**Communication Protocol**

**For UGS500**

Contents

[1 Communication Protocol 3](#_Toc161842229)

[1.1 Overview 3](#_Toc161842230)

[1.2 Data encryption Requirements 3](#_Toc161842231)

[1.3 Data upload process 3](#_Toc161842232)

[1.4 Communication Frame Format 3](#_Toc161842233)

[1.5 Data area format 4](#_Toc161842234)

[1.5.1 Registration Frame 4](#_Toc161842235)

[1.5.2 End Frame 4](#_Toc161842236)

[1.5.3 The meter is actively uploaded 4](#_Toc161842237)

[1.5.4 Set the Server IP and Port number 6](#_Toc161842341)

[1.5.5 Set the cumulative amount 6](#_Toc161842342)

[1.5.6 Set meter time 6](#_Toc161842343)

[1.5.7 Set meter number 7](#_Toc161842344)

2 [Code and status 7](#_Toc161842346)

# Communication Protocol

#### Overview

This standard communication protocol is based on TCP and UDP network transmission protocols, which standardize the application layer communication protocol between terminal devices and the main station. Meters can communicate directly through telecommunications platforms or TCP/UDP.

#### Data encryption Requirements

To solve the problem of data interaction security, add data encryption specifications. This specification uses the current application of the common AES encryption algorithm, the key length is selected as 128 bits, the encryption mode is selected as ECB mode (code Book mode, Electronic Codebook Book (ECB)), this mode is to divide the whole plaintext into several identical segments， and then encrypt each segment.), the specific specification is described as follows:

(1) The encryption key is 16 bytes;

(2) the plaintext is not enough for 16 bytes, use {0x80, 0x00, 0x00, ... ..., 0x00} as padding, such as 112233445566778899AABB, after padding, it becomes 112233445566778899AABB8000000000. After that, perform encryption operations.

(3) Encrypt only the protocol data area

#### Data upload process

The connection is initiated by the meter end, and the registration frame is sent first after the connection is successful. After receiving the normal response of registration frame from the system, the meter starts to send data. If the registration fails, the data is no longer sent. After the data upload is finished, the **upload** end frame is sent by meter, and the system can start to send commands after receiving this **upload** end frame. After receive the **download** end frame from server, the meter goes to sleep.

#### Communication Frame Format

**Table 1 the Format of Communication Protocol Frame**

|  |  |  |
| --- | --- | --- |
| **Name** | **Number of bytes** | **Format instructions** |
| Start of frame | 1 | 0xA8 |
| Frame length | 2 | Uint16, The number of bytes from the start character of the frame to the end character of the frame, with the low byte in the first |
| Comm number | 7 | BCD code, high in front |
| Control code | 1 | HEX |
| Transaction serial number | 4 | Hex, is 0 when active upload, and command return should be consistent with sent |
| Protocol version number | 1 | Always be 0x03 now |
| Command Byte | 1 | Hex |
| Data area (encrypted area) | 2 | Data area content length, low bytes before, excluding XOR |
| N | Data area content, please refer to the specific protocol data area, |
| 1 | Data area XOR (data area content length + data area content) |
| Check byte | 2 | CRC16 checksum from frame starter to data area |
| End of frame | 1 | 0x16 |

#### Data area format

#### Registration Frame

|  |  |  |
| --- | --- | --- |
|  | Up(meter to system) | Down(system to meter) |
| Command byte | 0x01 | 0x01 |
| Data area | 1byte, Information Length  Nbyte, module information | 1byte, status information  (0: registration succeeded, 1: meter information does not exist 2: decryption failed)  6byte, System time (year, month, day, hour, minute, second) |

Module information is ASCII code data, should contain IMEI, ICCID, IMSI and other information, such as:

IMEI:867726033942774, IMSI:460113011386018, ICCID:89861118246005721029

#### End Frame

|  |  |  |
| --- | --- | --- |
|  | Up | Down |
| Command byte | 0x02 | 0x02 |
| Data area | 0x00 | 6 byte, System Time (year, month, day, hour, minute, second) |

After the measurement data of the meter is sent, the uplink end frame is sent, and the remaining procedure is handed over to the system. The system starts to send commands. If no command is sent, the downlink end frame is sent, and the meter sleeps.

