China Tower Corporation BMS und Wechselschrank-Master-Controller 485 Serielles Kommunikationsprotokoll V2.0

Datum: 25. März 2020

Versionsverlauf:

Version	Änderungsinhalt	Datum
V1.0	Erstversion	29.04.2019
V2.0	Optimierter Inhalt	16.03.2020

Inhaltsverzeichnis

1. Kommunikationsparameter des Batterieschutzsystems

- Kommunikation über RS485-Schnittstelle, 1 Startbit, 8 Datenbits, keine Parität, 1 Stoppbit, Baudrate 9600
- MODBUS-Geräteadresse ist fest auf 1 eingestellt, jedes Schutzsystem kommuniziert über einen separaten RS485-Port, kein Bussystem
- Im Protokoll werden nur Funktionscodes zum Lesen von Schaltern (Code 01) und Lesen von Registern (Code 03) verwendet, andere Funktionscodes werden nicht genutzt
- Register ab Adresse 1000 enthalten Geräte-IDs, diese werden vom Schutzsystem übernommen, sind nur lesbar und nicht modifizierbar
- Abfragesequenz: 1. Geräte-ID abfragen, 2. Analogwerte abfragen, 3. Schaltzustände abfragen

2. MODBUS-Kommunikationstabellen

2.1. Schaltertabelle

Tabelle basierend auf 20 Zellen definiert, bei weniger Zellen werden Daten mit 0 aufgefüllt.

MODBUS-Adresse (Schalter)	Inhalt	Beschreibung	Bemerkung
0.	Reserviert	Standardwert ist 0	
1.	Zellspannungsdifferenz-Schutz	1 bedeutet zu hohe Spannungsdifferenz	
2.	Überladestromschutz	1 bedeutet Überstrom	
3.	Entladestromschutz	1 bedeutet Überstrom	
4.	Kurzschlussschutz	1 bedeutet Kurzschlussschutz	
5.	Ladeübertemperaturschutz	1 bedeutet Ladeübertemperaturschutz	
6.	Entladeübertemperaturschutz	1 bedeutet Entladeübertemperaturschutz	
7.	Ladeuntertemperaturschutz	1 bedeutet Ladeuntertemperaturschutz	
8.	Entladeuntertemperaturschutz	1 bedeutet Entladeuntertemperaturschutz	
9.	Lade-MOS-Beschädigung	1 bedeutet Beschädigung	
10.	Entlade-MOS-Beschädigung	1 bedeutet Beschädigung	

MODBUS-Adresse (Schalter)	Inhalt	Beschreibung	Bemerkung
11.	Interne Kommunikationsanomalie	1 bedeutet Anomalie	Analogfrontend-Kommunikationsanomalie
12.	Überladespannungsschutz 1	1 bedeutet Überladespannungsschutz	
13.	Überladespannungsschutz 2	1 bedeutet Überladespannungsschutz	
14.	Überladespannungsschutz 3	1 bedeutet Überladespannungsschutz	
15.	Überladespannungsschutz 4	1 bedeutet Überladespannungsschutz	
16.	Überladespannungsschutz 5	1 bedeutet Überladespannungsschutz	
17.	Überladespannungsschutz 6	1 bedeutet Überladespannungsschutz	
18.	Überladespannungsschutz 7	1 bedeutet Überladespannungsschutz	
19.	Überladespannungsschutz 8	1 bedeutet Überladespannungsschutz	
20.	Überladespannungsschutz 9	1 bedeutet Überladespannungsschutz	
21.	Überladespannungsschutz 10	1 bedeutet Überladespannungsschutz	
22.	Überladespannungsschutz 11	1 bedeutet Überladespannungsschutz	
23.	Überladespannungsschutz 12	1 bedeutet Überladespannungsschutz	
24.	Überladespannungsschutz 13	1 bedeutet Überladespannungsschutz	
25.	Überladespannungsschutz 14	1 bedeutet Überladespannungsschutz	
26.	Überladespannungsschutz 15	1 bedeutet Überladespannungsschutz	
27.	Überladespannungsschutz 16	1 bedeutet Überladespannungsschutz	
28.	Überladespannungsschutz 17	1 bedeutet Überladespannungsschutz	
29.	Überladespannungsschutz 18	1 bedeutet Überladespannungsschutz	
30.	Überladespannungsschutz 19	1 bedeutet Überladespannungsschutz	
31.	Überladespannungsschutz 20	1 bedeutet Überladespannungsschutz	
32.	Tiefentladeschutz 1	1 bedeutet Tiefentladeschutz	
33.	Tiefentladeschutz 2	1 bedeutet Tiefentladeschutz	
34.	Tiefentladeschutz 3	1 bedeutet Tiefentladeschutz	
35.	Tiefentladeschutz 4	1 bedeutet Tiefentladeschutz	
36.	Tiefentladeschutz 5	1 bedeutet Tiefentladeschutz	
37.	Tiefentladeschutz 6	1 bedeutet Tiefentladeschutz	
38.	Tiefentladeschutz 7	1 bedeutet Tiefentladeschutz	
39.	Tiefentladeschutz 8	1 bedeutet Tiefentladeschutz	
40.	Tiefentladeschutz 9	1 bedeutet Tiefentladeschutz	
41.	Tiefentladeschutz 10	1 bedeutet Tiefentladeschutz	
42.	Tiefentladeschutz 11	1 bedeutet Tiefentladeschutz	
43.	Tiefentladeschutz 12	1 bedeutet Tiefentladeschutz	
44.	Tiefentladeschutz 13	1 bedeutet Tiefentladeschutz	
45.	Tiefentladeschutz 14	1 bedeutet Tiefentladeschutz	
46.	Tiefentladeschutz 15	1 bedeutet Tiefentladeschutz	
47.	Tiefentladeschutz 16	1 bedeutet Tiefentladeschutz	
48.	Tiefentladeschutz 17	1 bedeutet Tiefentladeschutz	
49.	Tiefentladeschutz 18	1 bedeutet Tiefentladeschutz	
50.	Tiefentladeschutz 19	1 bedeutet Tiefentladeschutz	
51.	Tiefentladeschutz 20	1 bedeutet Tiefentladeschutz	

