UPS Product EA990 II Tower Machine
Modbus communication protocol

serial number	Version	Revised content	Revised date	Note
1	Ver 1.0	Determine the basic electrical quantity	2012-4-6	
2	Ver 1.1	Modify 04 function code	2012-9-1	
3	Ver 1.2	Add ECO mode fault info	2015-6-1	
4	Ver 1.3	Delete the last reserve items 02 function code	2016-3-2	
5	Ver 1.4	Modify active power radio and apparent power revised as 0.1 of 04 function code	2016-5-22	

Menu

Ⅰ Protocol related instructions

1 Protocol profile

Modbus Protocol is used for EA990 II Tower Machine and Monitoring center communication, through this protocol, the controller communicates with the client device via RS485 network.

This communication adopts the way of response, the client device sends the request (telemetry information), server execute the request and response, server need set different address to distinguish, the range is between1~247

2 Interface

RS485: asynchronous, half-duplex

Baud Rate: 9600 bps, configurable

Data bit length: 8 bits, configurable

Parity check: None, configurable

Stop bit length: 1bit, configurable

3 Protocol format

This protocol supports Modbus RTU mode

3.1 RTU mode frame format

When the controller communicate on Modbus in RTU mode, per 8 bit byte in the information include 2 4 Bits hexadecimal characters, each bit format in RTU mode is as below:

Coding system: eight binary

Start bit: 1 bit

Data bits: 8 bit, to send low byte first

Odd/even check: for odd parity or even check it is 1 bit, none odd/even check, it is 1 stop bit

Stop bit: 1 bit

Error checking area: cycle redundancy check (CRC)

RTU mode request frame format:

Start	Device address	Function code	Register start address	Number of registers	CRC Low byte	CRC high byte	End
At least 3.5 characters free time	8 bit	8 bit	16 bit	16 bit	8 bit	8 bit	At least 3.5 characters free time

Among it, the RTU mode character transmission format is 10 bit transmission, data bit is 8 bit, and bit sequence is (non odd/even check, so it is 10 bit)

Start	1	2	3	4	5	6	7	8	Stop bit (odd/even parity bit)	Stop bit

RTU mode request frame format:

Start	Device address	Function code	Data	CRC low byte	CRC high byte	End
At least 3.5 characters free time	8 bit	8 bit	8 bit	8 bit	8 bit	At least 3.5 characters free time

It needs at least 3.5 the time interval between characters for sending the message and it needs at least 3.5 characters-time pauses to end the message, one new message can be started after the pause.

The entire message frame must be transmitted as a continuous flow, If a silent interval of more th an 1.5 character times occurs before completion of the frame, frame error, stop receiving, and rest art the receiving, that is to ensure at least 3.5 the time interval between characters for two frames, It is 1.5 character times or 3.5 character times depends on specific communication baud rate, cal culation method as following (baud rate is 9600):

1.5 the time interval between characters =（1/9600）×11×1.5×1000 = 1.72 ms

3.5 the time interval between characters =（1/9600）×11×3.5×1000 = 4.01 ms

【e.g.】***

Request frame message: request frame message, request the data for machine 1, address: register start address0002, number of registers: 1pcs

	Address	Function code	Register start address		Number of registers		CRC	
Data	0x01	0x03	0x00	0x02	0x00	0x01	0x25	0xCA
Number of bytes	1	1	2		2		2	

Response frame information: severer 1 response frame

	Address	Function code	Returns the number of data bytes	Data content		CRC	
Data	0x01	0x03	0x02	0x12	0x22	0xE9	0x5C
Number of bytes	1	1	1	2		2	

When a client device sends a request to a server device it expects a normal response. One of four possible events can occur from the master’s query:

