KEHUA TECH

Three-phase String PV Grid-tied Inverter

Monitor Protocol V1.0

Trademarks and Permissions


and other Kehua trademarks are trademarks of Kehua Data Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Kehua and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specification in the contract, all statements, information, and recommendations in this document are provided “AS IS” without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

KEHUA DATA CO.,LTD.

Address:	No.457,MalongRoad,TorchHigh-TechIndustrialZone,Xiamen,Fujian,China
Website:	www.kehua.com
E-mail:	service@kehua.com
Customer Service Telephone:	400-808-9986
Tel:	0592-5160516
Fax:	0592-5162166

Contents

1 Overview

1.1 Protocol Intro

This document introduces the monitor protocol connected via RS485, Ethernet port of string PV grid-tied inverter. The protocol complies with standard Modbus specification. The version of the monitor protocol is V2.0.

1.2 Scope of Application

This protocol is applicable to following models.

- Three-phase String PV Grid-tied Inverter

Related Terms and Description

Name	Description
Host	The part that initiatively start to communicate.
Slave	The part that passively respond the command.
UINT16	Unsigned integer of 16 bit. High byte front, low byte behind.
UINT32	Unsigned integer of 32 bit. High byte front, low byte behind.
INT16	Signed integer of 16 bit. High byte front, low byte behind.
INT32	Signed integer of 32 bit. High byte front, low byte behind.
String	Character string that every byte marked by ASCII.
MLB	Multibyte
Bitfield16	The data that with 16 byte width and shows by bit. High byte front, low byte behind.
RW	The register can be read and written.

Name	Description
RO	The register that can be read only.

1.3 Communication Configuration

This protocol is suitable for RS485 and Ethernet etc communication mode.

1.3.1 Communication Configuration of RS485 Port

Name	Description
Baud rate	Default is 9600bps, and it can be set to 2400bps, 4800bps,
Start bite	1bit
Data bit	8bits
Check bit	None
Stop bit	1bit
Frame interval	Not less than the transmission time of 3.5 bytes
Intra-frame character interval	Not larger than the transmission time of 1.5 bytes
Max. frame length	200 bytes
Max. response time of the slave	The transmission time of 150 bytes
Min. polling interval of the host	The transmission time of 200 bytes

1.3.2 Communication Configuration of Ethernet Port

Name	Description
Transmission mode	TCP/IP
Baud rate	10M/100M
Port ID	502
Max. response time of the slave	100ms
Min. polling interval of the host	100ms

Name	Description
IP	Default: 192.168.1.10
Subnet mask	Default: 255.255.255.0
Gateway	Default: 192.168.1.1

2 Register Definition

2.1 Read Discrete Inputs

Function Code: 0x02

2.1.1 Standard status

- Inverter fault information:

Address (decimalism)	Meaning	Remark	Suitable device
2501	Grid voltage abnormal	0-Normal 1-Abnormal	
2502	Grid frequency abnormal	0-Normal 1-Abnormal	
2503	Grid phase sequence abnormal	0-Normal 1-Abnormal	
2504	Output current abnormal	0-Normal 1-Abnormal	
2505	Reserved	0-Normal 1-Abnormal	
2506	Hardware fault	0-Normal 1-Abnormal	
2507	DC component abnormal	0-Normal 1-Abnormal	
2508	AC SPD abnormal	0-Normal 1-Abnormal	
2509	Leakage current abnormal	0-Normal 1-Abnormal	
2510	AC Relay fault	0-Normal 1-Abnormal	
2511	Reduction alarm	0-Normal 1-Abnormal	
2512	Reserved	0-Normal 1-Abnormal	
2513	Heatsink over-temperature	0-Normal 1-Abnormal	
2514	Inverter amplitude abnormal	0-Normal 1-Abnormal	
2515	Reserved	0-Normal 1-Abnormal	
2516	Wait for triggering signal for recover grid-connected	0-Normal 1-Abnormal	
2517	Insulation fault	0-Normal 1-Abnormal	
2518	PV input over-voltage (total)	0-Normal 1-Abnormal	
2519	Power module over-temperature	0-Normal 1-Abnormal	
2520	Inner communication fault	0-Normal 1-Abnormal	

Address (decimalism)	Meaning	Remark	Suitable device
2521	Bus over-voltage	0-Normal 1-Abnormal	
2522	Boost over-current (total)	0-Normal 1-Abnormal	
2523	Temperature switch protection	0-Normal 1-Abnormal	
2524	Fan fault	0-Normal 1-Abnormal	
2525	Initialization fault	0-Normal 1-Abnormal	
2526	DC SPD abnormal	0-Normal 1-Abnormal	
2527	Inner over-temperature	0-Normal 1-Abnormal	
2528	Temperature low	0-Normal 1-Abnormal	
2529	External CT fault	0-Normal 1-Abnormal	
2530	Smart meter abnormal	0-Normal 1-Abnormal	
2531	Probation expired	0-Normal 1-Abnormal	
2532	Probation approching	0-Normal 1-Abnormal	
2533	HMI communication fault	0-Normal 1-Abnormal	
2534-2535	Reserved	0-Normal 1-Abnormal	
2536	Arc communication fault	0-Normal 1-Abnorma	
2537	Meter communication fault	0-Normal 1-Abnorma	
2538-2564	Reserved	0-Normal 1-Abnormal	

- Battery fault information:

Address (decimalism)	Meaning	Remark	Suitable device
2565	Battery over-voltage alarm	0-Normal 1-Abnormal	Energy storage device
2566	Battery low-voltage alarm	0-Normal 1-Abnormal	
2567	Battery over-voltage protection	0-Normal 1-Abnormal	
2568	Battery low-voltage protection	0-Normal 1-Abnormal	
2569	Battery over-temperature	0-Normal 1-Abnormal	
2570	Battery low-temperature	0-Normal 1-Abnormal	
2571	Battery charge over-current	0-Normal 1-Abnormal	
2572	Battery discharge over-current	0-Normal 1-Abnormal	
2573	Battery BMS communication abnormal	0-Normal 1-Abnormal	
2574-2596	Reserved for battery fault	0-Normal 1-Abnormal	

