SOFARSOLAR

ModBus-RTU Communication Protocol

1. General Information

The guide is to give you the definition of the protocol between Inverter and AP(Application Program and data Logger Devices ,hereinafter to as 'AP.').Through the protocol ,data packet will be transmitted between AP and Inverter.

About the setting of communication,the query data length is 8 bits;the parity is set to none and the stop bits is one.The Baud rate is 9600bps.

2. Modbus Function Format

2.1 Packet Format

Query

Slave Address	Function Code	Starting Address	Number of Registers	CRC16
1 byte	1 byte	2 bytes	2 bytes	2 bytes
0xxx	0xxx	Hi ByteLo Byte	Hi Byte Lo Byte	Lo Byte Hi Byte

Response

Slave Address	Function Code	Byte Count	Register-1 value	...	Register-N value	CRC16
1 byte	1 byte	1 byte	2 bytes	N-2	2 bytes	2 bytes
Byte	Byte	Byte	Hi Byte Lo Byte	...	HiByte Lo Byte	Lo Byte Hi Byte

2.2 Description

Slave Address	8-bit value representing the slave being address(1-31)
Function Code	Read the real time data(0x03) Read product information(0x04)
Starting Address (Hi)	The High byte of the Starting Address

Starting Address (Lo)	The Low byte of the Starting Address
Number of Registers (Hi)	The High byte of the Register number
Number of Registers (Lo)	The Low byte of the Register number
ByteCount	The bytes count of registers being requested
CRC16 Lo	The Low byte of the error check value
CRC16 Hi	The High byte of the error check value

3. Instruction

3.1 Read the real time data(Function Code 0x03)

Through the 0x03 function code, queries allow the register information, data format is as follows：

3.1.1 data frame format

Packet format of AP Request：

Slave Address	Function Code	Starting Address	Number of Registers	CRC16
1 byte	1 byte	2 bytes	2 bytes	2 bytes
0xxx	0x03	Hi ByteLo Byte	Hi Byte Lo Byte	Lo Byte Hi Byte

Packet format of Inverter Request：

Slave Address	Function Code	Byte Count	Register-1 value	。。。	Register-N value	CRC16
1 byte	1 byte	1 byte	2 bytes	N-2	2 bytes	2 bytes
Byte	Byte	Byte	Hi Byte Lo Byte	。。。	HiByte Lo Byte	Lo Byte Hi Byte

Example（query the state of the Inverter ）：

Query ：

Slave Address	0x01
Function Code	0x03
Starting Address Hi	0x00
Starting Address Lo	0x00
Number of Registers Hi	0x00
Number of Registers Lo	0x01
CRC16 Lo	0x84
CRC16 Hi	0x0A

response：

Slave Address	0x01
Function Code	0x03
Byte Count	0x02
Register-1 value Hi	0x00
Register-1 value Lo	0x00
CRC16 Lo	0xB8
CRC16 Hi	0x44

3.1.2 Data Address Table

Operating state

00： wait
01：check
02：Normal
03：Fault
04：Permanent

Fault Message：

Byte0

bit	Error Message	ID code(detailed)
Bit0	GridOVP	ID01 Grid Over Voltage Protection
Bit1	GridUVP	ID02 Grid Under Voltage Protection
Bit2	GridOFP	ID03 Grid Over Frequency Protection
Bit3	GridUFP	ID04 Grid Under Frequency Protection
Bit4	PVUVP	ID05 PV Under Voltage Protection
Bit5	GridLVRT	ID06 Grid Low Voltage Ride through
Bit6	reserve	ID07
Bit7	reserve	ID08