2.2. Registertabelle

Tabelle basierend auf 20 Zellen definiert, bei weniger Zellen werden Daten mit 0 aufgefüllt.

MODBUS-Adresse (Register)	Inhalt	Faktor	Einheit	Bemerkung
0.	Tatsächliche Gesamtspannung des Batteriepakets	0.01	V	
1.	Zellenanzahl, 20, 17 oder andere Werte	1		
2.	Ladezustand SOC (0 ~ 100%)	1	%	
3.	Restkapazität (kann geringer sein als Nennkapazität)	0.01	Ah	
4.	SOH (0 ~ 100%)	1	%	
5.	Ladestrom	0.01	A	
6.	Umgebungstemperatur	1	°C	
7.	Niedrigste Zellentemperatur	1	°C	
8.	Platintemperatur (MOS-Temperatur)	1	°C	
9.	Spannung Zelle 1	0.001	V	
10.	Spannung Zelle 2	0.001	V	
11.	Spannung Zelle 3	0.001	V	
12.	Spannung Zelle 4	0.001	V	
13.	Spannung Zelle 5	0.001	V	
14.	Spannung Zelle 6	0.001	V	
15.	Spannung Zelle 7	0.001	V	
16.	Spannung Zelle 8	0.001	V	
17.	Spannung Zelle 9	0.001	V	
18.	Spannung Zelle 10	0.001	V	
19.	Spannung Zelle 11	0.001	V	
20.	Spannung Zelle 12	0.001	V	
21.	Spannung Zelle 13	0.001	V	
22.	Spannung Zelle 14	0.001	V	
23.	Spannung Zelle 15	0.001	V	
24.	Spannung Zelle 16	0.001	V	
25.	Spannung Zelle 17	0.001	V	
26.	Spannung Zelle 18	0.001	V	
27.	Spannung Zelle 19	0.001	V	
28.	Spannung Zelle 20	0.001	V	
29.	Höchste Zellentemperatur	1	°C	
30.	Reserviert			
31.	Reserviert			
32.	Reserviert			
33.	Reserviert			
1000	Geräte-ID (1)			
1001	Geräte-ID (2)			
1002	Geräte-ID (3)			
1003	Geräte-ID (4)			
1004	Geräte-ID (5)			
1005	Geräte-ID (6)			
1006	Geräte-ID (7)			

MODBUS-Adresse (Register)	Inhalt	Faktor	Einheit	Bemerkung
1007	Geräte-ID (8)			
1008	Geräte-ID (9)			
1009	Geräte-ID (10)			
1010	Geräte-ID (11)			
1011	Geräte-ID (12)			
1012	Geräte-ID (13)			
1013	Geräte-ID (14)			
1014	Reserviert			
1015	Reserviert			

2.3. Nachrichtenbeispiele: Alle Beispielnachrichten sind in hexadezimaler Form

Abfrage der BMS-Geräte-ID: Je nach Länge der Batterie-Geräte-ID ändert sich auch die Länge der abgefragten Register gemäß dem MODBUS-Protokoll.

Abfrage einer 24-Bit-Batterie-Geräte-ID (insgesamt 12 Register, Rückgabe von 24 Bytes, die Daten sollten dem Format GBT 34014-2017 entsprechen)

Anfrage vom Wechselschrank: `01 03 03 E8 00 0C C5 BF`
Antwort vom Batteriegerät: `01 03 18 42 54 31 30 36 30 30 32 30 30 34 54 54 4E 59 32 30 30 32 32 34 30 30 32 46 79`

Die vom BMS zurückgegebene Geräte-ID ist: "BT106002004TTNY200224002"

```
42 54 31 30 36 30 30 32 30 30 34 54 54
B  T  1  0  6  0  0  2  0  0  4  T  T

4E 59 32 30 30 32 32 34 30 30 32
N  Y  2  0  0  2  2  4  0  0  2
```

Abfrage einer 28-Bit-Batterie-Geräte-ID (insgesamt 14 Register, Rückgabe von 28 Bytes, die Daten sollten dem Format GBT 34014-2017 entsprechen)

Anfrage: `01 03 03 E8 00 0E 44 7E`
Antwort vom Batteriegerät: `01 03 1C 42 54 31 30 36 30 30 32 30 30 34 4E 59 59 5A 54 54 48 44 32 30 30 32 32 34 30 30 32 7F 2E`

