



SmartGen
ideas for power

HGM4020T
GENSET CONTROLLER
(COMMUNICATION BASE STATION DEDICATED)
COMMUNICATION PROTOCOL

SmartGen

SMARTGEN (ZHENGZHOU) TECHNOLOGY CO., LTD.



Chinese trademark

SmartGen English trademark

SmartGen — make your generator *smart*

SmartGen Technology Co., Ltd.

No.28 Jinsuo Road

Zhengzhou

Henan Province

P. R. China

Tel: 0086-371-67988888/67981888

0086-371-67991553/67992951

0086-371-67981000(overseas)

Fax: 0086-371-67992952

Web: www.smartgen.com.cn

www.smartgen.cn

Email: sales@smartgen.cn

All rights reserved. No part of this publication may be reproduced in any material form (including photocopying or storing in any medium by electronic means or other) without the written permission of the copyright holder.

Applications for the copyright holder's written permission to reproduce any part of this publication should be addressed to Smartgen Technology at the address above.

Any reference to trademarked product names used within this publication is owned by their respective companies.

SmartGen Technology reserves the right to change the contents of this document without prior notice.

Table 1 - Software Version

Date	Version	Note
2018-04-20	1.0	Original release.

CONTENT

1.	INTRODUCTION.....	4
2.	MODBUS BASIC RULES	4
3.	DATA FRAME FORMAT.....	4
4.	COMMUNICATION PROTOCOL.....	4
4.1	ILLUSTRATION	4
4.2	INFORMATION FRAME FORMAT	5
4.3	ADDRESS CODE	5
4.4	FUNCTION CODE.....	5
4.4.1	ILLUSTRATION.....	5
4.4.2	01H READ COILS.....	5
4.4.3	03H READ HOLDING REGISTERS	5
4.4.4	05H FORCE SINGLE COIL	6
4.5	DATA FIELD.....	6
4.5.1	ILLUSTRATION.....	6
4.5.2	FUNCTION 01H –READ COILS	6
4.5.3	FUNCTION 03H –READ HOLDING REGISTERS	6
4.5.4	FUNCTION 05H –FORCE SINGLE COIL.....	6
4.6	ERROR CHECK CODE (CRC).....	7
4.7	EXAMPLES OF INFORMATION FRAME FORMAT	8
4.7.1	FUNCTION CODE 01H	8
4.7.2	FUNCTION CODE 03H	9
4.7.3	FUNCTION CODE 05H	10
4.8	ERROR HANDLING	11
5.	APPENDIX: ADDRESS AND DATA	12
5.1	FUNCTION CODE 01H MAP DATA FIELD	12
5.2	FUNCTION CODE 03H MAP DATA FIELD	15
5.3	FUNCTION CODE 05H MAP DATA FIELD	17
5.4	CONTROLLER RUNNING STATUS.....	17
5.5	ATS RUNNING STATUS.....	18

1. INTRODUCTION

This protocol describes read and write command format of PC serial port and the definition of internal information data for the third-party to develop and use.

MODBUS communication protocol allows the module to transfer information and data effectively with PLC, RTU, SCADA system of international brands (such as, Schneider, Siemens, and Modicon), and DCS or third-party monitoring system compatible with MODBUS. The monitoring system can be set up if only adding central communication master software (such as Kingview, Intouch, FIX, Synal) basing on PC (or IPC).

2. MODBUS BASIC RULES

- All RS232 communication loops should follow the master-slave mode. If so, data can be transferred between a master (e.g. PC) and 32 slaves.
- The master will initialize all messages sent from RS232 communication coil of the device.
- No communication can start from slaves.
- In RS232 communication loop, all communication should be transmitted in “information frame”.
- If received information frame contains unknown command, no response will be given.

3. DATA FRAME FORMAT

Communication is asynchronously transferred, using byte (data frame) as unit. Between master and slave, every transmitted data frame is 11-bit serial data stream.

Table 2 - Data Frame Format

Item	Description
Start bit	1-bit
Data bit	8-bit
Parity bit	No parity
Stop bit	2-bit can be set.

4. COMMUNICATION PROTOCOL

4.1 ILLUSTRATION

When communication command is sent to the slave, corresponding slave receives the communication command, then removes address code, and read the information. If no mistakes, it will execute commands, and sends the result back to the master. Response information includes address code, function code, data and error check code (CRC). If an error occurred in receipt of the command, it will send no information.