- Load fault information:

Address (decimalism)	Meaning	Remark	Suitable device
2597	Overload alarm	0-Normal 1-Abnormal	Energy storage device
2598	Overload protection	0-Normal 1-Abnormal	
2599	Short-circuit protection	0-Normal 1-Abnormal	
2600-2628	Reserved for load fault		

- PV fault inforamtion:

Address (decimalism)	Meaning	Remark	Suitable device
2629-2636	MPPT1 over-voltage -MPPT8 over-voltage (low address corresponds MPPT1)	0-Normal 1-Abnormal	
2637-2644	MPPT1 over-current -MPPT8 over-current (low address corresponds MPPT1)	0-Normal 1-Abnormal	
2645-2652	MPPT1 reverse connected -MPPT8 reverse connected (low address corresponds MPPT1)	0-Normal 1-Abnormal	
2653-2660	MPPT1 insulation fault-MPPT8 insulation fault (low address corresponds MPPT1)	0-Normal 1-Abnormal	
2661-2668	MPPT1 over-temperature - MPPT8 over-temperature (low address corresponds MPPT1)	0-Normal 1-Abnormal	
2669-2676	MPPT1 DC arc fault -MPPT8 DC arc fault (low address corresponds MPPT1)	0-Normal 1-Abnormal	
2677-2692	Reserved for MPPT fault	0-Normal 1-Abnormal	
2693-2724	PV1 over-current- PV32 over-current (low address corresponds PV1)	0-Normal 1-Abnormal	
2725-2756	PV1 reverse connected-PV32 reverse connected (low address corresponds PV1)	0-Normal 1-Abnormal	
2757-2820	Reserved for PV fault	0-Normal 1-Abnormal	

- Other discrete value information:

Address (decimalism)	Meaning	Remark
2821	Device lock status	0-Normal 1-Locked
2822	Probation status	0-Out of probation; 1-Probation
2823-2852	Reserved	

2.1.2 Expansion status

None

2.1.3 Inner status

None

2.2 Read input registers (analog quantity)

Function Code: 0x04

For the data of dobule word (32bit) or more, it will send high word and then send low word.

2.2.1 Standard analog quantity

- Inverter analog quantity information

Address (decimalism)	Meaning	Byte	Data type	Remark (unit)	Suitable device
4501	Device status	2	UINT16	0-standby 1-grid-connected 2-fault 3-power-off 4-off-grid 5- reduction due to device 6-reduction due to user	
4502-4505	Reserved	8	UINT16		Inverter Information
4506	Daily energy	2	UINT16	0.1kWh	
4507-4508	Total energy	4	UINT16	0.1kWh	
4509	Reserved	2	UINT16		
4510	Reserved	2	UINT16		
4511	Grid frequency	2	UINT16	0.01Hz	
4512	U-phase/UV grid voltage	2	UINT16	0.1V	
4513	V-phase/VW grid voltage	2	UINT16	0.1V	
4514	W-phase/WU grid voltage	2	UINT16	0.1V	
4515	U-phase grid current	2	UINT16	0.1A	
4516	V-phase grid current	2	UINT16	0.1A	
4517	W-phase grid current	2	UINT16	0.1A	
4518	Grid-connected total active power	2	INT16	0.1kW	
4519	Grid-connected total reactive power	2	INT16	0.1kVar	
4520	Heatsink temperature	2	INT16	0.1℃	

Address (decimalism)	Meaning	Byte	Data type	Remark (unit)	Suitable device
4521	Inner temperature	2	INT16	0.1℃	
4522	Grid-connected total apparent power	2	UINT16	0.1kVA	
4523	IGBT temperature	2	INT16	0.1℃	
4524	Reserved	2	UINT16		
4525	Reserved	2	UINT16		
4526	Output power factor	2	INT16	0.01	
4527	PV input total power	2	UINT16	0.1kw	
4528	AC leakage current	2	UINT16	0.1mA	
4529	Daily power consumption	2	UINT16		Energy storage device
4530-4531	Total power consumption	4	UINT16		Energy storage device
4532	On-grid active power	2	INT16	0.1kW	On-Gride Information
4533	On-grid apparent power	2	INT16	0.1kVA	
4534	On-grid reactive power	2	INT16	0.1kVar	
4535	On-grid Power factor	2	INT16	0.01	
4536-4550	Reserved		UINT16		

- Battery analog quantity information

Address (decimalism)	Meaning	Byte	Data type	Remark (unit)	Suitable device
4551	Battery status	2	UINT16	0-idle; 1-charge; 2-discharge; 3-abnormal	Energy storage device
4552	Batery voltage	2	UINT16	0.1V	
4553	Batery current	2	INT16	0.1A, singned number	
4554	Batery power	2	INT16	0.1kw , singned number	
4555	Batery max. temperature	2	INT16	0.1℃, singned number	
4556	Batery min. temperature	2	INT16	0.1℃, singned number	
4557	Cell's max voltage	2	UINT16	0.001V	
4558	Cell's min voltage	2	UINT16	0.001V	
4559	Batery capacity	2	UINT16	0.1%	
4560	Battery daily charge	2	UINT16	0.1Kwh	

Address (decimalism)	Meaning	Byte	Data type	Remark (unit)	Suitable device
	capacity				
4561	Battery daily discharge capacity	2	UINT16	0.1Kwh	
4562-4600	Battery related information, reserved	76	UINT16		

