KEHUA TECH

String PV Grid-tied Inverter

Monitor Protocol V2.0

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 Product 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.

- SPI320K-B-H series
- SPI250K-B-H series
- SPI125K-B series
- SPI33K-B X2 series
- SPI23K-B X2 series
- SPI12K-B X2 series
- SPI8000-B X2 series

1.3 Related Terms and Description

Name	Description
Host	The part that initiatively start to communicate.
Slave	The part that passively respond the command.
UINT16	Unsigned 16-bit integer. High byte front, low byte behind.
UINT32	Unsigned 32-bit integer. High byte front, low byte behind.

Name	Description
INT16	Signed 16-bit integer. High byte front, low byte behind.
INT32	Signed 32-bit integer. High byte front, low byte behind.
String	Character string that every byte marked by ASCII.
MLB	Multibyte
Bitfield16	16-bit bitfield. High bit front, low bit behind.
RW	The register can be read and write.
RO	The register that can be read only.

1.4 Communication Configuration

1.4.1 Communication Configuration of RS485 Port

Name	Description
Transmission mode	RTU
Baud rate	Default is 9600bps, and it can be set to 2400bps, 4800bps,19200bps,38400bps,115200bps.
Parity bit	none
Data bits	8bit
Stop bits	1bit
Frame interval	Not less than the transmission time of 3.5 bytes
Intra-frame bytes 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

1.4.2 Communication Configuration of Ethernet Port（Optional）

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
IP	Default: 192.168.1.10 It can be configured according to Chapter 10
Subnet mask	Default: 255.255.255.0 It can be configured according to Chapter 10
Gateway	Default: 192.168.1.1 It can be configured according to Chapter 10

2 Register Definition

2.1 Input Register Definition

Operation way: read: 0x04; compatible with the part protocol of V1.0.

2.1.1 System Information

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
4800-4809	Device Model	20	String	RO	
4810-4819	Reserved	20	String	RO	
4820-4824	HMI version	10	String	RO	
4825-4834	S/N	20	String	RO	
4835-4839	Version of control software 1	10	String	RO	
4840-4844	Version of control software 2	10	String	RO	
4845-4849	Version of control software 3	10	String	RO	
4850	Device type	2	UINT16	RO	1- PV inverter 2- PCS 10- Single-phase PV inverter
4851	MPPT number	2	UINT16	RO	
4852	Protocol type	2	UINT16	RO	1- three-phase protocol 2-single-phase protocol

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
					3-PID protocol
4853-4857	Protocol version	10	String	RO	V2.02
4858-4872	Manufacturer info	30	String	RO	
4873	Total PV array quantity	2	UINT16	RO	
4874	Probation remaining	2	UINT16	RO	1h

2.1.2 PID Analog Information

Register	Signal name	Size (Byte)	Type	Read/ write	Remark
5000	Inverter running status	2	UINT16	RO	0-standby;1-grid-tied; 2- fault;3-off;4-off-line; If there is screen, it maps according to register 11016. 0x00xx means standby 0x01xx means grid-tied 0x02xx means fault 0x03xx means off 0x04xx means off-line
5001	CRC16 check	2	UINT16	RO	Check code of 5000 and 5002.
5002	Bus voltage	2	UINT16	RO	0.1V
5003	Reserved fault word 1	2	UINT16	RO	
5004	Reserved fault word 2	2	UINT16	RO	

2.2 Holding Registers Definition

2.2.1 System Infor

Table2-1 Registers definition (10000-10084)

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
10000-10014	Manufacturer info	30	String	RO	
10015-10024	Device Model	20	String	RO	
10025-10034	S/N	20	String	RO	
10035-10039	HMI version	10	String	RO	
10040-10044	Version of control software 1	10	String	RO	
10045-10049	Version of control software 2	10	String	RO	
10050-10054	Version of control software 3	10	String	RO	
10055-10059	Version of control software 4	10	String	RO	
10060-10064	Version of control software 5	10	String	RO	
10065-10069	Version of control software 6	10	String	RO	
10070	Device type	2	UINT16	RO	1- Three-phase PV inverter 2- Three-phase PV energy-storage inverter 10- Single-phase PV inverter

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
10071	Protocol type	2	UINT16	RO	1- Three-phase protocol 2- Single-phase protocol 3- PID protocol
10072-10076	Protocol version	10	String	RO	V2.02
10077	Total PV array quantity	2	UINT16	RO	
10078	MPPT number	2	UINT16	RO	
10079	Probation remaining	2	UINT16	RO	1h
10080	Rated power	2	UINT16	RO	0.1kW
10081	Max. apparent power (max. scheduling value)	2	UINT16	RO	0.1kVA
10082	Max. active power (max. scheduling value)	2	UINT16	RO	0.1kW
10083	Max. reactive power (min. scheduling value)	2	UINT16	RO	0.1kVar
10084	Min. power factor (min. scheduling value)	2	UINT16	RO	0.001

Table2-2 Registers definition (11000-11199)

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
11000	Alarm 1	2	Bitfield16	RO	For detailed alarm definition, please see chapter 3
11001	Alarm 2	2	Bitfield16	RO	
11002	Alarm 3	2	Bitfield16	RO	
11003	Alarm 4	2	Bitfield16	RO	