Die vom BMS zurückgegebene Geräte-ID ist: "BT106002004NYYZTTHD200224002"

```
42 54 31 30 36 30 30 32 30 30 34 4E 59 59 5A
B  T  1  0  6  0  0  2  0  0  4  N  Y  Y  Z

54 54 48 44 32 30 30 32 32 34 30 30 32
T  T  H  D  2  0  0  2  2  4  0  0  2
```

Abfrage von Analogwerten

Anfrage: `01 03 00 00 00 1E C5 C2`
Antwort vom Batteriegerät: `01 03 3C 19 FF 00 14 00 5A 06 5E 00 5A 00 00 00 1D 00 1C 00 1D 0C FD 0C FD 0C FA 0C FA 0C FA 0C FB 0C FE 0C FE 0C FE 0C FD 0C FB 0C FD 0C FD 0C FB 0C FB 0D 01 0D 03 0D 04 0D 03 0D 03 00 1D 8A 50`

Hexadezimal	Dezimal	Tatsächlicher Wert	Beschreibung	Adresse
19 FF	6654	66.54V	Tatsächliche Gesamtspannung des Batteriepakets	0
00 14	20	20	Zellenanzahl, 20, 17 oder andere Werte	1
00 5A	90	90%	Ladezustand SOC (0 ~ 100%)	2
06 5E	1630	16.30Ah	Restkapazität (kann geringer sein als Nennkapazität)	3
00 5A	90	90%	SOH (0 ~ 100%)	4
00 00	0	0A	Ladestrom	5
00 1D	29	29°C	Umgebungstemperatur	6
00 1C	28	28°C	Niedrigste Zellentemperatur	7
00 1D	29	29°C	Platintemperatur (MOS-Temperatur)	8

Hexadezimal	Dezimal	Tatsächlicher Wert	Beschreibung	Adresse
0C FD	3325	3.325V	Spannung Zelle 1	9
0C FD	3325	3.325V	Spannung Zelle 2	10
0C FA	3322	3.322V	Spannung Zelle 3	11
0C FA	3322	3.322V	Spannung Zelle 4	12
0C FA	3322	3.322V	Spannung Zelle 5	13
0C FB	3323	3.323V	Spannung Zelle 6	14
0C FE	3326	3.326V	Spannung Zelle 7	15
0C FE	3326	3.326V	Spannung Zelle 8	16
0C FE	3326	3.326V	Spannung Zelle 9	17
0C FD	3325	3.325V	Spannung Zelle 10	18
0C FB	3323	3.323V	Spannung Zelle 11	19
0C FD	3325	3.325V	Spannung Zelle 12	20
0C FD	3325	3.325V	Spannung Zelle 13	21
0C FB	3323	3.323V	Spannung Zelle 14	22
0C FB	3323	3.323V	Spannung Zelle 15	23
0D 01	3329	3.329V	Spannung Zelle 16	24
0D 03	3331	3.331V	Spannung Zelle 17	25
0D 04	3332	3.332V	Spannung Zelle 18	26
0D 03	3331	3.331V	Spannung Zelle 19	27
0D 03	3331	3.331V	Spannung Zelle 20	28
00 1D	29	29°C	Höchste Zellentemperatur	

Abfrage der Schaltzustände

Anfrage: `01 01 00 00 00 34 3D DD`
Antwort: `01 01 07 12 08 49 80 10 04 09 69 F0`

`12` in Binärform: `00010010`

Binärposition	Binärwert	Schaltzustand	Beschreibung	Adresse
D0	0	Nein	Normal	0
D1	1	Ja	Fehler	1
D2	0	Nein	Überladestrom	2
D3	0	Nein	Entladestrom	3
D4	1	Ja	Kurzschlussschutz	4
D5	0	Nein	Ladeübertemperaturschutz	5
D6	0	Nein	Entladeübertemperaturschutz	6
D7	0	Nein	Ladeuntertemperaturschutz	7

`08` in Binärform: `00001000`

Binärposition	Binärwert	Schaltzustand	Beschreibung	Adresse
D0	0	Nein	Entladeuntertemperaturschutz	8
D1	0	Nein	Lade-MOS-Beschädigung	9
D2	0	Nein	Entlade-MOS-Beschädigung	10
D3	1	Ja	Interne Kommunikationsanomalie	11
D4	0	Nein	Überladespannungsschutz 1	12
D5	0	Nein	Überladespannungsschutz 2	13

Binärposition	Binärwert	Schaltzustand	Beschreibung	Adresse
D6	0	Nein	Überladespannungsschutz 3	14
D7	0	Nein	Überladespannungsschutz 4	15

`49` in Binärform: `01001001`

Binärposition	Binärwert	Schaltzustand	Beschreibung	Adresse
D0	1	Ja	Überladespannungsschutz 5	16
D1	0	Nein	Überladespannungsschutz 6	17
D2	0	Nein	Überladespannungsschutz 7	18
D3	1	Ja	Überladespannungsschutz 8	19
D4	0	Nein	Überladespannungsschutz 9	20
D5	0	Nein	Überladespannungsschutz 10	21
D6	1	Ja	Überladespannungsschutz 11	22
D7	0	Nein	Überladespannungsschutz 12	23

Und so weiter für die weiteren Bytes `80`, `10`, `04`, `09`.

