SG2V3 ModBus Protocol

(V type: RS485 port)

Series: SG2 V type
Version: V06

A	C	D
		2011-01-02

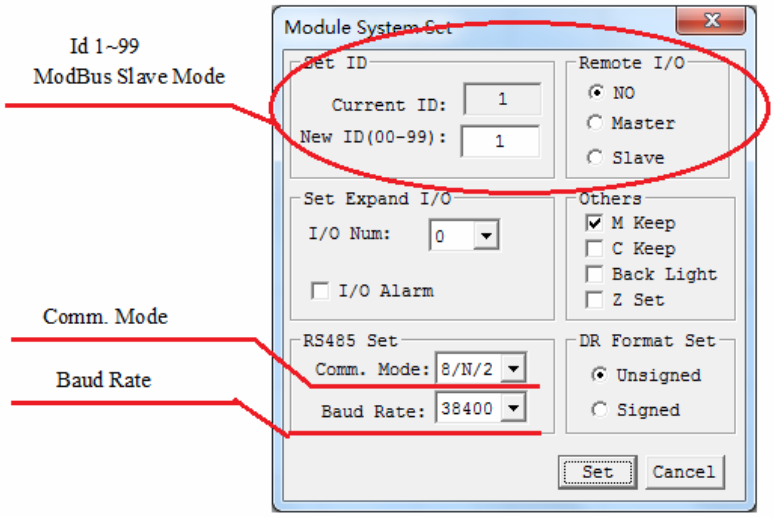
1. Communication Data Frame

SG2 series PLC can be communication controlled by the PC or other controller with the communication protocol, ModBus RTU slave Mode, via RS485.

1.1 Communication parameter

SG2 provides different communication parameter to satisfy your needs. And there are two ways to set that parameter.

1. Setting communication parameter via SG2 Client.
   - Insert the plastic connector end of the programming cable into the SG2 smart relay. Connect the opposite end of the cable to an RS232 serial port on the computer.
   - In SG2 Client Soft Select Operation>>Module System Set, to open the dialog box as show below.

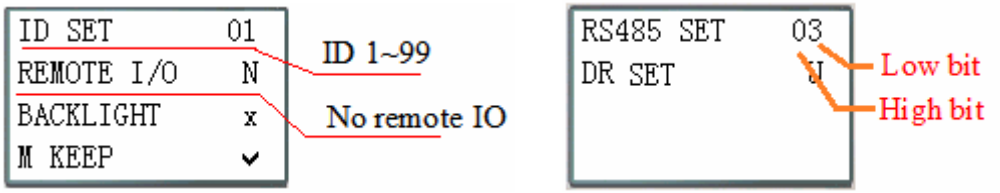


   - As the illustration show, you can set Communication Mode and Baud Rate.
   - In the table below, list the options which you can choose from.

Comm. Mode	8/N/2 Data 8bit, No Parity, 2 Stop bit.
	8/E/1 Data 8bit, Even Parity, 1 Stop bit.
	8/O/1 Data 8bit, Odd Parity, 1 Stop bit.
	8/N/1 Data 8bit, No Parity, 1 Stop bit.
Baud Rate.	4800 bps 9600 bps 19200 bps 38400 bps 57600 bps 115200 bps

2. Set communication format and Baud Rate on SG2.

- Press ESC to enter main menu.
- Press UP/DOWN to choose SET menu, and press OK to enter it.
- Press UP/DOWN makes the LCD to display the options as show below.



- System setting is N Remote I/O and ID SET isn't 0.
- Changing high bit would set Comm. Mode; changing low bit would set Baud Rate.

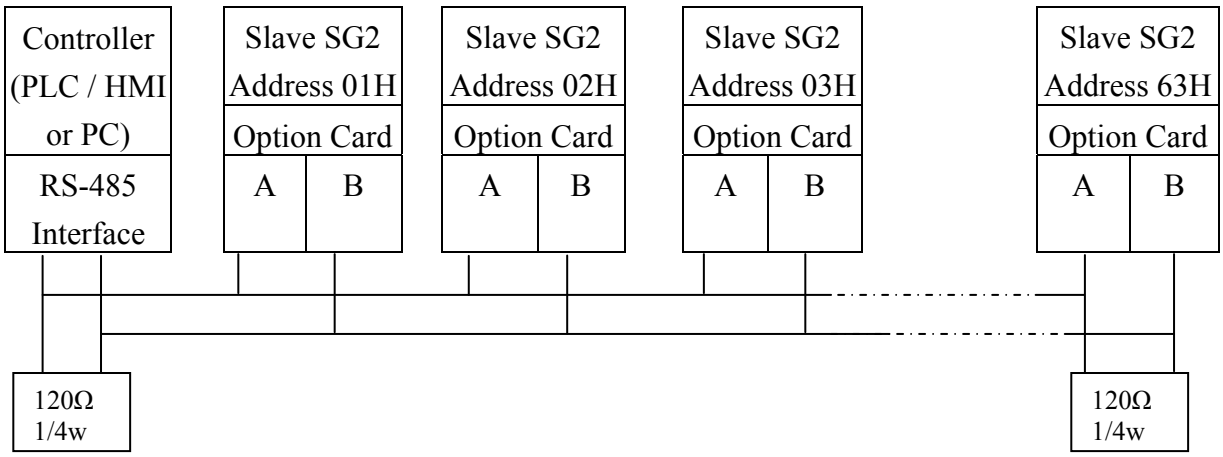
Content	Data	meaning
High bit	0	8/N/2 Data 8bit, No Parity, 2 Stop bit.
	1	8/E/1 Data 8bit, Even Parity, 1 Stop bit.
	2	8/O/1 Data 8bit, Odd Parity, 1 Stop bit.
	3	8/N/1 Data 8bit, No Parity, 1 Stop bit.
Low bit	0	4800 bps
	1	9600 bps
	2	19200 bps
	3	38400 bps
	4	57600 bps
	5	115200 bps

3. SG2 RS485 port default communication parameter as table show below:

Baud rate	38400bps
Data bit	8
Stop bit	2
Parity	No
Frame length maximum	128 bytes

- SG2 V2 RS485 port communication parameter as table show above.
- The communication parameter setting takes effect after power up again.

1.2 Hardware Installation



*It is necessary to connect the terminal impedance (120Ω, 1/4W) at both ends of the communication wire.

1.3 Data frame for RTU Mode

MASTER (PLC etc.) send request to SLAVE, whereas SLAVE response to MASTER. The signal receiving is illustrated here. The data length is varied with the command (Function).

