

iHM Communication Protocol

1.0.1

Version No.	Revised on	Revisions and Reasons
1.0.0	2025-03-31	Initial release
1.0.1	2025-04-31	Added Channel 2 meter data, firmware version, and power limit switch functionalities

I. General Description

This protocol defines the communication specifications between Sungrow's iHM and host monitoring software. It adopts MODBUS RTU/TCP communication protocol. This protocol enables real-time monitoring of iHM system-wide operational data. The iHM Communication Address is 247.

iHM only supports system energy dispatch-related data forwarding and does not support data forwarding for individual inverter devices.

II. Physical Interface

1. RS485

Default port: A2B2

	Default Setting (Note: Changes are not supported)
Communication address	247
Broadcast	Yes
Baud rate	9600 bit/s
Check	None
Data bit	8
Stop bit	1
Mode	RTU

2. Ethernet

Device	Default IP	Default Port	Remarks
iHM	12.12.12.12	502/503/504	Each port supports only 1 TCP connection

III. Communication Description

1. Data type

U16 — Unsigned 16-bit integer, big-endian byte order (MSB first, LSB last);

S16 — Signed 16-bit integer, big-endian byte order (MSB first, LSB last);

U32 — Unsigned 32-bit integer, MODBUS hybrid byte order (low-word first with big-endian within words)

S32 — Signed 32-bit integer, MODBUS hybrid byte order (low-word first with big-endian within words)

U64 — Unsigned 64-bit integer data, big-endian format;

S64 — Signed 64-bit integer data, big-endian format;

Example: U16 data 0x0102 is transmitted in the order 01, 02.

Example: U32 data 0x01020304 is transmitted in the order 03, 04, 01, 02.

Example: U64 data 0x0102030405060708 is transmitted in the order 01, 02, 03, 04, 05, 06, 07, 08.

The address register starts counting at 1, so the communication address = protocol address - 1.

Example: To access register address 8000, use communication address 7999 in commands. Example: "01 04 1F 3F 00 02 + CRC" queries data at address 8000.

2. Numerical description

Decimal numbers are transmitted as integers after expansion. Example: 10.333 KW is transmitted as 10 333 in expanded form; 800.5 V is transmitted as 8005. Negative numbers are transmitted as complements. Example: 0xFFFF denotes -1.

"Reserved" or unsupported registers cannot be queried or set. "F"s are returned when unsigned numbers are queried. For example, U16 returns "0xFFFF", U32 returns "0xFFFFFFFF", and U64 returns "0xFFFFFFFFFFFFFFFF". Signed number returns the maximum positive number, for example: S16 returns "0x7FFF", S32 returns "0x7FFFFFFF", and S64 returns "0x7FFFFFFFFFFFFFFF"; UTF-8 returns 0x00. UTF-8 occupies 1 byte. An odd length is padded with 0x00.

3. Address type

The input register is a read-only register and supports 0x04 function code read.

The holding register is a read/write register and supports 0x03 function code query and 0x06/0x10 function code write.

4. Check type

CRC16, polynomial 0xA001, little-endian.