3. MODBUS-Kommunikationsprotokoll

3.1. Datenübertragung

- Master und Gerät sind seriell verbunden, der Master kommuniziert mit dem Schutz- und Kontrollgerät im Frage-Antwort-Modus. Jeder Frame darf 255 Bytes nicht überschreiten.
- Wenn das Gerät eine vom Master gesendete Nachricht mit korrekter Geräteadresse, Nachrichtentyp, Daten und Prüfcode empfängt, sollte es innerhalb von 500ms mit einer normalen Nachricht antworten.
- Wenn das Gerät eine vom Master gesendete Nachricht mit falscher Geräteadresse oder falschem Prüfcode empfängt, antwortet es nicht. Die Masterseite erkennt ein Timeout und setzt die Kommunikation fort.
- Wenn das Gerät eine Nachricht empfängt, bei der die Geräteadresse und der Prüfcode korrekt sind, aber der Nachrichtentyp oder Dateninhalt falsch ist, sollte es innerhalb von 500ms mit einer Fehlermeldung antworten.
- Es wird RS485 verwendet, 1 Startbit, 8 Datenbits, keine Parität, 1 Stoppbit, Baudrate 9600 (Werte zwischen 1200-57600 sind möglich).

3.2. Datenformat

Geräteadresse	Funktionscode	Datenbereich	CRC-Prüfung
1 Byte	1 Byte	N Bytes	2 Bytes (16-Bit-CRC)

Hinweis: 1 Byte besteht aus 8 Bits

3.2.1. Geräteadresse

Die Geräteadresse ist das erste Byte jedes Kommunikationsframes, von 0 bis 255. Dieses Byte gibt an, dass das vom Benutzer mit dieser Adresse eingestellte Gerät diese Nachricht vom Master empfängt. Jedes Gerät muss eine eindeutige Adresse haben, und nur das Gerät mit dieser Adresse kann auf den Master antworten. Wenn das Gerät eine Nachricht zurücksendet, ist das erste Byte der Antwortdaten ebenfalls die Adresse dieses Geräts.

Die Geräteadresse in den vom Master gesendeten Daten gibt an, an welches Gerät gesendet werden soll, die Geräteadresse in den vom Gerät zurückgesendeten Daten gibt an, woher diese Daten stammen.

3.2.2. Funktionscode

Der Funktionscode ist das zweite Byte der Kommunikationsdaten. Der MODBUS-Kommunikationsstandard kann Funktionscodes im Bereich von 1 bis 127 definieren, das Überwachungssystem verwendet jedoch nur einen Teil dieser Funktionscodes:

Funktionscode (HEX)	Definition	Beschreibung
01	Schalter lesen	Status eines oder mehrerer Schalter lesen (Fernmeldung)
03	Register lesen	Einen oder mehrere Register (Analogwert) Daten lesen (Fernmessung)
05	Einzelschalter schreiben	Ein Schalter zum Öffnen oder Schließen steuern (Fernsteuerung)
06	Einzelregister schreiben	In ein Register/Analogwertdaten schreiben (Ferneinstellung)

Funktionscode (HEX)	Definition	Beschreibung
0F	Mehrfachschalter schreiben	Mehrere Schalter zum Öffnen oder Schließen steuern (gleichzeitige Fernsteuerung mehrerer Schalter)
10	Mehrfachregister schreiben	In mehrere Register/Analogwertdaten schreiben (gleichzeitige Ferneinstellung mehrerer Register)

Wenn der Master einen Befehl an das Gerät sendet:

- Bei korrektem Befehl, der normale Daten zurückgeben kann, ist der Funktionscode in der Antwort des Geräts identisch mit dem vom Master gesendeten Funktionscode;
- Bei einem falschen Befehl, der keine normalen Daten zurückgeben kann, ist der Funktionscode in der Antwort des Geräts gleich dem vom Master gesendeten Funktionscode ODER 80H, d.h. das höchste Bit des Funktionscodes wird auf 1 gesetzt. In diesem Fall enthält der Datenbereich des Geräts nur ein Byte, den Fehlercode.

3.2.3. Geräteantworten auf korrekte und fehlerhafte Befehle

Geräteantwort auf korrekte Befehle:

Geräteadresse	Funktionscode	Datenbereich	CRC-Prüfung
1 Byte	1 Byte, identisch mit dem vom Master gesendeten Funktionscode	N Bytes	2 Bytes (16-Bit-CRC)

Geräteantwort auf fehlerhafte Befehle:

Geräteadresse	Funktionscode	Datenbereich	CRC-Prüfung
1 Byte	1 Byte, höchstes Bit auf eins gesetzt, d.h. = Funktionscode | 0x80	1 Byte Fehlercode	2 Bytes (16-Bit-CRC)

Fehlercodes:

Code	Bedeutung
1	Ungültiger Nachrichtentyp
2	Ungültige Datenadresse, einschließlich Datengrößenüberschreitung
3	Ungültiger geschriebener Datenwert
6	Gerät beschäftigt

Beispielnachrichten:

- `01 81 02 C1 91`: Empfangener Befehl mit Funktionscode 01 ist fehlerhaft (81), Fehlercode 02: Adresse ungültig oder Länge überschritten
- `01 83 02 C0 F1`: Empfangener Befehl mit Funktionscode 03 ist fehlerhaft (83), Fehlercode 02: Adresse ungültig oder Länge überschritten
- `01 85 03 02 91`: Empfangener Befehl mit Funktionscode 05 ist fehlerhaft (85), Fehlercode 03: Geschriebener Wert ungültig

3.2.4. Datenbereich

Der Inhalt des Datenbereichs wird im Big-Endian-Format gespeichert, bei der Kommunikation wird zuerst das höherwertige Byte und dann das niederwertige Byte gesendet.