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
11004	Alarm 5	2	Bitfield16	RO	
11005	Alarm 6	2	Bitfield16	RO	
11006	Alarm 7	2	Bitfield16	RO	
11007	Alarm 8	2	Bitfield16	RO	
11008	Alarm 9	2	Bitfield16	RO	
11009	Alarm 10	2	Bitfield16	RO	
11010	Alarm 11	2	Bitfield16	RO	
11011	Alarm 12	2	Bitfield16	RO	
11012	Alarm 13	2	Bitfield16	RO	
11013	Alarm 14	2	Bitfield16	RO	
11014	Alarm 15	2	Bitfield16	RO	
11015	Alarm 16	2	Bitfield16	RO	
11016	Running status	2	UINT16	RO	0x0000-standby (no DC input) 0x0001- standby (DC under-voltage) 0x0002-standby (self-check) 0x0100-grid-tied 0x0101-inverter prestart 0x0102- Unit derating 0x0103- Ration derating 0x0104- night SVG

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
					0x0200-fault 0x0201-fault (waiting for fault recovery) 0x0300-off 0x0400-off-line
11017	Daily grid-tied energy	2	UINT16	RO	0.1kWh
11018-11019	Total grid-tied energy	4	UINT32	RO	0.1kWh
11020	Grid frequency	2	UINT16	RO	0.01Hz
11021-11022	Apparent power	4	UINT32	RO	1VA
11023-11024	Active power	4	UINT32	RO	1W
11025-11026	Reactive power	4	INT32	RO	1Var
11027	Total power factor	2	INT16	RO	0.001
11028	Grid voltage (U/UV)	2	UINT16	RO	0.1V
11029	Grid voltage (V/VW)	2	UINT16	RO	0.1V，Single-phase SPI is displayed as 0.
11030	Grid voltage (W/WU)	2	UINT16	RO	0.1V, Single-phase SPI is displayed as 0.
11031	Grid current (U)	2	UINT16	RO	0.1A
11032	Grid current (V)	2	UINT16	RO	0.1A, Single-phase SPI is displayed as 0.
11033	Grid current (W)	2	UINT16	RO	0.1A, Single-phase SPI is displayed as 0.
11034	AC Residual current	2	UINT16	RO	0.1mA
11035	Temperature of heat sink (boost)	2	INT16	RO	0.1℃

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
11036	Temperature of heat sink (inverter)	2	INT16	RO	0.1℃
11037	Temperature of power module (boost)	2	INT16	RO	0.1℃
11038	Temperature of power module (inverter)	2	INT16	RO	0.1℃
11039	Inner temperature	2	INT16	RO	0.1℃
11040	Bus voltage (inverter)	2	UINT16	RO	0.1V
11041	Insulation resistance	2	UINT16	RO	0.1kΩ
11042	PV input power	2	UINT16	RO	0.1kW
11043	Bus cap value	2	UINT16	RO	1uF
11044	PID running status	2	UINT16	RO	0- standby，1-repairing，2-off，3-fault
11045	PID repair voltage	2	UINT16	RO	0.1V
11046-11063	Reserved	21*2	UINT16	RO	
11064-11079	Voltage of MPPT1-MPPT16	16*2	UINT16	RO	0.1V
11080-11095	Current of MPPT1-MPPT16	16*2	INT16	RO	0.1A
11096-11103	Reserved	8*2	UINT16	RO	
11104-11135	Voltage of PV 1-32	32*2	UINT16	RO	0.1V
11136-11167	Current of PV 1-32	32*2	INT16	RO	0.1A
11168-11199	Power of PV 1-32	32*2	INT16	RO	0.1KW

Table2-3 Registers definition (12000-12099)

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
12000	ON/OFF	2	UINT16		0-OFF; 1-ON
12001	Self-start after power on	2	UINT16	RW	0-disable; 1-enable
12002	Recover grid-tied	2	UINT16	RW	0-not recovery; 1-recovery, it only valid after disable the "self-start after abnormal recovers" and grid abnormal recovers.
12003	Self-recover once grid abnormal	2	UINT16	RW	0-disable; 1-enable
12004	H/LVRT	2	UINT16	RW	1-Zero reactive power modle 2-Supplied by reactive power modle 3-Zero current modle
12005	Initiative islanding	2	UINT16	RW	0-disable; 1-enable
12006	Insulation resistance detection	2	UINT16	RW	0-disable; 1-enable
12007	Phase self-adapt	2	UINT16	RW	0-disable; 1-enable
12008	Night SVG	2	UINT16	RW	0-disable; 1-enable
12009	Reactive first	2	UINT16	RW	0-disable; 1-enable
12010	Rated grid frequency	2	UINT16	RW	0-50Hz; 1-60Hz
12011	SPD abnormal alarm	2	UINT16	RW	0-disable; 1-enable
12012	PID repair function	2	UINT16	RW	0-disable; 1-night PID

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
					2-day PID；3-24h PID
12013	DC arc detection	2	UINT16	RW	0-disable; 1-enable
12014	Clear the alarm of DC arc	2	UINT16	RW	0-disable; 1-enable
12015	Recover default setting	2	UINT16	RW	0-invalid; 1-recover
12016	Active power control mode	2	UINT16	RW	0: no response for scheduling. 1: response for SI value scheduling; 2: response for p.u. value scheduling (default is 1)
12017	Active power setting (SI value)	2	UINT16	RW	0.1kW
12018	Active power setting (p.u.)	2	UINT16	RW	0.1%; 100%=max. active power
12019	Reactive power control mode	2	UINT16	RW	0: no response for scheduling; 1: response for SI value scheduling; 2: response for p.u. value scheduling; 3: response for power factor scheduling (default is 1)
12020	Reactive power (SI value)	2	INT16	RW	0.1kVar
12021	Reactive power (p.u. value)	2	INT16	RW	0.1%; 100%= max. reactive power