- If the server device receives the request without a communication error, and can handle the query normally, it returns a normal response.
- If the server does not receive the request due to a communication error, no response is returned. The client program will eventually process a timeout condition for the request.
- If the server receives the request, but detects a communication error (parity, LRC, CRC,), no response is returned. The client program will eventually process a timeout condition for the request.
- If the server receives the request without a communication error, but cannot handle it (for example, if the request is to read a non–existent output or register), the server will return an exception response informing the client of the nature of the error.
- The exception response message has two fields that differentiate it from a normal response:
- Function Code Field: In a normal response, the server echoes the function code of the original request in the function code field of the response. All function codes have a most–significant bit (MSB) of 0 (their values are all below 80 hexadecimal). In an exception response, the server sets the MSB of the function code to 1. This makes the function code value in an exception response exactly 80 hexadecimal higher than the value would be for a normal response.
- With the function code’s MSB set, the client's application program can recognize the exception response and can examine the data field for the exception code.
- Data Field: In a normal response, the server may return data or statistics in the data field (any information that was requested in the request). In an exception response, the server returns an exception code in the data field. This defines the server condition that caused the exception.

Abnormal code and meaning are shown in the following table:

Code	Name	Meaning
0x01	Illegal function	The function code received in the query is not an allowable action for the server (or slave).
0x02	Illegal data address	The data address received in the query is not an allowable address for the server (or slave).

0x03	Illegal data value	A value contained in the query data field is not an allowable value for server (or slave).
0x04	Slave device failure	An unrecoverable error occurred while the server (or slave) was attempting to perform the requested action.
0x05	Confirmation	The server accepts the service call, but it takes a relatively long time to complete the service. therefore, the server only returns a service call received confirmation
0x06	Server busy	Server data may not be ready

【e.g.】***

RTU mode:

Command information: request data of sever 1, address: register start address: 0066, number of registers: 2

	Address	Function code	Register start address		Number of registers		CRC	
Data	0x01	0x03	0x00	0x66	0x00	0x02	0x24	0x14

Response message: Response frame of sever 1, for the error of register start address; return message is illegal data address.

	Address	Function code	Data	CRC	
Data	0x01	0x83	0x02	0xC0	0xF1

5 Function code

Function code	Name	Usage
0x02	Read Discrete Inputs	Read server discrete magnitude input register binary data
0x03	Read Registers	Get the current binary value from one or more registers
0x04	Read Input Registers	Get the current binary value from one or more input registers
0x06	Write Single Register	Write a single register from the sever (can be used as the function code setting a single parameter)
0x10	Write Multiple Registers	Write a Multiple register from the sever (can be used as the function code setting a single parameter)

Ⅱ Communication content

1 Remote communication data (function code 0x02)

1) Client device Request command format:

Definition	Address	Function code	Initial discrete magnitude address		Number of discrete magnitude		CRC	
Data	ADDR	02 H	High byte	Lower byte	High byte	Lower byte	Lower byte	High byte
Number of bytes	1	1	2		2		2	

2) Normal response format:

Definition	Address	Function code	Response data bytes	Returned discrete magnitude status	CRC	
Data	ADDR	02H	DATA_BYTES		Lower byte	High byte
Number of bytes	1	1	1		2	

3) Abnormal response format:

Definition	Number of bytes	Error code	Exception code	CRC	
Data	ADDR	82 H	ERR_CODE	Lower byte	High byte
Number of bytes	1	1	1	2	

Remote communication data register table:

Address	Name	Data length	Description
0	Bus Volt High	1 bit	1 module failure occur, 0 did not occur (0~31For module fault information)
1	Bus Volt Low	1 bit	
2	Bus Imbalance	1 bit	
3	Bus Short circuit	1 bit	
4	The Bypass Wrong Wiring	1 bit	
5	Bus Softstart timeout	1 bit	
6	Inv Softstart timeout	1 bit	
7	Inverter Volt High	1 bit	
8	Inverter Volt Low	1 bit	
9	R phase Out Short	1 bit	
10	S phase Out Short	1 bit	