4.2 INFORMATION FRAME FORMAT

Table 3 – Information Frame Format

Initiating structure	Address code	Function code	Data field	CRC	End structure
Delay (equivalent to 4 bytes)	1 byte 8-bit	1 byte 8-bit	N bytes N*8-bit	2 bytes 16-bit	Delay (equivalent to 4 bytes)

4.3 ADDRESS CODE

Address code is the first data frame (8-bit) in each transmitted information frame (from 0-255). Single device address range is 1–247; this byte shows that the slave defined by users will receive the information sent by the master. Each slave has a unique address code, and responses begin with the address code. A master addresses a slave by placing the slave address in the address field of the message. When the slave sends its response, it places its own address in this address field of the response to let the master know which slave is responding.

4.4 FUNCTION CODE

4.4.1 ILLUSTRATION

This is the second byte of each transmission. ModBus communication protocol defined function code as 1-255 (01H-0FFH). HGM4020T controller use part of it. Master sends the request and the slave executes actions according to the function code. If the function code sent by slave is same as that sent by master, it means the response is active. But if the function code MSB is 1 (function code range>127), it means there is no response or response has error.

The following table shows the specific signification and operation of function code.

Table 4 - ModBus Partial Function Codes

Function code	Definition	Operation
01H	Read Coils	Reads the contents of coils
03H	Read Holding Registers	Reads the contents of holding registers
05H	Force Single Coil	Forces a single coil to either ON or OFF.

4.4.2 01H READ COILS

Master can read all coils (like switch on/off, fault information, auto or manual status and so on) of the device via function code 01 communication command.

4.4.3 03H READ HOLDING REGISTERS

With function code 03H command, the master can read the numerical registers inside the device (numerical registers contains various analog and parameter setting values). Input register values of function code 03H mapping data field are 16 bits (2 bytes). So, from the device reads registers values are 2 bytes. Maximum number of readable registers is 125 each time.

The slave received command format is slave address, function code, data field and the CRC code. The data of data field is in double bytes with every two bytes for a group, and high byte is in advance.

4.4.4 05H FORCE SINGLE COIL

Master uses this command to save a single coil data into bit registers in the device (such as ATS transfer control). The slave also uses this function code to feedback information to the master.

4.5 DATA FIELD

4.5.1 ILLUSTRATION

Data field varies with different function codes.

4.5.2 FUNCTION 01H –READ COILS

Request:

Data Sequence	Data Signification	Byte Count
1	Starting address	2
2	Read coils	2

Response:

Data Sequence	Data Signification	Byte Count
1	Loopback byte count	1
2	N – coil data	1

4.5.3 FUNCTION 03H –READ HOLDING REGISTERS

Request:

Data Sequence	Data Signification	Byte Count
1	Starting address	2
2	Read registers	2

Response:

Data Sequence	Data Signification	Byte Count
1	Loopback byte count	1
2	N - register data	N

4.5.4 FUNCTION 05H –FORCE SINGLE COIL

Request:

Data Sequence	Data Signification	Byte Count
1	Coil address	2
2	Forced single coil value	2

Response:

Data Sequence	Data Signification	Byte Count
1	Coil address	2
2	Single coil value	2

4.6 ERROR CHECK CODE (CRC)

The Error Check Code allows the receiving device to detect a packet that has been corrupted with transmission errors. Sometimes, the transmission information occur imperceptible changes due to electronic noise and other interference and the CRC code ensure the error information does not work to increase the system's safety and efficiency. CRC adapts CRC-16 method of calibration.

When the CRC is appended to the message, the low-order byte is appended first, followed by the high-order byte.

▲Note: All information frame format are same: address code, function code, data area and CRC code.

The CRC field is two bytes, containing a 16-bit binary value. The CRC value is calculated by the transmitting device, which appends the CRC to the message. The receiving device recalculates a CRC during receipt of the message, and compares the calculated value to the actual value that received in the CRC field. If the two values are not equal, an error will result.

