HGM1790N

GENSET CONTROLLER

COMMUNICATION PROTOCOL

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

Table 1 - Software Version

Date	Version	Note
2018-05-7	1.0	Original release.

CONTENT

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

1) 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.
2) The master will initialize all messages sent from communication coil of the device.
3) No communication can start from slaves.
4) In RS232 communication loop, all communication should be transmitted in "information frame".
5) 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). The 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). HGM1790N controller uses 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	Read one or more coils.
03H	Read Holding Registers	Read one or more holding registers.
05H	Force Single Coil	Force a single coil to either ON or OFF.

4.4.2 01H READ COILS

Master uses 01 function code command to read all kinds of coils in the device (such as breaker close, breaker open, breaker default, auto mode, or manual mode).

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). Function code 03H mapping data field are 16-bit (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 data into registers in the device (such as coil controlled ATS to transfer). Slave also uses this function code to send information back 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 CODE 03H –READ HOLDING REGISTERS

Request:

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

Response:

Data Sequence	Data Signification	Byte Count
1	Loopback byte count	1
2	N – holding 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. 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 starting address is 20H(decimal 32) coil data of 0000H.

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 master.
		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	Return to coil count: 28 coils(total 4 bytes)
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	

The value of the coil 07–00 is expressed in hexadecimal as 30H, and in binary as 00110000. Coil 07 is the high byte, 00 is the low byte. 07-00 coils status is OFF－OFF－ON－ON－OFF－OFF－OFF－OFF.

4.7.2 FUNCTION CODE 03H

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

Point data address is as below,

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
Read Number of Points	2	00 Read 3 registers (total 6 bytes) 03
CRC code	2	E4 CRC code which calculated by master 00

Response

Response	Bytes	Example (Hex)
Slave address	1	01 Respond to the slave 01
Function code	1	03 Read registers
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

Slave address is 01 and starting address is 1 coil value of 0002H. Set 0002 unit as 1.

Coil data address is as below,

Address	Data(Hex)
0000	0
0001	1
0002	0

Hex value 00FF forced coil is 1, 000H is forced as 0, other values are illegal and do not affect the state of the coil.

Request	Bytes	Example (Hex)	
Slave Address	1	01	Respond to the slave 01
Function Code	1	05	Forced coil
Starting Address	2	00 00	Starting address is 0000
Data	2	00 FF	set coil as 1
CRC Code	2	CD FB	CRC code which calculated by master

Slave Response	Bytes	For Example (Hex)	
Slave Address	1	01	Respond to slave address 01
Function Code	1	05	Forced coil
Starting address	2	00 00	Starting address is 0000
Data	2	00 FF	set coil as 1
CRC Code	2	CD FB	CRC code which calculated by master

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	Reserved	1 for active
0005H	Reserved	1 for active
0006H	Reserved	1 for active
0007H	Gen On-load	1 for active
0008H	Emergency Stop	1 for active
0009H	Overspeed Shutdown	1 for active
000AH	Underspeed Shutdown	1 for active
000BH	Reserved	1 for active
000CH	Overfrequency Alarm Shutdown	1 for active
000DH	Underfrequency Alarm Shutdown	1 for active
000EH	Overvoltage Alarm Shutdown	1 for active
000FH	Undervoltage Alarm Shutdown	1 for active
0010H	Gen Overcurrent Shutdown	1 for active
0011H	Failed to Start	1 for active
0012H	High Water Temp. Alarm Shutdown	1 for active
0013H	Low Oil Pressure Alarm Shutdown	1 for active
0014H	Reserved	1 for active
0015H	Input Port Shutdown Alarm	1 for active
0016H	Reserved	1 for active
0017H	Reserved	1 for active
0018H	Reserved	1 for active
0019H	Reserved	1 for active
001AH	Gen Overcurrent Warning Alarm	1 for active
001BH	Failed to Stop Warning Alarm	1 for active
001CH	Low Fuel Level Warning	1 for active
001DH	Reserved	1 for active
001EH	Battery Low Voltage Warning Alarm	1 for active
001FH	Battery High Voltage Warning Alarm	1 for active
0020H	Reserved	1 for active