- Load analog quantity information

Address (decimalism)	Meaning	Byte	Data type	Remark (unit)	Suitable device
4601	U-phase load voltage	2	UINT16	0.1V	
4602	V-phase load voltage	2	UINT16	0.1V	
4603	W-phase load voltage	2	UINT16	0.1V	
4604	U-phase load current	2	UINT16	0.1A	
4605	V-phase load current	2	UINT16	0.1A	
4606	W-phase load current	2	UINT16	0.1A	
4607	Load total active power	2	INT16	0.1kw, singned number	
4608	Load total reactive power	2	INT16	0.1kVar , singned number	
4609	Load total apparent power	2	UINT16	0.1kVA	
4610	U-phase load active power	2	INT16	0.1kW	
4611	V-phase load active power	2	INT16	0.1kW	
4612	W-phase load active power	2	INT16	0.1kW	
4613	U-phase load reactive power	2	INT16	0.1kVar	
4614	V-phase load reactive power	2	INT16	0.1kVar	
4615	W-phase load reactive power	2	INT16	0.1kVar	
4616	U-phase load apparent power	2	UINT16	0.1kVA	
4617	V-phase load apparent power	2	UINT16	0.1kVA	
4618	W-phase load apparent power	2	UINT16	0.1kVA	
4619	U-phase load power factor	2	UINT16	0.01	
4620	V-phase load power factor	2	UINT16	0.01	
4621	W-phase load power factor	2	UINT16	0.01	

Address (decimalism)	Meaning	Byte	Data type	Remark (unit)	Suitable device
4622	Load power factor	2	UINT16	0.01	
4623	Daily load power consumption	2	UINT16	0.1kwh	
4624-4625	Total load power consumption	4	UINT16	0.1kwh, low address corresds the low bit of electric auantity	
4626-4650	Load related information, reserved	48	UINT16		

- PV analog quantity information

Address (decimalism)	Meaning	Byte	Data type	Remark (unit)	Suitable device
4651	Daily PV energy	2	UINT16	0.1Kwh	
4652-4653	Total PV energy	4	UINT16	0.1Kwh	
4654	Total insulation impedance	2	UINT16	0.1kΩ	
4655-4660	Reserved	12	UINT16		
4661-4668	Voltage of MPPT1-MPPT8	2	UINT16	0.1V	
4669-4676	Current of MPPT1-MPPT8	2	INT16	0.1A singned number	
4677-4692	Reserved	32	UINT16	Parameter of MPPT1-MPPT8	
4693-4700	Reserved	16	UINT16		
4701-4732	Voltage of PV 1 -PV32	32	UINT16	0.1V 4701 corresponding to PV1	
4733-4764	Current of PV 1-PV32	32	INT16	0.1A singned number 4733 corresponding to PV1	
4765-4796	Power of PV 1-PV32	32	INT16	0.1Kw 4765 corresponding to PV1	

- Sysatem information

Address (decimalism)	Meaning	Byte	Data type	Remark (unit)	Suitable device
4800-4809	Model (ASCII)	20	UINT8	The place less than	

Address (decimalism)	Meaning	Byte	Data type	Remark (unit)	Suitable device
4810-4814	Reserved	10	UINT8	the required character is filled with zero (ASCII code literal translation)	
4815-4819	Reserved	10	UINT8		
4820	HMI version (ASCII)	10	UINT8		
4825-4834	S/N (ASCII)	20	UINT8		
4835-4839	Reserved	10	UINT8		
4840-4844	Control software 1's version (ASCII)	10	UINT8	The place less than the required character is filled with zero (ASCII code literal translation)	
4845-4849	Control software 2's version (ASCII)	10	UINT8		
4850	Device type	2	UINT16	1-Three-phase PV inverter 2- Three-phase PV energy-storage inverter	
4851	MPPT quantity	2	UINT16	MPPT branch's quantiry	
4852	Protocol type	2	UINT16	1-three-phase protocol 2-single-phase protocol 3-PID protocol	
4853-4857	Protocol version (ASCII)	10	UINT8	The place less than the 10 characters is filled with zero. For example: If the protocol version's content is V1.04, detail vaule is 56 31 2E 30 34 00 00 00 00 00, it expands from low register address to high register address. Default:V1.08	
4858-4872	Manufacturer info. (ASCII)	30	UINT8	The place less than the 30 characters is filled with zero.	
4873	PV branch's quantity	2	UINT16	Total branch quantity	
4874	Remaining probation time				

Address (decimalism)	Meaning	Byte	Data type	Remark (unit)	Suitable device
4875-4879	Control software 3's version (ASCII)	10	UINT8	The place less than the required character is filled with zero (ASCII code literal translation)	

➢ PID analog quantity information

Address (decimalism)	Meaning	Byte	Data type	Remark (unit)	Suitable device
5000	Device status	2	UINT16	0-standby 1-grid-connected 2-fault 3-power-off 4-off-grid 5- reduction due to device 6-reduction due to user	
5001	CRC16 check (manufacturer)	2	UINT16	5000 and 5002 check code. For customer, it is reserved.	
5002	Bus voltage	2	UINT16	0.1V	
5003	Reserved fault word 1	2	UINT16		
5004	Reserved fault word 2	2	UINT16		

NOTE

when useing PID module, it needs to check the list completely (that is to say, the register address 5000-5004 must be read in one frame) and the read data can be not disposed.

Reserved fault word 1

Bit address	Meaning	Remark
bit0	Grid amplitude abnormal (reserved)	0-Normal 1-Abnormal
bit1	Grid frequency abnormal (reserved)	0-Normal 1-Abnormal
bit2	Leakage current fault (reserved)	0-Normal 1-Abnormal
bit3-bit15	Reserved	Reserved

Reserved fault word 2

Bit address	Meaning	Remark
Bit0-bit15	Reserved	Reserved

2.2.2 Expansion analog quantity

None

2.2.3 Inner analog quantity

None

2.3 Read / write single coil (status quantity)

read function code: 0x01; write function code: 0x05

2.3.1 Standard swirch quantity setting

Address (decimalism)	Meaning	Byte	Remark (unit)	Suitable device
5000	ON/OFF setting	2	OFF-power off; ON-power on	
5001	Power control strategy	2	OFF-battery power control first; ON-grid control power first	Energy storage device
5002	External control mode enable	2	OFF- forbidden (inverter self-control); ON-allow (controlled by external control command)	Energy storage device
5003	Active islanding enable	2	OFF- forbidden; ON-enable	
5004	Plant mode	2	OFF-small; ON-big	
5005	Anti- PID function	2	OFF-forbidden; ON-enable	
5006	Reset	2	ON-reset	
5007	Self-start after powering on	2	OFF- forbidden; ON-enable	
5008	Clear arcing fault	2	OFF-invalid; ON-clear	
5009	Reserved			