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
12022	Power factor	2	INT16	RW	0.001
12023	Grid-tied recover time	2	UINT16	RW	1s
12024	Power rate	2	UINT16	RW	0.01%/s
12025	ON/OFF soft-start rate	2	UINT16	RW	0.01%/s
12026	Standard type	2	UINT16	RW	0-China; 1-UL1741; 2-UL1741(SA); 3-Germany; 4-Australia; 5-new Zealand; 6-UK; 7-Thailand PEA; 8-Thailand MEA; 9-Italy0-16; 10- Italy0-21; 11-user-defined ; 12- France VFR; 13- France SEI; 14- France CRAE; 15- France VDE; 16-Netherlands; 17-Spain; 18-EN50438; 19- country grid; 20-city grid; 21-India;

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
					22-Korea; 23-Canada; 24-Mexico; 25-Japan; 26-Morocco; 27-Poland; 28-Ukraine; 29-Brazil
12027-12028	PV alarm enable	4	UINT32	RW	[0x0000,0xFFFF] bit0~15: Branch 1～16; 0-Branch alarm enable; 1-Branch alarm shielded
12029	Anti-countercurrent function	2	UINT16	RW	0-disable; 1-enable
12030	Power of backflow control	2	INT16	RW	0.1%， 100%= max active power
12031	Power of backflow protection	2	INT16	RW	0.1%
12032	Time of backflow protection	2	UINT16	RW	0.1s
12033	backflow recovery time	2	UINT16	RW	0.1s
12034	PV type	2	UINT16	RW	0-N 型；1-P 型
12035	PID repairing voltage setting	2	UINT16	RW	0.1V
12036	PID repairing time	2	UINT16	RW	1min
12037	Bus cap value detect	2	UINT16	RO	0-disable; 1-enable
12038	Telecommunication abnormal protection	2	UINT16	RW	0-disable; 1-enable

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
	function				
12039	Telecommunication abnormal protection time	2	UINT16	RW	1s
12040	DRM function	2	UINT16	RW	0-disable; 1-enable
12041	AC watt-hour meter	2	UINT16	RW	0-nil， 1- CHINT three-phase DTSU666 2- YADA three-phase DTSD3366D-W1 -A 6- CHINT singlee-phase DDSU666， 7-YADA -DDS3366D-1P
12042	DC fast shutdown	2	UINT16	RW	0-disable; 1-enable
12043	Detection of switch between off-line and grid-tied	2	UINT16	RW	0-disable; 1-enable
12044	Control of switch between off-line and grid-tied	2	UINT16	RW	0-disable; 1-enable
12045-12091	Reserved	2*47	UINT16	RW	
12092-12093	Total energy calibration	4	UINT32	RW	0.1kWh
12094	System time setting-year	2	UINT16	RW	Register 12094-12099 must be totally written at one time, or the setting will be invalid.
12095	System time setting-month	2	UINT16	RW	
12096	System time setting- day	2	UINT16	RW	

Register	Signal name	Size (Byte)	Type	Read/ write	Remark/unit
12097	System time setting- hour	2	UINT16	RW	For example: set system time to 2020/1/514:15:30, the register 12094-12099 must write 202015141530 at one time.
12098	System time setting- minute	2	UINT16	RW	
12099	System time setting- second	2	UINT16	RW	

3 Alarm Information Definition

3.1 Alarm Information

Table3-1 Alarm information list

No.	Bit	Alarm name	No.	Bit	Alarm name
Alarm 1	bit0	Probation expire	Alarm 2	bit0	Grid amplitude abnormal
	bit1	Probation approaching		bit1	Grid frequency abnormal
	bit2	Device locked status		bit2	Phase sequence abnormal
	bit3	Probation status		bit3	Inverter over-current
	bit4	Reserved		bit4	Inverter voltage abnormal
	bit5	Reserved		bit5	Telecommunication abnormal
	bit6	Reserved		bit6	Current DC component abnormal
	bit7	Reserved		bit7	Residual current abnormal
	bit8	Reserved		bit8	AC SPD abnormal
	bit9	Reserved		bit9	DC SPD abnormal
	bit10	Reserved		bit10	Load reduction alarm
	bit11	Reserved		bit11	Anti-countercurrent communication abnormal
	bit12	Reserved		bit12	External CT abnormal
	bit13	Reserved		bit13	Smart meter abnormal
	bit14	Reserved		bit14	Reserved
	bit15	Reserved		bit15	Wait for recovering grid-tied signal
Alarm 3	bit0	Insulation impedance abnormal	Alarm 4	bit0	Reserved
	bit1	Bus over-voltage		bit1	Reserved

No.	Bit	Alarm name	No.	Bit	Alarm name
	bit2	Bus unbalance		bit2	Reserved
	bit3	LVRT Run		bit3	Reserved
	bit4	HVRT Run		bit4	Reserved
	bit5	Islanding Alarm		bit5	Reserved
	bit6	Reserved		bit6	Reserved
	bit7	Inner abnormal		bit7	Reserved
	bit8	Advise to replace bus capacitor		bit8	Reserved
	bit9	Advise to maintain fan		bit9	Reserved
	bit10	Fan abnormal (external)		bit10	Reserved
	bit11	Fan abnormal (inner)		bit11	Reserved
	bit12	Temperature control protection		bit12	Reserved
	bit13	Inner over-temperature		bit13	Reserved
	bit14	IGBT over-temperature		bit14	Reserved
	bit15	Heat sink over-temperature		bit15	Reserved
Alarm 5	bit0	Reserved	Alarm 6	bit0	Reserved
	bit1	Reserved		bit1	Reserved
	bit2	Reserved		bit2	Reserved
	bit3	Reserved		bit3	Reserved
	bit4	Reserved		bit4	Reserved
	bit5	Reserved		bit5	Reserved
	bit6	Reserved		bit6	Reserved
	bit7	Reserved		bit7	Reserved
	bit8	Reserved		bit8	Reserved
	bit9	Reserved		bit9	Reserved
	bit10	Reserved		bit10	Reserved
	bit11	Reserved		bit11	Reserved
	bit12	Reserved		bit12	Reserved
	bit13	Reserved		bit13	Reserved

