Protokollbeschreibung
Modbus TCP für EMU TCP/IP Modul

Version 1.1	30. Oktober 2013	Initialversion
Version 1.2	13. Juni 2019	Ungültige Register entfernt

1 Ziel, Zweck

Mit den TCP/IP Modul soll der Zähler über das Modbus TCP Protokoll mit anderen Geräten kommunizieren können.

2 Grundlagen

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

3 Modbus TCP

Modbus TCP wird über TCP/IP Packet versendet. Im Grunde ist Modbus TCP sehr ähnlich wie Modbus RTU. Die Modbus Daten werden als Nutzdaten in das TCP/IP Packet eingefügt.

TCP Port für Modbus TCP: 502

Jedes Modbus Packet beginnt mit dem Modbus Header (7 Byte).

Allgemeiner Protokollaufbau

Byte Nr.	Grösse (Byte)	Wert (Hex)	Beschreibung
1-2	2	xx xx	Transaktionsnummer
3-4	2	00 00	Protokollkennzeichen (ist immer 00 00)
5-6	2	xx xx	Zahl der noch folgenden Bytes
7	1	xx	Adresse (Slave-ID)
8	1	xx	Funktion
9-n	X		n Byte Daten (Modbus Daten)

Die Mobus Slave Adresse (Unit ID) wird ignoriert. Die Adressierung der Modus Geräte übernimmt bei Modbus TCP der TCP/IP Layer.

3.1 Grundlagen

Die Zählerdaten werden als Integer übertragen. Üblicherweise ist ein Messwert auf mehrere Register verteilt. (Wirkenergie z.B. Benötigt 4 Register).

Die Daten werden „Big-Endian“ übertragen. d.H das höherwertige Byte wird an erster Stelle übertragen.

Beispiel: An erster Stelle des Werts 0x1234 wird 0x12 und an zweiter Stelle 0x34 übertragen.

Die maximale Länge eines Modbus Telegramms ist 260 Bytes. (253 Byte Nutzdaten). Möchte man alle Messwerte des Zählers auslesen, müssen die Register auf mehrere Telegramme aufgeteilt werden.

3.2 Funktionen (Steuerbefehle)

Das Modul unterstützt zwei Modbus Funktionen.

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

Read Holding Registers wird zum Auslesen der Zählerdaten (z.B. Aktuelle Wirkleistung) benötigt. Write Single Register wird für das setzen der Konfigurationsdaten (z.B. IP Addresse) eingesetzt.

3.2.1 Read Holding Registers

Mit der Modbus Funktion „Read Holding Registers“ wird eines oder mehrere Register auf dem Modul ausgelesen und die Daten zurück gesendet. Pro Register werden 2 Byte gesendet. (High Byte first)

Protokollaufbau Anfrage

Byte Nr.	Grösse (Byte)	Wert (Hex)	Beschreibung
1-2	2	xx xx	Transaktionsnummer
3-4	2	00 00	Protokollkennzeichen (ist immer 00 00)
5-6	2	xx xx	Zahl der noch folgenden Bytes
7	1	xx	Adresse (Slave-ID)
8	1	03	Funktionscode
9-10	2	10 00	Startadresse des zu lesenden Registers (z.b. 0x1000)
11-12	2	00 02	Anzahl der zu lesenden Register (Words). (z.B. 2 für 4 Byte)

Protokollaufbau Antwort

Byte Nr.	Grösse (Byte)	Wert (Hex)	Beschreibung
1-2	2	xx xx	Transaktionsnummer
3-4	2	00 00	Protokollkennzeichen (ist immer 00 00)
5-6	2	xx xx	Zahl der noch folgenden Bytes
7	1	xx	Adresse (Slave-ID)
8	1	03	Funktionscode
9	1	xx	Zahl der noch folgenden Bytes
10-x	N	xx xx	Register Daten

3.2.2 Write Multiple Registers

Mit dieser Funktion kann ein oder mehrere Register auf dem Modul geschrieben werden. Diese Funktion wird benötigt um Konfigurationen auf dem Modul vorzunehmen.