5010	Recover grid-connected enable	2	OFF- not recover; ON-recover	
5011-5063	Reserved			

2.3.2 Expansion switch quantity setting

None

2.3.3 Innver switch quantity setting

None

2.4 Read/write single holding register (analog quantity)

read function code: 0x03, write function code: 0x06

2.4.1 Standard analog quantity setting

Address (decimalism)	Meaning	Byte	Remark (unit)	Suitable device
6000	Active power setting	2	0.1kW	
6001	ON/OFF setting	2	1- ON ; 0-OFF	
6002	Power factor	2	0.01(Negative complement in the form of complement)	
6003	Reactive power	2	0.1kVar	
6004	Grid control power	2	0.1kW +: power generation -: power consumption	Energy storage device
6005	Battery charge/discharge power	2	0.1kW +: discharge -: charge	
6006-6019	Reserved	2		
6020-6199	Occupied		Occupied by standard multiple analog quantity	

Address (decimalism)	Meaning	Byte	Remark (unit)	Suitable device
6200	Grid-teid recover time	2	1s	
6201	MPPT disturbance step	2	1V/s	
6202	Active soft start rate	2	0.01%	
6203	Max charge current	2	0.1A	Energy storage device
6204	Max sidcharge current	2	0.1A	
6205	Battery max charge power	2	1W	
6206	Battery max discharge power	2	1W	
6207-6304	Reserved			

2.4.2 Expansion analog quantity setting

Address (decimalism)	Meaning	Byte	Remark (unit)	Suitable device
6305	PV alarm shielding	2	[0x0000,0xFFFF] bit0~15: PV 1～16 0: PV alarm enable; 1: PV alarm shielding	
6306-6349	Reserved	2		

2.4.3 Energy storage battery analog quantity setting

Address (decimalism)	Meaning	Byte	Remark (unit)	Suitable device
6350	Battery type	2	[0,3] 0-Lead-acid battery; 1-lithium iron phosphate battery; 2-ternary battery; 3-lead-carbon battery	Energy storage device

Address (decimalism)	Meaning	Byte	Remark (unit)	Suitable device
6351	Parallel battery quantity	2	[1,3]	
6352	Battery capacity setting	2	1	
6353	Discharge ending voltage	2	0.1V	
6354	Charge rate	2	[0,3] 0-0.1C, 1-0.2C, 2-0.5C, 3-1C	
6355	Equalizing charge voltage	2	0.1 V	
6356	Floating charge voltage	2	0.1 V	
6357	Battery over-voltage protection	2	0.1V	
6358	Battery low-voltage protection	2	0.1V	
6359	Battery cell over-voltage protection	2	0.1mV	
6360	Battery cell low-voltage protection	2	0.1mV	
6361-6399	Reserved			

2.4.4 Inner mode setting

the green content in following table is suitable for SPI60K (V1.3) only

Address (decimalism)	Meaning	Byte	Remark	Suitable device
6400	Grid level 1 low-voltage protection ponit	2	0.1%	
6401	Grid level 2 low-voltage protection ponit	2	0.1%	
6402	Grid level 3 low-voltage protection ponit	2	0.1%	
6403	Grid level 1 over-voltage protection ponit	2	0.1%	

Address (decimalism)	Meaning	Byte	Remark	Suitable device
6404	Grid level 2 over-voltage protection ponit	2	0.1%	
6405	Grid level 1 low-voltage protection time	2	0.01s	
6406	Grid level 2 low-voltage protection time	2	0.01s	
6407	Grid level 3 low-voltage protection time	2	0.01s	
6408	Grid level 1 over-voltage protection time	2	0.01s	
6409	Grid level 2 over-voltage protection time	2	0.01s	
6410	Grid low-voltage protection recover point	2	0.1%	
6411	Grid over-voltage protection recover point	2	0.1%	
6412	Grid level 1 low-frequency protection time	2	0.01Hz	
6413	Grid level 2 low-frequency protection time	2	0.01Hz	
6414	Grid level 1 over-frequency protection time	2	0.01Hz	
6415	Grid level 2 over-frequency protection time	2	0.01Hz	
6416	Grid level 1 low-frequency protection time	2	0.01s	
6417	Grid level 2 low-frequency protection time	2	0.01s	
6418	Grid level 1 over-frequency protection time	2	0.01s	
6419	Grid level 2 over-frequency protection time	2	0.01s	
6420	Grid low-frequency protection recover point	2	0.01Hz	
6421	Grid over-frequency	2	0.01Hz	

Address (decimalism)	Meaning	Byte	Remark	Suitable device
	protection recover point			
6426	L/HVRT mode	2	[0,2] 0-off; 1-reactive power support mode;2-zero reactive mode	
6427	L/HVRT protection voltage HV2	2	0.1% zero reactive power mode take effect	
6428	L/HVRT protection time HT2	2	0.01s zero reactive power mode take effect	
6429	L/HVRT protection voltage HV1	2	0.1% zero reactive power mode take effect	
6430	L/HVRT protection time HT1	2	0.01s zero reactive power mode take effect	
6431	L/HVRT protection voltage LV1	2	0.1% zero reactive power mode take effect	
6432	L/HVRT protection time LT1	2	0.01s zero reactive power mode take effect	
6433	L/HVRT protection voltage LV2	2	0.1% zero reactive power mode take effect	
6434	L/HVRT protection time LT2	2	0.01s zero reactive power mode take effect	
6435	L/HVRT protection voltage LV3	2	0.1% zero reactive power mode take effect	
6436	L/HVRT protection time LT3	2	0.01s zero reactive power mode take effect	
6437	L/HFRT mode	2	[0,1] 0-off;1-on	
6438	L/HFRT protection frequency HF2	2	0.01Hz	