11	T phase Out Short	1 bit	
12	RS phase Out Short	1 bit	
13	ST phase Out Short	1 bit	
14	TR phase Out Short	1 bit	
15	R Reactive Abnormal	1 bit	
16	S Reactive Abnormal	1 bit	
17	T Reactive Abnormal	1 bit	
18	Overload Fail	1 bit	
19	Work Mode Inconformity	1 bit	
20	Reserved	1 bit	
21	Overtemp Fault	1 bit	
22	Comm Syn Sig Fail	1 bit	
23	Comm Syn Pulse Fail	1 bit	
24	Relay Stick Death	1 bit	
25	Line SCR Fault	1 bit	
26	Can Bus Fault	1 bit	
27	Total Reactive Fault	1 bit	
28	Id Error	1 bit	
29	IGBT Short Circuit	1 bit	
30	Inverter Fault	1 bit	
31	The power setting error	1 bit	
32	Buck Softstart Fail	1 bit	1 charger failure occur 0 did not occur, (32~41For charger fault information)
33	Reserved	1 bit	
34	Charger Short circuit	1 bit	
35	Reverse battery	1 bit	
36	Disconnect the input fuse	1 bit	
37	Disconnect the output fuse	1 bit	
38	Charger physical address error	1 bit	
39	Reserved	1 bit	
40	Reserved	1 bit	
41	Reserved	1 bit	
42	Emergency shutdown	1 bit	1 alarm module occur, 0 did not occur (42~73For module fault information)
43	Abnormal overload	1 bit	
44	Communication failure	1 bit	
45	UPS overload	1 bit	
46	The battery is not connected	1 bit	
47	ECO instability	1 bit	

48	UPS Over Current	1 bit	
49	Electric Supply bypass is not consistent	1 bit	
50	The battery voltage is abnormal	1 bit	
51	Read and write eerom errors	1 bit	
52	Fan module fault	1 bit	
53	Electric phase error	1 bit	
54	Bypass phase error	1 bit	
55	Module N Line Loss	1 bit	
56	Comm Syn Sig Fail	1 bit	
57	Comm Syn Pulse Fail	1 bit	
58	Electric anomaly	1 bit	
59	Bypass anomaly	1 bit	
60	Battery Low voltage	1 bit	
61	Reserved	1 bit	
62	The module does not detect the charger	1 bit	
63	Battery Temperature Abnormal	1 bit	
64	The frequency of abnormal bypass	1 bit	
65	Output overvoltage	1 bit	
66	Physical address conflict	1 bit	
67	R phase PFC anomaly	1 bit	
68	S phase PFC anomaly	1 bit	
69	T phase PFC anomaly	1 bit	
70	Relay abnormal	1 bit	
71	Bypass STS disconnect	1 bit	
72	Bypass STS anomaly	1 bit	
73	ECO exit abnormal	1 bit	
74	Battery Over Charge	1 bit	1 charger alarm occur 0 did not occur (74~83 For charger fault information)
75	Battery Unconnect	1 bit	
76	Abnormal charger	1 bit	
77	Charger LCD dropped	1 bit	
78	Charge voltage setting error	1 bit	
79	Charge current setting error	1 bit	
80	Charger emergency shutdown	1 bit	
81	Charger fan failure	1 bit	
82	Charger Over temperature	1 bit	
83	The battery number setting error	1 bit	

Note: Bit type is a binary number, no special instructions baud rate is 1, signify this event or state is valid, 0 signify the event or state is not valid.

2 Telemetry measurement value (function code 0x04)

1) Client device request command format:

Definition	Address	Function code	Initial register address		Number of registers		CRC	
Data	ADDR	04 H	High byte	Low byte	High byte	Low byte	Low byte	High byte
Number of bytes	1	1	2		2		2	

2) Normal response format:

Definition	Address	Function code	Response Number of data bytes	Returned data		CRC	
Data	ADDR	04 H	DATA_BYTES	High byte	Low byte	Low byte	High byte
Number of bytes	1	1	1	2* register		2	

3) Abnormal response format:

Definition	Address	Error code	Exception code	CRC	
Data	ADDR	84 H	ERR_CODE	Low byte	High byte
Number of bytes	1	1	1	2	

Telemetry measurement value register table:

