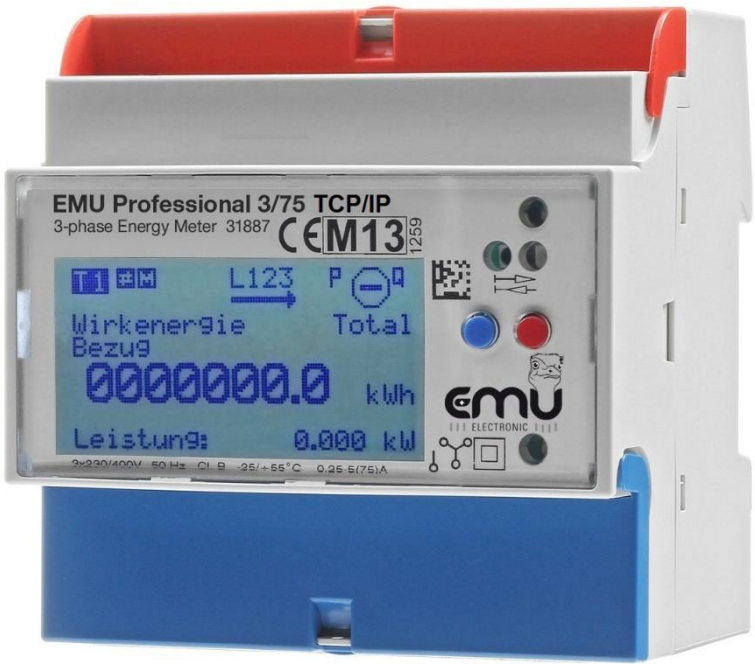
MODBUS TCP SPECIFICATIONS



MODBUS TCP

V1.1	30.10.2013	Initial version
V1.2	13.06.2019	Invalid registers removed from table
V1.3	12.09.2022	Incorrect numbering system of the registers corrected

EMU Electronic AG
Jöchlerweg 2 | CH-6340 Baar | Switzerland | Phone +41 (0) 41 545 03 00 | Fax +41 (0) 41 545 03 01 | info@emuag.ch | www.emuag.ch

1. Preamble

The EMU Professional can be equipped with an optional TCP/IP module. This module supports the Modbus TCP protocol. This document describes the implemented Modbus TCP protocol.

2. Purpose

The TCP/IP module allows the meter to communicate with other Modbus TCP devices.

3. Basics

1	Modbus Messaging on TCP/IP Implementation Guide V1.0b: http://www.modbus.org
2	Modbus Application Protocol Specification V1.1b: http://www.modbus.org

4. Modbus TCP

Modbus TCP is sent over TCP/IP packages. Modbus TCP is similiar to Modbus RTU. The TCP/IP Package contains the Modbus data as payload.

TCP Port for Modbus: 502

Every Modbus package begins with the Modbus Header (7 Byte)

General protocol structure

Byte Nr.	Size (Byte)	Value (Hex)	Description
1-2	2	xx xx	Transaction number
3-4	2	00 00	Protocoll ID (always 00 00)
5-6	2	xx xx	Number of following Bytes
7	1	xx	Adress (Slave-ID)
8	1	xx	Function
9-n	X		n Byte Data (Modbus Data)

The Modbus slave address (unit ID) is ignored. The Modbus TCP addressing is handled by the TCP/IP Layer.

4.1. Basics

The meter readings are sent as Integer. A meter reading is normally stored in multiple registers. (e.g.: active energy import total requires 4 registers).

Data is sent in the „Big-Endian“ format. The most significant Byte is sent first.

e.g.:The Value 0x1234: 0x12 is sent first followed by 0x34

The maximum length of a Modbus telegram is 260 Bytes. (253 Bytes payload)

To read all meter readings, the data must be sent in multiple telegrams.

4.2. Functions (control commands)

The module supports two Modbus functions.

- Read Holding Registers (Code 03)
- Write Multiple Registers (Code 16)

«Read Holding Registers» reads out meter readings.