Byte1

bit 位	Error Message	ID code(detailed)
Bit0	PVOVP	ID09 PV Over Voltage Protection
Bit1	IpvUnbalance	ID10 PV Input Current Unbalance
Bit2	PvConfigSetWrong	ID11 PV Input Mode Configure wrong
Bit3	GFCIFault	ID12 Ground-Fault circuit interrupters Fault
Bit4	PhaseSequenceFault	ID13 Phase sequence Fault
Bit5	HwBoostOCP	ID14 hardware boost over current protection
Bit6	HwAcOCP	ID15 Hardware AC over current protection
Bit7	AcRmsOCP	ID16 The Grid current is too high

Byte2

bit	Error Message	ID code(detailed)
Bit0	HwADFaultIGrid	ID17 The Grid current sampling is error
Bit1	HwADFaultDCI	ID18 The DCI sampling is error
Bit2	HwADFaultVGrid	ID19 The Grid voltage sampling is error
Bit3	GFCIDeviceFault	ID20 GFCI device sampling is error
Bit4	MChip_Fault	ID21 Main chip fault
Bit5	HwAuxPowerFault	ID22 Hardware auxiliary power fault
Bit6	BusVoltZeroFault	ID23 Bus voltage zero fault
Bit7	IacRmsUnbalance	ID24 The output current is not balanced

Byte3

bit	Error Message	ID code(detailed)
Bit0	BusUVP	ID25 Bus under voltage protection
Bit1	BusOVP	ID26 Bus over voltage protection
Bit2	VbusUnbalance	ID27 Bus voltage unbalance
Bit3	DciOCP	ID28 The DCI is too high
Bit4	SwOCPInstant	ID29 The Grid current is too high
Bit5	SwBOCPInstant	ID30 The input current is too high
Bit6	reserved	ID31
Bit7	reserved	ID32

Byte4，byte5

bit	Error Message	ID code(detailed)
Bit0	reserved	33/41
Bit1	reserved	34 /42
Bit2	reserved	35/43
Bit3	reserved	36/44
Bit4	reserved	37/45
Bit5	reserved	38/46
Bit6	reserved	39/47
Bit7	reserved	40/48

Byte6

bit	Error Message	ID code(detailed)
Bit0	ConsistentFault_VGrid	ID49 The grid voltage sampling value between the master and slave DSP is Vary widely
Bit1	ConsistentFault_FGrid	ID50 The grid frequency sampling value between the master and slave DSP is Vary widely
Bit2	ConsistentFault_DCI	ID51 The DCI sampling value between the master and slave DSP is Vary widely
Bit3	ConsistentFault_GFCI	ID52 The GFCI sampling value between the master and slave DSP is Vary widely
Bit4	SpiCommLose	ID53 The communication between the master and slave DSP is fail
Bit5	SciCommLose	ID53 The communication between the slave and communication board is fail
Bit6	RelayTestFail	ID55 The relay is fault
Bit7	PvIsoFault	ID56 The insulation resistance between the PV array and the earth is too low

Byte7

bit	Error Message	ID code(detailed)
Bit0	OverTempFault_Inv	ID57 The inverter temp is too high
Bit1	OverTempFault_Boost	ID58 The boost temp is too high
Bit2	OverTempFault_Env	ID59 The environment temp is too high
Bit3	PEConnectFault	ID60 The inverter is not connect the PE wire
Bit4	reserved	ID61
Bit5	reserved	ID 62
Bit6	reserved	ID 63
Bit7	reserved	ID 64

Byte8

bit	Error Message	ID code(detailed)
Bit0	unrecoverHwAcOCP	ID65 The grid current is too high,and has cause unrecoverable fault
Bit1	unrecoverBusOVP	ID66 The bus voltage is too high,and has cause unrecoverable fault

Bit2	unrecoverIacRmsUnbalance	ID67 The grid current is unbalance,and has cause unrecoverable fault
Bit3	unrecoverIpvUnbalance	ID68 The input current is unbalance,and has cause unrecoverable fault
Bit4	unrecoverVbusUnbalance	ID69 The bus voltage is unbalance,and has cause unrecoverable fault
Bit5	unrecoverOCPInstant	ID70 The grid current is too high,and has cause unrecoverable fault
Bit6	unrecoverPvConfigSetWrong	ID65 PV Input Mode Configure wrong,and has cause unrecoverable fault
Bit7	reserved	72