Der Inhalt des Datenbereichs hängt von den verschiedenen Funktionscodes ab, die spezifischen Regeln finden sich in der detaillierten Funktionscodebeschreibung unten.

3.3. Detaillierte Funktionscode-Beschreibung

3.3.1. Funktionscode 01: Lesen von Schaltern (Fernmeldung)

Alle Schalter werden als Binärbits codiert, wobei jeder Schalter ein Bit darstellt. Ein Byte kann den Status von 8 Schaltern enthalten, wobei 1 den geschlossenen Zustand und 0 den offenen Zustand repräsentiert.

Die Schalteradressen sind bitcodiert. Beispielsweise befindet sich der Schalter mit Adresse 0 im D0-Bit des ersten Bytes im Datenbereich, der Schalter mit Adresse 1 im D1-Bit des ersten Bytes usw. Der Schalter mit Adresse X befindet sich im Byte X/8+1 im Datenbereich an Bitposition D[X%8].

Format der vom Master gesendeten Nachricht:

Geräteadresse	1 Byte	Geräteadresse
Funktionscode	1 Byte	01: Schaltstatus lesen
Startadresse	2 Bytes	Ab welcher Schalteradresse sollen Schaltzustände gelesen werden (Start-Bit)
Schalteranzahl	2 Bytes	Wie viele Schalter sollen gelesen werden (Bit-Anzahl)

Geräteadresse	1 Byte	Geräteadresse
CRC-Prüfcode	2 Bytes	CRC-Prüfcode für Geräteadresse, Funktionscode, Startadresse, Schalteranzahl

Format der vom Gerät zurückgesendeten Daten:

Geräteadresse	1 Byte	Geräteadresse
Funktionscode	1 Byte	01: Schaltstatus lesen
Daten-Byteanzahl N	1 Byte	Anzahl der nachfolgenden Datenbytes, jedes Byte enthält 8 Schaltzustände. Daten-Byteanzahl N = (Schalteranzahl+7)÷8
Daten	N Bytes	D0-Bit des ersten Bytes ist der Status des ersten Schalters (Startadresse); D1-Bit des ersten Bytes ist der Status des zweiten Schalters (Startadresse+1); usw.
CRC-Prüfcode	2 Bytes	CRC-Prüfcode für Geräteadresse, Funktionscode, Daten-Byteanzahl, Daten

Beispiel:

Angenommen, die Geräteadresse ist 2 und die Schaltzustände sind wie folgt:

Adresse	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Status	Offen	Geschl.	Offen	Offen	Offen	Geschl.	Geschl.	Offen	Offen	Offen	Offen	Geschl.	Offen	Geschl.	Offen	Geschl.

Abfrage der Schalter von Adresse 4 bis 8 (5 Schalter):

Master sendet: `02 01 00 04 00 05 BD FB`

Byte	Bedeutung
02	Geräteadresse: 02
01	Funktionscode 01: Schaltstatus lesen
00 04	Startadresse: 0004, zuerst höherwertiges Byte 00, dann niederwertiges Byte 04
00 05	0005 Schalter lesen, zuerst höherwertiges Byte 00, dann niederwertiges Byte 05
BD FB	CRC-Prüfcode für 02 01 00 04 00 05

Gerät antwortet: `02 01 01 06 D1 CE`

Byte	Bedeutung
02	Geräteadresse
01	Funktionscode 01: Schaltstatus lesen
01	Es folgt 1 Byte Daten, das maximal 8 Schaltzustände darstellen kann
06	Da nur 5 Schalter abgefragt werden, stellen D0-D4 die Schaltzustände dar, D5-D7 haben keine Bedeutung. Der Wert 06 in Binärform ist 00000110

Bit D7 und D6 haben keine Bedeutung, da nur 5 Schalter abgefragt werden. Bit D5 hat keine Bedeutung, da nur 5 Schalter abgefragt werden. Bit D4=0: Schalter an Adresse 8 ist offen Bit D3=0: Schalter an Adresse 7 ist offen Bit D2=1: Schalter an Adresse 6 ist geschlossen Bit D1=1: Schalter an Adresse 5 ist geschlossen Bit D0=0: Schalter an Adresse 4 ist offen

D1 CE	CRC-Prüfcode für 02 01 01 06

3.3.2. Funktionscode 03: Lesen von Registern (Fernmessung)

Jedes Register besteht aus zwei Bytes (16-Bit-Binärdaten), mit dem höherwertigen Byte zuerst und dem niederwertigen Byte danach. Jedes Register repräsentiert einen Datenbereich von -32768 bis 32767, wobei negative Zahlen im Zweierkomplement dargestellt werden.

Die Registeradressen können so verstanden werden, dass sich das Register mit Adresse 0 im ersten und zweiten Byte des Datenbereichs befindet, das Register mit Adresse 1 im dritten und vierten Byte des Datenbereichs, das Register mit Adresse 2 im fünften und sechsten Byte des Datenbereichs usw.