Address	Name	Data length	note		
			Unit	Ratio	Remark
0	Version	2bytes	1	0.1	Program Version
1	Input voltage ph_R	2bytes	V	1	
2	Input voltage ph_S	2bytes	V	1	
3	Input voltage ph_T	2bytes	V	1	
4	Input frequency R	2bytes	Hz	0.1	
5	Input frequency S	2bytes	Hz	0.1	
6	Input frequency T	2bytes	Hz	0.1	
7	Bypass R phase Voltage	2bytes	V	1	
8	Bypass S phase Voltage	2bytes	V	1	
9	Bypass T phase Voltage	2bytes	V	1	
10	R phase frequency of the bypass	2bytes	Hz	0.1	
11	S phase frequency of the bypass	2bytes	Hz	0.1	
12	T phase frequency of the bypass	2bytes	Hz	0.1	

13	Output voltage ph_R	2bytes	V	0.1	
14	Output voltage ph_S	2bytes	V	0.1	
15	Output voltage ph_T	2bytes	V	0.1	
16	Output current ph_R	2bytes	A	0.1	
17	Output current ph_S	2bytes	A	0.1	
18	Output current ph_T	2bytes	A	0.1	
19	Output frequency R	2bytes	Hz	0.1	
20	Output frequency S	2bytes	Hz	0.1	
21	Output frequency T	2bytes	Hz	0.1	
22	R phase active power	2bytes	KW	0.1	
23	S phase active power	2bytes	KW	0.1	
24	T phase active power	2bytes	KW	0.1	
25	R phase apparent power	2bytes	KVA	0.1	
26	S phase apparent power	2bytes	KVA	0.1	
27	T phase apparent power	2bytes	KVA	0.1	
28	R phase load factor	2bytes	%	1	
29	S phase load factor	2bytes	%	1	
30	T phase load factor	2bytes	%	1	
31	Positive charging voltage	2bytes	V	1	
32	Negative charging voltage	2bytes	V	1	
33	Positive charging current	2bytes	A	0.1	
34	Negative charging current	2bytes	A	0.1	
35	The charger temperature	2bytes	℃	0.1	
36	The positive battery voltage	2bytes	V	1	
37	The negative battery voltage	2bytes	V	1	
38	Battery capacity	2bytes	%	1	
39	The rest power	2bytes	Min	1	
40	Reserved	2bytes	/	/	
41	Reserved	2bytes	/	/	
42	Reserved	2bytes	/	/	
43	Reserved	2bytes	/	/	
44	The module temperature	2bytes	℃	0.1	
45	Working mode	2bytes	/	/	1:Standby mode 2: bypass mode 3: normal mode 4: battery mode 5: Battery self diagnosis 6: failure mode 7: variable frequency

					mode 8: ECO mode 9: shutdown mode
46	Charging mode	2bytes	/	/	0: power on mode 1:Standby mode 2: charging mode 3: failure mode 4: shutdown mode

Note: unsigned short is without signed short, 2 byte wide, short is with signed short, 2 byte wide. Actual value of Remote measurement data is transfer value* coefficient, if reading address 6 and response value is 50, PV1 current is 50 * 0.1=5.0 A

3 Read device parameters (function code 0x03)

1) Client device request command format:

Definition	Address	Function code	Initial register address		Number of registers		CRC	
Data	ADDR	03H	High byte	Low byte	High byte	Low byte	Low byte	High byte
	1	1	2		2		2	

2) Normal response format :

Definition	Address	Function code	Response Number of data bytes	Returned data		CRC	
Data	ADDR	03H	DATA_BYTES	High byte	Low byte	Low byte	High byte
Number of bytes	1	1	1	2*registers		2	

3) Abnormal response format:

Definition	Address	Error code	Abnormal code	CRC	
Data	ADDR	83H	ERR_CODE	Low byte	High byte
Number of bytes	1	1	1	2	

4) Holding register table:

Address	Name	Data type	Coefficient	Unit	Note

Note: Unsigned short, 2 bytes wide, the real value of the holding register is transfer value* coefficient

4 Set device parameters (function code 0x06/0x10)

4.1 0x06 Command frame format

1) PC request command format:

Definition	Address	Function	Register address	Register value	CRC

		code					
Data	ADDR	06 H	High byte	Low byte	High byte	Low byte	Low byte	High byte
Number of bytes	1	1	2		2		2	

