SmartGen

MAKING CONTROL SMARTER

HAT560

ATS CONTROLLER

COMMUNICATION PROTOCOL

郑州众智科技股份有限公司
SMARTGEN(ZHENGZHOU)TECHNOLOGY CO.,LTD.

CONTENT

SmartGen Registered trademark
No. 28 Xuemei Street, Zhengzhou, Henan, China
Tel: +86-371-67988888/67981888/67992951
+86-371-67981000 (overseas)
Fax: +86-371-67992952
Web: www.smartgen.com.cn/
www.smartgen.cn/
Email: sales@smartgen.cn

Table 1 Software Version

Date	Version	Content
2015-06-10	V1.0	Original release.
2024-06-07	V1.1	1. Add the settings of communication stop bit and baud rate for HAT560NC/HAT560NBC; 2. Add some monitoring parameters.

1 DESCRIPTION

This protocol describes the controller RS485 half-duplex serial port's reading and writing command format, and the definition of internal information & data for the third-party to develop and use.

There is one RS485 port in HAT560NC/HAT560NBC ATS controller.

The controller works as a slave module, and uses Modbus-RTU protocol, but it doesn't support other protocols, such as Modbus-ASCII, etc.

HAT560NC/HAT560NBC communication configuration:

Communication address: 1~254 (Default: 1)
Baud rate: 9600/19200bps (Default: 9600bps)
Start bit: 1 bit
Data bit: 8 bits
Parity bit: no parity
Stop bit: 1 bit or 2 bits (Default: 2 bits)

HAT560N communication configuration:

Communication address: 1~254 (Default: 1)
Baud rate: 9600bps
Start bit: 1 bit
Data bit: 8 bits
Parity bit: no parity
Stop bit: 2 bits

Function code supported: 01H, 03H, and 05H. Function code 01H is used for reading controller's alarms and status information; Function code 03H is used for monitoring controller's electric parameters; Function code 05H is used for sending remote command.

Data checking method: CRC16.

The register data inside the controller are packed as two bytes per register.

Communication timeout period: over 200ms.

Transmission distance: At a baud rate of 9600bps, the maximum transmission distance can reach up to 1,000 meters with 120-ohm shielded twisted pair cable.

A maximum of 120 registers can be read per request.

It can support the communication of 32 networked controllers.

RS485 cabling must use 120-ohm shielded twisted pair cable, and one end of the shield should be grounded.

2 WIRING DIAGRAM

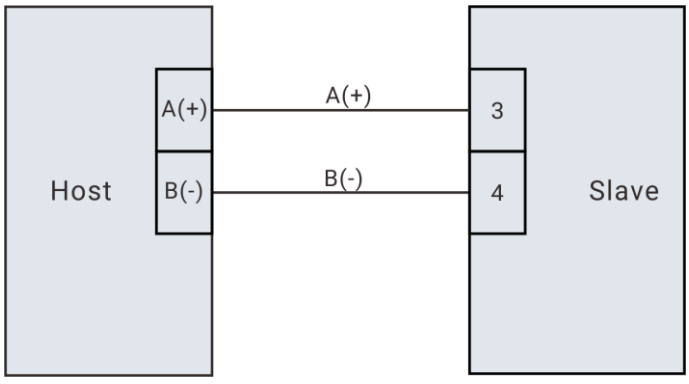

Fig. 1 Single Device Communication Wiring Diagram

3 CONTROLLER INTERNAL REGISTER ADDRESS AND DATA

In the table below, S1 refers to the first power supply, S2 refers to the second power supply, and the slash mark ("/") means the address is reserved.

3.1 FUNCTION CODE 01H MAPPING ALARM AND STATUS COIL

Table 2 Alarm and Status Coil

Modbus Address	PLC Address	Item	Description
0000H	1.0	S1 Switch Status	1: Close, 0: Open
0001H	1.1	S1 Volt Normal	1: Normal, 0: Abnormal
0002H	1.2	S2 Switch Status	1: Close, 0: Open
0003H	1.3	S2 Volt Normal	1: Normal, 0: Abnormal
0004H	1.4	Auto/Manual	1: Auto, 0: Manual
0005H	1.5	S1 Switch Prior	1: Master, 0: Backup
0006H	1.6	S2 Switch Prior	1: Master, 0: Backup
0007H	1.7	Gens Start Output Status	1: Start output, 0: Stop output
0008H	1.8	Serious Fault	1: Fault, 0: No Fault
0009H	1.9	S1 Switch Alarm	1 for active
000AH	1.1	S2 Switch Alarm	1 for active
000BH	1.11	S1 Close Failed	1 for active
000CH	1.12	S2 Close Failed	1 for active
000DH	1.13	S1 Open Failed	1 for active
000EH	1.14	S2 Open Failed	1 for active
000FH	1.15	Switch Transfer Fault	1 for active
0010H	2.0	Common Warning	1: Warning, 0: No Warning
0011H	2.1	S1 Over Volt	1: Over voltage, 0: Normal
0012H	2.2	S1 Under volt	1: Under voltage, 0: Normal
0013H	2.3	S1 Loss of Phase	1: Loss of Phase, 0: Normal
0014H	2.4	S2 Over Volt	1: Over voltage, 0: Normal
0015H	2.5	S2 Under volt	1: Under voltage, 0: Normal
0016H	2.6	S2 Loss of Phase	1: Loss of Phase, 0: Normal
0017H	2.7	/	
0018H	2.8	S1 Over Freq	1: Over frequency, 0: Normal
0019H	2.9	S1 Under Freq	1: Under frequency, 0: Normal
001AH	2.10	S2 Over Freq	1: Over frequency, 0: Normal
001BH	2.11	S2 Under Freq	1: Under frequency, 0: Normal
001CH	2.12	Common Alarm	1 for active
001DH	2.13	Delay Alarm Output	1 for active
001EH	2.14	Digital Input 1 Status	1 for active
001FH	2.15	S1 Volt Abnormal	1 for active
0020H	3.0	S2 Volt Abnormal	1 for active
0021H	3.1	S1 Gens Start	1 for active
0022H	3.2	S2 Gens Start	1 for active