Protokollaufbau Anfrage

Byte Nr.	Grösse (Byte)	Wert (Hex)	Beschreibung
1-2	2	xx xx	Transaktionsnummer
3-4	2	00 00	Protokollkennzeichen (ist immer 00 00)
5-6	2	xx xx	Zahl der noch folgenden Bytes
7	1	xx	Adresse (Slave-ID)
8	1	10	Funktionscode
9-10	2	10 03	Startadresse des zu schreibenden Registers (z.b. 0x1003)
11-12	2	00 02	Anzahl der zu schreibende Register (Words).
13	1	04	Anzahl der zu schreibende Bytes
14-x	n	xx xx	Register Daten

Protokollaufbau Antwort

Byte Nr.	Grösse (Byte)	Wert (Hex)	Beschreibung
1-2	2	xx xx	Transaktionsnummer
3-4	2	00 00	Protokollkennzeichen (ist immer 00 00)
5-6	2	xx xx	Zahl der noch folgenden Bytes
7	1	xx	Adresse (Slave-ID)
8	1	10	Funktionscode
9	1	xx xx	Startadresse
10-11	2	xx xx	Anzahl geschriebener Register

3.3 Register Adressierung

Die Startadresse des zu lesenden oder zu schreibenden Registers im Modbus Protokoll bezeichnet das erste zu adressierende Register im Zähler. Aus Historischen Gründen startet die Register Adresse der Werte bei 1, die Startadresse in Modbus aber bei 0.

Das heisst, dass im Modbus Telegramm als Startadresse die Registeradresse minus 1 steht.

Beispiel:

Momentane Systemzeit (4200) wird im als Modbus Startadresse 4199 gesendet.

3.4 System Parameter

Die Parameter geben Auskunft über die Konfiguration des Zählers und des TCP / IP Moduls. Alle System Parameter können gelesen werden. Die System Parameter IP-Adresse, Subnetzmaske, Standard – Gateway und Modbus Port können zusätzlich geschrieben werden.

System Parameter TCP / IP Modul

Register	Name	Grösse (Byte)	Beschreibung	r	w
4096	MAC - Adresse	6	Weltweit eindeutige physikalische Adresse.	x	
4099	IP-Adresse	4	IP Adresse des Moduls	x	x
4101	Subnetzmaske	4	Subnet Maske des Moduls	x	x
4103	Standard - Gateway	4	Default Gateway des Moduls	x	x
4105	Modbus Port	2	Modbus TCP Port Adresse (Standard: 502)	x	x
4106	HTTP Port	2	HTTP TCP Port	x	
4107	Bacnet Port	2	Bacnet Port	x	
4108	Firmware Version Modul	2	Version der Firmware des Moduls	x	

System Parameter Zähler

Register (Hex)	Name	Grösse (Byte)	Beschreibung	r	w
4109	Seriennummer Zähler	4	Seriennummer des Zählers	x	
4111	Software Version und Checksumme	4	Software Version (2 byte) und Checksumme (2 byte) der Zählerfirmware.	x	

3.5 Auslese Daten

Folgende Tabelle gibt eine Überblick über alle Messwerte und deren Register:

