

IST230A-485 communication protocol

一、 IST230A communication data can be divided into functional code data, non-functional code data, the latter includes running commands, running status, running parameters, alarm information and so on.

I.1 IST230A Functional code data

The function code data is the important setting parameter of the frequency converter, as follows:

IST230A Functional code data	Group P (readable)	P0、 P1、 P2、 P3、 P4、 P5、 P6、 P7、 P8、 P9、 PA、 PB
	Group A (readable)	A0、 A1、 A2、 A5、 A6、 A7、 A8、 A9、 AA、 AB、 AC

The function code data communication address is defined as follows: 1.
When reading the function code data for communication,
for the communication address of the P0 – PF, A0 – AF, group function
code data high 16 bits is the function group number and the low 16 bits

is the function code sequence number in the function group. Examples are as follows:

1) P0-16 functional parameters, whose communication address is F010H, where F0H represents the functional parameters of P0 group, and 10H represents the hexadecimal data format of the serial number 16 of the function code in the functional group.

2) AC-08 functional parameters, whose communication address is AC08, where ACH represents the functional parameters of AC group, and 08H represents the hexadecimal data format of the serial number 8 of the function code in the functional group.

2 When writing function code data for communication

For the function code data of P0 – PF group, the communication address is 16 bits higher, which is divided into 00 – 0F or F0 – FF according to whether the EEPROM is written, and the low 16 bits are the serial number of the function code in the function group. Examples are as follows.

1) Write function parameter P0-16

When you do not need to write to EEPROM, its communication address is 0010H.

When you need to write to EEPROM, its communication address is F010H.

For A0 – AF group function code data, the communication address is high 16 bits. According to whether to write to EEPROM, it is divided into 40 – 4F or A0 – AF, and the low 16 bits are the serial number of the function code in the function group.

2) Write function parameter AC-08

When you do not need to write to EEPROM, its communication address is 4C08H.

When you need to write to EEPROM, its communication address is AC08H.

1.2 IST230A non-functional code data

IST230A non-functional code data	Status data (read-only)	U Group monitoring parameters, frequency converter fault
----------------------------------	-------------------------	--

		description, frequency converter operating status
	Control parameters (write only)	Control command, communication setting value, digital output terminal control, analog output AO1 control, analog output AO2 control, high speed pulse (output control, parameter initialization)

1. status data

The status data is divided into U group monitoring parameters, frequency converter fault description, frequency converter operation status.

1) U-group parameter monitoring parameters

U-Group the data description of group monitoring is described in Chapter 5, Chapter 6, and its address is defined as follows: U0 – UF, and its address is as follows: The high 16 bits address is 70–7F, and the low 16 bits is the serial number of the monitoring parameter in the group. For example, the following U0 – 11. Its communication address is 700BH.

2) Frequency converter fault description

When the communication reads the frequency converter fault description, the communication address is fixed to 8000H, and the upper computer can obtain the current frequency converter fault code by reading the address data. The fault code description is defined in Chapter 5 F9–14 function code.

3) Operation state of frequency converter

When the communication reads the running state of the frequency converter, the communication address is fixed to 3000H, and the upper computer reads the address data by reading the address data, you can get the current frequency converter running status information, defined as follows:

Frequency converter operating status	Read status definition
---	------------------------

communication address	
3000H	1: forward running
	2: reverse running
	3: stop

2. Control parameters

The control parameters are divided into control command, digital output terminal control, analog output AO1 control, analog output AO2 control, high speed pulse (output control).

1) Control command

When F0-02(command source) is selected as 2: communication control, the upper computer can control the frequency converter start-stop and other related commands through the communication address. The control command is defined as follows:

Control command communication address	command function
2000H	1: forward running
	2: reverse running
	3: forward jog

	4: reverse jog
	5: free stop
	6: deceleration stop
	7: fault reset

2) Communication setting value

The frequency source, torque upper limit source, VF separated voltage source, PID given source, PID feedback source and so on are selected as the given data of communication timing in SKI780. The communication address is 1000H, and when the communication address value is set by the upper computer, the data range is -10000 - 10000, and the corresponding relative given value is -100.00% - 100.00%.