SLAVE Address	1byte
Function Code	1byte
DATA	nbyte
CRC16 CHECK	2byte
Signal Interval	Signal Interval

** The interval should be maintained at 10ms between command signal and request.

1.4 Slave Address

00H : Broadcast to all the drivers
01H : to the No.01 Driver
0FH : to the No.15 Driver
10H : to the No.16 Driver
and so on...., Max to No.99(63H)

1.5 Function Code

01H: Read coils
03H: Read registers
05H: Write single coil
06H: Write single register
08H: Diagnostic
10H: Write multiple registers

2. CMS (Checksum and time-out definition)

2.1 CRC CHECK:

CRC check code is from Slave Address to end of the data. The calculation method is illustrated as follow:

(1) Load a 16-bit register with FFFF hex (all1's). Call this the CRC register.

(2) Exclusive OR the first 8-bit byte of the message with the low-order byte of the 16-bit 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 examines the LSB.

(4) (If the LSB was 0): Repeat Steps (3) (another shift) (If the LSB was 1): Exclusive OR the CRC register with the polynomial value A001 hex (1010 0000 0000 0001).

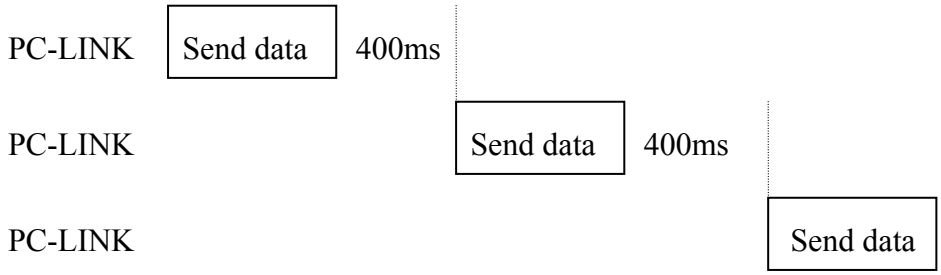
(5) Repeat Steps (3) and (4) until 8 shifts been performed. When this is done, a complete 8-bit byte will be processed.

(6) Repeat Steps (2) through (5) for next 8-bit byte of the message, Continue doing this until all bytes have been processed. The final content of the CRC register is the CRC value. Placing the CRC into the message: When the 16-bit CRC (2 8-bit bytes) is transmitted in the message, the low-order byte will be transmitted first, followed by the high-order byte, For example, if the CRC value is 1241 hex, the CRC-16 (Low) put the 41h, the CRC-16 (Hi) put the 12h.

- **CRC calculation application program**

```
UWORD ch_sum ( UBYTE long , UBYTE *rxdbuff ) {
    BYTE i = 0;
    UWORD wkg = 0xFFFF;
    while ( long-- ) {
      wkg ^= rxdbuff++;
      for ( i = 0 ; i < 8; i++ ) {
          if ( wkg & 0x0001 ) {
            wkg = ( wkg >> 1 ) ^ 0xa001;
          }
          else {
            wkg = wkg >> 1;
          }
      }
    }
  return( wkg );
}
```

2.2 TIME-OUT (400ms) & RETRY (max. : 2 times)



3. Command

3.1 01H Read Coils

This function code is used to read from 1 to 960 contiguous statuses of coils in a remote device.

PC → PLC

SLAVE Address		01 H
Function Code		01H
Starting Address	High	05H
	Low	40H
Quantity of coils	High	00H
	Low	10H
CRC-16	Low	3CH
	High	DEH

PLC→PC(OK)

SLAVE Address		01H
Function Code		01H
Byte count		02H
Outputs status M8~1		45H
Outputs status MF~9		34H
CRC-16	Low	8AH
	High	BBH

PLC→PC(ERROR)

SLAVE Address		01H
Function Code		81H
Exception Code		51H
CRC-16	Low	81H
	High	ACH

*: User set the start address equal multiple of 10H, and quantity of coils also equal multiple of 10H (read word coil status).

Sample: M8~1=45H (01000101B), coil M8~M1 status is OFF-ON-OFF-OFF, OFF-ON-OFF-ON;

3.2 03H Read Registers

This function code is used to read the contents of from 1 to approx. 61 contiguous block of holding registers in a remote device.

PC → PLC

SLAVE Address		01H
Function Code		03H
*Register Address	(High)	00H
	(Low)	00H
Data Length（Hi）		00H
Data Length（Lo）		13H
CRC-16 (Lo)		04H
CRC-16 (Hi)		07H

PLC→PC(OK)

SLAVE Address	01H
Function Code	03H
Data (byte)	26H
*Send out the data	
CRC-16 (Lo)	?
CRC-16 (Hi)	?

PLC→PC(ERROR)

SLAVE Address	01H
Function Code	83H
Exception Code	52H
CRC-16 (Lo)	C0H
CRC-16 (Hi)	CDH

3.3 05H Write Single Coil

This function code is used to write a single output to either ON or OFF in a remote device.

PC → PLC

SLAVE Address		01H
Function Code		05H
Coil Address	High	05H
	Low	02H
Coil Value	High	FFH
	Low	00H
CRC-16	Low	2DH
	High	36H

PLC→PC(OK)

SLAVE Address		01H
Function Code		05H
Coil Address	High	05H
	Low	02H
Coil Value	High	FFH
	Low	00H
CRC-16	Low	2DH
	High	36H

PLC→PC(ERROR)

SLAVE Address		01H
Function Code		85H
Exception Code		52H
CRC-16	Low	C3H
	High	6DH

A value of 0xFF00 requests the coil to be ON.

A value of 0x0000 requests the coil to be OFF.

3.4 06H Write single Register

This function code is used to write a single holding register in a remote device.

PC → PLC

SLAVE Address		01 H
Function Code		06H
*Register Address	(High)	01H
	(Low)	02H
Write Data	High	17H
	Low	70H
CRC-16 (Lo)		27H
CRC-16 (Hi)		E2H

PLC→PC(OK)

SLAVE Address		01H
Function Code		06H
*Register Address	High	01H
	Low	02H
Write Data	High	17H
	Low	70H
CRC-16 (Lo)		27H
CRC-16 (Hi)		E2H

PLC→PC(ERROR)

SLAVE Address	01H
Function Code	86H
Exception Code	52H
CRC-16 (Lo)	C3H
CRC-16 (Hi)	9DH

3.5 08H Diagnostic

The function code 08 provides a series of tests for checking the communication system between a client (Master) device and a server (Slave), or for checking various internal error conditions within a server.

Sub-Function 00: Return Query Data

Address		01 H
Function Code		08H
Sub Function	High	00H
	Low	00H
DATA	High	A5H
	Low	37H
CRC-16	High	DAH
	Low	8DH

Address		01H
Function Code		08H
Sub Function	High	00H
	Low	00H
DATA	High	A5H
	Low	37H
CRC-16	High	DAH
	Low	8DH

Address		01H
Function Code		88H
Exception Code		51H
CRC-16	High	87H
	Low	FCH

Data is a random word.