Byte9

bit 位	Error Message	ID code(detailed)
Bit0	reserved	73
Bit1	unrecoverIPVInstant	ID74 The input current is too high.and has cause unrecoverable fault
Bit2	unrecoverWRITEEEPROM	ID75 The EEPROM is fault
Bit3	unrecoverREADEEPROM	ID76 The EEPROM is fault
Bit4	unrecoverRelayFail	ID77 The relay is fault, and has cause unrecoverable fault
Bit5	reserved	ID 78
Bit6	reserved	ID 79
Bit7	reserved	ID 80

Inverter alert message Message：

byte0

bit 位	Error Message	ID code(detailed)
Bit0	OverTempDerating	ID81 The inverter has derated because of the temperature is too high
Bit1	OverFreqDerating	ID82 inverter has derated because of the grid frequency is too high
Bit2	RemoteDerating	ID83 inverter has derated by remote control
Bit3	RemoteOff	ID84 inverter has shut down by remote control
Bit4	reserved	ID85

Bit5	reserved	ID86
Bit6	reserved	ID87
Bit7	reserved	ID88

Inverter alert message：byte1

bit	Error Message	ID code(detailed)
Bit0	reserved	reserved
Bit1	reserved	reserved
Bit2	reserved	reserved
Bit3	reserved	reserved
Bit4	reserved	reserved
Bit5	reserved	reserved
Bit6	reserved	reserved
Bit7	reserved	reserved

Communication board inner message：byte0

bit	Error Message	ID code(detailed)
Bit0	Fan1 alarm	ID91 Fan1 alarm
Bit1	Fan2 alarm	ID92 Fan2 alarm
Bit2	Lightning protection alarm	ID93 Lightning protection alarm
Bit3	Software version is not consistent	ID94 Software version is not consistent
Bit4	Communication board EEPROM fault	ID95 The communication board EEPROM is fault
Bit5	RTCFatult	ID96 RTC clock chip is fault
Bit6	InValidCountry	ID97 The country is invalid
Bit7	SDfault	ID98 The SD card is fault

Communication board inner message：byte1

bit	Error Message	ID code(detailed)
Bit0	Fan3 alarm	ID90 Fan3 alarm
Bit1	reserved	reserved
Bit2	reserved	reserved
Bit3	reserved	reserved
Bit4	reserved	reserved
Bit5	reserved	reserved
Bit6	reserved	reserved
Bit7	reserved	reserved

Inverter Data Address table

Address	Define	Variable type	length	range	Default value	Remarks
0x0000	Operating state	Uint	16			Only Low-Byte

						availability
0x0001	Fault1	Uint	16			High-Byte:byte1 Low-Byte:byte0
0x0002	Fault2	Uint	16			High-Byte:byte3 Low-Byte:byte2
0x0003	Fault3	Uint	16			High-Byte:byte5 Low-Byte:byte4
0x0004	Fault4	Uint	16			High-Byte:byte7 Low-Byte:byte6
0x0005	Fault5	Uint	16			High-Byte:byte9 Low-Byte:byte8

PV Input Message						
Address	Define	Variable type	Length	range	Default value	Remarks
0x0006	PV1 voltage	Uint	16	0-1000V		Unit:0.1V
0x0007	PV1 current	int	16	0-100A		Unit:0.01A
0x0008	PV2 voltage	Uint	16	0-1000V		Unit:0.1V
0x0009	PV2 current	int	16	0-100A		Unit:0.01A
0x000A	PV1 power	Uint	16	0-100kw		Unit:0.01kw
0x000B	PV2 power	Uint	16	0-100kw		Unit:0.01kw