3) Digital output terminal control.

When the digital output terminal function is selected as 20: During communication control, the upper computer can realize the control of digital output terminal of frequency converter through the communication address. Defined as follows:

Digital output terminal control communication address	Command content
2001H	BIT0 : DO1 output control

	BIT1 : DO2 output control BIT2 : RELAY1 output control BIT3 : RELAY2 output control BIT4 : FMR output control BIT5 : VDO1 BIT6 : VDO2 BIT7 : VDO3 BIT8 : VDO4 BIT9 : VDO5
--	---

4) Analog output AO1, AO2, high-speed pulse output FMP control

when analog output AO1, AO2, high-speed pulse output FMP output function is 12: when the communication setting, the upper computer can realize the control of frequency converter analog and high-speed pulse output, the definition is as follows:

Output control communication address		Command content
AO1	2002H	0 ~ 7FFF shows 0% ~ 100%
AO2	2003H	
FMP	2004H	

5) Parameter initialization

When it is necessary to initialize the parameters of frequency converter through the upper computer, this function needs to be used.

If FP-00 (user password) is not 0, the password is first required to be verified by the communication, and after the check is passed, The upper computer performs the parameter initialization operation within 30 seconds.

The communication address for user password verification is 1F00H. If the correct user password is written directly to this address, password verification can be completed.

The address where the communication initializes the parameter is 1F01H, and its data content is defined as follows:

Parameter initialization address	Command function
1F01H	1: Restore factory parameters
	2: Clear record information
	4: Restore user backup parameters
	5: Backing up the user's current parameters

二. IST230A Modbus communication protocol

SKI780 series frequency converter provides RS485 communication interface and supports Modbus-RTU slave communication protocol.

The user can realize centralized control through computer or PLC, set the running command of frequency converter through this communication protocol, modify or read the function code parameters, read the working state and fault information of frequency converter, and so on.

2.1 Protocol content

The serial communication protocol defines the information content and use format transmitted in serial communication. This includes host polling(or broadcast) format; Encoding method of host, including: function code requiring action, transmitting data and error checking. etc. The response of the slave machine also adopts the same structure, including action confirmation, return data and error check. If an error occurs while receiving information from the slave or fails to complete the required action of the host, it will organize a fault message. The interest is fed back to the host in response.

2.1.1 Application method

The converter is connected to the single master multi-slave PC/PLC control network with RS485 bus as the communication slave.

2.1.2 Bus configuration

1. Hardware interface

Need to insert RS485 extension card MD38TX1 into frequency converter.

2. Topology single host multi-slave system. Each communication

device in the network has a unique slave site, in which a device acts as a communication host (often a flat PC upper computer, PLC, HMI, etc.), actively initiates communication, reads or writes parameters to the slave, and other devices are responding to the host computer's inquiry or communication operation for the communication slave.

Only one device can send data at the same time, while other devices are in the receiving state. The setting range of slave address is 1 – 247, 0 is broadcast communication address. The slave address in the network must be unique.

3. The communication transmission mode is asynchronous serial and half-duplex transmission mode. the data is in the form of a message in the serial asynchronous communication process, Send one frame at a time According to the MODBUS-RTU protocol, the idle time of no data on the communication data line is bigger than 3.5 Byte's

transmission time, indicating the start of a new communication frame.

IST230A The communication protocol built-in of the series frequency converter is that the communication protocol of the Modbus-RTU slave can be in response to the host "The query/command" or the corresponding action is made according to "the query/command" of the host, and the communication data is answered. the host may refer to a personal computer (PC), industrial control equipment, or programmable logic controller (PLC), etc. The host not only can communicate with a certain slave, but also can issue the broadcast information to all the subordinate slaves. For the single unit of the host one-to-one visit a "query command" that is accessed from the machine to return an answer frame; for broadcast information sent by the host, from The machine does not need to feed back the response to the host.