3.6 10H Write multiple Registers

This function code is used to write a block of contiguous registers (1 to approx. 59 registers) in a remote device.

PC → PLC

Address		01H
Function Code		10H
*Register Address	(High)	00H
	(Low)	00H
Data Length（Hi）		00H
Data Length（Lo）		13H
Byte counters		26H
Send out the data		
CRC-16 (Lo)		?
CRC-16 (Hi)		?

PLC→PC(OK)

Address		01H
Function Code		10H
*Register Address	(High)	00H
	(Low)	00H
Data Length（Hi）		00H
Data Length（Lo）		13H
CRC-16 (Lo)		81H
CRC-16 (Hi)		C4H

PLC→PC(ERROR)

Address	01H
Function Code	90H
Exception Code	52H
CRC-16 (Lo)	ACH
CRC-16 (Hi)	3DH

3.7 Exception Code

Under communication linking, the controller responses the Exception Code and send Function Code add 80H to main system if there is error happened.

Exception Code	Description
51	Frame error (Function Code error, Register Encoding error, Data Quantity Error)
52	Run mode and command disable
53	Secret mode and command disable
54	Data value over rang
55	Reserved
56	Reserved
57	SG2 the other error
58	Commands do not match SG2 edit mode
59	Reserved

4. Register Address

4.1 00xxH: Coil Status Address (word)

Register Address	Data Length	Usable Comm.	Content															
			F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
0000H	1	03H 06H 10H	R10	R0F	R0E	R0D	R0C	R0B	R0A	R09	R08	R07	R06	R05	R04	R03	R02	R01
0001H	1		G10	G0F	G0E	G0D	G0C	G0B	G0A	G09	G08	G07	G06	G05	G04	G03	G02	G01
0002H	1		T10	T0F	T0E	T0D	T0C	T0B	T0A	T09	T08	T07	T06	T05	T04	T03	T02	T01
0003H	1		C10	C0F	C0E	C0D	C0C	C0B	C0A	C09	C08	C07	C06	C05	C04	C03	C02	C01
0004H	1		M10	M0F	M0E	M0D	M0C	M0B	M0A	M09	M08	M07	M06	M05	M04	M03	M02	M01
0005H	1		Z04	Z03	Z02	Z01	I0C	I0B	I0A	I09	I08	I07	I06	I05	I04	I03	I02	I01
0006H	1		—	—	—	—	X0C	X0B	X0A	X09	X08	X07	X06	X05	X04	X03	X02	X01
0007H	1		—	—	—	—	—	—	—	—	Q08	Q07	Q06	Q05	Q04	Q03	Q02	Q01
0008H	1		—	—	—	—	Y0C	Y0B	Y0A	Y09	Y08	Y07	Y06	Y05	Y04	Y03	Y02	Y01
0009H	1		N10	N0F	N0E	N0D	N0C	N0B	N0A	N09	N08	N07	N06	N05	N04	N03	N02	N01
000AH	1		H10	H0F	H0E	H0D	H0C	H0B	H0A	H09	H08	H07	H06	H05	H04	H03	H02	H01
000BH	1		W10	W0F	W0E	W0D	W0C	W0B	W0A	W09	W08	W07	W06	W05	W04	W03	W02	W01
000CH	1		W20															W11
000DH	1		W30															W21
000EH	1		W40															W31
000FH	1		—	—	—	—	—	—	P02	P01	L08	L07	L06	L05	L04	L03	L02	L01
0010H	1	03H (Only FBD)	B16	B15	B14	B13	B12	B11	B10	B09	B08	B07	B06	B05	B04	B03	B02	B01
0011H	1		B32															B17
0012H	1		B48															B33
0013H	1		B64															B49
0014H	1		B80															B65
0015H	1		B96															B81
0016H	1		—	—	—	—	—	—	—	—	—	—	—	—	—	B99	B98	B97

Z can't be written.

R10, G10, T10, C10, M10, N10, H10, P02 only effective on SG2V3.

4.2 01xxH: Control register Address

Register Address	Data Length	Usable Comm.	Content															
			F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
0100H	1	03H 06H 10H	00								S1							
			RUN / STOP : S1 = 0 STOP S1 = 1 RUN															

<table>
<tr><td rowspan="2">0101H</td><td rowspan="2">1</td><td rowspan="2">03H</td><td colspan="8">BRAND ID</td><td colspan="8">GENIE MODE</td></tr>
<tr><td colspan="16">GENIE MODE (Hex) Only V-Type model
30=20VR-D, 70=20VR-12D
34=20VT-D, 74=20VT-12D</td></tr>
<tr><td rowspan="2">0102H</td><td rowspan="2">1</td><td rowspan="2">03H
06H
10H</td><td>A</td><td>Z</td><td>I1</td><td>I0</td><td>L3</td><td>L2</td><td>L1</td><td>L0</td><td>-</td><td>S1</td><td>S2</td><td>B</td><td>-</td><td>-</td><td>D1</td><td>D0</td></tr>
<tr><td colspan="16">STATUS1:
A： alarm at expand I/O No. unmatched
＝0： alarm
＝1： don’t alarm
Z: Z set
＝0： Z disable
＝1： Z enable
I1I0：expand I/O No.(0~3)
L3 L2 L1 L0: language
=1 : English
=2 : French
=3 : Spanish
=4 : Italian
=5 : German
=6 : Portugal
=7 : Chinese
B: Backlight on/off
=0 ： auto on/off
=1 ： always on
s1:Power down retain(M coil)
=1 : unretain
=0 : retain
S2:run/stop retain(Counter current value)
=1 : retain
=0 : unretain
D1D0：Data communication mode
=0： data link
=1： remote I/O master
=2： remote I/O slave</td></tr>
</table>

			PA	Error code
0103H	1	03H	STATUS2 (PA,Error) Error code: 0 = OK 1 = ROM error 2 = RAM error 3 = EEPROM error 4 = Program error 5 = Program logic error 6 = Watchdog error 7 = Expand error 8 = Communication error 9 = RTC error PA: 0 = PASSWORD OFF 1 = PASSWORD ON	
0104H	1	03H 10H	A01 Gain value	
0105H	1		A01 Offset value	
0106H	1		A02 Gain value	
0107H	1		A02 Offset value	
0108H	1		A03 Gain value	
0109H	1		A03 Offset value	
010AH	1		A04 Gain value	
010BH	1		A04 Offset value	
0110H	1	06H	0	1
		10H	CLEAR CODE	
0120H	1	03H 10H	A01 Gain value	
0121H	1		A01 Offset value	
0122H	1		A02 Gain value	
0123H	1		A02 Offset value	
0124H	1		A03 Gain value	
0125H	1		A03 Offset value	
0126H	1		A04 Gain value	
0127H	1		A04 Offset value	
0128H	1		A05 Gain value	
0129H	1		A05 Offset value	

012AH	1	03H 10H	A06 Gain value
012BH	1		A06 Offset value
012CH	1		A07 Gain value
012DH	1		A07 Offset value
012EH	1		A08 Gain value
012FH	1		A08 Offset value
			Analog configure: Note: GAIN = (0~999) OFFSET = (-50~50) (complement)

- Warning : change control register, data save to flash. (flash memory endurance 10k cycles).