Output Grid Message						
Address	Define	Variable type	length	range	Default value	Remarks
0x000C	Output active power	Uint	16			Unit:0.01kW
0x000D	Output reactive power	int	16			Unit:0.01kVar
0x000E	Grid frequency	Uint	16			Unit:0.01Hz
0x000F	A-phase voltage	Uint	16			Unit:0.1V
0x0010	A-phase current	Uint	16			Unit:0.01A
0x0011	B-phase voltage	Uint	16			Unit:0.1V
0x0012	B-phase current	Uint	16			Unit:0.01A
0x0013	C-phase voltage	Uint	16			Unit:0.1V
0x0014	C-phase current	Uint	16			Unit:0.01A

Inverter Generation message						
Address	Define	Variable type	Length	range	Default value	Remarks
0x0015	Total production high-byte	Uint	16	0-65536		Unit:1kWh
0x0016	Total production	Uint	16	0-		

	low-byte			65536		
0x0017	Total generation time high-byte	Uint	16	0-65536		Unit:1 hour
0x0018	Total generation time low-byte	Uint	16	0-65536		
0x0019	Today production	Uint	16	0-1000V		Unit:0.01kWh
0x001A	Today generation time	Uint	16	0-65536		Unit:1 Minute

Inverter inner message

Address	Define	Variable type	Length	Range	Default value	Remarks
0x001B	Inverter module temperature	int	16			
0x001C	Inverter inner temperature	int	16			
0x001D	Inverter Bus voltage	Uint	16	0-1000V		Unit:0.1V
0x001E	PV1 voltage sample by slave CPU	Uint	16	0-1000V		Unit:0.1V
0x001F	PV1 current sample by slave CPU	Uint	16	0-100A		Unit:0.01A
0x0020	Count-down time	Uint	16			
0x0021	Inverter alert message	Uint	16			
0x0022	Input mode	Uint	16			0x00: in parallal 0x01: in dependent
0x0023	Communication board inner message	Uint	16			
0x0024	Insulation of PV1+ to ground					
0x0025	Insulation of PV1+ to ground					
0x0026	Insulation of PV - to ground					
0x0027	Country					

3.1.3 Read built-in combiner data address table

Address table

Alarm table

Byte0

bit	Description	Remarks
Bit0		PV11 over voltage alarm
Bit1		PV12 over voltage alarm
Bit2		PV13 over voltage alarm
Bit3		PV14 over voltage alarm
Bit4		reserved
Bit5		reserved
Bit6		reserved
Bit7		reserved

Byte1

bit	Description	Remarks
Bit0		PV21 over voltage alarm
Bit1		PV22 over voltage alarm
Bit2		PV23 over voltage alarm
Bit3		PV24 over alarm voltage
Bit4		reserved
Bit5		reserved
Bit6		reserved
Bit7		reserved

Byte2

bit	Description	Remarks
Bit0		PV11 under voltage alarm
Bit1		PV12 under voltage alarm
Bit2		PV13 under voltage alarm
Bit3		PV14 under voltage alarm
Bit4		reserved
Bit5		reserved
Bit6		reserved
Bit7		reserved

Byte3

bit 位	Description	Remarks
Bit0		PV21 under voltage alarm

Bit1		PV22 under voltage alarm
Bit2		PV23 under voltage alarm
Bit3		PV24 under voltage alarm
Bit4		reserved
Bit5		reserved
Bit6		reserved
Bit7		reserved

Byte4

bit 位	Description	Remarks
Bit0		PV11 Reflux alarm
Bit1		PV12 reflux alarm
Bit2		PV13 reflux alarm
Bit3		PV14 reflux alarm
Bit4		reserved
Bit5		reserved
Bit6		reserved
Bit7		reserved

Byte5

bit 位	Description	Remarks
Bit0		PV21 reflux alarm
Bit1		PV22 reflux alarm
Bit2		PV23 reflux alarm
Bit3		PV24 reflux alarm
Bit4		reserved
Bit5		reserved
Bit6		reserved
Bit7		reserved