The CRC is started by first preloading a 16-bit register to all 1's. Then a process begins of applying successive 8-bit bytes of the message to the current contents of the register. Only the eight bits of data in each character are used for generating the CRC. Start and stop bits do not apply to the CRC.

During generation of the CRC, each 8-bit character is exclusive OR with the register contents. Then the result is shifted in the direction of the least significant bit (LSB), with a zero filled into the most significant bit (MSB) position. The LSB is extracted and examined. If the LSB was a 1, the register is then exclusive OR with a preset, fixed value. If the LSB was a 0, no exclusive OR takes place.

This process is repeated until eight shifts have been performed. After the last (eighth) shift, the next 8-bit byte is exclusive OR with the register's current value, and the process repeats for eight more shifts as described above. The final contents of the register, after all the bytes of the message have been applied, is the CRC value.

CRC-16 CALCULATIONPROCEDURE

- 1) Load a 16-bit register with FFFF hex (all 1's). Call this the CRC register.
- 2) Exclusive OR the first 8-bit byte of the message with the low-order byte of the CRC register, putting the result in the CRC register.
- 3) Shift the CRC register one bit to the right (toward the LSB), zero-filling the MSB. Extract and examine the LSB.
- 4) (If the LSB was 0): Repeat Step 3 (another shift).
(If the LSB was 1): Exclusive OR the CRC register with the polynomial value A001 hex (1010 0000 0000 0001).
- 5) Repeat Steps 3 and 4 until 8 shifts have been performed. When this is done, a complete 8-bit byte will have been processed.
- 6) Repeat Steps 2 through 5 for the next 8-bit byte of the message. Continue doing this until all bytes have been processed.
- 7) The final contents of the CRC register are the CRC value. Least Significant Byte first. When the 16-bit CRC (two 8-bit bytes) is transmitted in the message, the low-order byte will be transmitted first, followed by the high-order byte.

▲Note: The calculating of CRC code starts from <slave address> and except for all bytes of <CRC code>.

4.7 EXAMPLES OF INFORMATION FRAME FORMAT

4.7.1 FUNCTION CODE 01H

Slave address is 00 and read starting address is 20H of 0000H (decimalism 32).

Request

Request	Bytes	Example (Hex)
Slave address	1	01 Send to the slave 01
Function code	1	01 Read coils
Starting address	2	00 Starting address is 0000 00
No. of Points	2	00 Read 28 coils 1C
CRC code	2	3D CRC code which calculated by PC. C3

Response

Response	Bytes	Example (Hex)
Slave address	1	01 Respond to the slave 01
Function code	1	01 Read coils
Read count	1	04 Respond coils: 28 coils (total 4bytes)
Data 1	1	30 The content of address 07-00
Data 2	1	00 The content of address 0F-08
Data 3	1	93 The content of address 17-10
Data 4	1	0A The content of address 1C-18
CRC code	2	18 CRC code which calculated by slave. 26

Discrete value 07-00 expressed as 30H of hexadecimal and 00110000 of binary, 07 is in MSB and 00 is in LSB. 07-00 discrete value status are: OFF – OFF – ON – ON – OFF – OFF – OFF – OFF.

4.7.2 FUNCTION CODE 03H

Slave address is 01 and starting address is 3 data of 0026H.

Address	Data(Hex)
0026	0014
0027	0014
0028	0005

Request

Request	Bytes	Example (Hex)
Slave address	1	01 Send to the slave 01
Function code	1	03 Read Holding Registers
Starting address	2	00 Starting address is 0026 26
No. of Points	2	00 Read 3 registers (total 6 bytes) 03
CRC code	2	E4 CRC code which calculated by PC. 00

Response

Response	Bytes	Example (Hex)
Slave address	1	01 Respond to the slave 01
Function code	1	03 Read register
Read count	1	06 3 registers (total 6 bytes)
Data 1	2	00 The content of address 0026 14
Data 2	2	00 The content of address 0027 14
Data 3	2	00 The content of address 0028 05
CRC code	2	91 CRC code which calculated by slave. 71

4.7.3 FUNCTION CODE 05H

Read coil for slave address is 01 and starting address is 1 discrete value of 0002H. 0002 unit is 1.

Address	Data(Hex)
0000	0
0001	1
0002	0

▲ Note: A value of 00FF hex requests the coil to be ON. A value of 00 0H requests it to be OFF. All other values are illegal and will not affect the coil.