2) Normal response format:

Definition	Address	Function code	Register address		Register value		CRC	
Data	ADDR	06 H	High byte	Low byte	High byte	Low byte	Low byte	High byte
Number of bytes	1	1	2		2		2	

3) Abnormal response format:

definition	address	error code	Exception code	CRC	
Data	ADDR	86H	ERR_CODE	Low byte	High byte
Number of bytes	1	1	1	2	

4.2 0x10 Command frame format

1) PC request command format:

Definition	Address	Function Code	Start register address		Number of registers		Number of bytes	Register value	CRC	
Data	ADDR	10 H	High byte	Low byte	high byte	Low byte			Low byte	High byte
No. of bytes	1	1	2		2		1	2* Register qty	2	

2) Normal response format:

Definition	Address	Function code	Start register address		Number of registers		CRC	
Data	ADDR	10H	High byte	Low byte	High byte	Low byte	Low byte	High byte
Number of bytes	1	1	2		2		2	

3) Abnormal response format:

Definition	Address	Error code	Exception code	CRC	
Data	ADDR	90 H	ERR_CODE	Low byte	High byte
Number of bytes	1	1	1	2	

Address	Register content	Data length	Note
0	Reserved	2 bytes	/
1	Battery test for 10 seconds	2 bytes	Write 0xFFFF 10s clock after the test is effective; sustained return. If the battery voltage is low in the process of testing, the system immediately return to the initial state.
2	Battery low voltage test	2 bytes	Write 0xFFFF, system testing until the battery voltage is low to inverter power supply.
3	Buzzer fault	2 bytes	Write 0xFFFF, UPS alarm system, alarm sound can be open or cancel.
4	Cancel test command	2 bytes	Writing 0xFFFF is valid, cancel all the testing state, the system return to output state immediately
5	Cancel shut down command	2 bytes	writing 0xFFFF is valid, a) If the system is on shut down mode, the command will cancel shut down; b) System in the state of restore after shutdown, the command immediately restore the system output, but UPS must maintain prohibited state at least 10s
6	The battery test N minutes	2 bytes	writing N N [0,99], writing time, effective continuous testing for n minutes. If the battery voltage is low in the process of testing, the system returns immediately;
7	The timing of N seconds after shutdown	2 bytes	Writing N N [12，600], writing time, effective; close UPS system in N seconds.
8	shutdown for N minutes then restart UPS	2 bytes	Writing N N [1，9999], writing time, effective; UPS system is closed, and then restart the system after N minutes. Pay attention to this, separate register address invalid operation, must be continuous to 0x0007 to 0x0008, this function will take effect.
9	Set year	2 bytes	2012~2099 Effective
10	Set month	2 bytes	1~12 Effective
11	Set day	2 bytes	According to whether the leap, set the correct time, otherwise it will refuse to modify
12	Set hour	2 bytes	0~23 Effective
13	Set min	2 bytes	0~59 Effective
14	Set second	2 bytes	0~59 Effective

Appendix A CRC (Cycle Redundancy Check)

□ CRC

CRC cycle redundancy check

Cycle redundancy check area is 2 bytes, including one 16-bit binary data, the CRC value is calcul ated by the transmitting device, and attached the calculated value to the message, the receiving d evice recalculates the CRC value when receiving message, and compares the calculated value with the actual value received in CRC area, if the value is different, it encounters an error.

First set register 16 bit to “1” when start CRC, then input adjacent two 8-bit bytes of data into cur rent register, only the eight bits of data in each character are used for generating the CRC. Start bit, stop bit and parity bit are not added to CRC.

During CRC period, every 8 bits of data and register values are used for exclusive-or operation, to move the result to the right one (LSB direction), fill the MSB with “0”, detect lSB, if LSB is “1”, wi ll to do exclusive-or operation with preset value, if ISB is “0”, will not to de exclusive-or operation.

Repeat above process until shift 8 times, after finishing the 8 times shift, to do exclusive-or operati on with current register value, after processing al the messages, the final value in the register is C RC value.