Register	Name	Grösse (Byte)	Einheit
4200	Momentane Systemzeit	4	Unix time stamp
4202	Wirk- Energie Bezug Total	8	Wh
4206	Wirk- Energie Bezug Total Phase L1	8	Wh
4210	Wirk- Energie Bezug Total Phase L2	8	Wh
4214	Wirk- Energie Bezug Total Phase L3	8	Wh
4218	Wirk- Energie Bezug Phase L1 Tarif 1	8	Wh
4222	Wirk- Energie Bezug Phase L2 Tarif 1	8	Wh
4226	Wirk- Energie Bezug Phase L3 Tarif 1	8	Wh
4230	Wirk- Energie Bezug Total Tarif 1	8	Wh
4234	Wirk- Energie Bezug Phase L1 Tarif 2	8	Wh
4238	Wirk- Energie Bezug Phase L2 Tarif 2	8	Wh
4242	Wirk- Energie Bezug Phase L3 Tarif 2	8	Wh
4246	Wirk- Energie Bezug Total Tarif 2	8	Wh
4250	Wirk- Energie Bezug Phase L1 Tarif 3	8	Wh
4254	Wirk- Energie Bezug Phase L2 Tarif 3	8	Wh
4258	Wirk- Energie Bezug Phase L3 Tarif 3	8	Wh
4262	Wirk- Energie Bezug Total Tarif 3	8	Wh
4266	Wirk- Energie Bezug Phase L1 Tarif 4	8	Wh
4270	Wirk- Energie Bezug Phase L2 Tarif 4	8	Wh
4274	Wirk- Energie Bezug Phase L3 Tarif 4	8	Wh
4278	Wirk- Energie Bezug Total Tarif 4	8	Wh
4282	Wirk- Energie Lieferung Total Lieferung	8	Wh
4310	Wirk- Energie Lieferung Total Tarif 1	8	Wh
4326	Wirk- Energie Lieferung Total Tarif 2	8	Wh
4342	Wirk- Energie Lieferung Total Tarif 3	8	Wh
4358	Wirk- Energie Lieferung Total Tarif 4	8	Wh
4362	Blind- Energie Total Induktiv	8	varh
4366	Blind- Energie Induktiv Total Phase L1	8	varh
4370	Blind- Energie Induktiv Total Phase L2	8	varh
4374	Blind- Energie Induktiv Total Phase L3	8	varh
4378	Blind- Energie Induktiv Phase L1 Tarif 1	8	varh
4382	Blind- Energie Induktiv Phase L2 Tarif 1	8	varh
4386	Blind- Energie Induktiv Phase L3 Tarif 1	8	varh
4390	Blind- Energie Induktiv Total Tarif 1	8	varh
4394	Blind- Energie Induktiv Phase L1 Tarif 2	8	varh
4398	Blind- Energie Induktiv Phase L2 Tarif 2	8	varh
4402	Blind- Energie Induktiv Phase L3 Tarif 2	8	varh
4406	Blind- Energie Induktiv Total Tarif 2	8	varh
4410	Blind- Energie Induktiv Phase L1 Tarif 3	8	varh

4414	Blind- Energie Induktiv Phase L2 Tarif 3	8	varh
4418	Blind- Energie Induktiv Phase L3 Tarif 3	8	varh
4422	Blind- Energie Induktiv Total Tarif 3	8	varh
4426	Blind- Energie Induktiv Phase L1 Tarif 4	8	varh
4430	Blind- Energie Induktiv Phase L2 Tarif 4	8	varh
4434	Blind- Energie Induktiv Phase L3 Tarif 4	8	varh
4438	Blind- Energie Induktiv Total Tarif 4	8	varh
4442	Blind- Energie Kapazitiv Total	8	varh
4470	Blind- Energie Kapazitiv Total Tarif 1	8	varh
4486	Blind- Energie Kapazitiv Total Tarif 2	8	varh
4502	Blind- Energie Kapazitiv Total Tarif 3	8	varh
4518	Blind- Energie Kapazitiv Total Tarif 4	8	varh
4522	Aktuelle Wirk- Leistung Phase L1	4	W
4524	Aktuelle Wirk- Leistung Phase L2	4	W
4526	Aktuelle Wirk- Leistung Phase L3	4	W
4528	Aktuelle Wirk- Leistung Total	4	W
4530	Aktuelle Blind- Leistung Phase L1	4	var
4532	Aktuelle Blind- Leistung Phase L2	4	var
4534	Aktuelle Blind- Leistung Phase L3	4	var
4536	Aktuelle Blind- Leistung Total	4	var
4538	Aktuelle Schein- Leistung Phase L1	4	VA
4540	Aktuelle Schein- Leistung Phase L2	4	VA
4542	Aktuelle Schein- Leistung Phase L3	4	VA
4544	Aktuelle Schein- Leistung Total	4	VA
4546	Max. Wirk- Leistung Tarif 1 (15min)	4	W
4548	Max. Wirk- Leistung Tarif 2 (15min)	4	W
4550	Max. Wirk- Leistung Tarif 3 (15min)	4	W
4552	Max. Wirk- Leistung Tarif 4 (15min)	4	W
4554	Max. Wirk- Leistung Total (15min)	4	W
4556	Max. Wirk- Leistung Phase L1	4	W
4558	Max. Wirk- Leistung Phase L2	4	W
4560	Max. Wirk- Leistung Phase L3	4	W
4562	Max. Wirk- Leistung Phase L1 Datum / Uhrzeit	4	Unix time stamp
4564	Max. Wirk- Leistung Phase L2 Datum / Uhrzeit	4	Unix time stamp
4566	Max. Wirk- Leistung Phase L3 Datum / Uhrzeit	4	Unix time stamp
4568	Aktuelle Spannung Phase L1	2	V/10
4569	Aktuelle Spannung Phase L2	2	V/10
4570	Aktuelle Spannung Phase L3	2	V/10
4571	Aktuelle Spannung Phase L1 – L2	2	V/10
4572	Aktuelle Spannung Phase L2 – L3	2	V/10
4573	Aktuelle Spannung Phase L3 – L1	2	V/10
4574	Min. Spannung Phase L1	2	V/10
4575	Min. Spannung Phase L2	2	V/10
4576	Min. Spannung Phase L3	2	V/10
4577	Min. Spannung Phase L1 Datum / Uhrzeit	4	Unix time stamp
4579	Min. Spannung Phase L2 Datum / Uhrzeit	4	Unix time stamp