4.3 02xxH: Current value Address

Register Address	Data Length	Usable Comm.	Content		Remark
Timer Current value					
0200H	1	03H	Timer01 current value		Scale: 00000~09999
0201H	1		Timer02 current value		
.....	.....		.....		
020EH	1		Timer0F current value		
Counter Current value					
0210H	2	03H	Counter01 current value		*1 Scale: 000000~999999
0211H	2		Counter02 current value		
.....	.....		.....		
021EH	2		Counter0F current value		
RTC Current value					
0220H	1	03H 10H	Current Year	Current Moon	Scale: Year:00~99 Month:01~12 Day:01~31 Week:00~06 Hour:00~23 Minute:00~59 Second:00~59
0221H	1		Current Day	Current Week	
0222H	1		Current Hour	Current Minute	
0223H	1		Current Second	00	
0224H	1		00	Current Year	
0225H	1		00	Current Moon	
0226H	1		00	Current Day	
0227H	1		00	Current Week	
0228H	1		00	Current Hour	
0229H	1		00	Current Minute	
022AH	1		00	Current Second	

ANALOG Current value					
0230H	1	03H	A01 Current Value		
0231H	1		A02 Current Value		
0232H	1		A03 Current Value		Scale: 0000~0999
0233H	1		A04 Current Value		
0234H	1		A05 Current Value		
0235H	1		A06 Current Value		
0236H	1		A07 Current Value		
0237H	1		A08 Current Value		
PWM current value					
0260H	3H	03H	00	PWM current Run number	Scale: P01 PWM mode PW: 0~32767 PT: 1~32767
			P01 Current PW Value		
			P01 Current PT Value		

4.4 03xxH: User character Address (Chinese lattice)

Register Address	Data Length	Usable Comm.	Content	Remark
0300H	10H	03H 10H	Character5	
0301H	10H		Character6	
……	……		……	
033BH	10H		Character64	

- Warning : change user character, data save to flash. (flash memory endurance 10k cycles).

4.5 04xxH: Preset value Address

Register Address	Data Length	Usable Comm.	Content	Remark
Timer Preset value				
0400H	1H	03H 10H	Timer01 preset value	Scale: 00000~09999
0401H	1H		Timer02 preset value	
……	……		……	
040EH	1H		Timer0F preset value	
Counter Preset value				
0410H	2H/5H	03H 10H	Counter01 preset value	*2
0411H	2H/5H		Counter02 preset value	
……	……		……	
041EH	2H/5H		Counter0F preset value	

RTC Preset value				
0420H	3H	03H 10H	RTC01 preset value	*3
0421H	3H		RTC02 preset value	
……	……		……	
042EH	3H		RTC0F preset value	
ANALOG Preset value				
0430H	1H	03H 10H	ANALOG01 preset value	Scale: 0~9999
0431H	1H		ANALOG02 preset value	
……	……		……	
043EH	1H		ANALOG0F preset value	
PWM Preset value				
0460H	10H	03H 10H	PWM01 preset value	*4

- Warning : change preset value, data save to flash. (flash memory endurance 10k cycles).

4.6 05xxH: Coils Address (bit)

Register Address	Data Length	Usable Comm.	Content	Remark
0500H~050FH	10H (Read)	01H 05H	R01~R10	
0510H~051FH			G01~G10	
0520H~052FH			T01~T10	
0530H~053FH			C01~C10	
0540H~054FH			M01~M10	
0550H~055FH			I01~I0C,Z01~Z04	Z01~Z04 can't be written;
0560H~056FH			X01~X0C	056CH~056FH, reserved;
0570H~057FH			Q01~Q08	0578H~057FH, reserved;
0580H~058FH			Y01~Y0C	058CH~058FH, reserved;
0590H~059FH			N01~N10	
05A0H~05AFH	10H (Read)	01H 05H	H01~H10	
05B0H~05BFH			W01~W16	
05C0H~05CFH			W17~W32	
05D0H~05DFH			W33~W48	
05E0H~05EFH			W49~W64	
05F0H~05FFH			L01~L08,P01~P02, S01	05FBH~05FFH, reserved;

*: 01H: user set the start address equal multiple of 10H, and quantity of coils also equal multiple of 10H (01H: read word coil status).

Z can't be written. Reserved address can't be written.

R10, G10, T10, C10, M10, N10, H10, P02 only effective on SG2V3.