«Write Multiple Registers» is used to set configuration registers. (e.g. IP address)

4.3. Read holding registers

The function „Read Holding Registers“ reads out one or more register and sends back the data. One register contains 2 Byte. (High Byte first)

Protocol structure: Request

Byte Nr.	Size (Byte)	Value (Hex)	Description
1-2	2	xx xx	Transaction number
3-4	2	00 00	Protocoll ID (always 00 00)
5-6	2	xx xx	Number of following Bytes
7	1	xx	Adress (Slave-ID)
8	1	03	Function code
9-10	2	10 00	Starting address reading register(e.g. 0x1000)
11-12	2	00 02	Number of registers to read (Words). (e.g. 2 for 4 Byte)

Protocol structure: Receive

Byte Nr.	Size (Byte)	Value (Hex)	Description
1-2	2	xx xx	Transaction number
3-4	2	00 00	Protocoll ID (always 00 00)
5-6	2	xx xx	Number of following Bytes
7	1	xx	Adress (Slave-ID)
8	1	03	Function code
9	1	xx	Number of following Bytes
10-x	N	xx xx	Register Data

4.4. Write multiple registers

This function allows to write one or multiple registers. This function is used to configurate the module.

Protocol structure: Request

Byte Nr.	Size (Byte)	Value (Hex)	Description
1-2	2	xx xx	Transaction number
3-4	2	00 00	Protocoll ID (always 00 00)
5-6	2	xx xx	Number of following Bytes
7	1	xx	Address (Slave-ID)
8	1	10	Functioncode
9-10	2	10 03	Startaddress of the register to write (z.b. 0x1003)
11-12	2	00 02	Number of registers to write. (Words).
13	1	04	Number of Bytes to write
14-x	n	xx xx	Register data

Protocol structure: Receive

Byte Nr.	Size (Byte)	Value (Hex)	Description
1-2	2	xx xx	Transaction number
3-4	2	00 00	Protocoll ID (always 00 00)
5-6	2	xx xx	Number of following Bytes
7	1	xx	Address (Slave-ID)
8	1	10	Functioncode
9	1	xx xx	Startaddress
10-11	2	xx xx	Number of written registers

4.5. Register addressing

The startadress of the register to read or write addresses the first register.
For historical reasons the register address starts at 1, the startaddress in the Modbus protocol starts at 0.

Which means, the Modbus telegram holds as startaddress the registeraddress minus 1.

Example:

Inst. System time (4200) is sent with the Modbus Startaddress 4199.

4.6. System parameters

This parameters hold information about the configuration of the TCP/IP module.

All system parameters can be read over Modbus. The system Parameter IP address, subnet mask, default gateway and modbus port are writable.

System parameters TCP / IP Modul

Register (Dez)	Name	Size (Byte)	Description	r	w
4096	MAC adress	6	MAC address	x	
4099	IP adress	4	IP address	x	x
4101	Subnet mask	4	Subnet mask	x	x
4103	Default gateway	4	Default Gateway	x	x
4105	Modbus port	2	Modbus TCP port address (default: 502)	x	x
4106	HTTP port	2	HTTP TCP port	x	
4107	Bacnet port	2	Bacnet port	x	
4108	Firmware version	2	Firmware version	x	

System parameters meter

Register (Dez)	Name	Size (Byte)	Description	r	w
4109	Serial number	4	serial number of the meter	x	
4111	Software version and checksum	4	Software version (2 byte) and checksum (2 byte) of the firmware.	x	