Discrete Values		
Address	Item	Description
0021H	Reserved	1 for active
0022H	Reserved	1 for active
0023H	Reserved	1 for active
0024H	Reserved	1 for active
0025H	Reserved	1 for active
0026H	Reserved	1 for active
0027H	Reserved	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	Emergency Stop Input	1 for active
0031H	Digital Input 1	1 for active
0032H	Reserved	1 for active
0033H	Remote Start Input	1 for active
0034H	Reserved	1 for active
0035H	Reserved	1 for active
0036H	Reserved	1 for active
0037H	Reserved	1 for active
0038H	Start Relay Output	1 for active
0039H	Fuel Relay Output	1 for active
003AH	Relay Output 3 Status	1 for active
003BH	Relay Output 1 Status	1 for active
003CH	Relay Output 2 Status	1 for active
003DH	Reserved	1 for active
003EH	Reserved	1 for active
003FH	Reserved	1 for active
0040H	Reserved	1 for active
0041H	Reserved	1 for active
0042H	Reserved	1 for active
0043H	Reserved	1 for active
0044H	Reserved	1 for active
0045H	Reserved	1 for active
0046H	Reserved	1 for active
0047H	Reserved	1 for active
0048H	Gen Normal	1 for active
0049H	Gen Overvoltage	1 for active
004AH	Gen Undervoltage	1 for active

Discrete Values		
Address	Item	Description
004BH	Gen Overfrequency	1 for active
004CH	Gen Underfrequency	1 for active
004DH	Gen Overcurrent	1 for active
004EH	Reserved	1 for active
004FH	Reserved	1 for active

5.2 FUNCTION CODE 03H MAP DATA FIELD

Address	Item & Description
0000H	Reserved
0001H	Reserved
0002H	Reserved
0003H	Reserved
0004H	Reserved
0005H	Reserved
0006H	Reserved
0007H	Gen UA
0008H	Reserved
0009H	Reserved
000AH	Reserved
000BH	Reserved
000CH	Reserved
000DH	Gen frequency (*10)
000EH	A-phase current (*10)
000FH	Reserved
0010H	Reserved
0011H	Water temperature value
0012H	Water temperature resistance(*10)
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	Reserved
001AH	Active power (*10)
001BH	Reserved
001CH	Reserved
001DH	Reserved
001EH	Reserved
001FH	Reserved
0020H	Reserved
0021H	Reserved

Address	Item & Description
0022H	Controller running status(details please to see *5.4 controller running status*)
0023H	Delay
0024H	Auto running status: 0 start 1 stop 2 no delay
0025H	Delay
0026H	Reserved
0027H	Reserved
0028H	Reserved
0029H	Reserved
002AH	Engine total running time (hour) MSB (0-19)
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	Reserved
0031H	Reserved
0032H	Software version
0033H	Hardware version
0034H	Reserved
0035H	Reserved
0036H	Reserved
0037H	Load output percentage
0038H	Reserved
0039H	Reserved
003AH	Software release time (year)
003BH	Software release time (month)
003CH	Software release time (day)
003DH	Reserved
003EH	Reserved
003FH	Reserved
0040H	Reserved

5.3 FUNCTION CODE 05H MAP DATA FIELD

Discrete Values		
Address	Item	Description
0000H	Remote control unit is started	1 for active (which means 0xFF00 active)
0001H	Remote control unit is stopped	1 for active (which means 0xFF00 active)
0002H	Remote control unit is in auto status	1 for active (which means 0xFF00 active)

5.4 GENERATOR RUNNING STATUS

No.	Item & Description
0	Standby
1	Preheat
2	Fuel
3	Crank
4	Crank rest
5	Safety on
6	Start idle
7	Hi-speed warming up
8	On-load
9	Normal running
10	Hi-speed cooling
11	Stop idle
12	Energize to stop
13	Wait for stop
14	Failed to stop