CanadianSolar

2024

RS485 MODBUS Protocol

MANUAL – CSI SOLAR BRASIL

CSI Solar Co., Ltd.
199 Lushan Road, SND, Suzhou, Jiangsu, China, 215129, www.csisolar.com, support@csisolar.com

Contents

Tables

1. Purpose

This protocol was developed to implement data exchange between the Inverter, WIFI / GPRS collector. The protocol format is Modbus protocol.

2. Communication parameters

Physical interface: RS485
Data Bit: 8
Parity Checking Bit: None Stop
Bit：1
Baud Rate：9600
All the data formats follow the rule, which is high-bits first and low-bits last.

3. Teams Explanation

Host Computer/Collector	Modbus Host
Device/Inverter	Modbus Slave
Broadcast address	0x00
Register address	Register address corresponds to a 2-byte message
U16	UInt16
S16	Signed Int16
U32	UInt32
S32	Signed Int32
ASCii	String，use ASCii code

Table 1 - Teams Explanation

4. Communication Format

4.1 Read register command:

Request format	Device address (1Byte)	Function code (1Byte)	Start address (2 Bytes)	Register number (2 Bytes)	CRC16 (2 Bytes)
Response format	Device address (1Byte)	Function code (1Byte)	Byte number (1Byte)	Data field (N Bytes)	CRC16 (2 Bytes)

Table 2 – Register Command

4.2 Write one register command:

Request format	Device address (1Byte)	Function code (1Byte)	Register address (2 Bytes)	Data field (2 Bytes)	CRC16 (2 Bytes)
Response format	Device address (1Byte)	Function code (1Byte)	Register address (2 Bytes)	Data field (2 Bytes)	CRC16 (2 Bytes)

Table 3 - One register command

4.3 Write more than one registers command:

Request format	Device address (1Byte)	Function code (1Byte)	Start address (2 Bytes)	Register number (2 Bytes)	Byte number (1 Byte)	Data field (N Bytes)	CRC16 (2 Bytes)
Response format	Device address (1Byte)	Function code (1Byte)	Start address (2 Bytes)			Register number (2 Bytes)	CRC16 (2 Bytes)

Table 4 - More than one registers command

Note：
a. All data is hexadecimal format;
b. Register address range is 1~100；
c. Function code

Function code （Hex）	Description	Address Range (Decimal)	Unit	Single/Muti	Comments
01H	Read coil	1000~1999	Bit	Muti	Currently only supports one-time full read, the command is：01 01 03 E8 00 40 BD 8A
03H	Read hold register	2000~2999	One register	Single/Muti	
04H	Read input register	3000~4999	One register	Single/Muti	
05H	Write one coil	1000~1999	Bit	Single	
06H	Write one hold register	2000~2499	One register	Single	
10H	Write more than one hold register	2500~2999	One register	Muti	

Table 5 - Function code

5. Device register

5.1 Description

When the communication address is 0, it is a broadcast instruction.
Each device of the subnet must report the current device sub-address (the default is 0x64) and SN. Then the host device will assign a communication address to each device based on the received device SN. To ensure that the communication addresses of the devices in the subnet are unique one, the steps are as follows:

5.1.1 Offline register:

The host device sends a broadcast instruction to receive the SN and communication address of each device in the subnet;

Request format	Device address (1Byte)	Function code (1Byte)	Start address (2 Bytes)	Register number (2 Bytes)		CRC16 (2 Bytes)
Example	0x00	0x03	0x09 0xC4	0x00 0x01		
Response format	Device address (1Byte)	Function code (1Byte)	Byte number (1 Byte)	Sub device SN (16 Bytes)	Sub device current sub address （2Bytes）	CRC16 (2 Bytes)
Example	0x64	0x03	0x12	0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10 0x11 0x12 0x13 0x14 0x15 0x16	0x00 0x64	

Table 6 - Offline registe

5.2.2 Address allocation:

The host device assigns a unique communication address to each device in the subnet through broadcast instructions, and the sub-device recognizes and sets its own sub-address through the SN.

Request format	Device address (1Byte)	Function code (1Byte)	Start address (2 Bytes)	Sub device SN (16 Bytes)	Sub device current sub address （2Bytes）	CRC16 (2 Bytes)
Example	0x00	0x06	0x09 0xC4	0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10 0x11 0x12 0x13 0x14 0x15 0x16	0x00 0x02	
Response format	Device address (1Byte)	Function code (1Byte)	Byte number (1 Byte)	Sub device SN (16 Bytes)	Sub device current sub address （2Bytes）	CRC16 (2 Bytes)
Example	0x02	0x06	0x12	0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10 0x11 0x12 0x13 0x14 0x15 0x16	0x00 0x02	

Table 7 - Address allocation

5.2 Logout:

The computer host can remove a device from the communication network and restore its address to the default value

