x	x	x	
4111	Protocol type	x	x	x	x	Writing registers
4112	Speed	x	x	x	x	
4113	Parity	x	x	x	x	
4114	Stop bits	x	x	x	x	
4115	Modbus address	x	x	x	x	
4116	Reset interface command	x	x	x	x	
4117	Value format	x	x	x	x	
4118	Reset energy counters command	x	x	x	x	
4119	Active Energy 1st phase T1, imp (kWh)	x	x	x	x	Reading quantities registers
4123	Active Energy 2nd phase T1, imp (kWh)	x	x			
4127	Active Energy 3rd phase T1, imp (kWh)	x	x			
4131	Active Energy Σ T1, imp (kWh)	x	x			
4135	Active Energy 1st phase T2, imp (kWh)	x	x	x	x	
4139	Active Energy 2nd phase T2, imp (kWh)	x	x			
4143	Active Energy 3rd phase T2, imp (kWh)	x	x			
4147	Active Energy Σ T2, imp (kWh)	x	x			
4151	Active Power 1st phase (kW)	x	x	x	x	
4153	Active Power 2nd phase (kW)	x	x			
4155	Active Power 3rd phase (kW)	x	x			
4157	Active Power Σ (kW)	x	x			
4161	Active Energy 1st phase T1, exp (kWh)	x	x	x	x	
4165	Active Energy 2nd phase T1, exp (kWh)	x	x			
4169	Active Energy 3rd phase T1, exp (kWh)	x	x			
4173	Active Energy Σ T1, exp (kWh)	x	x			
4177	Active Energy 1st phase T2, exp (kWh)	x	x	x	x	
4181	Active Energy 2nd phase T2, exp (kWh)	x	x			
4185	Active Energy 3rd phase T2, exp (kWh)	x	x			
4189	Active Energy Σ T2, exp (kWh)	x	x			
4193	Reactive Energy 1st phase T1, imp (kvarh)	x	x	x	x	
4197	Reactive Energy 2nd phase T1, imp (kvarh)	x	x			
4201	Reactive Energy 3rd phase T1, imp (kvarh)	x	x			
4205	Reactive Energy Σ T1, imp (kvarh)	x	x			
4209	Reactive Energy 1st phase T2, imp (kvarh)	x	x	x	x	
4213	Reactive Energy 2nd phase T2, imp (kvarh)	x	x			
4217	Reactive Energy 3rd phase T2, imp (kvarh)	x	x			
4221	Reactive Energy Σ T2, imp (kvarh)	x	x			
4225	Reactive Energy 1st phase T1, exp (kvarh)	x	x	x	x	
4229	Reactive Energy 2nd phase T1, exp (kvarh)	x	x			

4233	Reactive Energy 3rd phase T1, exp (kvarh)	x	x		
4237	Reactive Energy Σ T1, exp (kvarh)	x	x		
4241	Reactive Energy 1st phase T2, exp (kvarh)	x	x	x	x
4245	Reactive Energy 2nd phase T2, exp (kvarh)	x	x		
4249	Reactive Energy 3rd phase T2, exp (kvarh)	x	x		
4253	Reactive Energy Σ T2, exp (kvarh)	x	x		
4257	Reactive Power 1st phase (kvar)	x	x	x	x
4259	Reactive Power 2nd phase (kvar)	x	x		
4261	Reactive Power 3rd phase (kvar)	x	x		
4263	Reactive Power Σ (kvar)	x	x		
4267	L1-N voltage (V)	x		x	
4269	L2-N voltage (V)	x			
4271	L3-N voltage (V)	x			
4273	L1-L2 voltage (V)	x			
4275	L2-L3 voltage (V)	x			
4277	L3-L1 voltage (V)	x			
4279	phase1 current (A)	x		x	
4281	phase2 current (A)	x			
4283	phase3 current (A)	x			
4285	apparent power phase1 (kVA)	x		x	
4287	apparent power phase2 (kVA)	x			
4289	apparent power phase3 (kVA)	x			
4291	apparent power Σ (kVA)	x			
4295	power factor cos φ phase1	x		x	
4297	power factor cos φ phase2	x			
4299	power factor cos φ phase3	x			
4301	power factor cos φ Σ	x			
4303	frequency (Hz)	x		x	

4.1. Interface and counter types

Depending on the type of the Modbus interface (Basic or Full) you are working with and depending also on the counter connected to the Modbus interface, you have a different set of registers at your disposal.
In the table above, you can see four columns where all the possible combination are listed:

DRM--3P** **Three-Phase counter and Full interface. All the quantities**.
TE Three-Phase counter and Basic interface. Energy quantities on all the phases.
DRM--1P** **Single-Phase counter and Full interface. All the quantities on a single phase**.
SE Single-Phase counter and Basic interface. Energy quantities on a single phase.