4.7 06xxH: Coil Status Address (word) for V3 type only

Register Address	Data Length	Usable Comm.	Content															
			F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
0600H	1		R10	R0F	R0E	R0D	R0C	R0B	R0A	R09	R08	R07	R06	R05	R04	R03	R02	R01
0601H	1		-	R1F	R1E	R1D	R1C	R1B	R1A	R19	R18	R17	R16	R15	R14	R13	R12	R11
0602H	1		G10	G0F	G0E	G0D	G0C	G0B	G0A	G09	G08	G07	G06	G05	G04	G03	G02	G01
0603H	1		-	G1F	G1E	G1D	G1C	G1B	G1A	G19	G18	G17	G16	G15	G14	G13	G12	G11
0604H	1		T10	T0F	T0E	T0D	T0C	T0B	T0A	T09	T08	T07	T06	T05	T04	T03	T02	T01
0605H	1		-	T1F	T1E	T1D	T1C	T1B	T1A	T19	T18	T17	T16	T15	T14	T13	T12	T11
0606H	1		C10	C0F	C0E	C0D	C0C	C0B	C0A	C09	C08	C07	C06	C05	C04	C03	C02	C01
0607H	1		-	C1F	C1E	C1D	C1C	C1B	C1A	C19	C18	C17	C16	C15	C14	C13	C12	C11
0608H	1		M10	M0F	M0E	M0D	M0C	M0B	M0A	M09	M08	M07	M06	M05	M04	M03	M02	M01
0609H	1		M20	M1F	M1E	M1D	M1C	M1B	M1A	M19	M18	M17	M16	M15	M14	M13	M12	M11
060AH	1		M30	M2F	M2E	M2D	M2C	M2B	M2A	M29	M28	M27	M26	M25	M24	M23	M22	M21
060BH	1		-	M3F	M3E	M3D	M3C	M3B	M3A	M39	M38	M37	M36	M35	M34	M33	M32	M31
060CH	1		N10	N0F	N0E	N0D	N0C	N0B	N0A	N09	N08	N07	N06	N05	N04	N03	N02	N01
060DH	1	03H	N20	N1F	N1E	N1D	N1C	N1B	N1A	N19	N18	N17	N16	N15	N14	N13	N12	N11
060EH	1	06H	N30	N2F	N2E	N2D	N2C	N2B	N2A	N29	N28	N27	N26	N25	N24	N23	N22	N21
060FH	1	10H	-	N3F	N3E	N3D	N3C	N3B	N3A	N39	N38	N37	N36	N35	N34	N33	N32	N31
0610H	1		-	-	-	-	I0C	I0B	I0A	I09	I08	I07	I06	I05	I04	I03	I02	I01
0611H	1		-	-	-	-	X0C	X0B	X0A	X09	X08	X07	X06	X05	X04	X03	X02	X01
0612H	1		-	-	-	-	Y0C	Y0B	Y0A	Y09	Y08	Y07	Y06	Y05	Y04	Y03	Y02	Y1
0613H	1		-	-	-	-	-	-	-	-	Q08	Q07	Q06	Q05	Q04	Q03	Q02	Q01
0614H	1		-	-	-	-	-	-	-	-	-	-	-	-	Z04	Z03	Z02	Z01
0615H	1		H10	H0F	H0E	H0D	H0C	H0B	H0A	H09	H08	H07	H06	H05	H04	H03	H02	H01
0616H	1		-	H1F	H1E	H1D	H1C	H1B	H1A	H19	H18	H17	H16	H15	H14	H13	H12	H11
0617H	1		-	-	-	-	-	-	-	-	L08	L07	L06	L05	L04	L03	L02	L01
0618H	1		-	-	-	-	-	-	-	-	-	-	-	-	-	S01	P02	P01
0619H	1		W10	W0F	W0E	W0D	W0C	W0B	W0A	W09	W08	W07	W06	W05	W04	W03	W02	W01
061AH	1		W20	W1F	W1E	W1D	W1C	W1B	W1A	W19	W18	W17	W16	W15	W14	W13	W12	W11
061BH	1		W30	W2F	W2E	W2D	W2C	W2B	W2A	W29	W28	W27	W26	W25	W24	W23	W22	W21
061CH	1		W40	W3F	W3E	W3D	W3C	W3B	W3A	W39	W38	W37	W36	W35	W34	W33	W32	W31
0620H	1	03H	B16	B15	B14	B13	B12	B11	B10	B09	B08	B07	B06	B05	B04	B03	B02	B01
0621H	1	(Only	B32															B17

0622H	1		B48															B33
0623H	1		B64															B49
0624H	1		B80															B65
0625H	1		B96															B81
0626H	1		B112															B97
0627H	1		B128															B113
0628H	1	03H	B144															B129
0629H	1	(Only	B160															B145
062AH	1	FBD)	B176															B161
062BH	1		B192															B177
062CH	1		B208															B193
062DH	1		B242															B209
062EH	1		B240															B243
062FH	1		B256															B241
0630H	1		-	-	-	-	-	-	-	-	-	-	-	-	B260	B259		B257

Z can't be written.

4.8 07xxH: Control register Address for V3 type only

Register Address	Data Length	Usable Comm.	Content
			F E D C B A 9 8 7 6 5 4 3 2 1 0
0700H	1	03H 06H 10H	00 S1 RUN / STOP : S1 = 0 STOP S1 = 1 RUN
0701H	1	03H	BRAND ID GENIE MODE GENIE MODE (Hex) Only V-Type model 30=20VR-D, 70=20VR-12D 34=20VT-D, 74=20VT-12D
0702H	1	03H 06H 10H	A Z I1 I0 L3 L2 L1 L0 - S1 S2 B - - D1 D0 STATUS1: A: alarm at expand I/O No. unmatched =0: alarm =1: don't alarm Z: Z set =0: Z disable =1: Z enable I1I0: expand I/O No.(0~3)

			L3 L2 L1 L0: language =1 : English =2 : French =3 : Spanish =4 : Italian =5 : German =6 : Portugal =7 : Chinese B: Backlight on/off =0 ： auto on/off =1 ： always on s1:Power down retain(M coil) =1 : unretain =0 : retain S2:run/stop retain(Counter current value) =1 : retain =0 : unretain D1D0：Data communication mode =0： data link =1： remote I/O master =2： remote I/O slave
0703H	1	03H	PA | Error code STATUS2 (PA,Error) Error code: 0 = OK 1 = ROM error 2 = Vpd error 3 = EEPROM error 4 = Program error 5 = Program logic error 6 = Watchdog error 7 = Expand error 8 = Communication error 9 = RTC error PA: 0 = PASSWORD OFF 1 = PASSWORD ON

0704H	1		A01 Gain value	
0705H	1		A01 Offset value	
0706H	1		A02 Gain value	
0707H	1	03H	A02 Offset value	
0708H	1	10H	A03 Gain value	
0709H	1		A03 Offset value	
070AH	1		A04 Gain value	
070BH	1		A04 Offset value	
0710H	1	06H	0	1
		10H	CLEAR CODE	
0720H	1		A01 Gain value	
0721H	1		A01 Offset value	
0722H	1		A02 Gain value	
0723H	1		A02 Offset value	
0724H	1		A03 Gain value	
0725H	1		A03 Offset value	
0726H	1		A04 Gain value	
0727H	1		A04 Offset value	
0728H	1	03H	A05 Gain value	
0729H	1	10H	A05 Offset value	
072AH	1		A06 Gain value	
072BH	1		A06 Offset value	
072CH	1		A07 Gain value	
072DH	1		A07 Offset value	
072EH	1		A08 Gain value	
072FH	1		A08 Offset value	
			Analog configure: Note: GAIN = (0~999) OFFSET = (-50~50) (complement)	

- Warning : change ontrol register, data save to flash. (flash memory endurance 10k cycles).