Request format	Device address (1Byte)	Function code (1Byte)	Start address (2 Bytes)	Sub device SN (16 Bytes)	Sub device current sub address （2Bytes）	CRC16 (2 Bytes)
Example	0x02	0x06	0x09 0xC4	0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10 0x11 0x12 0x13 0x14 0x15 0x16	0x00 0x64	
Response format	Device address (1Byte)	Function code (1Byte)	Byte number (1 Byte)	Sub device SN (16 Bytes)	Sub device current sub address （2Bytes）	CRC16 (2 Bytes)
Example	0x64	0x06	0x12	0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10 0x11 0x12 0x13 0x14 0x15 0x16	0x00 0x64	

Table 8 - Logout

6. Wireless Communication

TBD

7. Register Address Definition

7.1 Address definition of Real-time data (Input registers)

Real time data

Address	Name	Data Type	Unit	Open Level	Limits
3000	Protocol No.	U16	x0.01	Monitoring system	
3001	Protocol Version	U16	x0.01	Monitoring system	
3002	Inverter Model (MODEL)1	U16	ASCii	Monitoring system	
3003	Inverter Model (MODEL)2	U16	ASCii	Monitoring system	
3004	Inverter Model (MODEL)3	U16	ASCii	Monitoring system	
3005	Inverter Model (MODEL)4	U16	ASCii	Monitoring system	
3006	Inverter Model (MODEL)5	U16	ASCii	Monitoring system	
3007	Inverter Model (MODEL)6	U16	ASCii	Monitoring system	
3008	Inverter Model (MODEL)7	U16	ASCii	Monitoring system	
3009	Inverter Model (MODEL)8	U16	ASCii	Monitoring system	

3010	Serial number 1	U16	ASCii	Monitoring system	
3011	Serial number 2	U16	ASCii	Monitoring system	
3012	Serial number 3	U16	ASCii	Monitoring system	
3013	Serial number 4	U16	ASCii	Monitoring system	
3014	Serial number 5	U16	ASCii	Monitoring system	
3015	Serial number 6	U16	ASCii	Monitoring system	
3016	Serial number 7	U16	ASCii	Monitoring system	
3017	Serial number 8	U16	ASCii	Monitoring system	
3018	Hardware version	U16	x0.01	Monitoring system	
3019	ARM boot version	U16	x0.01		
3020	ARM version	U16	x0.01		
3021	DSP boot version	U16	x0.01		
3022	DSP version	U16	x0.01		
3023	Safety standard	U16	x1	Monitoring system	
3024	Package of safety standard, version 1	U16	x1		
3025	Package of safety standard, version 2	U16	x1		
3026					
3027					
3028					
3029					
3030					
3031					
3032	Software SN 1	U16	x0.01	Monitoring system	
3033	Software SN 2	U16	x0.01	Monitoring system	
3034	Device Time: Year	U16		Monitoring system	
3035	Device Time: Month	U16		Monitoring system	
3036	Device Time: Day	U16		Monitoring system	
3037	Device Time: Hour	U16		Monitoring system	
3038	Device Time: Minute	U16		Monitoring system	
3039	Device Time: Second	U16		Monitoring system	
3040	Device type number	U16			
3041	Rated output power	U16	x1W	Monitoring system	
3042	Output type	U16	x1	Monitoring system	
3043	PV Input type	U16	x1	Monitoring system	0-NotConnect 1-Panel1Only 2-Panel2Only 3-DiffPanel 4-SamePanel
3044					
3045	Today's electric energy production-high	U16	x0.1kWh	Monitoring system	

3046	Today's electric energy production-low	U16		Monitoring system	
3047	Total electric energy production-high	U16	x0.1kWh	Monitoring system	
3048	Total electric energy production-low	U16		Monitoring system	
3049	Total run time-high	U16		Monitoring system	
3050	Total run time-low	U16	x1h	Monitoring system	
3051					
3052	PV1 input voltage	U16	x0.1V	Monitoring system	
3053	PV1 input current	U16	x0.01A	Monitoring system	
3054	PV1 input power	U16	x1W	Monitoring system	
3055	PV2 input voltage	U16	x0.1V	Monitoring system	
3056	PV2 input current	U16	x0.01A	Monitoring system	
3057	PV2 input power	U16	x1W	Monitoring system	
3058					
3059					
3060					
3061					
3062					
3063					
3064					
3065	Total DC power-high	U16	x1W		
3066	Total DC power-low	U16	x1W		
3067	Voltage (Phase A)	U16	x0.1V	Monitoring system	
3068	Voltage (Phase B)	U16	x0.1V		
3069	Voltage (Phase C)	U16	x0.1V		
3070	Current (Phase A)	U16	x0.01A	Monitoring system	
3071	Current (Phase B)	U16	x0.01A		
3072	Current (Phase C)	U16	x0.01A		
3073					
3074	Active power (Phase A)	U16	x1W	Monitoring system	
3075	Active power (Phase B)	U16	x1W		
3076	Active power (Phase C)	U16	x1W		
3077	Total active power-high	U16	x1W		
3078	Total active power-low	U16			
3079	Total reactive power-high	S16	x1var	Monitoring system	
3080	Total reactive power-low	S16		Monitoring system	
3081	Apparent power-high	U16	x1VA	Monitoring system	
3082	Apparent power-low	U16		Monitoring system	
3083	Power factor	S16	x0.001	Monitoring system	
3084	Grid frequency	U16	x0.01Hz	Monitoring system	
3085					

