KSTAR KSG1-60K Inverter

Modbus RS485 Communications Protocol V1.8

1. Introduction to the Modbus Protocol

1.1. Overview

This document formulates the communication standard between Kstar KSG1K-60K power system and the PC. This standard is a subset of the Modbus protocol. The Modbus protocol is not described in this document. For details, see the Modbus RTU protocol available at www.modicon.com.

1.2. Communications Port

The RS485 serial port is used.

Information is transmitted in asynchronous mode, which involves 1 start bit, 8 data bits, 1 stop bit, and no parity bit.

Multiple baud rates are supported for data transmission, 2400 bps, 4800 bps and 9600 bps, with 9600 bps as the default rate.

Data is transmitted in big-endian mode. For example, if 0x1234 is to be transmitted, 0x12 is transmitted first and then 0x34.

1.3. Communications Mode

The PC (host) communicates with the inverter (client) in simplex mode. A maximum of 32 clients can be connected to the RS485 bus. The host polls each client. If a client does not respond or if the host receives a response error message, the host considers that the communication fails.

2. Frame

2.1. Frame Format

Endian	0	1	N	N+1	N+2
Byte count	1	1		2	
Content	Client address	Function code	Data domain	Checksum	
Format	ID	FUNC	ADDR	CRC	

2.2. Frame Description

2.3.1 ID

The range of the client address is 0–32. 0 is a broadcast address. The client address is unique on the Modbus.

2.3.2 FUNC

Function codes

Function Code	Description
0x03	Read keep register for querying inverter information.
0x04	Read input register for querying inverter information.
0x06	Single write register for executing remote instructions.

Error codes

Error Code	Description
0x01	Invalid function code
0x02	Invalid data address
0x03	Invalid value
0x06	The instruction is valid because the client is busy.

2.3.3 CRC

The host or client can verify whether received information is correct by using the CRC. Due to electric noise on the bus or other types of interference, errors may occur when information is being transmitted. To address this issue, the recipient can verify whether received information is correct by using the CRC and drop incorrect frames, thus improving the security and reliability of the communication system.

The CRC of Modbus contains two bytes, namely, 16 bits. The sender calculates the CRC and appends it to the information frame. The recipient recalculates the CRC for all received information (including the received CRC) and checks whether the CRC is 0. If so, the received information frame is correct. Otherwise, the received information frame is incorrect.

Only 8 data bits are used for CRC calculation. The start bit and stop bit are excluded from CRC calculation.

- The procedure for calculating the CRC code is as follows:

1. Preset a 16-bit register to FFFF (containing 1 only) in hexadecimal format. This register is called CRC register.
2. Perform an exclusive OR operation for the first 8 bits (the first byte of the information frame) and the lower 8 bits of the 16-bit CRC register. Then store the result in the CRC register.
3. Move the content of the CRC register rightwards by one bit and add a 0 as the most significant

bit. Then check the evicted bit.

4. If the evicted bit is 0, repeat step 3 (move the content of the CRC register rightwards by one bit again).

If the evicted bit is 1, perform an exclusive operation for the CRC register and polynomial A001 (1010 0000 0000 0001).

5. Repeat steps 3 and 4 to move the content of the CRC register rightwards for 8 times so that all 8 bits are processed.

6. Repeat steps 2 through 5 to process the next byte of the information frame.

7. After processing all bytes of the information frame, exchange the most significant and least significant bytes of the 16-bit CRC register.

8. The content of the CRC register is the CRC code.

3. Inverter Information Address Table

3.1. Basic Inverter Information (04H Telemetry)

Table 3.1.1

Register Address	Item	Byte	Byte No.	Unit	Data Type	Remarks	FUNC
3000	PV1 input voltage	2	0	0.1V	U16		04H
3001	PV2 input voltage	2	2	0.1V	U16	1-3K not have.	04H
3002	PV3 input voltage	2	4	0.1V	U16	1-5K not have.	04H
3003	PV input current	2	6	0.01A	U16		04H
3004	PV2 input current	2	8	0.01A	U16	1-3K not have.	04H
3005	PV3 input current	2	10	0.01A	U16	1-5K not have.	04H
3006	PV1 input power	4	12	1W	S32		04H
3007							04H
3008	PV2 input power	4	16	1W	S32	1-3K not have.	04H
3009							04H
3010	PV3 input power	4	20	1W	S32	1-5K not have.	04H
3011							04H
3012	PBUS voltage	2	24	0.1V	U16		04H
3013	NBUS voltage	2	26	0.1V	U16	1-5K not have.	04H