No.	Bit	Alarm name	No.	Bit	Alarm name
	bit14	Reserved		bit14	Reserved
	bit15	Reserved		bit15	Reserved
Alarm 7	bit0	Reserved	Alarm 8	bit0	Reserved
	bit1	Reserved		bit1	Reserved
	bit2	Reserved		bit2	Reserved
	bit3	Reserved		bit3	Reserved
	bit4	Reserved		bit4	Reserved
	bit5	Reserved		bit5	Reserved
	bit6	Reserved		bit6	Reserved
	bit7	Reserved		bit7	Reserved
	bit8	Reserved		bit8	Reserved
	bit9	Reserved		bit9	Reserved
	bit10	Reserved		bit10	Reserved
	bit11	Reserved		bit11	Reserved
	bit12	Reserved		bit12	Reserved
	bit13	Reserved		bit13	Reserved
	bit14	Reserved		bit14	Reserved
	bit15	Reserved		bit15	Reserved
Alarm 9	bit0	PV1 over-current	Alarm 10	bit0	PV17 over-current
	bit1	PV2 over-current		bit1	PV18 over-current
	bit2	PV3 over-current		bit2	PV19 over-current
	bit3	PV4 over-current		bit3	PV20 over-current
	bit4	PV5 over-current		bit4	PV21 over-current
	bit5	PV6 over-current		bit5	PV22 over-current
	bit6	PV7 over-current		bit6	PV23 over-current
	bit7	PV8 over-current		bit7	PV24 over-current
	bit8	PV9 over-current		bit8	PV25 over-current
	bit9	PV10 over-current		bit9	PV26 over-current
	bit10	PV11 over-current		bit10	PV27 over-current

No.	Bit	Alarm name	No.	Bit	Alarm name
	bit11	PV12 over-current		bit11	PV28 over-current
	bit12	PV13 over-current		bit12	PV29 over-current
	bit13	PV14 over-current		bit13	PV30 over-current
	bit14	PV15 over-current		bit14	PV31 over-current
	bit15	PV16 over-current		bit15	PV32 over-current
Alarm 11	bit0	PV1 polarity reverse	Alarm 12	bit0	PV17 polarity reverse
	bit1	PV2 polarity reverse		bit1	PV18 polarity reverse
	bit2	PV3 polarity reverse		bit2	PV19 polarity reverse
	bit3	PV4 polarity reverse		bit3	PV20 polarity reverse
	bit4	PV5 polarity reverse		bit4	PV21 polarity reverse
	bit5	PV6 polarity reverse		bit5	PV22 polarity reverse
	bit6	PV7 polarity reverse		bit6	PV23 polarity reverse
	bit7	PV8 polarity reverse		bit7	PV24 polarity reverse
	bit8	PV9 polarity reverse		bit8	PV25 polarity reverse
	bit9	PV10 polarity reverse		bit9	PV26 polarity reverse
	bit10	PV11 polarity reverse		bit10	PV27 polarity reverse
	bit11	PV12 polarity reverse		bit11	PV28 polarity reverse
	bit12	PV13 polarity reverse		bit12	PV29 polarity reverse
	bit13	PV14 polarity reverse		bit13	PV30 polarity reverse
	bit14	PV15 polarity reverse		bit14	PV31 polarity reverse
	bit15	PV16 polarity reverse		bit15	PV32 polarity reverse
Alarm 13	bit0	MPPT1 over-voltage	Alarm 14	bit0	MPPT1 over-current
	bit1	MPPT2 over-voltage		bit1	MPPT2 over-current
	bit2	MPPT3 over-voltage		bit2	MPPT3 over-current
	bit3	MPPT4 over-voltage		bit3	MPPT4 over-current
	bit4	MPPT5 over-voltage		bit4	MPPT5 over-current
	bit5	MPPT6 over-voltage		bit5	MPPT6 over-current
	bit6	MPPT7 over-voltage		bit6	MPPT7 over-current
	bit7	MPPT8 over-voltage		bit7	MPPT8 over-current

No.	Bit	Alarm name	No.	Bit	Alarm name
	bit8	MPPT9 over-voltage		bit8	MPPT9 over-current
	bit9	MPPT10 over-voltage		bit9	MPPT10 over-current
	bit10	MPPT11 over-voltage		bit10	MPPT11 over-current
	bit11	MPPT12 over-voltage		bit11	MPPT12 over-current
	bit12	MPPT13 over-voltage		bit12	MPPT13 over-current
	bit13	MPPT14 over-voltage		bit13	MPPT14 over-current
	bit14	MPPT15 over-voltage		bit14	MPPT15 over-current
	bit15	MPPT16 over-voltage		bit15	MPPT16 over-current
Alarm 15	bit0	MPPT1 arc abnormal	Alarm 16	bit0	Reserved
	bit1	MPPT2 arc abnormal		bit1	Reserved
	bit2	MPPT3 arc abnormal		bit2	Reserved
	bit3	MPPT4 arc abnormal		bit3	Reserved
	bit4	MPPT5 arc abnormal		bit4	Reserved
	bit5	MPPT6 arc abnormal		bit5	Reserved
	bit6	MPPT7 arc abnormal		bit6	Reserved
	bit7	MPPT8 arc abnormal		bit7	Reserved
	bit8	MPPT9 arc abnormal		bit8	Reserved
	bit9	MPPT10 arc abnormal		bit9	Reserved
	bit10	MPPT11 arc abnormal		bit10	Reserved
	bit11	MPPT12 arc abnormal		bit11	Reserved
	bit12	MPPT13 arc abnormal		bit12	Reserved
	bit13	MPPT14 arc abnormal		bit13	Reserved
	bit14	MPPT15 arc abnormal		bit14	Reserved
	bit15	MPPT16 arc abnormal		bit15	Reserved