Anyway, all the registers can always be read but if you try to access a register not supported in the combination counter-interface you have, you will get a value of 0.
Example: if you try to read the register 4267 (voltage on L1) when you have a three-phase counter and a Basic interface (TE column) you will always get a value of 0, because the interface is not allowed to send out this quantity.

4.2. General reading registers

This family of registers store general information about the interface.
All the registers are always available regardless to the combination counter-interface you have.

Register	Designation	Description
4099	Device type	Code that identify the combination interface-counter 0 No communication with the counter on the IR port 1 Three-phase Full 2 Three-phase Basic 3 Single-phase Full 4 Single-phase Basic
4100	Firmware version	Version of the interface firmware

4101	Range overflow alarm	The register is set by the counter if it has the detected a value over the voltage or the current nominal threshold. The lowest order byte of the register is bit-coded as follows: n.u.|n.u.|OFV3|OFI3|OFV2|OFI2|OFV1|OFI1 Where: OFV Voltage overflow (on phase 1, 2 and 3) OFI Current overflow (on phase 1, 2 and 3) n.u. Not Used
4102-03	Running tariff	0 Tariff 1 is currently in use 1 Tariff 2 is currently in use
4104-10	PID	Part number identification string (a maximum of 14 bytes)

4.3. Writing registers

This set of registers is for the interface configuration. One register (4118) is dedicated to request the reset of the counter internal energy registers.
All the registers are always available regardless to the combination counter-interface you have.

The registers from 4111 to 4115 are controlled by the Reset interface command register (4116): all the changing you make to the first ones take effect only when you ask a reset of the interface by assigning a value of 1 to the last one.
Any change to the registers 4117 and 4118 is immediately effective.

Register	Designation	Description	
4111	Protocol type	0	Modbus RTU protocol
		1	Modbus ASCII protocol
4112	Speed	One of the following: 1200, 2400, 4800, 9600, 19200, 38400	
4113	Parity	0	None
		1	Even
		2	Odd
4114	Stop bits	1 or 2	
4115	Modbus address	From 1 to 247	
4116	Reset interface command	0	Changes made on registers 4111-4115 are not effective
		1	Changes made on registers 4111-4115 take effect
4117	Value format	0	Quantities coded as floating point 32 bit
		1	Quantities coded as integers (see par. 4.4)
4118	Reset energy counters command	1	Reset active energy registers
		2	Reset reactive energy registers
		3	Reset all the registers

Note!
The register 4118, is a "pass-through" register because the final target of the command is the counter connected to the interface. If you change the register value, a command will be given to the counter in order to call a reset of the counter internal registers.
All the other writing registers modify the interface behaviour.

4.4. Reading quantities

These registers holds the electrical quantities controlled by the counter connected to the interface. As stated in paragraph 4.1 the available quantities are dependent from the combination counter/interface type you have (TA: Three phase counter/Full interface, TE: Three phase counter/Basic interface, SA: Single phase counter/Full interface, SE: Single phase counter/Basic interface).

Register address	Designation	Interface & counter types				Length (bytes)
		DRM--3P**	TE	**DRM-**-1P**	SE	
4119	Active Energy 1st phase T1, imp (kWh)	x	x	x	x	8
4123	Active Energy 2nd phase T1, imp (kWh)	x	x			8
4127	Active Energy 3rd phase T1, imp (kWh)	x	x			8
4131	Active Energy Σ T1, imp (kWh)	x	x			8
4135	Active Energy 1st phase T2, imp (kWh)	x	x	x	x	8