4581	Min. Spannung Phase L2 Datum / Uhrzeit	4	Unix time stamp
4583	Max. Spannung Phase L1	2	V/10
4584	Max. Spannung Phase L2	2	V/10
4585	Max. Spannung Phase L3	2	V/10
4586	Max. Spannung Phase L1 Datum / Uhrzeit	4	Unix time stamp
4588	Max. Spannung Phase L2 Datum / Uhrzeit	4	Unix time stamp
4590	Max. Spannung Phase L3 Datum / Uhrzeit	4	Unix time stamp
4592	Aktueller Strom Phase L1	4	mA
4594	Aktueller Strom Phase L2	4	mA
4596	Aktueller Strom Phase L3	4	mA
4598	Aktueller Strom Total	4	mA
4600	Min. Strom Phase L1	4	mA
4602	Min. Strom Phase L2	4	mA
4604	Min. Strom Phase L3	4	mA
4606	Min. Strom Phase L1 Datum / Uhrzeit	4	Unix time stamp
4608	Min. Strom Phase L2 Datum / Uhrzeit	4	Unix time stamp
4610	Min. Strom Phase L3 Datum / Uhrzeit	4	Unix time stamp
4612	Max. Strom Phase L1	4	mA
4614	Max. Strom Phase L2	4	mA
4616	Max. Strom Phase L3	4	mA
4618	Max. Strom Phase L1 Datum / Uhrzeit	4	Unix time stamp
4620	Max. Strom Phase L2 Datum / Uhrzeit	4	Unix time stamp
4622	Max. Strom Phase L3 Datum / Uhrzeit	4	Unix time stamp
4624	Aktueller Formfaktor Phase L1 (cos phi)	2	Cos/100
4625	Aktueller Formfaktor Phase L2 (cos phi)	2	Cos/100
4626	Aktueller Formfaktor Phase L3 (cos phi)	2	Cos/100
4627	Aktuelle Netzfrequenz	2	Hz/10
4628	Anzahl Spannungsausfälle am Zähler	2	-
4629	Stromwandlerfaktor	2	-
4630	Momentan aktueller Tarif	1	-
4631	Wirk- Energie Bezug Total (4 byte Wert)	4	Wh
4633	Wirk- Energie Bezug Tarif 1 (4 byte Wert)	4	Wh
4635	Wirk- Energie Bezug Tarif 2 (4 byte Wert)	4	Wh
4637	Wirk- Energie Lieferung Total (4 byte Wert)	4	Wh
4639	Wirk- Energie Lieferung Tarif 1 (4 byte Wert)	4	Wh
4641	Wirk- Energie Lieferung Tarif 2 (4 byte Wert)	4	Wh
4643	Blind- Energie Induktiv Total (4 byte Wert)	4	varh
4645	Blind- Energie Induktiv Tarif 1 (4 byte Wert)	4	varh
4647	Blind- Energie Induktiv Tarif 2 (4 byte Wert)	4	varh
4649	Blind- Energie Kapazitiv Total (4 byte Wert)	4	varh
4651	Blind- Energie Kapazitiv Tarif 1 (4 byte Wert)	4	varh
4653	Blind- Energie Kapazitiv Tarif 2 (4 byte Wert)	4	varh