Request

Request	Bytes	Example (Hex)
Slave address	1	01 Send to the slave 01
Function code	1	05 Force single coil
Starting address	2	00 Starting address for 0000 00
Data	2	00 Set coil as 1 FF
CRC code	2	CD CRC code which calculated by PC. FB

Response

Slave Response	Bytes	For Example (Hex)
Slave address	1	01 Respond to the slave 01
Function code	1	05 Force single coil
Starting address	2	00 Starting address is 0000 00
Data	2	00 Set coil as 1 FF
CRC code	2	CD CRC code which calculated by slave. FB

4.8 ERROR HANDLING

When device detected other errors except the CRC code, the slave must send information to the master. The function code MSB is 1, which means the response function code by slave should add 128 based on the function code. The following codes show that unexpected errors have occurred.

CRC error received from the master will be ignored by the device.

The frame format of error code that responds by slave is as follows (CRC excluded):

Type	Byte
Address code	1 byte
Function code	1 byte (MSB is 1)
Error code	1 byte
CRC code	2 bytes

Error code:

01 illegal function code

The function code received in the query is not an allowable action for the slave.

02 illegal data address

The data address received in the query is not an allowable address for the slave.

03 illegal data value

A value contained in the query data field is not an allowable value for the slave.

5. APPENDIX: ADDRESS AND DATA

5.1 FUNCTION CODE 01H MAP DATA FIELD

Discrete Values		
Address	Item	Description
0000H	Common Alarm	1 for active
0001H	Common Warning Alarm	1 for active
0002H	Common Shutdown Alarm	1 for active
0003H	Reserved	1 for active
0004H	Common Trip And Stop Alarm	1 for active
0005H	Reserved	1 for active
0006H	Reserved	1 for active
0007H	Reserved	1 for active
0008H	Reserved	1 for active
0009H	Overspeed Alarm Shutdown	1 for active
000AH	Underspeed Alarm Shutdown	1 for active
000BH	Speed Signal Loss Alarm Shutdown	1 for active
000CH	Gen Overfrequency Alarm Shutdown	1 for active
000DH	Gen Underfrequency Alarm Shutdown	1 for active
000EH	Gen Overvoltage Alarm Shutdown	1 for active
000FH	Gen Undervoltage Alarm Shutdown	1 for active
0010H	Gen Overcurrent Alarm Shutdown	1 for active
0011H	Failed to Start Alarm Shutdown	1 for active
0012H	High Temperature Alarm Shutdown(IN)	1 for active
0013H	Low Oil Pressure Alarm Shutdown	1 for active
0014H	Gen Unavailable Alarm Shutdown	1 for active
0015H	Input Port Alarm Shutdown	1 for active
0016H	Low Fuel Level Alarm Shutdown	1 for active
0017H	Reserved	1 for active
0018H	Reserved	1 for active
0019H	Low Oil Pressure Warning	1 for active
001AH	Gen Overcurrent Warning	1 for active
001BH	Failed to Stop Warning	1 for active
001CH	Low Fuel Level Warning	1 for active
001DH	Failed to Charge Warning	1 for active
001EH	Battery Undervoltage Warning	1 for active
001FH	Battery Overvoltage Warning	1 for active
0020H	Input Port Warning	1 for active
0021H	Speed Signal Loss Warning	1 for active
0022H	Room Temperature High Warning	1 for active
0023H	Reserved	1 for active
0024H	Oil Pressure Sensor Open Circuit Warning	1 for active
0025H	Fuel Level Sensor Open Circuit Warning	1 for active