2.2 Communication data structure

The Modbus protocol communication data format of SKI780 series inverter is as follows: the converter only supports the reading or writing of Word parameters, and the corresponding communication reading operation command is 0x03. The write operation command is

0x06, which does not support the read and write operation of bytes or bits. In theory, the upper computer can read several consecutive function codes at a time (that is, the maximum n can reach 12), but note that it can not cross the last function code of the function code group, otherwise the answer will be wrong.

If a communication frame error is detected from the slave computer, or if reading and writing is unsuccessful for other reasons, the error frame is answered.

1. Data frame field description:

Frame header START	Idle slave with a transmission time of more than 3.5 bytes.
Slave address ADR	Communication address range: 1–247; 0 = broadcast address
Command code CMD	03: read slave parameter 06: write slave parameter
Function code address H	The internal parameter address of the frequency converter, hexadecimal representation, divided into functional code type and non-functional code type
Function code address L	

	<p>(such as running state parameters, running commands, etc.) parameters, etc. See the definition of address for details.</p> <p>When transmitting, high bytes are in front and low bytes are in the back.</p>
Function code number H	<p>The number of function codes read by this frame, if 1 means reading 1 function code. When transmitting, high bytes are in front and low bytes are in the back. This agreement can only rewrite one function code at a time, without this field.</p>
Function code number L	
Data H	<p>Answered data, or data to be written, is transmitted with high bytes in front and low bytes in the back.</p>
Data L	
CRC CHK low bit	<p>Detection value: CRC16 check value. At the time of transmission, the low bytes are in</p>
CRC CHK high bit	

	front and the high bytes are in the back. The calculation method is detailed in the instructions for CRC verification in this section.
END	When it is 3.5 bytes

2. CRC verification mode

CRC(Cyclical Redundancy Check) uses RTU frame format, and the message includes error detection domain based on CRC method. The CRC domain detects the contents of the entire message. The CRC domain is a two-byte binary value containing 16 bits, which is calculated by the transmission device and added to the message. The receiving device recalculates the CRC of the received message and compares it with the value in the received CRC domain. If the two CRC values are not equal, the transmission is incorrect. CRC is first stored in 0xFFFF, and then a procedure is called to process the continuous 8-bit bytes in the message with the value in the current register. Only 8 Bit data in each character is valid for CRC, and the start and stop bits, as well as parity bits, are not valid. In the process of CRC generation, each 8-bit character is different from the contents of the register or the (XOR) result is inversely different from the lowest valid bit, if LSB is 0, it does not. The whole process is repeated eight times. After the

last bit (bit 8) is complete, the next 8-bit byte is separate from the current value of the register. The value in the final register is the CRC value after all the bytes in the message are executed. When CRC is added to the message, low bytes are added first, and then high bytes.

Address definition of communication parameters

Read and write function code parameters (some function codes cannot be changed, only for manufacturer use or monitoring use):

2.3 Functional code parameter address marking rules

The rule is represented by functional code group number and label as parameter address:

high bit byte: F0 – FF (P group), A0 – AF (A group) 70 – 7F (U group)

low bit byte: 00 – FF

for example: if you want the range function code F3 – 12, the access address of the function code is represented as 0xF30C note:

1) Group PF: neither the parameters could be read nor the parameters could be changed.

2) Group U: parameters can only be read and cannot be changed.

Some parameters can not be changed when the frequency converter is running; some parameters can not be changed regardless of the state of the frequency converter, but also pay attention to the range of parameters, units, and related instructions.

Function code group number	Communication access address	communication modification Function code address in RAM
P0 ~ PE Group	0xF000 ~ 0xFEFF	0x0000 ~ 0x0EFF
A0 ~ AC Group	0xA000 ~ 0xACFF	0x4000 ~ 0x4CFF
U0 Group	0x7000 ~ 0x70FF	none

note that, due to the fact that EEPROM is frequently stored, reducing the life of the EEPROM, so some features code in communication In the mode, no storage is required, as long as the value in the RAM is changed.