IV. Address Definition Table

1. Input register (address type: 3X)

Name	Address	Data Type	Factor	Unit	Remarks
Device type code	8000	U16			0x072A
Protocol number	8001	U32			AW0
Protocol version No.	8003	U32			Example: V1. 0. 1 Storage Format: 0x01 0x00 0x01 0x00
Total devices connected	8005	U16	1	Set	All devices connected to iHM
Total number of connected devices in fault	8006	U16	1	Set	Number of faulty devices (excluding third-party devices)
Total nominal active power	8145	U32	0.1	kW	
Total battery rated capacity	8147	U32	0.1	kWh	
Battery charge/discharge limit description	8149	U32	0.1	kW	
Maximum battery charge power	8151	U16	0.1	kW	
Minimum battery charge power	8152	U16	0.1	kW	
Maximum battery discharge power	8153	U16	0.1	kW	
Minimum battery discharge power	8154	U16	0.1	kW	
Total active power	8155	S32	0.01	kW	
Active power of the grid meter	8157	S32	0.01	kW	
Load power	8159	S32	0.01	kW	
Battery power	8161	S32	0.01	kW	
State of charge	8163	U16	0.1	%	
Import energy at the grid meter	8176	U32	0.1	kWh	
Export energy at the grid meter	8178	U32	0.1	kWh	
Application software version	8318~8332	UTF-8*30			
Charger charging status	8552	U16			1: Idle (unplugged) 2: Standby (plugged) 3: Charging 6: Charging completed
Output type	8554	U16			0 - Single-phase 1 - Three-phase four-wire 2 - Three-phase three-wire
A-B line voltage/A-phase voltage	8555	U16	0.1	V	Output type (address 8554) is 0: upload phase voltage; is 1: upload phase voltage; is 2: upload line voltage;
B-C line voltage/B-phase voltage	8556	U16	0.1	V	
C-A line voltage/C-phase voltage	8557	U16	0.1	V	
Grid Frequency	8558	U16	0.1	Hz	
Phase A active power	8559~8560	U32	1	W	
Phase B active power	8561~8562	U32	1	W	
Phase C active power	8563~8564	U32	1	W	
Channel 2 A-B line voltage/A-phase voltage	8565	U16	0.1	V	Output type (address 8554) is 0: upload phase voltage; is 1: upload phase voltage; is 2: upload line voltage;
Channel 2 B-C line voltage/B-phase voltage	8566	U16	0.1	V	
Channel 2 C-A line voltage/C-phase voltage	8567	U16	0.1	V	
Channel 2 Grid Frequency	8568	U16	0.1	Hz	
Channel 2 Phase A active power	8569~8570	U32	1	W	
Channel 2 Phase B active power	8571~8572	U32	1	W	
Channel 2 Phase C active power	8573~8574	U32	1	W	

2. Hold register (address type: 4X)

Name	Address	Data Type	Upper Limit	Lower Limit	Factor	Unit	Remarks
Energy management mode	8024	U16					1. Self-consumption (default) 4. VPP 5. Compulsory mode
Charging/discharging command	8025	U16					0xAA: Charge; 0xBB: Discharge; 0xCC: Stop (default);
Charging/discharging power	8026	U32	100%* battery charge/disch arge limit description	0	0.1	kW	
Feed-in power limit ratio	8031	S32	1000	0	0.1	%	
External VPP heartbeat	8033	U16	1000	0	1	s	600 (default)
Power-on/off	8047	U16					0xCF: Power-on 0xCE: Power-off
Charger charging modes	8048	U16					160: Fast charging mode 161: Eco charging mode
Charger enable/disable	8049	U16					0xAA: Enable 0x55: Disable
Grid power draw permission	8050	U16					0xAA: Enable 0x55: Disable The charging mode of chargers is Eco charging mode.
Enable power Limitation	8051	U16					85: Off 170: On
Limited power percentage	8052	U16	1000	0	0.1	%	

V. Examples

1. When the backend communicates with iHM (address: 247) via network and binds to port 502, to query iHM battery power:

Background sends: 09 79 00 00 00 06 F7 04 1F E1 00 04

iHM response data: 09 79 00 00 00 07 F7 04 04 00 00 00 00

In the data replied, "09 79 00 00 00 06" and "09 79 00 00 00 07" are headers of the Modbus TCP message, F7 is the address of the logger, 04 is the function code, and 0x1FE0 = 8160 is to query the data of Register 8161. According to this protocol, Register 8161 indicates the "Battery Power", and the data of Register 8161 in the logger reply message is 0.

2. Setting EMS local commands (multiple parameters supported)

Send command: 00 00 00 00 00 0F F7 10 1F 57 00 04 08 00 04 00 AA 00 64 00 00

Reply data: 00 00 00 00 00 06 F7 10 1F 57 00 04

In the command sent, "00 00 00 00 00 0b" is the Modbus TCP message header, F7 is the Logger address, 10 is the function code, 0x1F57 = 8023 is to write four consecutive register data to the starting address of Register 8024, and the value to write is 0x00AA00640000. The value represents setting energy management mode to VPP, charge/discharge command to 0xAA (charge), and charge power to 10 kW.