Byte6

bit 位	Description	Remarks
Bit0		PV11 over current alarm
Bit1		PV12 over current alarm
Bit2		PV13 over current alarm
Bit3		PV14 over current alarm
Bit4		reserved
Bit5		reserved
Bit6		reserved
Bit7		reserved

Byte7

bit 位	Description	Remarks
Bit0		PV21 over current alarm
Bit1		PV22 over current alarm

Bit2		PV23 over current alarm
Bit3		PV24 over current alarm
Bit4		reserved
Bit5		reserved
Bit6		reserved
Bit7		reserved

Byte8

bit 位	Description	Remarks
Bit0		PV11 Fuse alarm
Bit1		PV12 Fuse alarm
Bit2		PV13 Fuse alarm
Bit3		PV14 Fuse alarm
Bit4		reserved
Bit5		reserved
Bit6		reserved
Bit7		reserved

Byte9

bit 位	Description	Remarks
Bit0		PV21 Fuse alarm
Bit1		PV22 Fuse alarm
Bit2		PV23 Fuse alarm
Bit3		PV24 Fuse alarm
Bit4		reserved
Bit5		reserved
Bit6		reserved
Bit7		reserved

Address table of combiner data

Address	Define	Variable type	Length	Range	Default value	Remarks
0x0100	Alarm message table1	Uint	16			High-byte:byte1 Low-byte:byte0
0x0101	Alarm message table2	Uint	16			High-byte:byte3 Low-byte:byte2
0x0102	Alarm message table3	Uint	16			High-byte:byte5 Low-byte:byte4
0x0103	Alarm message table4	Uint	16			High-byte:byte7 Low-byte:byte6
0x0104	Alarm message table5	Uint	16			High-byte:byte9 Low-byte:byte8
DC input message						

Address	Define	Variable type	Length	Range	Default value	Remarks
0x0105	String 1 voltage	Uint	16	0-1000V		Unit:0.1V
0x0106	String 1 current	int	16	0-100A		Unit:0.01A
0x0107	String 2 voltage	Uint	16	0-1000V		Unit:0.1V
0x0108	String 2 current	int	16	0-100A		Unit:0.01A
0x0109	String 3 voltage	Uint	16	0-1000V		Unit:0.1V
0x010A	String 3 current	int	16	0-100A		Unit:0.01A
0x010B	String 4 voltage	Uint	16	0-1000V		Unit:0.1V
0x010C	String 4 current	int	16	0-100A		Unit:0.01A
0x010D	String 5 voltage	Uint	16	0-1000V		Unit:0.1V
0x010E	String 5 current	int	16	0-100A		Unit:0.01A
0x010F	String 6 voltage	Uint	16	0-1000V		Unit:0.1V
0x0110	String 6 current	int	16	0-100A		Unit:0.01A
0x0111	String 7 voltage	Uint	16	0-1000V		Unit:0.1V
0x0112	String 7 current	int	16	0-100A		Unit:0.01A
0x0113	String 8 voltage	Uint	16	0-1000V		Unit:0.1V
0x0114	String 8 current	int	16	0-100A		Unit:0.01A
0x0115 to 0x011F	reserved					

3.2 Read product information（Function Code 0x04）

3.2.1 Read data format

By function code 0x04,query data message of every allowable register,command format as below:

Host station request message format:

Slave address	Function code	Starting Address	Number of Registers	CRC16
1 byte	1 byte	2 bytes	2 bytes	2 bytes
0xxx	0x04	Hi Byte Lo Byte	Hi Byte Lo Byte	Lo Byte Hi Byte

Slave station request message format:

Slave Addres	Function code	Byte Count	Register-1 value	。。。	Register-N value	CRC16
1byte	1byte	1byte	1byte	N-2	1byte	1byte
Byte	Byte	Byte	Hi Byte Lo Byte	。。。	Hi Byte Lo Byte	Lo Byte Hi Byte