- 1) If it is a P group parameter, in order to realize this function, it can be realized by turning the high bit F of the function code address into 0.
- 2) If it is a A group parameter, in order to realize this function, it can be realized by turning the high bit A of the function code address

into 4. The corresponding function code address is represented as follows:

High bit bytes: 00~0F(P group), 40~4F(A group)

Low bit bytes: 00 – FF

Example:

functional code P3 – 12 is not stored in EEPROM, the address is represented as 030C;

functional code A0–05 is not stored in EEPROM, the address is represented as 4005;

This address indicates that you can only write to RAM, can not do read action, if read, then invalid address.

The command code can also be used for all parameters 07H.

The data is given by the host computer through the communication address 0x1000. The data format is the data with 2 decimal points, and the data range is -F0-10 – F0-10.

1. Stop/Start operation parameters:

Parameter address	Parameter description	Parameter address	Parameter description
----------------------	--------------------------	----------------------	--------------------------

1000H	*Communication setting value (decimal system) -10000 - 10000	1010H	PID set
1001H	Running frequency	1011H	PID feedback
1002H	Busbar voltage	1012H	PLC process
1003H	Output voltage	1013H	Pulse input frequency, unit: 0.01kHz
1004H	Output current	1014H	Feedback speed, unit 0.1Hz
1005H	Output power	1015H	Remaining run time
1006H	Output torque	1016H	AI1 Pre- correction voltage
1007H	Running speed	1017H	AI2 Pre- correction voltage

1008H	DI input sign	1018H	AI3 Pre- correction voltage
1009H	DO output sign	1019H	Linear speed
100AH	AI1 voltage	101AH	Current power on time
100BH	AI2 voltage	101BH	Current running time
100CH	AI3 voltage	101CH	Pulse input frequency, unit: 1Hz
100DH	Count value input	101DH	Communication set value
100EH	Length value input	101EH	Actual feedback speed
100FH	Loading speed	101FH	Main frequency X display
		1020H	Auxiliary frequency Y display

Note:

1) The communication setting value is the percentage of the relative value, and 10000 corresponds to 100.00%, -10000 corresponds to -100.00%.

2) For the data of frequency dimension, the percentage is the percentage of relative maximum frequency rate ($F0 - 10$), and for the data of torque dimension, the percentage is $F2 - 10$ and $A2 - 48$ (torque upper limit number setting, corresponding to the first and second motors, respectively).

2. Input control command into frequency converter: (write only)

Command address	Command function
2000H	0001: forward run
	0002: reverse run
	0003: forward jog
	0004: reverse jog
	0005: free stop
	0006: deceleration stop
	0007: fault reset

3. Read frequency converter status: (read only)

Status address	Status function
3000H	0001: forward run

	0002: reverse run
	0003: stop

4. Parameter lock password check: (if returned to 8888H, it means that the password check passed)

Password address	Password content
1F00H	*****

5. Digital output terminal control: (write only)

Command address	Command content
2001H	BIT0: DO1 output control BIT1: DO2 output control BIT2: relay1 output control BIT3: relay2 output control BIT4: FMR output control BIT5: VDO1 BIT6: VDO2 BIT7: VDO3 BIT8: VDO4 BIT9: VDO5

6. Analog output AO1 control: (write only)

Command address	Command content
2002H	0 – 7FFF means 0% – 100%

7. Analog output AO2 control: (write only)

Command address	Command content
2003H	0 – 7FFF means 0% – 100%

8. Pulse output control: (write only)

Command address	Command content
2004H	0 – 7FFF means 0% – 100%

9. Fault description of frequency converter.

Fault address	Fault information	Fault information
8000H	0000 : no fault 0001 : reserve 0002 : overcurrent	0015 : Parameter reading and writing abnormal

	during acceleration	0016 : hardware fault
	0003 : overcurrent	0017 : Short circuit
	during deceleration	fault of motor to
	0004 : overcurrent	ground
	during constant speed	0018 : reserve
	0005 : overvoltage	0019 : reserve
	during acceleration	001A : run time up
	0006 : overvoltage	001B : User custom
	during deceleration	failure 1
	0007 : overvoltage	001C : user custom
	during constant speed	failure 2
	0008 : Buffer	001D : Power on time
	resistance overload	up
	fault	001E : off load
	0009 : undervoltage	001F : Loss of PID
	fault	feedback at run time
	000A : frequency	0028 : Fast current
	converter overload	limit timeout fault
	000B : motor	0029 : Switching
	overload	motor fault at run
	000C : input lack	time
	phase	002A : The speed