Address (decimalism)	Meaning	Byte	Remark	Suitable device
6439	L/HFRT protection time HT2	2	0.01s	
6440	L/HFRT protection frequency HF1	2	0.01Hz	
6441	L/HFRT protection time HT1	2	0.01s	
6442	L/HFRT protection frequency LF1	2	0.01Hz	
6443	L/HFRT protection time LT1	2	0.01s	
6444	L/HFRT protection frequency LF2	2	0.01Hz	
6445	L/HFRT protection time LT2	2	0.01s	
6446	P-V mode	2	[0,2] 0-off;1-linear;2-loop	
6447	P-V mode V1 (discharge)	2	0.1%	
6448	P-V mode P1(discharge)	2	1%	
6449	P-V mode V2(discharge)	2	0.1%	
6450	P-V mode P2(discharge)	2	1%	
6451	P-V mode V3(discharge)	2	0.1%	
6452	P-V mode P3(discharge)	2	1%	
6459	P-F mode	2	[0,2] 0-off;1-linear;2-loop	
6460	P-F mode F1(discharge)	2	0.01Hz	
6461	P-F mode P1(discharge)	2	1%	
6462	P-F mode F2(discharge)	2	0.01Hz	
6463	P-F mode P2(discharge)	2	1%	
6464	P-F mode F3(discharge)	2	0.01Hz	
6465	P-F mode P3(discharge)	2	1%	
6472	Q-V mode	2	[0,1] 0-off;1-on	
6473	Q-V mode V1	2	0.1%	
6474	Q-V mode Q1	2	1%	
6475	Q-V mode V2	2	0.1%	

Address (decimalism)	Meaning	Byte	Remark	Suitable device
6476	Q-V mode V3	2	0.1%	
6477	Q-V mode V4	2	0.1%	
6478	Q-V mode Q4	2	1%	
6479	Q-V mode Hysteresis	2	0.1%	
6480	SPF mode	2	[0,1] 0-off;1-on	
6481	SPF mode P1	2	1%	
6482	SPF mode PF1	2	0.01	
6483	SPF mode P2	2	1%	
6484	SPF mode PF2	2	0.01	
6485	SPF mode P3	2	1%	
6486	SPF mode PF3	2	0.01	
6490	ON/OFF soft start rate	2	0.01%	
6491	P-F mode hysteresis time	2	0.01s	
6492	P-LF mode	2	[0,2] 0-off;1-linear;2-loop	
6493	P-LF mode F1(discharge)	2	0.01Hz	
6494	P-LF mode F2(discharge)	2	0.01Hz	
6495	P-LF mode F3(discharge)	2	0.01Hz	
6496	P-LF mode P1(discharge)	2	1%	
6497	P-LF mode P2(discharge)	2	1%	
6498	P-LF mode P3(discharge)	2	1%	
6499	Grid level 3 over-voltage protection	2	0.1%	
6500	Grid level 4 over-voltage protection	2	0.1%	
6501	Grid level 4 low-voltage protection point	2	0.1%	
6502	Grid level 3 over-voltage protection time	2	0.01s	
6503	Grid level 4 over-voltage protection time	2	0.01s	
6504	Grid level 4 low-voltage protection time	2	0.01s	

Address (decimalism)	Meaning	Byte	Remark	Suitable device
6505	Grid level 3 over-frequency protection point	2	0.01Hz	
6506	Grid level 4 over-frequency protection point	2	0.01Hz	
6507	Grid level 3 low-frequency protection point	2	0.01Hz	
6508	Grid level 4 low-frequency protection point	2	0.01Hz	

2.4.5 Inner analog quantity setting

None

2.5 Read/write multiple holding registers (analog quantity)

read function code: 0x03, write function code: 0x10

2.5.1 Standard multiple analog quantity setting

Address (decimalism)	Meaning	Byte	Remark (unit)	Suitable device
6020	System time setting-year	2	0~99	Common used
6021	System time setting-month	2	1~12	
6022	System time setting-day	2	Pay attention to leap year and big/small month	
6023	System time setting-hour	2	0~23	
6024	System time setting-minute	2	0~59	
6025	System time setting-second	2	0~59	
6026	Charge period setting-period quantity	2	[0,6]	Energy storage device
6027	Charge period setting - period 1 starting time	2	High byte- hour; low byte-minute	
6028	Charge period setting - period 1 anding time	2		
6029	Charge period setting - period 2 starting time	2		

Address (decimalism)	Meaning	Byte	Remark (unit)	Suitable device
6030	Charge period setting - period 2 anding time	2		
6031	Charge period setting - period 3 starting time	2		
6032	Charge period setting - period 3 anding time	2		
6033	Charge period setting - period 4 starting time	2		
6034	Charge period setting - period 4 anding time	2		
6035	Charge period setting - period 5 starting time	2		
6036	Charge period setting - period 5 anding time	2		
6037	Charge period setting - period 6 starting time	2		
6038	Charge period setting - period 6 anding time	2		
6039	Discharge period setting-period quantity	2		
6040	Discharge period setting - period 1 starting time	2		
6041	Discharg period setting - period 1 anding time	2		
6042	Discharge period setting - period 2 starting time	2		
6043	Discharg period setting - period 2 anding time	2		
6044	Discharge period setting - period 3 starting time	2		
6045	Discharg period setting - period 3 anding time	2		
6046	Discharge period setting - period 4 starting time	2		
6047	Discharg period setting - period 4 anding time	2		
6048	Discharge period setting - period 5 starting time	2		

Address (decimalism)	Meaning	Byte	Remark (unit)	Suitable device
6049	Discharg period setting - period 5 anding time	2		
6050	Discharge period setting - period 6 starting time	2		
6051	Discharg period setting - period 6 anding time	2		
6052-6199	Reserved			

NOTE

Function code 03 is used to judge whether the read content is wrote correctly.