Modbus Address	PLC Address	Item	Description
0023H	3.3	S1 Phase Seq Wrong	1 for active
0024H	3.4	S2 Phase Seq Wrong	1 for active
0025H	3.5	Digital 1 Output	1 for active
0026H	3.6	Digital 2 Output	1 for active
0027H	3.7	/	
0028H	3.8	/	
0029H	3.9	Digital Input 2 status	1 for active
002AH	3.10	Digital Input 3 status	1 for active
002BH	3.11	Digital Input 4 status	1 for active
002CH	3.12	Digital Output 3 Status	1 for active
002DH	3.13	Digital Output 4 Status	1 for active
002EH	3.14	Digital Output 5 Status	1 for active
002FH	3.15	Remote Start Input	1 for active
0030H	4.0	S1 Switch Prior Input	1 for active
0031H	4.1	S2 Switch Prior Input	1 for active
0032H	4.2	Forced Open	1 for active
0033H	4.3	/	
0034H	4.4	/	
0035H	4.5	S1 Genset Fault	1 for active
0036H	4.6	S2 Genset Fault	1 for active

EXAMPLE:

If “Auto/Manual” and “S1 Switch Prior” need to be read, check the table above and find their Modbus addresses are 4H, 5H and 7H, so it needs to read three data addresses.

Assuming the slave (controller) address is 01, the master or host (could be PC) request command is as following:

Table 3 Master (PC) Request Frame

Slave Address	Function Code	Start Address (505)		Request Data Length (2)		CRC 16	
		MSB	LSB	MSB	LSB	LSB	MSB
01	**01**	**00**	**00**	**00**	**08**	**3D**	**CC**

The slave response is as following:

Table 4 Slave (Controller) Response Frame

Slave Address	Function Code	Data Length (Bytes)	Data	CRC 16	
				LSB	MSB
01	**01**	**01**	**B0**	**50**	**3C**

Table 5 Data Analysis

Address	Data Received (Hex)	Convert to Binary	Meaning
00	B0H	10110000 (Mapping to 07H, 06H, 05H, 04H, 03H, 02H, 01H, 00H respectively)	Data of Bit 5 is 1, which means the controller is in Auto mode. Data of Bit 6 is 1, which means S1 switch has the priority. Data of Bit 8 is 1, which means the genset has started.

3.2 FUNCTION CODE 03H MAPPING PARAMETERS OF DATA FIELD

Table 6 Parameters of Data Field

Modbus Address	PLC Address	Item	Range (Decimal)	Ratio	Unit	Description	Remarks
0000H	40001	UAB1 (S1 Line A-B Voltage)	0~32760	1	V	16-bit Signed	
0001H	40002	UBC1 (S1 Line B-C Voltage)	0~32760	1	V	16-bit Signed	
0002H	40003	UCA1 (S1 Line C-A Voltage)	0~32760	1	V	16-bit Signed	
0003H	40004	UAB2 (S2 Line A-B Voltage)	0~32760	1	V	16-bit Signed	
0004H	40005	UBC2 (S2 Line B-C Voltage)	0~32760	1	V	16-bit Signed	
0005H	40006	UCA2 (S2 Line C-A Voltage)	0~32760	1	V	16-bit Signed	
0006H	40007	UA1 (S1 Phase A Voltage)	0~32760	1	V	16-bit Signed	NOTE 1
0007H	40008	UB1 (S1 Phase B Voltage)	0~32760	1	V	16-bit Signed	
0008H	40009	UC1 (S1 Phase C Voltage)	0~32760	1	V	16-bit Signed	
0009H	41010	UA2 (S2 Phase A Voltage)	0~32760	1	V	16-bit Signed	
000AH	41011	UB2 (S2 Phase B Voltage)	0~32760	1	V	16-bit Signed	
000BH	41012	UC2 (S2 Phase C Voltage)	0~32760	1	V	16-bit Signed	
000CH	41013	/					
000DH	41014	/					
000EH	41015	/					
000FH	41016	Frequency 1 (S1 Frequency)		0.1	Hz	16-bit Signed	NOTE 2
0010H	41017	Frequency 2 (S2 Frequency)		0.1	Hz	16-bit Signed	
0011H	41018	/					
0012H	41019	/					
0013H	41020	/					

NOTE 1：If the data received is 00DCH, it means the voltage is 220V.