	000D : output lack phase	deviation is too large
	000E : module overheating	002B : Motor overspeed
	000F : external fault	002D : motor overtemperature
	0010 : communication abnormal	005A : Encoder line number setting error
	0011 : Contactor abnormal	005B : Unconnected encoder
	0012 : Current detection fault	005C : Initial position error
	0013 : Motor tuning fault	005E : Speed feedback error
	0014 : Encoder / PG card failure	

2.4 Description of communication parameters of FD group

Fd-00	Baud rate	Factory value	6005
	Set range	The unit position: MODBUS baud rate	
		0 : 300BPS 1 : 600BPS	5 : 9600BPS 6 : 19200BPS

		2 : 1200BPS	7 : 38400BPS
		3 : 2400BPS	8 : 57600BPS
		4 : 4800BPS	9 : 115200BPS

This parameter is used to set the data transmission rate between the upper computer and the frequency converter. Note that the baud rate set by the upper computer and the frequency converter will The communication cannot proceed unless otherwise. The larger the baud rate, the faster the communication speed.

Fd-01	Data format	Factory value	0
	Set range	0 : No check: data format <8, N, 2> 1 : even check: data format <8, E, 1> 2 : odd check: data format <8, O, 1> 3 : No check: data format <8, N 1>	

The data format set by the upper computer and the frequency converter must be the same, otherwise, the communication can not be carried out.

Fd-02	Local address	Factory value	1
	Set range	1 – 247, 0 bit broadcast address	

When the local address is set to 0, that is the broadcast address, and the upper computer broadcasting function is realized. The local address has uniqueness (in addition to the broadcast address) is the basis for realizing point-to-point communication between the upper computer and the frequency converter.

Fd-03	Response delay	Factory value	2ms
	Set range	0 – 20ms	

Response time delay: refers to the intermediate time interval between the end of the data acceptance of the frequency converter and the sending data of the up-position machine. if that answer delay is less than the system processing time, the response time delay is processed by the system, The time shall be subject to the system processing if the response delay is longer than the system processing time. After the data is finished, the waiting is delayed until the response delay time is so as to send the data to the upper computer.

Fd-04	Communication timeout	Factory value	0.0s
	Set range	0.0s(invalid); 0.1 – 60.0s	

When the function code is set to 0.0s, the communication timeout time parameter is invalid. When the function code is set to a valid value, if the interval between one communication and the next communication exceeds the communication timeout time, the system reports fault error(Err16). Usually, it is set to be invalid. If in a continuous communication system, set parameters to monitor communication status.

Fd-05	communication protocol selection	Factory value	0
	Set range	0: non-standard Modbus protocol; 1: standard Modbus protocol	

Fd-05=1: Select the standard Modbus protocol.

Fd-05=0: When reading a command, the number of bytes returned from the slave is one more byte than the standard Modbus protocol, see the communication data structure section of this protocol 5.

Fd-06	Communication read current resolution	Factory value	0
-------	---	---------------	---

	Set range	0 : 0.01A ; 1 : 0.1A
--	-----------	----------------------

Used to determine the output unit of the current value when the communication reads the output current.

三. Actual use reference

Use 485 communication to control frequency, start, stop

3.1 Set P002 as 2, select communication command channel

Send control code: 01 06 F0 02 00 02 9A CB

3.2 Set P003 as 9, select communication set as main frequency source

Send control code: 01 06 F0 03 00 09 8A CC

3.3 Start

Send control code: : 01 06 20 00 00 01 43 CA

3.4 Set the running frequency as 10Hz and there are two decimal points, set the value to a high bit.

Send control code: 01 06 10 00 20 00 94 CA

3.5 Stop

Send control code: 01 06 20 00 00 06 02 08