4.9 08xxH~11xxH: Current value Address for V3 type only

Register Address	Data Length	Usable Comm.	Content		Remark
Timer Current value (08xxH)					
0800H	1H	03H	Timer01 current value		Scale: 00000~09999
0801H	1H		Timer02 current value		
……	……		……		
081EH	1H		Timer1F current value		
081FH	1H		Timer20 current value		Only FBD mode
……	……		……		
08F9H	1H		TimerFA current value		
Counter Current value (09xxH~0AxxH)					
0900H	1H	03H	C01 current Value middle byte	C01 current Value Low byte	
0901H	1H	03H	00	C01 current Value High byte	Scale: 000000~999999
0902H	1H		C02 current Value middle byte	C02 current Value Low byte	
0903H	1H		00	C02 current Value High byte	
……	……		……		
093CH	1H		C1F current Value middle byte	C1F current Value Low byte	
093DH	1H		00	C1F current Value High byte	
093EH	1H		C20 current Value middle byte	C20 current Value Low byte	Only FBD mode
093FH	1H		00	C20 current Value High byte	
……	……		……		
0AF2H	1H		CFA current Value middle byte	CFA current Value Low byte	
0AF3H	1H		00	CFA current Value High byte	
(0BxxH) RTC, Analog, PWM, AT,AQ Current value					

RTC Current value (0B0xH)					
0B00H	1	03H 10H	Current Year	Current Moon	Scale: Year:00~99 Month:01~12 Day:01~31 Week:00~06 Hour:00~23 Minute:00~59 Second:00~59
0B01H	1		Current Day	Current Week	
0B02H	1		Current Hour	Current Minute	
0B03H	1		Current Second	00	
0B04H	1		00	Current Year	
0B05H	1		00	Current Moon	
0B06H	1		00	Current Day	
0B07H	1		00	Current Week	
0B08H	1		00	Current Hour	
0B09H	1		00	Current Minute	
0B0AH	1		00	Current Second	
ANALOG Current value (0B1xH)					
0B10H	1H	03H	A01 Current Value		Scale: 0000~0999
0B11H	1H		A02 Current Value		
0B12H	1H		A03 Current Value		
0B13H	1H		A04 Current Value		
0B14H	1H	03H	A05 Current Value		
0B15H	1H		A06 Current Value		
0B16H	1H		A07 Current Value		
0B17H	1H		A08 Current Value		
PWM Current value (0B2xH)					
0B20H	1H	03H	00	P01 PWM current Run number	P01: mode1 PWM mode
0B21H	1H		P01 current PW value(0~32767)		
0B22H	1H		P01 current PT value(1~32767)		
0B20H	1H		00	00	P01: mode2 PLSY mode
0B21H	1H		PLSY frequency(0001~1000)		
0B22H	1H		PLSY pulse number(00000~32767)		
0B23H	1H		00	P02 PWM current Run number	P02: only PWM mode
0B24H	1H		P02 current PW value(0~32767)		
0B25H	1H		P02 current PT value(1~32767)		
AT (Analog Temperature) Current value (0B3xH)					
0B30H	1H	03H	AT01 Current Value		Scale: -1000~6000
0B31H	1H		AT02 Current Value		
0B32H	1H		AT03 Current Value		
0B33H	1H		AT04 Current Value		

AQ (Analog Output) Current value (0B4xH)				
0B40H	1H	03H	AQ01 Current Value	Scale: Voltage mode: 0~1000 Current mode: 0~500
0B41H	1H		AQ02 Current Value	
0B42H	1H		AQ03 Current Value	
0B43H	1H		AQ04 Current Value	
AS (ADD-Subtract) Current value (0CxxH)				
0C00H	1H	03H	AS01 Current Value	Scale: -32768~32767
0C01H	1H		AS02 Current Value	
……	……		……	
0C1EH	1H		AS1F Current Value	
0C1FH	1H		AS20 Current Value	Only FBD mode
……	……		……	
0CF9H	1H		ASFA Current Value	
MD (Multiply-Divide) Current value (0DxxH)				
0D00H	1H	03H	MD01 Current Value	Scale: -32768~32767
0D01H	1H		MD02 Current Value	
……	……		……	
0D1EH	1H		MD1F Current Value	
0D1FH	1H	03H	MD20 Current Value	Only FBD mode
……	……		……	
0DF9H	1H		MDFA Current Value	
PID (PID control) Current value (0ExxH)				
0E00H	1H	03H	PID01 Current Value	Scale: -32768~32767
0E01H	1H		PID02 Current Value	
……	……		……	
0E0EH	1H		PID0F Current Value	
0E0FH	1H		PID10 Current Value	Only FBD mode
……	……		……	
0E1DH	1H		PID1E Current Value	
MX (Data multiplexer) Current value (0FxxH)				
0F00H	1H	03H	MX01 Current Value	Scale: -32768~32767
0F01H	1H		MX02 Current Value	
……	……		……	
0F1EH	1H		MX1F Current Value	
0F1FH	1H		MX20 Current Value	Only FBD mode
……	……		……	
0FF9H	1H		MXFA Current Value	

AR (Analog ram control) Current value (10xxH)				
1000H	1H	03H	AR01 Current Value	Scale: 0~32767
1001H	1H		AR02 Current Value	
……	……		……	
100EH	1H		AR0F Current Value	
100FH	1H		AR10 Current Value	Only FBD mode
……	……		……	
101DH	1H		AR1E Current Value	
DR (Data register) Current value (11xxH)				
1100H	1H	03H 06H 10H	DR01 Current Value	Scale: Signed: -32768~32767 Unsigned: 0~65535
1101H	1H		DR02 Current Value	
……	……		……	
11EFH	1H		DRF0 Current Value	

4.10 12xxH~27xxH: Preset value Address for V3 type only

Register Address	Data Length	Usable Comm.	Content		Remark
Timer Preset value (12xxH)					
1200H	1H	03H 06H 10H	Timer01 preset value		Scale: 00000~09999
1201H	1H		Timer02 preset value		
……	……		……		
121EH	1H		Timer1F preset value		
121FH	1H		Timer20 preset value		Only FBD mode
……	……		……		
12F9H	1H		TimerFA preset value		
Counter Preset value (13xxH~14xxH)					
1300H	1H	03H 06H 10H	C01 preset Value middle byte	C01 preset Value Low byte	Scale: 000000~999999 Can't read or write mode8
1301H	1H		00	C01 preset Value High byte	
……	……		……		
133CH	1H		C1F preset Value middle byte	C1F preset Value Low byte	
133DH	1H		00	C1F preset Value High byte	
133EH	1H		C20 preset Value middle byte	C20 preset Value Low byte	Only FBD mode
133FH	1H		00	C20 preset Value High byte	
……	……		……		
14F2H	1H		CFA preset Value middle byte	CFA preset Value Low byte	
14F3H	1H		00	CFA preset Value High byte	
RTC Preset value (15xxH~17xxH)					
1500H	1H	03H 06H 10H	RTC01 preset Value		*3
1501H	1H				
1502H	1H				
……	……		……		
155AH	1H		RTC1F preset Value		
155BH	1H				
155CH	1H				