2.5.2 Expansion multiple analog quantity setting

None

2.5.3 Inner multiple analog quantity setting

the green content in following table is suitable for SPI60K-B (V1.3) only

Address (decimalism)	Meaning	Byte	Remark (unit)
6900-6901	Grid level 1 over-frequency protection time HT1	4	0.01s
6902-6903	Grid level 2 over-frequency protection time HT2	4	0.01s
6904-6905	Grid level 3 over-frequency protection time HT3	4	0.01s
6906-6907	Grid level 4 over-frequency protection time HT4	4	0.01s
6908-6909	Grid level 1 low-frequency protection time LT1	4	0.01s
6910-6911	Grid level 2 low-frequency protection time LT2	4	0.01s
6912-6913	Grid level 3 low-frequency protection time LT3	4	0.01s
6914-6915	Grid level 4 low-frequency protection time LT4	4	0.01s

2.6 Read multiple holding registers (analog quantity),

Function code: 0xE0

None

3 Batch broadcast setting power

function code 0x10, broadcast address 0xFF

Address (decimalism)	Meaning	Data type	Remark (unit)
8000	The broadcast write power point quantity	UINT16	
8001	Address 1	UINT16	
8002	Active power 1	INT16	
8003	Address 2	UINT16	
8004	Active power 2	INT16	
……	……		
……	……		
8063	Address 32	UINT16	
8064	Active power 32	INT16	
8100	The broadcast write power point quantity	UINT16	
8101	Address 1	UINT16	
8102	Reactive power 1	INT16	
8103	Address 2	UINT16	
8104	Reactive power 2	INT16	
……	……		
……	……		
8163	Address 32	UINT16	
8164	Reactive power 32	INT16	

NOTE

Active power and reactive power needs to be set separately, if n sets of inverter will be set, it needs to write 2*n+1 register.

For example:

Write active power of 3 inverter:

Address:	0xFF (default)
Function code:	0x10 (default)
Register setting starting address:	0x1F 0x40 (address is 8000)
Register setting quantity:	0x00 0x07 (2*n+1, for 3 inverter, it is 7)
Byte quantity:	0x0E (2*(2*n+1), it is 2 times of register setting quantity)
The broadcast write power point quantity:	0x00 0x03 (10 points)
Address 1: that will be broadcasted)	0x00 0x01 (Address 1, user can set the device address by themselive
Active power 1:	0x00 0x64 (100)
Address 2: themselive that will be broadcasted)	0x00 0x20 (Address 32, user can set the device address by
Active power 2:	0x01 0xF4 (500)
Address 3: themselive that will be broadcasted)	0x00 0x3F (Address 63, user can set the device address by
Active power 3:	0x02 0xDC (732)
CRC check:	0xB2 0x72 (check code please see chapter 7)

The send form is as follows:
FF 10 1F 40 00 07 0E 00 03 00 01 00 64 00 20 01 F4 00 3F 02 DC B2 72

Write reactive power of 3 inverter:
FF 10 1F A4 00 07 0E 00 03 00 01 00 64 00 20 01 F4 00 3F 02 DC C4 B5

4 CRC16 Check Function

```
Uint16 crc16(Uint16 *buf,Uint16 n)
{
Uint16uCRCHi=0xff;
Uint16 uCRCLow=0xff;
Uint16 CRC=0xffff;
Uint16 CRCFlag=0;
    Uint16 i=0,j=0;
    for(j=0;j<n;j++)
    {
        CRC=CRC^buf[j];
        for(i=0;i<8;i++)
        {
            CRCFlag=CRC&0x0001;
            CRC=CRC>>1;
            if(CRCFlag==1)
            {
                CRC=CRC^0xa001;
            }
        }
        uCRCHi=CRC&0x00ff;
        uCRCLow=(CRC>>8)&0x00ff;
        return (uCRCHi<<8|uCRCLow);
    }
}
```

5 Information frame example

If the slave's address is set to 0x01 and query running information (address is 4501-4510), the host will send the information frame as follows:

01 04 11 95 00 0A 65 1D // 00 0A means there are 10 registers, 65 1D is CRC check code

The salve returns following information frame (not real data):

01 04 14 00 01 00 02 00 03 00 04 00 05 00 06 00 07 00 08 00 09 00 0A B9 F0

6 Others

For the communicaiton protocol and inquiry logic of history record, I-V curve scan and fault wave etc, please contact us.

A ModBus Communication Protocol

A.1 Function Code Description

This protocol is appropriate for the communication between host and slave, the host requires data from the slave circularly, the slave receives the request command and responds corresponding data. This protocol is based on ***Kehua Standard ModBus Protocol.*** Details as follows.

Function code	Meaning	Remark
0x01	Read coil status	Read by byte
0x02	Read input status	Read by byte
0x03	Read holding registers	Read by word
0x04	Read input registers	Read by word
0x05	Force single coil	OFF-0x0000; ON-0xFF00
0x06	Preset single register	Write by word
0x10	Preset multiple registers	Write by word
0xE0	Write multiple holding registers (inner function code)	Write by word

A.2 Instruction Details

A.2.1 Read Coil Status (Function Code: 0x01)

Host request (Hexadecimal)

ID	Function code	Register starting address		Quantity		CRC check	
		High byte	Low byte	High byte	Low byte	Low byte	High byte
xx	0x01	xx	xx	xx	xx	xx	xx

Slave response (Hexadecimal)

ID	Function code	Byte quantity	Register 1	…	Register N	CRC check	
						Low byte	High byte
xx	0x01	xx	xx	…	xx	xx	xx

NOTE

The bit 0 of register 1 of response information is corresponding to the starting address in the request, If the returned register quantity is less than 8 or not a multiple of eight, the remaining bits in the final register will be padded with zeros.

A.2.2 Read Input Status (Function Code: 0x02)

Host request (Hexadecimal)

ID	Function code	Register starting address		Quantity		CRC check	
		High byte	Low byte	High byte	Low byte	Low byte	High byte
xx	0x02	xx	xx	xx	xx	xx	xx

Slave response (Hexadecimal)

ID	Function code	Byte quantity	Register 1	…	Register N	CRC check	
						Low byte	High byte
xx	0x02	xx	xx	…	xx	xx	xx

NOTE

The bit 0 of register 1 of response information is corresponding to the starting address in the request, If the returned register quantity is less than 8 or not a multiple of eight, the remaining bits in the final register will be padded with zeros.