#### The meter is actively uploaded

**The meter upload frame:**

|  |  |  |
| --- | --- | --- |
| **Bytes and**  **Format** | **Data Items** | **Instructions** |
| 1hex | Command byte | 0x03 |
| Data area | | |
| Uint16 | Supply voltage | Unit: 0.01V, low byte in front |
| Uint8 | Battery level | 0 ~ 100% |
| 1BCD | Signal strength | CSQ value |
| 1HEX | Reserve |  |
| 1HEX | Reserve |  |
| 1HEX | **Number of live data (0-1)** | ≤1:1 indicates there was real time data following, 0 indicates no real time data, when no real time data, the real-time data does not occupy the address location |
| nHex | The real time data | Check the data structure table for details |
| 1Hex | **Number of frozen data details (0-255)** | ≤255 (when is 0, frozen data does not occupy the address) |
| nHex | The frozen data | Check the data structure table for details |
| 1HEX | **Number of network messages** | ≤1 |
|  | 6ASC RSRP  4ASC SNR  2ASC ECL  10ASC CELL ID  5ASC EARFCN  1hex Operator logo (0 Telecom, 1 Mobile, 2 Unicom) | ASCII format, fill up with 0 after each missing part |
| 1HEX | **Indicates the number of event record details** |  |
| 6byte | Event record content | 1hex Event code +5BCD time |
| 6HEX | **Reserved** | Default 0 |

If there is a large amount of frozen data, multiple frames can be uploaded, and real-time data is only transmitted once. The number of real-time data should be changed to 0 after successful uploaded.

**Server response frame:**

|  |  |  |
| --- | --- | --- |
| Command byte | 0x03 | |
| Data area | 13hex | 0x00 |
| 6BCD System time | YYMMDD hh:mm:ss |
| 5hex reserved | 0x00 |

**Meter Type - Data structure**

|  |  |  |
| --- | --- | --- |
| **Real-time Data** | **Frozen details** | **Instructions** |
| 5bcd acquisition time | 5bcd acquisition time | Year - month - Day hour: min |
| 5hex Total cumulative number of standard conditions | 5hex Total accumulated status of standard conditions | AABBCCDD.EE, the integer part is uint32, low byte in the first  The decimal part is 0.01m3, which is divided by 100  e.g. 11 22 33 00 00 44 convert to 3351057.68 |
| 5hex Total accumulative quantity under operating condition | 5hex Total accumulative quantity in operating condition | AABBCCDD.EE, the integer part is uint32, low byte in the first  the decimal part represents 0.01m3, divided by 100 |
| 5hex instantaneous flow rate of standard conditions | 5hex instantaneous flow rate of standard conditions | AABBCCDD.EE, the integer part is uint32, the low byte in the first, the decimal part represents 0.01m3/h, divided by 100 |
| 5hex Instantaneous flow rate of operating conditions | 5hex Instantaneous flow rate in operating conditions | AABBCCDD.EE, the integer part is uint32, low byte in the first  The decimal part is 0.01m3/h, which is divided by 100 |
| 4byte temperature | 4byte temperature | Int32, unit: 0.001 ° C, actual value divided by 1000 |
| 4byte pressure | 4byte pressure | Uint32, 0.001Kpa, actual value divided by 1000 |
| 1hex Number of magnetic attacks |  |  |
| 2hex Meter status | 2hex Meter status | Look at the meter status instructions specifically |
| 2hex Meter Status 2 | 2hex Meter status 2 | Look at the meter status instructions specifically |

#### Set the Server IP and Port number

|  |  |  |
| --- | --- | --- |
|  | Down | Up |
| Command byte | 0x09 | 0x09 |
| Data area | 4 byte, IP address  2 byte, port number | 0xFF |

**Example 112.124.58.110:1002 , Set the value to 707C3A6E03EA**

#### Set the cumulative amount

|  |  |  |
| --- | --- | --- |
|  | Down | Up |
| Command byte | 0x14 | 0x14 |
| Data area | 5byte cumulative amount of standard conditions  5byte cumulative amount of operating condition | 0xFF |

#### Set meter time

|  |  |  |
| --- | --- | --- |
|  | Down | Up |
| Command byte | 0x15 | 0x15 |
| Data area | 6BCD time | 0xFF |

#### Set meter number

|  |  |  |
| --- | --- | --- |
|  | Down | Up |
| Command byte | 0x17 | 0x17 |
| Data area | 8BCD meter number | 0xFF |

# Code and status

* **Event code:**

|  |  |
| --- | --- |
| Incident Alarm code  (HEX) | Event type |
| 0x01 | Battery no power |
| 0x 06 | Battery power low |
| 0x 07 | Battery power very low |
| 0x 0B | Ultrasonic metering failure |
| 0x 0C | Reverse flow |
| 0x 19 | Open lid alarm |

* **Meter Status:**

BIT5: if was 1, means battery power very low

BIT6: if was 1, means battery power low

Other bits was reserved and should be ignore

Note: BIT0 indicates the lowest byte, the same below.

* **Meter status2:**

BIT0: if was 1, means ultrasonic metering failure

BIT1: if was 1, means reverse flow

BIT7: if was 1, means open lid alarm

Other bits was reserved and should be ignore

* **Control Code:**

BIT0: Data direction, 0 means upload, from meter to system, 1 means download, from system to meter

BIT1: Subsequent frame identify, 0 means no subsequent frame, 1 means there will be more subsequent frame

Other bits was reserved and should be ignore