3.2.2 Address table of read inverter's manufacturer message

Inverter's Manufacturer message						
Address	define	Variable type	length	range	Default value	Remarks
0x2000	Product code					0：5KW 1：6KW 2：8KW 3：10KW 4：12KW 5：15KW 6：17KW 7：20KW 8：25KW 9：30KW
0x2001 to 0x2007	Manufacturer serial number					
0x2008 to 0x2009	Software version code					
0x200A to 0x200B	Hardware version code					
0x200C to 0x200F	reserved					

Serial number definition table:

ID	Value	Remarks
1	'S'	sofar,other value represent OEM product
2-3	"A1"or "B1"or "C1"or "D1"	A1 (1-3K) ，B1（3-5K），C1（10-20K),D1(30-43K)
4	E/C	E（English），C(Chinese)
5-6	"S0"or"S1"or"S2"or""S3"or"S4"or"S5"or"S6"	Configure message
7-8	10/30/50/06/08/10/12/15/17/20/25/30	//If bit2、bit3 is A1 (1-3K)，10

		represent 1000W
		//If bit2、bit3 is B1 (3-5K) 30 represent 3000W
		//If bit2、bit3 is C1 (10-20K) represent 20000W
		//If bit2、bit3 is D1(30-40K) represent 30000W

9	year	00 year (0) 01 year (1) 02 year (2) 03 year (3) 04 year (4) 05 year (5) 06 year (6) 07 year (7) 08 year (8) 09 year (9) 10 year (A) 11 year (B) 12 year (C) 13 year (D) 14 year (E) 15 year (F) 16 year (G) 17 year (H) 18 year (I) 19 year (J) 20 year (K) 21 year (L) 22 year (M) 23 year (N) 24 year (O) 25 year (P) 26 year (Q) 27 year (R) 28 year (S) 29 year (T) 30 year (U) 31 year (V) 32 year (W) 33 year (X) 34 year (Y) 35 year (Z)
10	month	1 month (1) 2 month (2) 3 month (3) 4 month (4) 5 month (5) 6 month (6) 7 month (7) 8 month (8) 9 month (9) 10 month (A) 11 month (B) 12 month (C)
11	day	1date (1) 2 date (2) 3 date (3) 4 date (4) 5 date (5) 6 date (6) 7 date (7) 8 date (8) 9 date (9) 10 date (A) 11 date (B) 12 date (C) 13date (D) 14 date (E) 15 date (F) 16 date (G) 17 date (H) 18 date (I) 19 date (J) 20 date (K) 21 date (L) 22 date (M) 23 date (N) 24 date (O) 25 date (P) 26 date (Q) 27 date (R) 28 date (S) 29 date (T) 30 date (U) 31

		date（V）
12-14	xxx	001（the number of production）

Example

1. Get the real-time data(function code 0x03)

AP Request:

01 03 00 00 00 24 45 D1

Inverter response:

01 03 48 00 02 00 00 00 00 00 00 00 00 00 00 08 D5 01 A0 00 41 00 00 00 5E 00 00 00 59 00 00 13 87 09 05 01 85 00 00 00 00 00 00 00 00 00 00 00 8A 00 00 00 22 00 04 00 02 00 1C 00 26 0E 52 08 D5 00 41 00 1E 00 00 00 01 00 00 4E F2

The Operating state is:0x02(Normal)

2. Get the product information(function code 0x04)

AP Request:

01 04 20 00 00 10 FA 06

Inverter response:

01 04 20 00 02 53 42 31 45 53 30 34 30 45 38 47 30 31 34 56 31 37 30 56 31 30 30 00 00 00 00 00 00 00 00 5A BB

SN：SB1ES040E8G014

Software Version：V1.70

Hardware Version：V1.00