3014	RS-phase grid voltage	2	28	0.1V	U16		04H
3015	ST-phase grid voltage	2	30	0.1V	U16	1-5K not have.	04H
3016	TR-phase grid voltage	2	32	0.1V	U16	1-5K not have.	04H
3017	RS-phase grid frequency	2	34	0.01Hz	U16		04H
3018	ST-phase grid frequency	2	36	0.01Hz	U16	1-5K not have.	04H
3019	TR-phase grid frequency	2	38	0.01Hz	U16	1-5K not have.	04H
3020	R-phase grid-tied current	2	40	0.01A	U16		04H
3021	S-phase grid-tied current	2	42	0.01A	U16	1-5K not have.	04H
3022	T-phase grid-tied current	2	44	0.01A	U16	1-5K not have.	04H
3023	Grid-tied power	4	46	1W	S32		04H
3024							04H
3025	Radiator temperature	2	50	0. 1℃	U16		04H
3026	Module temperature	2	52	0. 1℃	U16	1-5K not have.	04H
3027	DSP alarm code	2	54		U16	Table 3.1.2	04H
3028	DSP error code	4	56		U32	Table 3.1.3	04H
3029							04H
3030	Operating mode of the inverter	1	60		U8	Table 3.1.4	04H
	Inverter model	1	61		U8	Table 3.1.5	04H
3031	Rotational speed of fan A	2	62	r/min	U16		04H
3032	Rotational speed of fan B	2	64	r/min	U16	1-5K not have.	04H
3033	Rotational speed of fan C	2	66	r/min	U16	1-5K not have.	04H
3034	Total energy yield	4	68	0.1Kwh	U32		04H
3035							04H
3036	ARM alarm code	1	72		U8	Table 3.1.6	04H
	ARM error code	1	73		U8	Table 3.1.7	04H

3037	Input mode	1	74		U8	Table 3.1.8	04H
	Mains standard	1	75		U8	Table 3.1.9	04H
3038	Total energy yield	4	76	0.1Kwh	U32		04H
3039							04H
3040	Annual energy yield	4	80	Kwh	U32		04H
3041							04H
3042	Daily energy yield	2	84	Kwh	U16		04H
3043	Power-on voltage	2	86	0.1V	U16	2500-8500	04H
3044	Power-on delay	2	88	S	U16	30-300	04H
3045	Lower grid voltage threshold	2	90	0.1V	U16	1500-2100	04H
3046	Upper grid voltage threshold	2	92	0.1V	U16	2300-2800	04H
3047	Lower grid frequency threshold	2	94	0.01Hz	U16	4950-4980	04H
3048	Upper grid frequency threshold	2	96	0.01 Hz	U16	5020-5050	04H
3049	Preset power factor	2	98		U16	Table 3.4.2	04H
3050	Preset active power	2	100	%	U16	Table 3.4.3	04H
3051	Preset reactive power	1	102	1KVar	S8	Table 3.4.4	04H
	Reactive control mode	1	103		U8	Table 3.4.5	04H
3052	Apparent power	4	104	1VA	S32		04H
3053							
3054	Reactive power	4	108	1Var	S32		04H
3055							
3056	Power factor	2	112		U16	Table 3.4.2	04H
3057	DC insulation resistance	2	114	Kohm	U16	1-5K not have.	04H
3058	Overfrequency derating	2	116			0: enabled 1: disabled	04H
3059	Overfrequency derating threshold	2	118			Table 3.4.7	04H
3060	High voltage of the QV curve	2	120			Table 3.3.3	04H
3061	High-voltage power	2	122			Table 3.3.3	04H

	factor of the QV curve						
3062	Low voltage of the QV curve	2	124			Table 3.3.3	04H
3063	Low-voltage power factor of the QV curve	2	126			Table 3.3.3	04H

Note:

The U16 data type indicates an unsigned 16-digit number and S16 indicates a signed 16-digit number.

The 04H function code indicates hexadecimal number 04.

Table 3.1.2

SN	Content	Code	Description
0	Bit0	W00	FanA Lock
1	Bit1	W01	FanB Lock
2	Bit2	W02	FanC Lock
3	Bit3	W04	Zero Power
4	Bit4	W05	Array Warning

Table 3.1.3

SN	Content	Code	Description
0	Bit0	F00	Grid Volt Low
1	Bit1	F01	Grid Volt High
2	Bit2	F02	Grid Freqecncy Low
3	Bit3	F03	Grid Freqency High
4	Bit4	F04	Bus Volt Low
5	Bit5	F05	Bus Volt High
6	Bit6	F06	Bus Volt Unbalance
7	Bit7	F07	Isolation Fault
8	Bit8	F08	PV Current High
9	Bit9	F09	Hard Inverter Current Over