4.7. Read out data

Register (Dez)	Name	Size (Byte)	Unit
4200	Inst. System time	4	Unix timestamp
4202	Active energy import total	8	Wh
4206	Active energy import total phase L1	8	Wh
4210	Active energy import total phase L2	8	Wh
4214	Active energy import total phase L3	8	Wh
4218	Active energy import phase L1 tariff 1	8	Wh
4222	Active energy import phase L2 tariff 1	8	Wh
4226	Active energy import phase L3 tariff 1	8	Wh
4230	Active energy import total tariff 1	8	Wh
4234	Active energy import phase L1 tariff 2	8	Wh
4238	Active energy import phase L2 tariff 2	8	Wh
4242	Active energy import phase L3 tariff 2	8	Wh
4246	Active energy import total tariff 2	8	Wh
4250	Active energy import phase L1 tariff 3	8	Wh
4254	Active energy import phase L2 tariff 3	8	Wh
4258	Active energy import phase L3 tariff 3	8	Wh
4262	Active energy import total tariff 3	8	Wh
4266	Active energy import phase L1 tariff 4	8	Wh
4270	Active energy import phase L2 tariff 4	8	Wh
4274	Active energy import phase L3 tariff 4	8	Wh
4278	Active energy import total tariff 4	8	Wh
4282	Active energy export total export	8	Wh
4310	Active energy export total tariff 1	8	Wh
4326	Active energy export total tariff 2	8	Wh
4342	Active energy export total tariff 3	8	Wh
4358	Active energy export total tariff 4	8	Wh
4362	Reactive energy total inductive	8	varh
4366	Reactive energy inductive total phase L1	8	varh
4370	Reactive energy inductive total phase L2	8	varh
4374	Reactive energy inductive total phase L3	8	varh
4378	Reactive energy inductive phase L1 tariff 1	8	varh
4382	Reactive energy inductive phase L2 tariff 1	8	varh
4386	Reactive energy inductive phase L3 tariff 1	8	varh
4390	Reactive energy inductive total tariff 1	8	varh
4394	Reactive energy inductive phase L1 tariff 2	8	varh
4398	Reactive energy inductive phase L2 tariff 2	8	varh
4402	Reactive energy inductive phase L3 tariff 2	8	varh
4406	Reactive energy inductive total tariff 2	8	varh
4410	Reactive energy inductive phase L1 tariff 3	8	varh
4414	Reactive energy inductive phase L2 tariff 3	8	varh
4418	Reactive energy inductive phase L3 tariff 3	8	varh
4422	Reactive energy inductive total tariff 3	8	varh
4426	Reactive energy inductive phase L1 tariff 4	8	varh
4430	Reactive energy inductive phase L2 tariff 4	8	varh
4434	Reactive energy inductive phase L3 tariff 4	8	varh
4438	Reactive energy inductive total tariff 4	8	varh
4442	Reactive energy capacitive total	8	varh
4470	Reactive energy capacitive total tariff 1	8	varh
4486	Reactive energy capacitive total tariff 2	8	varh
4502	Reactive energy capacitive total tariff 3	8	varh

4518	Reactive energy capacitive total tariff 4	8	varh
4522	Instantaneous active power phase L1	4	W
4524	Instantaneous active power phase L2	4	W
4526	Instantaneous active power phase L3	4	W
4528	Instantaneous active power total	4	W
4530	Instantaneous reactive power phase L1	4	var
4532	Instantaneous reactive power phase L2	4	var
4534	Instantaneous reactive power phase L3	4	var
4536	Instantaneous reactive power total	4	var
4538	Instantaneous apparent power phase L1	4	VA
4540	Instantaneous apparent power phase L2	4	VA
4542	Instantaneous apparent power phase L3	4	VA
4544	Instantaneous apparent power total	4	VA
4546	Max. active power tariff 1 (15min)	4	W
4548	Max. active power tariff 2 (15min)	4	W
4550	Max. active power tariff 3 (15min)	4	W
4552	Max. active power tariff 4 (15min)	4	W
4554	Max. active power total (15min)	4	W
4556	Max. active power phase L1	4	W
4558	Max. active power phase L2	4	W
4560	Max. active power phase L3	4	W
4562	Max. active power phase L1 date / time	4	Unix timestamp
4564	Max. active power phase L2 date / time	4	Unix timestamp
4566	Max. active power phase L3 date / time	4	Unix timestamp
4568	Instantaneous voltage phase L1	2	V/10
4569	Instantaneous voltage phase L2	2	V/10
4570	Instantaneous voltage phase L3	2	V/10
4571	Instantaneous voltage phase L1 – L2	2	V/10
4572	Instantaneous voltage phase L2 – L3	2	V/10
4573	Instantaneous voltage phase L3 – L1	2	V/10
4574	Min. voltage phase L1	2	V/10
4575	Min. voltage phase L2	2	V/10
4576	Min. voltage phase L3	2	V/10
4577	Min. voltage phase L1 date / time	4	Unix timestamp
4579	Min. voltage phase L2 date / time	4	Unix timestamp
4581	Min. voltage phase L2 date / time	4	Unix timestamp
4583	Max. voltage phase L1	2	V/10
4584	Max. voltage phase L2	2	V/10
4585	Max. voltage phase L3	2	V/10
4586	Max. voltage phase L1 date / time	4	Unix timestamp
4588	Max. voltage phase L2 date / time	4	Unix timestamp
4590	Max. voltage phase L3 date / time	4	Unix timestamp
4592	Instantaneous current phase L1	4	mA
4594	Instantaneous current phase L2	4	mA
4596	Instantaneous current phase L3	4	mA
4598	Instantaneous current total	4	mA
4600	Min. current phase L1	4	mA
4602	Min. current phase L2	4	mA
4604	Min. current phase L3	4	mA
4606	Min. current phase L1 date / time	4	Unix timestamp
4608	Min. current phase L2 date / time	4	Unix timestamp
4610	Min. current phase L3 date / time	4	Unix timestamp
4612	Max. current phase L1	4	mA
4614	Max. current phase L2	4	mA
4616	Max. current phase L3	4	mA
4618	Max. current phase L1 date / time	4	Unix timestamp