A.2.3 Read Holding Registers (Function Code: 0x03)

Host request (Hexadecimal)

ID	Function code	Register starting address		Register quantity		CRC check	
		High byte	Low byte	High byte	Low byte	Low byte	High byte
xx	0x03	xx	xx	xx	xx	xx	xx

Slave response(Hexadecimal)

ID	Function code	Byte quantity	Register 1		…		Register N		CRC check	
			High byte	Low byte	…	…	High byte	Low byte	Low byte	High byte
xx	0x03	xx	xx	xx	…	…	xx	xx	xx	xx

NOTE

Reading one or more registers is distinguished by the quantity of register. If the quantity of register is 1, it means that there is one register. If the quantity of register is more than 1, it means that there are several registers. Register 1 is corresponding to the starting address.

A.2.4 Read Input Registers (Function Code: 0x04)

Host request (Hexadecimal)

ID	Function code	Register starting address		Register quantity		CRC check	
		High byte	Low byte	High byte	Low byte	Low byte	High byte
xx	0x04	xx	xx	xx	xx	xx	xx

Slave response(Hexadecimal)

ID	Function code	Byte quantity	Register 1		…		Register N		CRC check	
			High byte	Low byte	…	…	High byte	Low byte	Low byte	High byte
xx	0x04	xx	xx	xx	…	…	xx	xx	xx	xx

NOTE

Reading one or more registers is distinguished by the quantity of register. If the quantity of register is 1, it means that there is one register. If the quantity of register is more than 1, it means that there are several registers. Register 1 is corresponding to the starting address.

A.2.5 Force Single Coil (Function Code: 0x05)

Host request (Hexadecimal)

ID	Function code	Register starting address		Register setting value		CRC check	
		High byte	Low byte	High byte	Low byte	Low byte	High byte
xx	0x05	xx	xx	xx	xx	xx	xx

For the write input status can be ON/OFF only, 0xFF00 request input status is ON, 0x0000 request input status is OFF.

Slave response(Hexadecimal):

ID	Function code	Register address		Register setting value		CRC check	
		High byte	Low byte	High byte	Low byte	Low byte	High byte
xx	0x05	xx	xx	xx	xx	xx	xx

A.2.6 Preset Single Register (Function Code: 0x06)

Host request (Hexadecimal)

ID	Function code	Register address		Register setting value		CRC check	
		High byte	Low byte	High byte	Low byte	Low byte	High byte
xx	0x06	xx	xx	xx	xx	xx	xx

Slave response(Hexadecimal)

ID	Function code	Register address		Register setting value		CRC check	
		High byte	Low byte	High byte	Low byte	Low byte	High byte
xx	0x06	xx	xx	xx	xx	xx	xx

A.2.7 Preset Multiple Registers (Function Code: 0x10)

Host request (Hexadecimal)

ID	Function code	Register setting start address		Register setting quantity(N)		Byte quantity	Register setting value		Register …	CRC check	
		High byte	Low byte	High byte	Low byte	2*N	High byte	Low byte	…	Low byte	High byte
xx	0x10	xx	xx	xx	xx	xx	xx	xx	…	xx	xx

Slave response(Hexadecimal)

ID	Function code	Register address		Preset register quantity		CRC check	
		High byte	Low byte	High byte	Low byte	Low byte	High byte
xx	0x10	xx	xx	xx	xx	xx	xx

A.2.8 Write Multiple Holding Registers (Inner Function Code: 0xE0)

Host request (Hexadecimal)

ID	Function code	Register setting start address		Register setting quantity(N)		Byte quantity	Register setting value		Register …	CRC check	
		High byte	Low byte	High byte	Low byte	2*N	High byte	Low byte	…	Low byte	High byte
xx	0xE0	xx	xx	xx	xx	xx	xx	xx	…	xx	xx

Slave response(Hexadecimal)

ID	Function code	Register address		Preset register quantity		CRC check	
		High byte	Low byte	High byte	Low byte	Low byte	High byte
xx	0xE0	xx	xx	xx	xx	xx	xx

A.2.9 Error Information and Data Processing

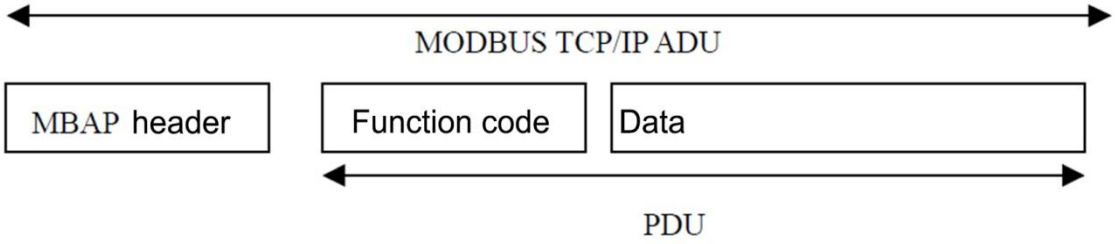
Slave response(Hexadecimal)

ID	Function code	Error code	CRC check	
			Low byte	High byte
xx	xx|0x80	xx	xx	xx

When the communication module of the inverter detects error except CRC error, it must send the information to the host. The highest bit of function codes is 1, that is, add 128 at the sent function code of host. The responded and sent error codes of inverter's communication module are as follows:

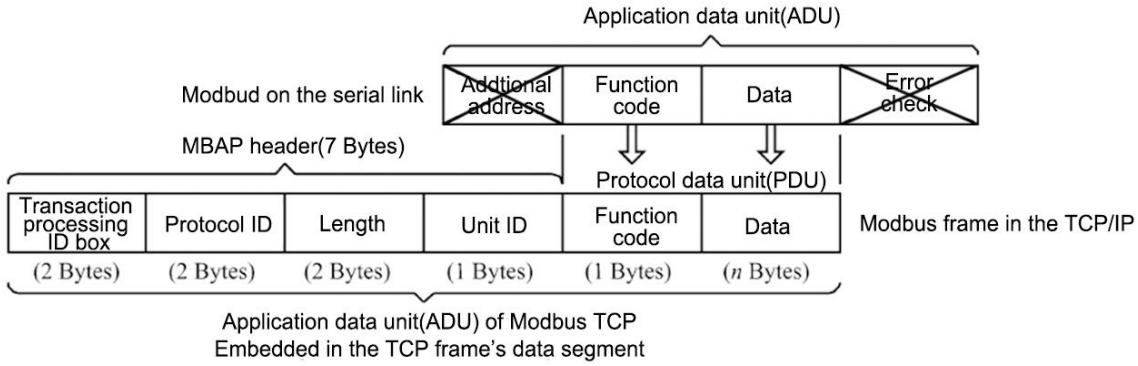
Error code	Definition	Remark
0x01	Invalid function code	The server does not understand the function code
0x02	Invalid data address	Related to the request
0x03	Invalid data value	Related to the request
0x04	Service fault	The communication module of inverter can not take out the data fault during processing
0x10	Wrong register setting value	Password mismatch, setting exceed setting range, etc.
0x11	No authority	

A.3 ModBus TCP Instruction Details



A special header used on the TCP/IP is to indentify ModBus application data unit, called MBAP header (ModBus protocol header).