Discrete Values		
Address	Item	Description
0026H	Flexible Sensor 1 Open Circuit Warning	1 for active
0027H	Flexible Sensor 2 Open Circuit Warning	1 for active
0028H	Reserved	1 for active
0029H	System In Auto Mode	1 for active
002AH	System In Manual Mode	1 for active
002BH	System In Stop Mode	1 for active
002CH	Reserved	1 for active
002DH	Reserved	1 for active
002EH	Reserved	1 for active
002FH	Reserved	1 for active
0030H	Reserved	1 for active
0031H	Digital Input 1	1 for active
0032H	Digital Input 2	1 for active
0033H	Digital Input 3	1 for active
0034H	Digital Input 4	1 for active
0035H	Digital Input 5	1 for active
0036H	Digital Input 6	1 for active
0037H	Digital Input 7	1 for active
0038H	Starter Relay Output	1 for active
0039H	Reserved	1 for active
003AH	Relay Output 1	1 for active
003BH	Relay Output 2	1 for active
003CH	Relay Output 3	1 for active
003DH	Relay Output 4	1 for active
003EH	5Relay Output 5 (fuel relay port)	1 for active
003FH	Reserved	1 for active
0040H	Mains Fail	1 for active
0041H	Mains OK	1 for active
0042H	Mains Overvoltage	1 for active
0043H	Mains Undervoltage (related to the electricity rules of the mains)	1 for active
0044H	Mains Loss of Phase (related to the electricity rules of the mains)	1 for active
0045H	Mains Unavailable	1 for active
0046H	Reserved	1 for active
0047H	Reserved	1 for active
0048H	Reserved	1 for active
0049H	Gen Overvoltage Warning	1 for active
004AH	Gen Undervoltage Warning	1 for active

Discrete Values		
Address	Item	Description
004BH	Gen Overfrequency Warning	1 for active
004CH	Gen Underfrequency Warning	1 for active
004DH	Gen Overcurrent Warning	1 for active
004EH	Reserved	1 for active
004FH	Reserved	1 for active
0050H	Flexible Sensor 1 Warning	1 for active
0051H	Flexible Sensor 2 Warning	1 for active
0052H	Overpower Warning	1 for active
0053H	Maintenance Time Due Warning	1 for active
0054H	Charger Failed to Charge Warning	1 for active
0055H	Fuel Level Low(IN)	1 for active
0056H	Battery Pack Undervoltage Warning	1 for active
0057H	Access Input Warning	1 for active
0058H	1#ATS Failed to Transfer Warning	1 for active
0059H	2#ATS Failed to Transfer Warning	1 for active
005AH	Reserved	1 for active
005BH	Reserved	1 for active
005CH	Reserved	1 for active
005DH	Reserved	1 for active
005EH	Reserved	1 for active
005FH	Reserved	1 for active
0060H	Oil Pressure Sensor Open Circuit Shutdown	1 for active
0061H	Fuel Level Sensor Open Circuit Shutdown	1 for active
0062H	Flexible Sensor 1 Open Circuit Shutdown	1 for active
0063H	Flexible Sensor 2 Open Circuit Shutdown	1 for active
0064H	Flexible Sensor 1 Shutdown	1 for active
0065H	Flexible Sensor 2 Shutdown	1 for active
0066H	Overpower Alarm Shutdown	1 for active
0067H	Maintenance Time Due Alarm Shutdown	1 for active
0068H	Reserved	1 for active
0069H	Reserved	1 for active
006AH	Reserved	1 for active
006BH	Reserved	1 for active
006CH	Overpower Trip And Stop	1 for active
006DH	Gen Overcurrent Trip And Stop	1 for active
006EH	Reserved	1 for active
006FH	Reserved	1 for active
0070H	Gen OK	1 for active
0071H	Reserved	1 for active
0072H	1#ATS Mains On-load	1 for active
0073H	1#ATS Gen On-load	1 for active

Discrete Values		
Address	Item	Description
0074H	2#ATS Mains On-load	1 for active
0075H	2#ATS Gen On-load	1 for active
0076H	Remote Control Mode	1 for active
0077H	In Scheduled Not Run Time	1 for active

5.2 FUNCTION CODE 03H MAP DATA FIELD

Address	Item & Description
0000H	Mains UA
0001H	Mains UB
0002H	Mains UC
0003H	Mains UAB
0004H	Mains UBC
0005H	Mains UCA
0006H	Mains frequency (*10)
0007H	Gen UA
0008H	Gen UB
0009H	Gen UC
000AH	Gen UAB
000BH	Gen UBC
000CH	Gen UCA
000DH	Gen frequency (*10)
000EH	A phase current (*10)
000FH	B phase current (*10)
0010H	C phase current (*10)
0011H	Reserved
0012H	Reserved
0013H	Oil pressure value
0014H	Oil pressure resistance (*10)
0015H	Fuel level value
0016H	Fuel level resistance (*10)
0017H	Speed
0018H	Battery voltage (*10)
0019H	D+ voltage(*10)
001AH	Active power (*10)
001BH	Reactive power (*10)
001CH	Apparent power (*10)
001DH	Power factor (*100)
001EH	Reserved
001FH	Reserved
0020H	Maintenance Countdown (hour)
0021H	Maintenance Countdown (minute)
0022H	Controller running status (details please to see 5.4 CONTROLLER RUNNING STATUS)
0023H	Delay