10	Bit10	F10	Inverter Current Over
11	Bit11	F11	Inverter Dc Currernt Over
12	Bit12	F12	Ambient Temperature Over
13	Bit13	F13	Sink Temperature Over
14	Bit14	F14	AC Relay Fault
15	Bit15	F15	Reserve
16	Bit16	F16	Remote Off
17	Bit17	F17	reserve
18	Bit18	F18	SPI Communication Fail
19	Bit19	F19	reserve
20	Bit20	F20	GFCI Over Fault
21	Bit21	F21	GFCI Device Fault
22	Bit22	F22	Voltage Consistent Fault
23	Bit23	F23	Frequency Consistent Fault
24	Bit24	F24	reserve
25	Bit25	F25	reserve
26	Bit26	F26	reserve
27	Bit27	F27	reserve
28	Bit28	F28	reserve
29	Bit29	F29	reserve
30	Bit30	F30	reserve
31	Bit31	F31	reserve

Table 3.1.4

SN	Content	Description
0	00H	System initialization
1	01H	Waiting
2	02H	Pre-detection
3	03H	Normal
4	04H	Error
5	05H	Permanent error
6	06H	Aging
7	07H	DSP Burning
8	08H	ARM Burning

Note: when the inverter is in the system initialization, the communication data is invalid data.

Table 3.1.5

SN	Content	Description
0	00H	KSG1KSM3
1	01H	KSG1.5KSM3
2	02H	KSG2KSM3
3	03H	KSG3KSM3
4	04H	KSG3.2KDM3
5	05H	KSG4KDM3
6	06H	KSG5KDM3
7	07H	KSG6KDM3/KSG10K
8	08H	KSG12.5K
9	09H	KSG15K
10	0AH	KSG17K
11	0BH	KSG20K
12	0CH	KSG30K
13	0DH	KSG40K
14	0EH	KSG50K
15	0FH	KSG60K
16	14H	KSG25KHV
17	15H	KSG36KHV
18	16H	KSG50KHV
19	17H	KSG60KHV

Note: 07H single phase model is KSG6KDM3, three-phase model is KSG10K;

Table 3.1.6

SN	Content	Code	Description
0	Bit0	W16	Clock Warning
1	Bit1	W17	Fan4 Lock
2	Bit2	W18	Fan5 Lock
3	Bit3	W19	Fan7 Lock
4	Bit4	W20	Fan8 Lock
5	Bit5	W21	Lighting Warning

Table 3.1.7

SN	Content	Code	Description
0	Bit 0	F32	Error in communication with the DSP

Table 3.1.8

SN	Content	Input Mode
0	00H	Independent mode
1	01H	Parallel mode
2	02H	Hybrid mode

Table 3.1.9

		10-60K	1-6K
SN	Content	Grid Connection Standard	Grid Connection Standard
0	00H	China	China
1	01H	German	German
2	02H	Australia	Australia
3	03H	Italy	Italy
4	04H	Spain	Spain
5	05H	Britain	Britain
6	06H	Hungary	Hungary
7	07H	Belgium	Belgium
8	08H	Western Australia	Western Australia
9	09H	Greece	Greece

10	0AH	France	France
11	0BH	Bangkok	Bangkok
12	0CH	Thailand	Thailand
13	0DH	Plant	Local
14	0EH	Local	60 Hz
15	0FH	60 Hz	Not have.

3.2. Inverter System Information (03H)

Table 3.2.1

Register Address	Item	Byte	Byte No.	Data Type	Remarks	FUNC
3200-3204	Machine model	10	0	U8	ASCII code	03H
3205	DSP version	1	10	U8	10 indicates V1.0.	03H
	ARM version	1	11	U8	10 indicates V1.0.	03H

3.3. Inverter Setup (10H)

Table 3.3.1

Register Address	Item	Byte	Byte No.	Data Type	Remarks	FUNC
3300-3306	Clock information	14	0	U8	Table 3.2.2	10H
3307-3310	QV reactive curve	8	14	U16	Table 3.2.3	

Note: When setting information, write the address at a time. For example, write clock setup information into register addresses 3300 to 3306 at a time.

Table 3.3.2

Register Address	Item	Byte	Byte No.	Data Type	Remark
3300	Year (tens place)	1	0	U8	ASCII code
	Year (ones place)	1	1	U8	ASCII code
3301	Month (tens place)	1	2	U8	ASCII code
	Month (ones place)	1	3	U8	ASCII code
3302	Day (tens place)	1	4	U8	ASCII code
	Day (ones place)	1	5	U8	ASCII code
3303	Hour (tens place)	1	6	U8	ASCII code
	Hour (ones	1	7	U8	ASCII code

	place)				
3304	Minute (tens place)	1	8	U8	ASCII code
	Minute (ones place)	1	9	U8	ASCII code
3305	Second (tens place)	1	10	U8	ASCII code
	Second (ones place)	1	11	U8	ASCII code
3306	Week	1	12	U8	ASCII code
		1	13	U8	ASCII code

Table 3.3.3

Register Address (W/R)	Content	Value Range	Description
3307/3058	High voltage V1 of the QV curve	2400 – 2800	If the mains phase voltage (LN) changes from 240 V to V1, the reactive power changes from 0 to Q1 gradually.
3308/3059	High-voltage reactive power percent(Q1) of the QV curve	Table 3.4.4	If the mains phase voltage (LN) is higher than V1, the reactive power factor remains Q1.
3309/3060	Low voltage V2 of the QV curve	1500–2100	If the mains phase voltage (LN) changes from 210 V to V2, the reactive power changes from 1 to Q2 gradually.
3310/3061	Low-voltage reactive power percent(Q2) of the QV curve	Table 3.4.4	If the mains phase voltage (LN) is lower than V2, the reactive power remains Q2.