3086	IGBT temperature	S16	x0.1℃	Monitoring system	
3087	Inverter temperature	S16	x0.1℃	Monitoring system	
3088	Insulation resistance	U16	x1kOhm	Monitoring system	
3089	Inverter countdown time	U16	x1s	Monitoring system	
3090	System state	U16	x1	Monitoring system	0: Waiting 1: Normal 2: Fault 3: 4: Flashing 5: Checking
3091	EPM Flag	U16	x1	Monitoring system	0: No limit 1: Limit
3092					
3093					
3094					
3095	Validity of date	U16			
3096					
3097	Inverter fault-high	U16		Monitoring system	
3098	Inverter fault-low	U16		Monitoring system	
3099	Inverter alarm-high	U16		Monitoring system	
3100	Inverter alarm-low	U16		Monitoring system	
3101	History fault-high	U16			
3102	History fault-low	U16			
3103	History warning-high	U16			
3104	History warning-low	U16			
3105					
3106					
3107					
3108					
3109					
3110					
3111					
3112					
3113					
3114					
3115					
3116					
3117					
3118					
3119					
3120					
3121					
3122					

3123					
3124					
3125					
3126					
3127					
3128					
3129					
3130					
3131					
3132					
3133					
3134					
3135					
3136					
3137					
3138					
3139					
3140					
3141					
3142					
3143					
3144					
3145					
3146					
3147					
3148					
3149					
3150					
3151					
3152					
3153					
3154					
3155					
3156					
3157					
3158					
3159					
3160	BUS Voltage	U16	x0.1V	Monitoring system	
3161	Boost1 State	U16	x1		
3162	Boost2 State	U16	x1		
3163	Output power limit flag	U16	x1		
3164	CT Current	S16	x0.01A	Monitoring system	

3165	CT Power	S16	x1W	Monitoring system	
3166	IODC Current (DCI)	S16	x1mA		
3167	Leakage current effective value (GFCI)	S16	x1mA		
3168	Insulation voltage	S16	x0.1V		
3169					
3170					
3171	Package of safety standard, standard 1	U16	N/A		
3172	Package of safety standard, standard 2	U16	N/A		
3173	Package of safety standard, standard 3	U16	N/A		
3174	Package of safety standard, standard 4	U16	N/A		
3175	Frequency（ARM）	U16	x0.01Hz	—	
3176	GFCI RMS ARM）	S16	x1mA		
3177	Grid voltage RMS (ARM)	U16	x0.1V		
3178	Frequency（DSP）	U16	x0.01Hz		
3179	GFCI RMS（DSP）	S16	x1mA		
3180	Grid voltage RMS (DSP)	U16	x0.1V		
3181	Meter Voltage	U16	x0.1V	Monitoring system	
3182	Meter Current	U16	x0.01A	Monitoring system	
3183	Meter Active power	S16	x1W	Monitoring system	
3184	Meter reactive power	S16	x1Var	Monitoring system	
3185	Meter apparent power	U16	x1VA	Monitoring system	
3186	Meter power factor	U16	x0.001	Monitoring system	
3187	Meter frequency	U16	x0.01Hz	Monitoring system	
3188	Meter total energy-high	U16	x0.01kWh	Monitoring system	
3189	Meter total energy-low	U16	x0.01kWh	Monitoring system	
3190	Meter total reverse energy-high	U16	x0.01kWh	Monitoring system	
3191	Meter total reverse energy-low	U16	x0.01kWh	Monitoring system	
3192					

Table 9 - Address definition of Real-time data (Input registers)

7.2 Remote Control Instructions (Coil)

When writing the coil, 1 means FF00 and 0 means 0000

When reading the coil, the instruction is represented by 1 and 0.

At present, the inverter can only support reading all coils at one time, does not support reading a single coil.

Location	Name	Data type	Unit	Open Level	Limit
1000	System shutdown and startup	Bit	N/A	Monitoring system	FF00：Shutdown 0000：Startup

Table 10 - Remote Control Instructions (Coil)