4 Power Broadcast Scheduling

Operation way: (write: 0x10; broadcast Slave ID.: 0xFF)

CAUTION

Before using the function, it is necessary to set the " active power scheduling options" (register 12016) and "reactive power scheduling options" (register 12019) to "response for absolute value scheduling" (1)

	Register	Signal name	type	Remark /unit
Active power scheduling	8000	The quantity of written power of this broadcast	UINT16	
	8001	The Slave Addres of inverter 1	UINT16	
	8002	Active power scheduling value of inverter 1	UINT16	0.1kW
	8003	The Slave Addres of inverter 2	UINT16	
	8004	Active power scheduling value of inverter 2	UINT16	0.1kW
	……	……		
	……	……		0.1kW
	……	The Slave Addres of inverter 32	UINT16	
	……	Active power scheduling value of inverter 32	INT16	0.1kW
Reactive power scheduling	8100	The quantity of written power of this broadcast	UINT16	
	8101	The Slave Addres of inverter 1	UINT16	
	8102	Reactive power scheduling value of inverter 1	INT16	0.1kVar

	Register	Signal name	type	Remark /unit
	8103	The Slave Addres of inverter 2	UINT16	
	8104	Reactive power scheduling value of inverter 2	INT16	0.1kVar
	……	……		
	……	……		0.1kVar
	……	The Slave Addres of inverter 32	UINT16	
	……	Reactive power scheduling value of inverter 32	INT16	0.1kVar

The active power and reactive power needs to be set respectively. If there are n sets of inverter, it needs to write 2*n+1 register.

Send active power scheduling value 10kW, 50kW, 73.2kW to the inverter of Slave Addres 1, 32, 63. The sending command as follows:

Address:	0xFF		(broadcast scheduling Slave Addres)
Function code:	0x10		(default)
Register start address:	0x1F	0x40	(register address: 8000)
Register quantity:	0x00	0x07	(2*n+1, e.g., if there are 3 inverters, the quantity is 7)
Byte quantity:	0x0E		(2*(2*n+1), it is 2 times of register setting quantity)
Inverter Quantity:	0x00	0x03	(The quantity of written power of this broadcast is 3)
Inverter 1 Address:	0x00	0x01	(The slave address of Inverter 1 is 1. The device Slave Addres of broadcast can be user-defined.)
Active power 1:	0x00	0x64	(100, Set active power 10kW)
Inverter 2 Address:	0x00	0x20	(The slave address of Inverter 2 is 32.)
Active power 2:	0x01	0xF4	(500, Set active power 50kW)
Inverter 3 Address:	0x00	0x3F	(The slave address of Inverter 3 is 63.)
Active power 3:	0x02	0xDC	(732, send active power 73.2kW)
CRC check:	0xB2	0x72	

The sent data frame 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

As the same, write the 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

5 Daily/ Monthly /Annual Energy Query

Operation way: (read: 0x03; write single register: 0x06; write multi registers: 0x10)

Register	Signal name	Byte	type	Read /write	Unit	Remark
13000	Query year of monthly energy - setting	2	UINT16	RW	2000~2099	After writing the query year, it needs to wait 2s to query the monthly energy data.
13001	Query year of monthly energy	2	UINT16	RO	2000~2099	
13002-13003	Total energy of query year in January	4	UINT32	RO	0.1kWh	
13004-13005	Total energy of query year in February	4	UINT32	RO	0.1kWh	
13006-13007	Total energy of query year in March	4	UINT32	RO	0.1kWh	
13008-13009	Total energy of query year in April	4	UINT32	RO	0.1kWh	
13010-13011	Total energy of query year in May	4	UINT32	RO	0.1kWh	
13012-13013	Total energy of query year in June	4	UINT32	RO	0.1kWh	
13014-13015	Total energy of query year in July	4	UINT32	RO	0.1kWh	
13016-13017	Total energy of query year in August	4	UINT32	RO	0.1kWh	
13018-13019	Total energy of query year in September	4	UINT32	RO	0.1kWh	
13020-13021	Total energy of query year in October	4	UINT32	RO	0.1kWh	
13022-13023	Total energy of query year in November	4	UINT32	RO	0.1kWh	
13024-13025	Total energy of query year in December	4	UINT32	RO	0.1kWh	