3.4. Instruction Execution (06H Telemetry)

Table 3.4.1

Register Address	Item	Byte	Byte No.	Unit	Data Type	Remarks	FUNC
4000	Clear statistical information	2	0		U16	DATA arbitrary number	06H
4001	Remote power-off	2	2		U16	DATA arbitrary number	06H
4002	Revoke remote power-off	2	4		U16	DATA arbitrary number	06H
4003	Set the power factor	2	6		U16	Table 3.4.2	06H
4004	Set the active power	2	8	%	U16	Table 3.4.3	06H
4005	Set the reactive power	2	10	1KVar	S16	Table 3.4.4	06H
4006	Set the reactive control mode	2	12		U16	Table 3.4.5	06H
4007	Overfrequency derating	2	14		U16	0: enabled 1: disabled	06H
4008	Overfrequency derating threshold	2	16	0.01Hz	U16	Table 3.4.6	06H

Note: Only the instruction of setting broadcast address 0 can be executed.

Table 3.4.2

Value Range	Description
800-1000	If the reactive power is negative, the power factor ranges from 0.8 to 1.
10800-11000	If the reactive power is positive, the power factor ranges from 0.8 to 1.

0xFFFF	Cancel power factor control (default power factor: 1)

Table 3.4.3

Value Range	Description
0-100	Maximum percentage of rated power

Table 3.4.4

Value Range	Description
-60 - +60	Set the reactive power (%). The acceptable maximum reactive power is +/- 60%

Table 3.4.5

Value Range	Description
0	Control based on the power factor
1	Control based on the reactive power
2	Control based on the QV curve

Table 3.4.6

Value Range	Description
5020 – 6500	1. If the mains frequency reaches this threshold, the current power of the inverter is locked, which is P_{frozen} . 2. If the mains frequency exceeds this threshold, the power decreases based on 40% * P_{frozen} / HZ.

4. Examples

4.1. Querying Basic Information

Read the input register. The start address is 3000 and the length is 1 unit (2 bytes).

Host

Endian	0	1	2	3	4	5	6	7
Content	01	04	0B	B8	00	01	B3	CB
Format	ID	FUNC	ADDR		DATA	DATA	CRC	

Client

Endian	0	1	2	3	4	6	7
Content	01	04	02	00	65	79	1B
Format	ID	FUNC	BYTE LEN	DATA	DATA	CRC	

4.2. Querying System Information

Read the keep register. The start address is 3200 and the length is 1 unit (2 bytes).

Host

Endian	0	1	2	3	4	5	6	7
Content	01	03	0C	80	00	01	86	B2
Format	ID	FUNC	ADDR		DATA	DATA	CRC	

Client

Endian	0	1	2	3	4	6	7
Content	01	03	02	4B	53	CE	89
Format	ID	FUNC	BYTE LEN	DATA	DATA	CRC	

4.3. Setting the Clock of the Inverter

Set the clock of the inverter to 2010-11-02 14:30:00 Tuesday.

Host

Endian	0	1	2	3	4	5	6	7
Content	01	10	0C	E4	00	07	0E	31
Format	ID	FUNC	ADDR		REGISTER QUANTITY		BYTE COUNT	DATA

Endian	8	9	10	11	12	13	14	15
Content	30	31	31	30	32	31	34	33
Format	DATA	DATA	DATA	DATA	DATA	DATA	DATA	DATA

Endian	16	17	18	19	20	21	22
Content	30	30	30	32	00	F2	AA
Format	DATA	DATA	DATA	DATA	DATA	CRC	

Host

Endian	0	1	2	3	4	5	6	7
Content	01	10	0C	E4	00	07	AC	C2
Format	ID	FUNC	ADDR		DATA	DATA	CRC	

4.4. Executing Remote Instructions

Maximum rated power: 85%

Host

Endian	0	1	2	3	4	5	6	7
Content	01	06	0F	A4	00	55	0B	02

Format	ID	FUNC	ADDR	DATA	DATA	CRC

Client

Endian	0	1	2	3	4	5	6	7
Content	01	06	0F	A4	00	55	0B	02
Format	ID	FUNC	ADDR		DATA	DATA	CRC	