Format der vom Master gesendeten Nachricht:

Geräteadresse	1 Byte	Geräteadresse
Funktionscode	1 Byte	03: Register lesen

Geräteadresse	1 Byte	Geräteadresse
Startadresse	2 Bytes	Ab welcher Adresse sollen Register gelesen werden
Registeranzahl	2 Bytes	Wie viele Register sollen gelesen werden (Byteanzahl = Registeranzahl × 2)
CRC-Prüfcode	2 Bytes	CRC-Prüfcode für Geräteadresse, Funktionscode, Startadresse, Registeranzahl

Format der vom Gerät zurückgesendeten Daten:

| Geräteadresse | 1 Byte | Geräteadresse | | Funktionscode | 1 Byte | 03: Register lesen | | Daten-Byteanzahl N | 1 Byte | Daten-Byteanzahl N = Registeranzahl × 2 | | Registerdaten | N Bytes | Registeranzahl = Daten-Byteanzahl ÷ 2. Das erste und zweite Byte sind die Daten des ersten Registers (Startadresse), das dritte und vierte Byte sind die Daten des zweiten Registers (Startadresse+1), usw. | | CRC-Prüfcode | 2 Bytes | CRC-Prüfcode für Geräteadresse, Funktionscode, Daten-Byteanzahl, Registerdaten |

Beispiel:

Angenommen, die Geräteadresse ist 2 und die Registerdaten sind wie folgt:

Adresse	0	1	2	3	4	5	6	7	8
Daten	500	1000	-900	2000	-10	800	300	-1000	600

Abfrage der Register von Adresse 2 bis 5 (4 Register):

Master sendet: `02 03 00 02 00 04 E5 FA`

Byte	Bedeutung
02	Geräteadresse: 02
03	Funktionscode 03: Register lesen
00 02	Startadresse: 0002, zuerst höherwertiges Byte 00, dann niederwertiges Byte 02
00 04	0004 Register lesen, zuerst höherwertiges Byte 00, dann niederwertiges Byte 04
E5 FA	CRC-Prüfcode für 02 03 00 02 00 04

Gerät antwortet: `02 03 08 FC 7C 07 D0 FF F6 03 20 39 2E`

Byte	Bedeutung
02	Geräteadresse: 02
03	Funktionscode 03: Register lesen
08	Es folgen 8 Bytes, also 4 Register Daten
FC 7C 07 D0 FF F6 03 20	Da die Abfrage bei Adresse 2 beginnt, ist das erste zurückgegebene Register das mit Adresse 2:
FC 7C	Register an Adresse 2 = 0xFC7C, also -900
07 D0	Register an Adresse 3 = 0x07D0, also 2000
FF F6	Register an Adresse 4 = 0xFFF6, also -10
03 20	Register an Adresse 5 = 0x0320, also 800
39 2E	CRC-Prüfcode für 02 03 08 FC 7C 07 D0 FF F6 03 20

3.3.3. Funktionscode 05: Schreiben eines einzelnen Schalters (Fernsteuerung)

Format der vom Master gesendeten Nachricht:

Geräteadresse	1 Byte	Geräteadresse
Funktionscode	1 Byte	05: Einzelschalter schreiben
Schalteradresse	2 Bytes	Welcher Schalter soll ferngesteuert werden
Steuerbefehl	2 Bytes	FF00 für Schließbefehl, 0000 für Öffnungsbefehl
CRC-Prüfcode	2 Bytes	CRC-Prüfcode für Geräteadresse, Funktionscode, Schalteradresse, Steuerbefehl

Format der vom Gerät zurückgesendeten Daten:

Die vom Gerät zurückgesendete Nachricht ist mit der vom Master gesendeten Nachricht identisch. Diese Antwort bedeutet, dass das Gerät den Steuerbefehl akzeptiert hat und mit der Ausführung beginnt. Um zu bestimmen, ob der Befehl erfolgreich ausgeführt wurde, muss der Schaltzustand (Fernmeldung) gleich

dem Zielwert der Steuerung sein, d.h. der gelesene Schaltzustand entspricht dem geschriebenen Schaltzustand, dann gilt die Fernsteuerung als erfolgreich abgeschlossen.

Beispiel:

Schalter an Adresse 1 schließen:

Master sendet: `02 05 00 01 FF 00 DD C9`
Gerät antwortet: `02 05 00 01 FF 00 DD C9`

Byte	Bedeutung
02	Geräteadresse: 02
05	Funktionscode 05: Einzelschalter schreiben
00 01	Schalteradresse: 0001, zuerst höherwertiges Byte 00, dann niederwertiges Byte 01
FF 00	Schalter-Schließbefehl: 0xFF00
DD C9	CRC-Prüfcode für 02 05 00 01 FF 00

Schalter an Adresse 1 öffnen:

Master sendet: `02 05 00 01 00 00 9C 39`
Gerät antwortet: `02 05 00 01 00 00 9C 39`

Byte	Bedeutung
02	Geräteadresse: 02
05	Funktionscode 05: Einzelschalter schreiben
00 01	Schalteradresse: 0001, zuerst höherwertiges Byte 00, dann niederwertiges Byte 01
00 00	Schalter-Öffnungsbefehl: 0x0000
9C 39	CRC-Prüfcode für 02 05 00 01 00 00

3.3.4. Funktionscode 06: Schreiben eines einzelnen Registers (Ferneinstellung)

Format der vom Master gesendeten Nachricht:

Geräteadresse	1 Byte	Geräteadresse
Funktionscode	1 Byte	06: Einzelregister schreiben
Registeradresse	2 Bytes	In welches Register sollen Daten geschrieben werden
Zu schreibende Daten	2 Bytes	In das Register zu schreibende Daten
CRC-Prüfcode	2 Bytes	CRC-Prüfcode für Geräteadresse, Funktionscode, Registeradresse, zu schreibende Daten

Format der vom Gerät zurückgesendeten Daten:

Die vom Gerät zurückgesendete Nachricht ist mit der vom Master gesendeten Nachricht identisch. Diese Antwort bedeutet, dass das Gerät den Befehl zum Schreiben des Registers akzeptiert hat und mit der Ausführung beginnt. Um zu bestimmen, ob die Daten erfolgreich geschrieben wurden, müssen die Registerdaten (Fernmessung) gleich dem geschriebenen Wert sein, d.h. die gelesenen Registerdaten entsprechen den geschriebenen Registerdaten, dann gilt das Schreiben (Ferneinstellung) als erfolgreich abgeschlossen.

Beispiel:

Daten -300 in Register mit Adresse 4 schreiben:

Master sendet: `02 06 00 04 FE D4 88 07`
Gerät antwortet: `02 06 00 04 FE D4 88 07`

Byte	Bedeutung
02	Geräteadresse: 02
06	Funktionscode 06: Einzelregister schreiben
00 04	Registeradresse: 0004, zuerst höherwertiges Byte 00, dann niederwertiges Byte 04
FE D4	In das Register zu schreibende Daten: -300 im Zweierkomplement ist 0xFED4, zuerst höherwertiges Byte FE, dann niederwertiges Byte D4
88 07	CRC-Prüfcode für 02 06 00 04 FE D4

3.3.5. Funktionscode 0F: Schreiben mehrerer Schalter (gleichzeitige Fernsteuerung mehrerer Schalter)

Format der vom Master gesendeten Nachricht:

Geräteadresse	**1 Byte**	**Geräteadresse**
Funktionscode	1 Byte	0F: Mehrfachschalter schreiben
Startadresse	2 Bytes	Ab welcher Schalteradresse soll die Fernsteuerung beginnen
Schalteranzahl	2 Bytes	Wie viele Schalter sollen ferngesteuert werden
Daten-Byteanzahl N	1 Byte	Byteanzahl der zu schreibenden Schalterdaten, d.h. nachfolgende Steuerbefehlsbytes. Daten-Byteanzahl N = (Schalteranzahl+7)÷8
Zu schreibende Daten	N Bytes	D0-Bit des ersten Bytes ist der Status des ersten Schalters (Startadresse); D1-Bit des ersten Bytes ist der Status des zweiten Schalters (Startadresse+1); usw.
CRC-Prüfcode	2 Bytes	CRC-Prüfcode für Geräteadresse, Funktionscode, Startadresse, Schalteranzahl, Byteanzahl, Daten

Format der vom Gerät zurückgesendeten Daten:

Geräteadresse	**1 Byte**	**Geräteadresse**
Funktionscode	1 Byte	0F: Mehrfachschalter schreiben
Startadresse	2 Bytes	Ab welcher Schalteradresse beginnt die Fernsteuerung
Schalteranzahl	2 Bytes	Wie viele Schalter werden ferngesteuert
CRC-Prüfcode	2 Bytes	CRC-Prüfcode für Geräteadresse, Funktionscode, Startadresse, Schalteranzahl

Diese Antwort bedeutet, dass das Gerät den Steuerbefehl akzeptiert hat und mit der Ausführung beginnt. Um zu bestimmen, ob der Befehl erfolgreich ausgeführt wurde, müssen die Schaltzustände (Fernmeldung) gleich dem Zielwert der Steuerung sein, d.h. die gelesenen Schaltzustände entsprechen den geschriebenen Schaltzuständen, dann gilt die Fernsteuerung als erfolgreich abgeschlossen.

Beispiel:

Schalter an Adresse 1 schließen, Schalter an Adresse 2 öffnen, Schalter an Adresse 3 schließen:

Master sendet: `02 0F 00 01 00 03 01 05 32 81`

Byte	**Bedeutung**
02	Geräteadresse: 02
0F	Funktionscode 0F: Mehrfachschalter schreiben
00 01	Startadresse: 0001, zuerst höherwertiges Byte 00, dann niederwertiges Byte 01
00 03	3 Schalter steuern, zuerst höherwertiges Byte 00, dann niederwertiges Byte 03
01	Daten-Byteanzahl: 1 Byte, maximal 8 Schalter darstellbar
05	Da nur 3 Schalter geschrieben werden, haben D0-D2 Bedeutung, D3-D7 nicht. Der Wert 05 in Binärform ist 00000101

Die Bits D7-D3 haben keine Bedeutung, da nur 3 Schalter geschrieben werden. Bit D2=1: Schalter an Adresse 3 soll geschlossen sein Bit D1=0: Schalter an Adresse 2 soll offen sein Bit D0=1: Schalter an Adresse 1 soll geschlossen sein