NOTE 2：Actual value = data received * ratio. Take the Frequency as the example: if the data received is 500 (01F4H), ratio is 0.1Hz, then the actual frequency value is 50.0Hz (500*0.1Hz).

3.3 FUNCTION CODE 05H MAPPING REMOTE COIL FIELD

Table 7 Remote Coil Field

Modbus Address	PLC Address	Item	Description
0000H	1	Remote S1 Close	Active only when sending FF00H
0001H	2	Remote Open	Active only when sending FF00H
0002H	3	Remote S2 Close	Active only when sending FF00H
0003H	4	Remote Open (Same as 0001H)	Active only when sending FF00H
0004H	5	Auto/Manual	Manual Mode: Active only when sending 0000H Auto Mode: Active only when sending FF00H
0005H	6	S1 Master Set	Active only when sending FF00H
0006H	7	S2 Master Set	Active only when sending FF00H
0007H	8	Alarm Reset	Active only when sending FF00H
0008H	9	Remote Genset Start	Active only when sending FF00H
0009H	10	Remote Genset Stop	Active only when sending FF00H

NOTE: The remote command in the table above only needs to be sent once.

EXAMPLE:

If the remote controller is in auto mode, check the table first and find its remote address is 0004H. Assuming the slave address is 01, the master request command is as following:

Table 8 Master Request Command

Slave Address	Function Code	Remote Address (4)		Remote Data		CRC 16	
		MSB	LSB	MSB	LSB	LSB	MSB
01	**05**	**00**	**04**	**FF**	**00**	**CD**	**FB**

The slave response command is as following:

Table 9 Slave Response Command

Slave Address	Function Code	Remote Address (15004)		Remote Data		CRC 16	
		MSB	LSB	MSB	LSB	LSB	MSB
01	**05**	**00**	**04**	**FF**	**00**	**CD**	**FB**

Whether the remote command is active and executed can be checked by sending function code 01H to read auto mode status of address 0004H.

4 FAQ

4.1 RS485 TO USB CONVERTER

It can communicate with PC via the SmartGen SG72A converter.

4.2 EXTEND TRANSMISSION DISTANCE

Adding two SmartGen SGCAN300 Repeaters can extend the communication distance to at most 10 kilometers.

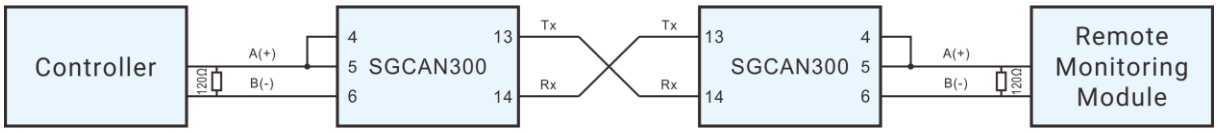

Fig. 2 SGCAN300 Application Diagram

4.3 SOLUTIONS FOR COMMUNICATION FAILURE

1) Check whether the positive and negative of RS485 or network cable is connected correctly, and check the RS485 converter (if any) is normal;
2) Check whether the communication parameters setting is correct, such as baud rate, data bit, parity bit, and stop bit, which are consistent with the requirements of the controller;
3) Check the Terminal COM is linked correctly with the USB port of PC via RS485 converter;
4) Check the communication address of controller is correct, and the default address is 01;
5) When using function code 03, the maximum data length to be read is 120 addresses, and the ending address can't exceed the greatest one of Modbus communication address. Please note that for the 06 function code mapping parameters data field, only one data can be written into one address at a time;
6) If there is offset address in the Modbus communication address, the actual Modbus communication address equals to the base address plus offset address;
7) If function code 05 adopts Modbus address to communicate: Although 1 means active, and 0 means inactive, it needs to send FF00H to load corresponding bit as 1, and send 0000H to load corresponding bit as 0. If function code 05 adopts PLC address to communicate: it needs to send 1 to load corresponding bit as 1, and send 0 to load corresponding bit as 0;
8) As for CRC-16, the low-order byte is checked first, the high-order byte is checked later;
9) The frequency of multiple read operations for controller data should not too high, and the recommended interval between two read operations is no less than 500ms;
10) Please configure each controller's communication module address before networking. Same module address is not allowed in one network;
11) Modbus serial protocol does not support multiple masters, so multiple software cannot communicate with the controller at the same time;
12) Disconnect the RS485 cables to the controller, test the voltage difference of RS485 Terminal A and B on the controller, if the result is between -200mV and +200mV, it means the communication port is abnormal;
13) It is recommended to download third-party communication test software to verify whether the communication is normal, such as modscan32, modbus poll, etc.