4620	Max. current phase L2 date / time	4	Unix timestamp
4622	Max. current phase L3 date / time	4	Unix timestamp
4624	Instantaneous form factor phase L1 (cos phi)	2	cos/100
4625	Instantaneous form factor phase L2 (cos phi)	2	cos/100
4626	Instantaneous form factor phase L3 (cos phi)	2	cos/100
4627	Instantaneous net frequency	2	Hz/10
4628	Number of power failure	2	-
4629	current transformer ratio	2	-
4630	Instantaneous active tariff	1	-
4631	Active energy import total (4 byte value)	4	Wh
4633	Active energy import tariff 1 (4 byte value)	4	Wh
4635	Active energy import tariff 2 (4 byte value)	4	Wh
4637	Active energy export Total (4 byte value)	4	Wh
4639	Active energy export Tarif 1 (4 byte value)	4	Wh
4641	Active energy export Tarif 2 (4 byte value)	4	Wh
4643	Reactive energy total inductive (4 byte value)	4	varh
4645	Reactive energy inductive tariff 1 (4 byte value)	4	varh
4647	Reactive energy inductive tariff 2 (4 byte value)	4	varh
4649	Reactive energy capacitive total (4 byte value)	4	varh
4651	Reactive energy capacitive tariff 1 (4 byte value)	4	varh
4653	Reactive energy capacitive tariff 2 (4 byte value)	4	varh

4.8. Datatype

All readings are transmitted as Integer. The size depends on the number of Bytes of the reading.

Number of Bytes	Datatype
2	int16
4	int32
8	int64

- If a datapoint is not present on the meter, the smallest possible Value is transmitted. (e.g. int32: −2'147'483'648)

4.9. Error Codes

If an error occurs a standardized error code is sent back. Following error codes exist:

Error code	Identifier	Description
1	Illegal Function	The desired modbus function is not supported.
2	Illegal Data Address	Invalid (Register) Address.
3	Illegal Data Value	Parameter is out of scope
4	Slave device failure	Communication watchdog timed out
6	Slave Device Busy	Device can not handle Modbus requests at the moment.

5. Examples

5.1. Readout active energy import phase L1 tariff 1

Request:

Byte Nr.	Size (Byte)	Value (Hex)	Description
1-2	2	00 01	Transaction number
3-4	2	00 00	Protocoll ID (always 00 00)
5-6	2	00 06	Number of following Bytes
7	1	00	Address (Slave-ID)
8	1	03	Functioncode (Read Holding Registers)
9-10	2	10 79	Register address (4217)
11-12	2	00 04	Number of registers (4 Register -> 8 Bytes Data)

Receive:

Byte Nr.	Size (Byte)	Value (Hex)	Description
1-2	2	00 01	Transaction number
3-4	2	00 00	Protocoll ID (always 00 00)
5-6	2	00 0B	Number of following Bytes
7	1	00	Address (Slave-ID)
8	1	03	Functioncode (Read Holding Registers)
9	1	08	Number of following Bytes
10-18	8	00 00 00 12 34 56 78 90	Data (in this example: Value: 0x0000001234567890 = 78'187'493'520 Wh)

5.2. Write Modbus Port

Request:

Byte Nr.	Size (Byte)	Value (Hex)	Description
1-2	2	00 01	Transaction number
3-4	2	00 00	Protocoll ID (always 00 00)
5-6	2	00 06	Number of following Bytes
7	1	00	Address (Slave-ID)
8	1	10	Functioncode (Write Multiple Register)
9-10	2	10 08	Registers startaddress (4105)
11-12	2	00 01	Number of registers (1 Register -> 2 Byte data)
13	1	02	Number of Databytes
14-15	2	01 F6	Data (Modbus port 502)

Receive:

Byte Nr.	Size (Byte)	Value (Hex)	Description
1-2	2	00 01	Transaction number
3-4	2	00 00	Protocoll ID (always 00 00)
5-6	2	00 06	Number of following Bytes
7	1	00	Address (Slave-ID)
8	1	10	Functioncode (Write Multiple Registers)
9-10	2	10 08	Registers startaddress (4105)
11-12	2	00 01	Number of registers (1 register -> 2 Bytes data)