32 81	**CRC-Prüfcode für 02 0F 00 01 00 03 01 05**

Gerät antwortet: `02 0F 00 01 00 03 44 39`

Byte	**Bedeutung**
02	Geräteadresse: 02
0F	Funktionscode 0F: Mehrfachschalter schreiben
00 01	Startadresse: 0001, zuerst höherwertiges Byte 00, dann niederwertiges Byte 01
00 03	3 Schalter steuern, zuerst höherwertiges Byte 00, dann niederwertiges Byte 03
44 39	CRC-Prüfcode für 02 0F 00 01 00 03

3.3.6. Funktionscode 10: Schreiben mehrerer Register (gleichzeitige Ferneinstellung mehrerer Register)

Format der vom Master gesendeten Nachricht:

Geräteadresse	1 Byte	Geräteadresse
Funktionscode	1 Byte	10: Mehrfachregister schreiben
Startadresse	2 Bytes	Ab welcher Registeradresse soll geschrieben werden
Registeranzahl	2 Bytes	Wie viele Register sollen beschrieben werden
Daten-Byteanzahl N	1 Byte	Byteanzahl der zu schreibenden Registerdaten, d.h. nachfolgende Ferneinstellungsbefehle. Daten-Byteanzahl N = Registeranzahl × 2
Zu schreibende Daten	N Bytes	Das erste und zweite Byte sind die Daten des ersten Registers (Startadresse), das dritte und vierte Byte sind die Daten des zweiten Registers (Startadresse+1), usw.
CRC-Prüfcode	2 Bytes	CRC-Prüfcode für Geräteadresse, Funktionscode, Startadresse, Registeranzahl, Byteanzahl, Daten

Format der vom Gerät zurückgesendeten Daten:

Geräteadresse	1 Byte	Geräteadresse
Funktionscode	1 Byte	10: Mehrfachregister schreiben
Startadresse	2 Bytes	Ab welcher Registeradresse beginnt das Schreiben
Registeranzahl	2 Bytes	Wie viele Register werden beschrieben
CRC-Prüfcode	2 Bytes	CRC-Prüfcode für Geräteadresse, Funktionscode, Startadresse, Registeranzahl

Diese Antwort bedeutet, dass das Gerät den Ferneinstellungsbefehl akzeptiert hat und mit der Ausführung beginnt. Um zu bestimmen, ob die Daten erfolgreich geschrieben wurden, müssen die Registerdaten (Fernmessung) gleich dem geschriebenen Wert sein, d.h. die gelesenen Registerdaten entsprechen den geschriebenen Registerdaten, dann gilt die Ferneinstellung als erfolgreich abgeschlossen.

Beispiel:

Daten 400 in Register mit Adresse 2, -500 in Register mit Adresse 3 und 700 in Register mit Adresse 4 schreiben:

Master sendet: `02 10 00 02 00 03 06 01 90 FE 0C 02 BC 72 7F`

Byte	Bedeutung
02	Geräteadresse: 02
10	Funktionscode 10: Mehrfachregister schreiben
00 02	Startadresse: 0002, zuerst höherwertiges Byte 00, dann niederwertiges Byte 02
00 03	3 Register beschreiben
06	Daten-Byteanzahl: 6 Bytes, für 3 Register
01 90 FE 0C 02 BC	Da der Schreibbefehl bei Adresse 2 beginnt, sind die Daten des ersten Registers die von Adresse 2:
01 90	Register an Adresse 2 = 0x0190, also 400
FE 0C	Register an Adresse 3 = 0xFE0C, also -500
02 BC	Register an Adresse 4 = 0x02BC, also 700
72 7F	CRC-Prüfcode für 02 10 00 02 00 03 06 01 90 FE 0C 02 BC

Gerät antwortet: `02 10 00 02 00 03 21 FB`

Byte	Bedeutung
02	Geräteadresse: 02
10	Funktionscode 10: Mehrfachregister schreiben
00 02	Startadresse: 0002, zuerst höherwertiges Byte 00, dann niederwertiges Byte 02
00 03	3 Register beschrieben

Byte	Bedeutung
21 FB	CRC-Prüfcode für 02 10 00 02 00 03

3.4. CRC16-Berechnungsmethode

3.4.1. Algorithmusbeschreibung

- Initialisiere ein 16-Bit-Register mit dem hexadezimalen Wert FFFF (alle Bits auf 1); bezeichne dieses Register als CRC-Register.
- Führe eine XOR-Operation zwischen dem ersten 8-Bit-Binärwert (d.h. dem ersten Byte des Kommunikationsframes) und den niederwertigen 8 Bits des 16-Bit-CRC-Registers durch, speichere das Ergebnis im CRC-Register.
- Schiebe den Inhalt des CRC-Registers ein Bit nach rechts (in Richtung des niederwertigen Bits), fülle das höchstwertige Bit mit 0 und prüfe das hinausgeschobene Bit.
- Wenn das hinausgeschobene Bit 0 ist: Wiederhole Schritt 3 (erneut um 1 Bit nach rechts schieben); wenn das hinausgeschobene Bit 1 ist: führe eine XOR-Operation zwischen dem CRC-Register und dem Polynom A001 (1010 0000 0000 0001) durch.
- Wiederhole die Schritte 3 und 4, bis 8 Verschiebungen durchgeführt wurden, wodurch das gesamte 8-Bit-Datenelement verarbeitet wurde.
- Wiederhole die Schritte 2 bis 5 für das nächste Byte des Kommunikationsframes.
- Nachdem alle Bytes des Kommunikationsframes nach den obigen Schritten verarbeitet wurden, tausche das höher