The difference between ModBus TCP data frame and serial link data frame:



MBAP header includes the following fields:

Field	Length	Description	Client	Server
Transaction processing ID box	2 byte	ModBus request response transaction processing ID	Client start	Server recopys from the received request
Protocol ID	2 byte	0: ModBus protocol	Client start	Server recopys from the received request
Length	2 byte	Number of bytes	Client start(request)	Client(response) start
Unit ID	1 byte	The ID of the remote slave connected to the serial link or other bus	Client start	Server recopys from the received request

Header length is 7 bytes:

- Transaction processing ID box: Used for transaction matching. In response, the ModBus server copies the transaction processing ID of the request.

- Protocol ID: Used for multiplexing within system. The ModBus protocol is indentified by a value of 0.
- Length: The length filed is the number of bytes in the next field, including unit ID and data field.
- Unit ID: This field is used for intra-system routing. Dedicated to communication between ModBus or ModBus + serial link slaves by a gateway between an Ethernet TCP-IP network and a ModBus serial link. The ModBus client sets this field in the request, and the server must return this field with the same value in the response.
- All ModBus/TCP ADUs are sent through TCP on the registered port 502.

A.3.1 Read Coil Status (Function Code: 0x01)

Request PDU

Function code	Starting address		Quantity	
	High byte	Low byte	High byte	Low byte
0x01	xx	xx	xx	xx

Response PDU

Function code	Byte quantity	Status of No.1 byte coil	…	Status of No.N byte coil
0x01	xx	xx	…	xx

NOTE

The bit 0 of register 1 of response information is corresponding to the starting address in the request, If the returned register quantity is less than 8 or not a multiple of eight, the remaining bits in the final register will be padded with zeros.

A.3.2 Read Input Status (Function Code: 0x02)

Request PDU

Function code	Starting address		Quantity	
	High byte	Low byte	High byte	Low byte
0x02	xx	xx	xx	xx

Response PDU

Function code	Byte quantity	Register 1	…	Register N
0x02	xx	xx	…	xx

NOTE

The bit 0 of register 1 of response information is corresponding to the starting address in the request, If the returned register quantity is less than 8 or not a multiple of eight, the remaining bits in the final register will be padded with zeros.

A.3.3 Read Holding Registers (Function Code: 0x03)

Request PDU

Function code	Starting address		Register quantity	
	High byte	Low byte	High byte	Low byte
0x03	xx	xx	xx	xx

Response PDU

Function code	Byte quantity	Register 1		…		Register N	
		High byte	Low byte	…	…	High byte	Low byte
0x03	xx	xx	xx	…	…	xx	xx

NOTE

Reading one or more registers is distinguished by the quantity of register. If the quantity of register is 1, it means that there is one register. If the quantity of register is more than 1, it means that there are several registers. Register 1 is corresponding to the starting address.

A.3.4 Read Input Registers (Function Code: 0x04)

Request PDU

Function code	Starting address		Register quantity	
	High byte	Low byte	High byte	Low byte
0x04	xx	xx	xx	xx

Response PDU

Function code	Byte quantity	Register 1		…		Register N	
		High byte	Low byte	…	…	High byte	Low byte
0x04	xx	xx	xx	…	…	xx	xx

NOTE

Reading one or more registers is distinguished by the quantity of register. If the quantity of register is 1, it means that there is one register. If the quantity of register is more than 1, it means that there are several registers. Register 1 is corresponding to the starting address.

A.3.5 Force Single Coil (Function Code: 0x05)

Request PDU

Function code	Register address		Register setting value	
	High byte	Low byte	High byte	Low byte
0x05	xx	xx	xx	xx

NOTE

For the write input status can be ON/OFF only, 0xFF00 request input status is ON, 0x0000 request input status is OFF.

A.3.6 Preset Single Register (Function Code: 0x06)

Request PDU

Function code	Register address		Register setting value	
	High byte	Low byte	High byte	Low byte
0x06	xx	xx	xx	xx

Response PDU

Function code	Register address		Register setting value	
	High byte	Low byte	High byte	Low byte
0x06	xx	xx	xx	xx

A.3.7 Preset Multiple Registers (Function Code: 0x10)

Request PDU

Function code	Register setting start address		Register setting quantity (N)		Byte quantity	Register setting value		Register….	
	High byte	Low byte	High byte	Low byte	2*N	High byte	Low byte	…	…
0x 10	xx	xx	xx	xx	xx	xx	xx	…	

Response PDU

Function code	Register address		Reset register quantity	
	High byte	Low byte	High byte	Low byte
0x 10	xx	xx	xx	xx

A.3.8 Error Information and Data Processing

Response PDU

Function code	Error code
xx|0x80	xx

When the communication module of slave detects error except CRC error, it must send the information to the host. The highest bit of function code is 1, that is, add 128 at the sent function code of host. The responded and sent error codes of slave's communication module are as follows:

Error code	Definition	Remark
0x01	Invalid function code	The server does not understand the function code
0x02	Invalid data address	Related to the request
0x03	Invalid data value	Related to the request
0x04	Service fault	The communication module of slave cannot take out the data fault during processing

KEHUA DATA CO., LTD.

ADD: No. 457, Malong Road, Torch High-Tech Industrial
Zone, Xiamen, Fujian, China (361000)
TEL: 0592-5160516 (8 lines)
FAX: 0592-5162166
Http://www.kehua.com