155DH	1H	03H 06H 10H	RTC20 preset Value	Only FBD mode
155EH	1H			
155FH	1H			
……	……		……	
17EBH	1H		RTCFA preset Value	
17ECH	1H			
17EDH	1H			
Analog Preset value (18xxH)				
1800H	1H	03H 06H 10H	Analog01 comparative preset value	Scale: 00000~09999
……	……		……	
181EH	1H		Analog1F comparative preset value	
181FH	1H		Analog20 comparative preset value	Only FBD mode
……	……		……	
18F9H	1H		AnalogFA comparative preset value	
PWM Preset value (19xxH)				
1900H	1H	03H 06H 10H	P01 PWM mode PW1 preset value (or PLSY mode frequency value)	Scale: P01~P02 PWM mode PW1~8: 0~32767 PT1~8: 1~32767 P01 PLSY mode frequency: 0001~1000 pulse number: 00000~32767
1901H	1H		P01 PWM mode PT1 preset value (or PLSY mode pulse number value)	
1902H	1H		P01 PWM mode PW2 preset value (or PLSY mode 0)	
1903H	1H		P01 PWM mode PT2 preset value (or PLSY mode 0)	
……	……		……	
190EH	1H		P01 PWM mode PW8 preset value (or PLSY mode 0)	
190FH	1H		P01 PWM mode PT8 preset value (or PLSY mode 0)	
1910H	1H		P02 PWM mode PW1 preset value	
1911H	1H		P02 PWM mode PT1 preset value	
1912H	1H		P02 PWM mode PW2 preset value	
1913H	1H		P02 PWM mode PT2 preset value	
……	……		……	
191CH	1H		P02 PWM mode PW7 preset value	
191DH	1H		P02 PWM mode PT7 preset value	
191EH	1H		P02 PWM mode PW8 preset value	
191FH	1H		P02 PWM mode PT8 preset value	

AS (ADD-Subtract) Preset value (1AxxH~1CxxH)				
1A00H	1H	03H 06H 10H	AS01 V1 preset value	Scale: V1:-32768~32767 V2:-32768~32767 V3:-32768~32767
1A01H	1H		AS01 V2 preset value	
1A02H	1H		AS01 V3 preset value	
……	……		……	
1A5AH	1H		AS1F V1 preset value	
1A5BH	1H		AS1F V2 preset value	
1A5CH	1H		AS1F V3 preset value	
1A5DH	1H		AS20 V1 preset value	Only FBD mode
1A5EH	1H		AS20 V2 preset value	
1A5FH	1H		AS20 V3 preset value	
……	……		……	
1CEBH	1H		ASFA V1 preset value	
1CECH	1H		ASFA V2 preset value	
1CEDH	1H		ASFA V3 preset value	
MD (Multiply-Divide) Preset value (1DxxH~1FxxH)				
1D00H	1H	03H 06H 10H	MD01 V1 preset value	Scale: V1:-32768~32767 V2:-32768~32767 V3:-32768~32767
1D01H	1H		MD01 V2 preset value	
1D02H	1H		MD01 V3 preset value	
……	……		……	
1D5AH	1H		MD1F V1 preset value	
1D5BH	1H		MD1F V2 preset value	
1D5CH	1H		MD1F V3 preset value	
1D5DH	1H		MD20 V1 preset value	Only FBD mode
1D5EH	1H		MD20 V2 preset value	
1D5FH	1H		MD20 V3 preset value	
……	……		……	
1FEBH	1H		MDFA V1 preset value	
1FECH	1H		MDFA V2 preset value	
1FEDH	1H		MDFA V3 preset value	
PID Preset value (20xxH)				
2000H	1H	03H 06H 10H	PI01 SV preset value	Scale: SV:-32768~32767 PV:-32768~32767 Ts:1~32767 Kp:1~32767 Ti:1~32767 Td:1~32767
2001H	1H		PI01 PV preset value	
2002H	1H		PI01 Ts preset value	
2003H	1H		PI01 Kp preset value	
2004H	1H		PI01 Ti preset value	
2005H	1H		PI01 Td preset value	
……	……		……	

2054H	1H		PI0F SV preset value	
2055H	1H		PI0F PV preset value	
2056H	1H		PI0F Ts preset value	
2057H	1H		PI0F Kp preset value	
2058H	1H		PI0F Ti preset value	
2059H	1H		PI0F Td preset value	
205AH	1H		PI10 SV preset value	
205BH	1H		PI10 PV preset value	
205CH	1H	03H	PI10 Ts preset value	
205DH	1H	06H	PI10 Kp preset value	
205EH	1H	10H	PI10 Ti preset value	
205FH	1H		PI10 Td preset value	
……	……		……	Only FBD mode
20AEH	1H		PI1E SV preset value	
20AFH	1H		PI1E PV preset value	
20B0H	1H		PI1E Ts preset value	
20B1H	1H		PI1E Kp preset value	
20B2H	1H		PI1E Ti preset value	
20B3H	1H		PI1E Td preset value	
MX (Data multiplexer) Preset value (21xxH~24xxH)				
2100H	1H		MX01 V1 preset value	
2101H	1H		MX01 V2 preset value	
2102H	1H		MX01 V3 preset value	Scale:
2103H	1H		MX01 V4 preset value	V1:-32768~32767
……	……		……	V2:-32768~32767
2178H	1H		MX1F V1 preset value	V3:-32768~32767
2179H	1H		MX1F V2 preset value	V4:-32768~32767
217AH	1H		MX1F V3 preset value	
217BH	1H	03H	MX1F V4 preset value	
217CH	1H	06H	MX20 V1 preset value	
217DH	1H	10H	MX20 V2 preset value	
217EH	1H		MX20 V3 preset value	
217FH	1H		MX20 V4 preset value	
……	……		……	Only FBD mode
24E4H	1H		MXFA V1 preset value	
24E5H	1H		MXFA V2 preset value	
24E6H	1H		MXFA V3 preset value	
24E7H	1H		MXFA V4 preset value	