Register	Signal name	Byte	type	Read /write	Unit	Remark
13026	Query year of daily energy - setting	2	UINT16	RW	2000~2099	1. The register 13026-13027 must be totally written at one time, or the setting will be invalid. 2. After writing the query year and month, it needs to wait 2s to query the daily energy data.
13027	Query month of daily energy-setting	2	UINT16	RW	1~12	
13028	Query year of daily energy	2	UINT16	RO	2000~2099	
13029	Query month of daily energy	2	UINT16	RO	1~12	
13030	Energy of query month on 1st	2	UINT16	RO	0.1kWh	
13031	Energy of query month on 2nd	2	UINT16	RO	0.1kWh	
13032	Energy of query month on 3rd	2	UINT16	RO	0.1kWh	
13033	Energy of query month on 4th	2	UINT16	RO	0.1kWh	
13034	Energy of query month on 5th	2	UINT16	RO	0.1kWh	
13035	Energy of query month on 6th	2	UINT16	RO	0.1kWh	
13036	Energy of query month on 7th	2	UINT16	RO	0.1kWh	
13037	Energy of query month on 8th	2	UINT16	RO	0.1kWh	
13038	Energy of query month on 9th	2	UINT16	RO	0.1kWh	
13039	Energy of query month on 10th	2	UINT16	RO	0.1kWh	
13040	Energy of query month on 11th	2	UINT16	RO	0.1kWh	
13041	Energy of query month on 12th	2	UINT16	RO	0.1kWh	
13042	Energy of query month on 13th	2	UINT16	RO	0.1kWh	
13043	Energy of query month on 14th	2	UINT16	RO	0.1kWh	
13044	Energy of query month on 15th	2	UINT16	RO	0.1kWh	
13045	Energy of query month on 16th	2	UINT16	RO	0.1kWh	
13046	Energy of query month on 17th	2	UINT16	RO	0.1kWh	
13047	Energy of query month on 18th	2	UINT16	RO	0.1kWh	
13048	Energy of query month on 19th	2	UINT16	RO	0.1kWh	
13049	Energy of query month on 20th	2	UINT16	RO	0.1kWh	
13050	Energy of query month on 21th	2	UINT16	RO	0.1kWh	
13051	Energy of query month on 22th	2	UINT16	RO	0.1kWh	
13052	Energy of query month on 23th	2	UINT16	RO	0.1kWh	1. The

Register	Signal name	Byte	type	Read /write	Unit	Remark
13053	Energy of query month on 24th	2	UINT16	RO	0.1kWh	register 13061-13062 must be totally written at one time, or the setting will be invalid. 2. After writing the query start year of annual energy and query quantities of annual energy, it needs to wait 2s to query the annual energy data.
13054	Energy of query month on 25th	2	UINT16	RO	0.1kWh	
13055	Energy of query month on 26th	2	UINT16	RO	0.1kWh	
13056	Energy of query month on 27th	2	UINT16	RO	0.1kWh	
13057	Energy of query month on 28th	2	UINT16	RO	0.1kWh	
13058	Energy of query month on 29th	2	UINT16	RO	0.1kWh	
13059	Energy of query month on 30th	2	UINT16	RO	0.1kWh	
13060	Energy of query month on 31th	2	UINT16	RO	0.1kWh	
13061	Query start year of annual energy –setting	2	UINT16	RW	2000~2099	
13062	Query quantities of annual energy-setting	2	UINT16	RW	1~25	
13063	Query start year of annual energy	2	UINT16	RO	2000~2099	
13064	Query quantities of annual energy	2	UINT16	RO	1~25	
13065-13066	Total energy of 1th year	4	UINT32	RO	0.1 kWh	
13067-13068-	Total energy of 2th year	4	UINT32	RO	0.1 kWh	
13069-13070	Total energy of 3th year	4	UINT32	RO	0.1 kWh	
13071-13072	Total energy of 4th year	4	UINT32	RO	0.1 kWh	
13073-13074	Total energy of 5th year	4	UINT32	RO	0.1 kWh	
13075-13076	Total energy of 6th year	4	UINT32	RO	0.1 kWh	
13077-13078	Total energy of 7th year	4	UINT32	RO	0.1 kWh	
13079-13080	Total energy of 8th year	4	UINT32	RO	0.1 kWh	
13081-13082	Total energy of 9th year	4	UINT32	RO	0.1 kWh	
13083-13084	Total energy of 10th year	4	UINT32	RO	0.1 kWh	
13085-13086	Total energy of 11th year	4	UINT32	RO	0.1 kWh	
13087-13088	Total energy of 12th year	4	UINT32	RO	0.1 kWh	
13089-13090	Total energy of 13th year	4	UINT32	RO	0.1 kWh	
13091-13092	Total energy of 14th year	4	UINT32	RO	0.1 kWh	

Register	Signal name	Byte	type	Read /write	Unit	Remark
13093-13094	Total energy of 15th year	4	UINT32	RO	0.1 kWh	
13095-13096	Total energy of 16th year	4	UINT32	RO	0.1 kWh	
13097-13098	Total energy of 17th year	4	UINT32	RO	0.1 kWh	
13099-13100	Total energy of 18th year	4	UINT32	RO	0.1 kWh	
13101-13102	Total energy of 19th year	4	UINT32	RO	0.1 kWh	
13103-13104	Total energy of 20th year	4	UINT32	RO	0.1 kWh	
13105-13106	Total energy of 21th year	4	UINT32	RO	0.1 kWh	
13107-13108	Total energy of 22th year	4	UINT32	RO	0.1 kWh	
13109-13110	Total energy of 23th year	4	UINT32	RO	0.1 kWh	
13111-13112	Total energy of 24th year	4	UINT32	RO	0.1 kWh	
13113-13114	Total energy of 25th year	4	UINT32	RO	0.1 kWh	

6 I&V Curve Scan

Operation way: (read: 0x03; write single register: 0x06; write multi registers: 0x10)

6.1 Register Definition

Register	Signal name	Byte	Type	Read/ write	Remark
13200	I&V curve configuration - sampling setting word 1	2	UINT16	RW	1. Bit0 ～ Bit15: MPPT1~MPPT16 0- not sampled; 1- sampling 2. The number of MPPT refer to register 10078.
13201	I&V curve configuration - sampling setting word 2	2	UINT16	RW	Reserved
13202	I&V curve configuration - sampling setting word 3	2	UINT16	RW	Reserved
13203	I&V curve configuration - sampling setting word 4	2	UINT16	RW	Reserved
13204	I&V curve query -MPPT no.	2	UINT16	RW	1. The register of this section must be totally written at one time, or the setting will be invalid. 2. The number of MPPT refer to register 10078.
13205	I&V curve query - channel code	2	UINT16	RW	
13206	I&V curve - sampling finished	2	UINT16	RO	0-not sampled; 1-sampling; 2- sampling succeed; 3-