4139	Active Energy 2nd phase T2, imp (kWh)	x	x			8
4143	Active Energy 3rd phase T2, imp (kWh)	x	x			8
4147	Active Energy Σ T2, imp (kWh)	x	x			8
4151	Active Power 1st phase (kW)	x	x	x	x	4
4153	Active Power 2nd phase (kW)	x	x			4
4155	Active Power 3rd phase (kW)	x	x			4
4157	Active Power Σ (kW)	x	x			8
4161	Active Energy 1st phase T1, exp (kWh)	x	x	x	x	8
4165	Active Energy 2nd phase T1, exp (kWh)	x	x			8
4169	Active Energy 3rd phase T1, exp (kWh)	x	x			8
4173	Active Energy Σ T1, exp (kWh)	x	x			8
4177	Active Energy 1st phase T2, exp (kWh)	x	x	x	x	8
4181	Active Energy 2nd phase T2, exp (kWh)	x	x			8
4185	Active Energy 3rd phase T2, exp (kWh)	x	x			8
4189	Active Energy Σ T2, exp (kWh)	x	x			8
4193	Reactive Energy 1st phase T1, imp (kvarh)	x	x	x	x	8
4197	Reactive Energy 2nd phase T1, imp (kvarh)	x	x			8
4201	Reactive Energy 3rd phase T1, imp (kvarh)	x	x			8
4205	Reactive Energy Σ T1, imp (kvarh)	x	x			8
4209	Reactive Energy 1st phase T2, imp (kvarh)	x	x	x	x	8
4213	Reactive Energy 2nd phase T2, imp (kvarh)	x	x			8
4217	Reactive Energy 3rd phase T2, imp (kvarh)	x	x			8
4221	Reactive Energy Σ T2, imp (kvarh)	x	x			8
4225	Reactive Energy 1st phase T1, exp (kvarh)	x	x	x	x	8
4229	Reactive Energy 2nd phase T1, exp (kvarh)	x	x			8
4233	Reactive Energy 3rd phase T1, exp (kvarh)	x	x			8
4237	Reactive Energy Σ T1, exp (kvarh)	x	x			8
4241	Reactive Energy 1st phase T2, exp (kvarh)	x	x	x	x	8
4245	Reactive Energy 2nd phase T2, exp (kvarh)	x	x			8
4249	Reactive Energy 3rd phase T2, exp (kvarh)	x	x			8
4253	Reactive Energy Σ T2, exp (kvarh)	x	x			8
4257	Reactive Power 1st phase (kvar)	x	x	x	x	4
4259	Reactive Power 2nd phase (kvar)	x	x			4
4261	Reactive Power 3rd phase (kvar)	x	x			4
4263	Reactive Power Σ (kvar)	x	x			8
4267	L1-N voltage (V)	x		x		4
4269	L2-N voltage (V)	x				4
4271	L3-N voltage (V)	x				4
4273	L1-L2 voltage (V)	x				4
4275	L2-L3 voltage (V)	x				4
4277	L3-L1 voltage (V)	x				4
4279	phase1 current (A)	x		x		4
4281	phase2 current (A)	x				4
4283	phase3 current (A)	x				4
4285	apparent power phase1 (kVA)	x		x		4
4287	apparent power phase2 (kVA)	x				4
4289	apparent power phase3 (kVA)	x				4
4291	apparent power total (kVA)	x				8
4295	power factor cos phi phase1	x		x		4
4297	power factor cos phi phase2	x				4
4299	power factor cos phi phase3	x				4
4301	power factor cos phi total	x				4
4303	frequency (Hz)	x		x		4

Notes
T1/T2 stand for Tariff 1 and tariff 2.

The symbol **Σ** indicates a total amount (for example: the Reactive Power Σ (kvar) value is the total Reactive Power on the three phases. It is of course significant only if you have a three phase counter connected to the interface).
imp/exp (imported/exported) indicates whether the energy is generated (exported) or consumpted (imported).
Length in bytes of the quantity. Note that because a Modbus register is 2 bytes long, all the quantities are splitted on more registers (4 bytes: 2 registers; 8 bytes: 4 registers).

Tip!
Remember that all the quantities are coded as 32 bit floating point values.
Each type of interface (Basic or Full) is available in two versions:
BE – the floating point values are transmitted in *big-endian* format
LE – the floating point values are transmitted in *little-endian* format
If you want to switch to an integer representation, you have to change the value of the configuration register 4117 (see the paragraph 4.3)

4.4.1. Quantities coded as Integer values

While the notation using floating point 32 bit values is unambigous, when you switch to the integer notation something must be explained in order to allow the correct interpretation of original value.

Quantities 4 bytes long

The integer value stored in these registers (2) must be devided by a factor of 10000 to rebuild the original value.
Example: Active Power 1st phase
Integer value: 122447
Original value: 122447/10000=12,2447 (kW)

Quantities 8 bytes long

The rebuilding of the original value is slightly more complicated.
The value stored in the first 4 bytes must be multiplied by a factor of 10^9 (1000000000).
Then it must be added to the value stored in the following 4 bytes.
Finally, the result must be divided by 10000.
Example: Active Power total
Integer value (most significat 4 bytes): 12344
Integer value (less significant 4 bytes): 765532
Original value: (12344*1000000000+765532)/10000=1234400076,5532 (kW)

5. References

For any further information concerning the Modbus protocol implementation, you can consult the following documents and references:

Modbus application protocol specifications V 1.1b, at http://www.modbus-IDA.org

Modbus over serial line – Specification and implementation guide V. 1.02, at http://www.modbus.org

Tyco Electronics UK Ltd.
a TE Connectivity Ltd. company
Freebournes Road, Witham, CM8 3AH
Tel: +44 (0) 1376 509509, Fax: +44 (0) 1376 509511
www.crompton-instruments.com
www.energy.te.com