3.5.1 Datentyp

Alle Messwerte werden als Interger übertragen. Die Grösse der Integers ist abhängig von der Länge des Messwertes:

Länge Messwert (bytes)	Datentyp
2	int16
4	int32
8	int64

- Ist ein Messwert auf dem Zähler nicht vorhanden. Wird der kleinstmögliche Wert übertragen (z.B. bei int32: −2'147'483'648) .

3.6 Fehlercodes

Falls bei der Bearbeitung des Modbus Telegramms ein Fehler auftritt, wird ein standardisierter Fehlercode zurückgesendet.

Es wird zwischen folgenden Fehlercodes unterschieden:

Fehlercode	Bezeichnung	Beschreibung
1	Illegal Function	Diese Modbus Funktion wird nicht unterstützt.
2	Illegal Data Address	Ungültige (Register) Adresse.
3	Illegal Data Value	Parameter ausserhalb des gültigen Bereichs
4	Slave device failure	Kommunikations Watchdog ist abgelaufen
6	Slave Device Busy	Gerät kann zur Zeit keine Modbus Befehle verarbeiten.

3.7 Beispiele

3.7.1 Auslesung Wirkleistung Tarif 1 Positiv

Anfrage:

Byte Nr.	Grösse (Byte)	Wert (Hex)	Beschreibung
1-2	2	00 01	Transaktionsnummer
3-4	2	00 00	Protokollkennzeichen (ist immer 00 00)
5-6	2	00 06	Zahl der noch folgenden Bytes
7	1	00	Adresse
8	1	03	Funktion (Read Holding Registers)
9-10	2	10 67	Register Adresse (4200)
11-12	2	00 04	Anzahl Register (4 Register -> 8 Byte Daten)

Antwort:

Byte Nr.	Grösse (Byte)	Wert (Hex)	Beschreibung
1-2	2	00 01	Transaktionsnummer
3-4	2	00 00	Protokollkennzeichen (ist immer 00 00)
5-6	2	00 0B	Zahl der noch folgenden Bytes
7	1	00	Adresse
8	1	03	Funktion (Read Holding Registers)
9	1	08	Zahl der noch folgenden Bytes
10-18	8	00 00 00 12 34 56 78 90	Daten (in diesem Beispiel Wert: 0x0000001234567890 = 78'187'493'520 Wh)

3.7.2 Modbus Port ändern

Anfrage:

Byte Nr.	Grösse (Byte)	Wert (Hex)	Beschreibung
1-2	2	00 01	Transaktionsnummer
3-4	2	00 00	Protokollkennzeichen (ist immer 00 00)
5-6	2	00 06	Zahl der noch folgenden Bytes
7	1	00	Adresse
8	1	10	Funktion (Write Multiple Register)
9-10	2	10 08	Start Register Adresse (4105)
11-12	2	00 01	Anzahl Register (1 Register -> 2 Byte Daten)
13	1	02	Anzahl Bytes Daten
14-15	2	01 F6	Daten (Modbus port 502)

Antwort:

Byte Nr.	Grösse (Byte)	Wert (Hex)	Beschreibung
1-2	2	00 01	Transaktionsnummer
3-4	2	00 00	Protokollkennzeichen (ist immer 00 00)
5-6	2	00 06	Zahl der noch folgenden Bytes
7	1	00	Adresse
8	1	10	Funktion (Write Multiple Registers)
9-10	2	10 08	Start Register Adresse (4105)
11-12	2	00 01	Anzahl Register (1 Register -> 2 Byte Daten)