Register	Signal name	Byte	Type	Read/ write	Remark
					sampling failed.
13207	I&V curve - channel quantity	2	UINT16	RO	
13208	I&V curve - sampling point quantity	2	UINT16	RO	
13209	I&V curve - MPPT no.	2	UINT16	RO	
13210	I&V curve - channel no.	2	UINT16	RO	Channel 1 is PV; Channel 2 and above are array current.
13211-13260	I&V curve - channel data 1-50	2*50	INT16	RO	Voltage:0.1V; current: 0.01A

6.2 I&V Curve Scanning Procedure

Step 1 Host send sampling setting frame of I&V curve to inform the inverter scan the I&V curve of which MPPT.

Function code	Regsiter	Content	Remark
0x10	13200	Sampling setting word	0- not sampled; 1- sampling Bit0～Bit16：MPPT1~MPPT16

Step 2 Slave query sampling status.

Function code	Regsiter	Content	Remark
0x03	13206	Sampling finished status	0- not sampled; 1- sampling 2- sampling succeed; 3- sampling failed

When the read status of sampling is 0 or 1, it will query the read status of waveform. (there need have a timeout exit mechanism)

When the read status is 1, the sampling succeed, go on next step.

When the read status is 2, the sampling failed, host will end the reading.

Step 3 Query the related parameters of I&V curve.

Function code	Address	Content	Remark
0x03	13207	Channel number	The sampling channel of each MPPT
	13208	Sampled point number	

Query the above two info to confirm the data quantity in Step 4, Step 5.

Step 4 Read the channel data: send MPPT number, channel number.

Function code	Address	Content	Remark
0x10	13204	MPPT number	Start from 1
	13205	Channel number	Start from 1

Step 5 Obtain the channel data.

Function code	Address	Content	Remark
0x03	13209	MPPT number	
	13210	Channel number	Start from 1
	13211-13260	Channel data 1～50	

Query if the MPPT number, channel number and subpackage number matches the data sent in Step 4, if matches, it will export the channel data 1～50 (reserved 50 points, details decided by sampling point quantity.

Repeat Step 4, Step 5 till queried all channel data of all MPPT that sent in Step 1.

----End

7 User-defined Function

Operation way: (read: 0x03; write: 0xE0).

7.1 Register Definition

Register	Signal name	Byte	Type	Read/ write	Remark
13800-13809	Station no. configuration-S/N	20	String	RW	1. The register of this section must be totally written at one time, or the setting will be invalid. 2. Register 13800-13809 is used to judge if it matches that of the device, it is not stored. 3. Range of register 13810: 1~247.
13810	Station no. configuration-station no.	2	UINT16	RW	
13811	IP configuration-obtain method	2	UINT16	RW	1. The register of this section must be totally written at one time, or the setting will be invalid. 2. Register 13811: 0-manual; 1-auto. 3. Register 13812-13821 is used to judge if it matches that of the device, it is not saved.
13812-13821	IP configuration -S/N	20	String	RW	
13822-13823	IP configuration -IP address	4	UINT16	RW	
13824-13825	IP configuration -mask	4	UINT16	RW	
13826-13827	IP configuration -gateway	4	UINT16	RW	

7.2 Address Assignment Procedure

Assign theSlave Addres of ModbusRTU according to the uniqueness of S/N.

Step 1 Using the inner function code, broadcast to send the S/N,Slave Addres of configured device.

Function code	Register	Signal name	Byte	Data type	Remark/ unit
E0	13800-13809	Station no. configuration-S/N	20	String	ASCII code (the S/N is used to judge if it matches that of the device, it is not stored.)
	13810	Station no. configuration-Slave Addres	2	UINT16	

After ARM received the broadcast frame, it compares the received S/N with the S/N of itself, if matches, it will set the S/N as itsSlave Addres

Step 2 After all configurations are send, the upper-computer needs to confirm whether the configuration is successful. The configuration method is the same as that using the uniqueness of S/N to query the S/N according to slave no.

Function code	Register	Signal name	Byte	Data type	Remark/ unit
03	10025-10034	S/N	20	String	Device S/N

----End

Example

Host needs to configure 2 sets of device.

No.	S/N	Slave no.
1	5001 0010 0002 0003 0001	2
2	5001 0010 0002 0003 0002	4

Procedure:

1. Broadcast sends S/N 50010010000200030001+Slave Addres 2 (register 13800～13810).
2. QuerySlave Addres 2, register 10025-10034 according to function code 03, and judge whether the S/N matches that sent in step 1. If matches, it means the configuration is successful.
3. Broadcast sends S/N 50010010000200030002+Slave Addres 4.
4. Query slave addres 4, register 10025-10034 according to function code 03, and judge whether the S/N matches that sent in step 3. If matches, it means the configuration is successful.

8 CRC16 Check Function

```
Uint16crc16(Uint16*buf,Uint16n)
{
  Uint16uCRCHi=0xff;
  Uint16uCRCLow=0xff;
  Uint16CRC=0xffff;
  Uint16CRCFlag=0;
  Uint16i=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);
        }
    }
```

9 Example for Information Frame

Set the address of slave to 0x01, and needs to query running information (address is 4501-4510).