AR (Analog ram control) Preset value (25xxH)				
2500H	1H	03H 06H 10H	AR01 LEVEL1 preset value(mode1)	
			AR01 Level0 preset value(mode2)	
2501H	1H		AR01 LEVEL2 preset value(mode1)	
			AR01 Level1 preset value(mode2)	
2502H	1H		AR01 MAXL preset value(mode1)	Scale: Mode1: LEVEL1: -10000~20000 LEVEL2: -10000~20000 MAXL: -10000~20000 StSp:0~20000 Rate:0~10000 A:0~01000 B:-10000~10000 Mode2: Level0~Level3, MaxL: 0~32767 Ta:1~32767
			AR01 Level2 preset value(mode2)	
2503H	1H		AR01 StSp preset value(mode1)	
			AR01 Level3 preset value(mode2)	
2504H	1H		AR01 Rate preset value(mode1)	
			AR01 MaxL preset value(mode2)	
2505H	1H		AR01 A preset value(mode1)	
			AR01 Ta preset value(mode2)	
2506H	1H		AR01 B preset value(mode1)	
			00(mode2)	
……	……		……	
2564H	1H		AR0F MAXL preset value(mode1)	
			AR0F Level2 preset value(mode2)	
2565H	1H		AR0F StSp preset value(mode1)	
			AR0F Level3 preset value(mode2)	
2566H	1H		AR0F Rate preset value(mode1)	
			AR0F MaxL preset value(mode2)	
2567H	1H		AR0F A preset value(mode1)	
			AR0F Ta preset value(mode2)	
2568H	1H		AR0F B preset value(mode1)	
			00(mode2)	
2569H	1H		AR10 LEVEL1 preset value(mode1)	Only FBD mode
			AR10 Level0 preset value(mode2)	
256AH	1H		AR10 LEVEL2 preset value(mode1)	
			AR10 Level1 preset value(mode2)	
256BH	1H		AR10 MAXL preset value(mode1)	
			AR10 Level2 preset value(mode2)	
256CH	1H		AR10 StSp preset value(mode1)	
			AR10 Level3 preset value(mode2)	
256DH	1H		AR10 Rate preset value(mode1)	
			AR10 MaxL preset value(mode2)	
……	……		……	

25CBH	1H		AR1E LEVEL1 preset value(mode1)	
			AR1E Level0 preset value(mode2)	
25CCH	1H		AR1E LEVEL2 preset value(mode1)	
			AR1E Level1 preset value(mode2)	
25CDH	1H		AR1E MAXL preset value(mode1)	
			AR1E Level2 preset value(mode2)	
25CEH	1H		AR1E StSp preset value(mode1)	
			AR1E Level3 preset value(mode2)	
25CFH	1H		AR1E Rate preset value(mode1)	
			AR1E MaxL preset value(mode2)	
25D0H	1H		AR1E A preset value(mode1)	
			AR1E Ta preset value(mode2)	
25D1H	1H		AR1E B preset value(mode1)	
			00(mode2)	
DR (Data register) Preset value (26xxH)				
2600H	1H	03H 06H 10H	DR01 preset value	Scale: Signed: -32768~32767 Unsigned: 0~65535
2601H	1H		DR02 preset value	
……	……		……	
26EFH	1H		DRF0 preset value	
AQ (Analog Output) Preset value (27xxH)				
2700H	1H	03H 06H 10H	AQ01 preset value	Scale: Voltage mode: 0~1000 Current mode: 0~500
2701H	1H		AQ02 preset value	
2702H	1H		AQ03 preset value	
2703H	1H		AQ04 preset value	

- Warning : change preset value, data save to flash. (flash memory endurance 10k cycles).

4.11 2BxxH~2ExxH: Coils Address (bit) for V3 type only

Register Address	Data Length	Usable Comm.	Content	Remark
2B00H~2B1FH	10H (Read)	01H 05H	R01~R1F	2B1FH, reserved;
2B20H~2B3FH			G01~G1F	2B3FH, reserved;
2B40H~2B5FH			T01~T1F	2B5FH, reserved;
2B60H~2B7FH			C01~C1F	2B7FH, reserved;
2B80H~2BBFH			M01~M3F	2BBFH, reserved;
2BC0H~2BFFH			N01~N3F	2BFFH, reserved;
2C00H~2C0FH			I01~I0C	2C0CH~2C0FH, reserved;
2C10H~2C1FH			X01~X0C	2C1CH~2C1FH reserved;
2C20H~2C2FH			Y01~Y0C	2C2CH~2C2FH, reserved;
2C30H~2C3FH			Q01~Q08	2C38H~2C3FH, reserved;
2C40H~2C4FH			Z01~Z04	Z01~Z04 can't be written; 2C44H~2C4FH, reserved;
2C50H~2C6FH			H01~H31	2C6FH, reserved;
2C70H~2C7FH			L01~L08	2C78H~2C7FH, reserved;
2C80H~2C8FH			P01,P02 ,S01	2C83H~2C8FH, reserved;
2C90H~2CCFH			W01~W64	
2D00H~2E0FH			B001~B260	2E04H~2E0FH, reserved; FBD only

*: 01H: user set the start address equal multiple of 10H, and quantity of coils also equal multiple of 10H (01H: read word coil status).

Z can't be written. Reserved address can't be written.

5. NOTE

5.1 Note 1: Counter current value

	Length	High bytes	Low bytes
	2H	Counter current Value middle byte	Counter current Value Low byte
		00	Counter current Value High byte

Counter value: 0~999999(0~0F423FH)

5.2 Note 2: Counter Preset Value

	Length	High bytes	Low bytes
Counter mode 1~7	2H	Counter preset Value middle byte	Counter preset Value Low byte
		00	Counter preset Value High byte
Counter mode8	5H	Interval time preset value	
		Counter ON preset Value middle byte	Counter ON preset Value Low byte
		00	Counter ON preset Value High byte
		Counter OFF preset Value middle byte	Counter OFF preset Value Low byte
		00	Counter OFF preset Value High byte

Counter value: 0~999999(0~0F423FH);

5.3 Note 3: RTC Preset Value

	Length	High bytes	Low bytes
RTC mode1~2	3H	Turn on week	Turn off week
		Turn on hour	Turn on minute
		Turn off hour	Turn off minute
RTC mode3	3H	Turn on year	Turn off year
		Turn on month	Turn on day
		Turn off month	Turn off day
RTC mode4	3H	00	Round time (week)
		Round time (hour)	Round time (minute)
		00	Round time (second)

Year:00~99 Month:01~12 Day:01~31 Week:00~06

Hour:00~23 Minute:00~59 Second:00~59

5.4 Note 4: PWM Preset Value

Length	High bytes	Low bytes
10H	PW1 preset value	
	PT1 preset value	
	PW2 preset value	
	PT2 preset value	
	PW3 preset value	
	PT3 preset value	
	PW4 preset value	
	PT4 preset value	
	PW5 preset value	
	PT5 preset value	
	PW6 preset value	
	PT6 preset value	
	PW7 preset value	
	PT7 preset value	
	PW8 preset value	
	PT8 preset value	

PW: Pulse Width Value(00000~32767)

PT: Period Value(00001~32767)

6. Which is important

2006.07.05, add command : read or write analog set (A1~A8 gain + offset) .

2006.08.14, add write single coil status.

The protocol is applicable to SG2 which version about V1.7 (include V1.7).

2006-09-22, add RTC mode4 (V1.8) ;

2009-04-10, add SG2 V3 type;

2009-12-29, add data format description;

2010-06-18, V05, add AR mode2(V3.3);

2010-01-02, V06, add function, can write DR current value (V3.4) ;

Add dexcription : when writing function block preset value, maybe write flash (flash memory endurance 10k cycles).