Address	Item & Description
0024H	Auto running status 0 Start 1 Stop 2 No delay
0025H	Delay
0026H	1#ATS Running status (details please to see 5.5 ATS RUNNING STATUS)
0027H	Delay
0028H	Mains status 0 Normal 1 Abnormal 2 No delay
0029H	Delay
002AH	Engine total running time (hour) MSB (0-9999)
002BH	Engine total running time (hour) LSB (0-9999)
002CH	Engine total running time (minute) (0-9999)
002DH	Engine total running time (second) (0-9999)
002EH	Total start times MSB (0-9999)
002FH	Total start times LSB (0-9999)
0030H	Total Energy MSB (0-9999)
0031H	Total Energy LSB (0-9999)
0032H	Software version
0033H	Hardware version
0034H	A phase active power (*10)A
0035H	B phase active power (*10)A
0036H	C phase active power (*10)A
0037H	Load output percentage
0038H	Reserved
0039H	Reserved
003AH	Reserved
003BH	2#ATS Status (details please to see 5.5 ATS RUNNING STATUS)
003CH	2#ATS Delay
003DH	Reserved
003EH	Reserved
003FH	Battery pack voltage value (*10)
0040H	Flexible sensor 1 value
0041H	Flexible sensor 1 value (*10)
0042H	Flexible sensor 2 value
0043H	Flexible sensor 2 value (*10)
0044H	Reserved
0045H	Reserved
0046H	Reserved
0047H	Reserved
0048H	Controller time: year
0049H	Controller time: month
004AH	Controller time: day
004BH	Controller time: week
004CH	Controller time: hour
004DH	Controller time: minute
004EH	Controller time: second

Address	Item & Description
004FH	Issue time (year)
0050H	Issue time (month)
0051H	Issue time (day)
0052H	Reserved
0053H	Reserved
0054H	Reserved
0055H	Reserved
0056H	Reserved
0057H	Reserved
0058H	Reserved
0059H	Reserved
005AH	Gen A phase
005BH	Gen B phase
005CH	Gen C phase
005DH	Mains A phase
005EH	Mains B phase
005FH	Mains C phase

5.3 FUNCTION CODE 05H MAP DATA FIELD

Discrete Value		
Address	Item	Description
0000H	Remote control engine in start status	1 for active (that is 0xFF00 is active)
0001H	Remote control engine in sop status	1 for active (that is 0xFF00 is active)
0002H	Reserved	1 for active (that is 0xFF00 is active)
0003H	Remote control engine in auto status	1 for active (that is 0xFF00 is active)
0004H	Remote control engine in manual status	1 for active (that is 0xFF00 is active)
0005H	Remote control 1#ATS gen close/open key	1 for active (that is 0xFF00 is active)
0006H	Remote control 1#ATS mains close/open key	1 for active (that is 0xFF00 is active)
0007H	Remote control 2#ATS gen close/open key	1 for active (that is 0xFF00 is active)
0008H	Remote control 2#ATS mains close/open key	1 for active (that is 0xFF00 is active)

5.4 CONTROLLER RUNNING STATUS

No.	Item & description
0	Standby
1	Preheat
2	Fuel
3	Crank
4	Start interval
5	Safety on
6	Start idle
7	High speed warming up
8	Ramp on load
9	Normal running
10	High speed cooling



11	Stop idle
12	Energize to stop
13	Wait for stop
14	Failed to stop

5.5 ATS RUNNING STATUS

No.	Item & description
0	Load disconnected
1	Mains closed
2	Gen closed
3	Open delay
4	Breaker transfer delay
5	Mains close delay
6	Gen close delay
7	Wait for opening breaker
8	Wait for closing generator breaker
9	Wait for closing mains breaker