Host sends the following information frame:

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

Slave returns the 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

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 single coil	Read by byte
0x02	Read discrete inputs	Read by byte
0x03	Read holding registers	Read by word
0x04	Read input registers	Read by word
0x05	Write single coil	OFF-0x0000; ON-0xFF00
0x06	Write single holding register	Write by word
0x10	Write multiple holding registers	Write by word
0xE0	Write multiple holding registers (inner function code)	Write by word

A.2 Instruction Details

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

Host request (Hexadecimal):

Address	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):

Address	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 Discrete Inputs (Function Code: 0x02)

Host request (Hexadecimal):

Address	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):

Address	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):

Address	Function code	Register starting address		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):

Address	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):

Address	Function code	Register starting address		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):

Address	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 Write Single Coil (Function Code: 0x05)

Host request (Hexadecimal):

Address	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):

Address	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 Write Single Holding Register (Function Code: 0x06)

Host request (Hexadecimal):

Address	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):

Address	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 Write Multiple Holding Registers (Function Code: 0x10)

Host request (Hexadecimal):

Address	Function code	Register setting start address		Register setting quantity		Byte quantity	Register setting value		Register …	CRC check	
		High byte	Low byte	High byte	Low byte		High byte	Low byte	…	Low byte	High byte
xx	0x10	xx	xx	xx	xx	xx	xx	xx	…	xx	xx

Slave response(Hexadecimal):

Address	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):

Address	Function code	Register setting start address		Register setting quantity		Byte quantity	Register setting value		Register …	CRC check	
		High byte	Low byte	High byte	Low byte		High byte	Low byte	…	Low byte	High byte
xx	0xE0	xx	xx	xx	xx	xx	xx	xx	…	xx	xx

Slave response(Hexadecimal):

Address	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

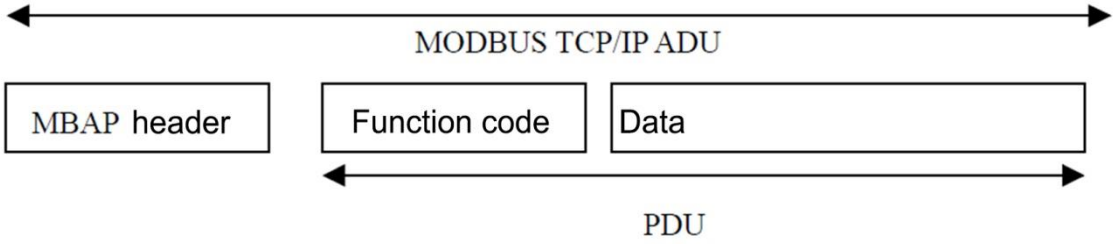
Slave response(Hexadecimal):

Address	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:

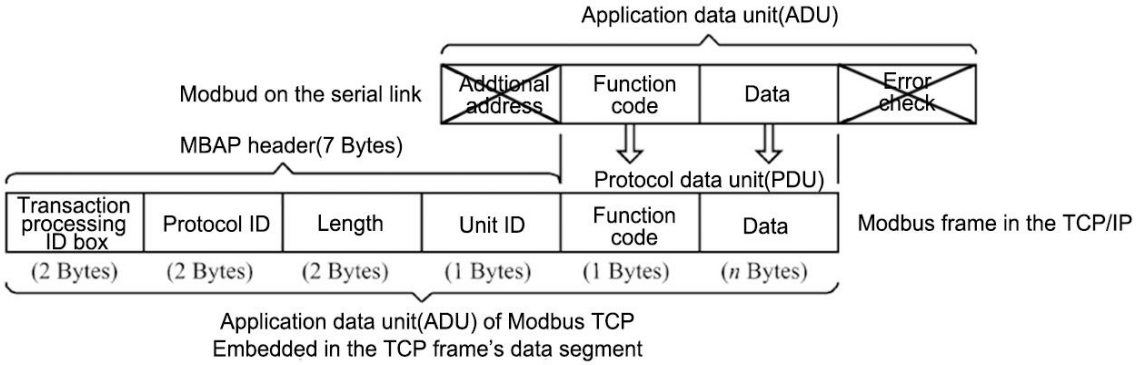
Error code	Definition	Remark
0x01	Invalid function code	The server does not understand the function code
0x02	Invalid data address	Related to the request
0x03	Invalid data value	Related to the request
0x04	Service fault	The communication module of inverter can not take out the data fault during processing
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 heade(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 ID	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: 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 Single Coil (Function Code: 0x01)

Request PDU

Function code	Starting address		Quantity	
	High byte	Low byte	High byte	Low byte
0x 01	xx	xx	xx	xx

Response PDU

Function code	Byte quantity	No.1 byte coil status	…	No.N byte coil status
0x 01	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 Discrete Inputs (Function Code: 0x02)

Request PDU

Function code	Starting address		Quantity	
	High byte	Low byte	High byte	Low byte
0x 02	xx	xx	xx	xx

Response PDU

Function code	Byte quantity	Register 1	…	Register N
0x 02	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
0x 03	xx	xx	xx	xx

Response PDU

Function code	Byte quantity	Register 1		…		Register N	
		High byte	Low byte	…	…	High byte	Low byte
0x 03	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
0x 04	xx	xx	xx	xx

Response PDU

Function code	Byte quantity	Register 1		…		Register N	
		High byte	Low byte	…	…	High byte	Low byte
0x 04	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 Write Single Coil (Function Code: 0x05)

Request PDU

Function code	Register address		Register setting value	
	High byte	Low byte	High byte	Low byte
0x 05	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 Write Single Holding Register (Function Code: 0x06)

Request PDU

Function code	Register address		Register setting value	
	High byte	Low byte	High byte	Low byte
0x 06	xx	xx	xx	xx

Response PDU

Function code	Register address		Register setting value	
	High byte	Low byte	High byte	Low byte
0x 06	xx	xx	xx	xx

A.3.7 Write Multiple Holding 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

WRWF-1501-06338-01 005