

SG2 Expansion Communication Modbus Protocol

- 1. Communication Data Frame2
 - 1.1 Hardware Installation2
 - 1.2 Data Frame for RTU Mode2
 - 1.3 Slave Address2
 - 1.4 Function Code2
- 2. CMS (Checksum and Time-out Definition)3
 - 2.1 CRC Check:3
 - 2.2 Time-out (500ms) & Retry (max. : 2 times).....3
- 3. Command.....4
 - 3.1 03H Read Register.....4
 - 3.2 06H Write Single Register.....4
 - 3.3 08H Loop Back Check4
 - 3.4 10H Write Multiple Registers4
 - 3.5 Exception Code5
- 4. Register Address6
 - 4.1 (00xxH) Coil Status Address.....6
 - 4.2 (01xxH) Control Register Address.....6
 - 4.3 (02XXH) Current Value Address.....6
 - 4.4 (04XXH) Preset Value Address7
 - TMR.....7
 - Counter.....7
 - RTC.....7
 - Analog.....7
 - PWM.....7
- 5. Notes8
 - 5.1 Note 1: Counter Current Value.....8
 - 5.2 Note 2: Counter Preset Value8
 - 5.3 Note 3: RTC Preset Value8
 - 5.4 Note 4: PWM Preset Value8



International Headquarters: 707 Dayton Road PO Box 1040 Ottawa, IL 61350 USA
 815-433-5100 Fax 433-5104 www.bb-elec.com orders@bb-elec.com support@bb-elec.com

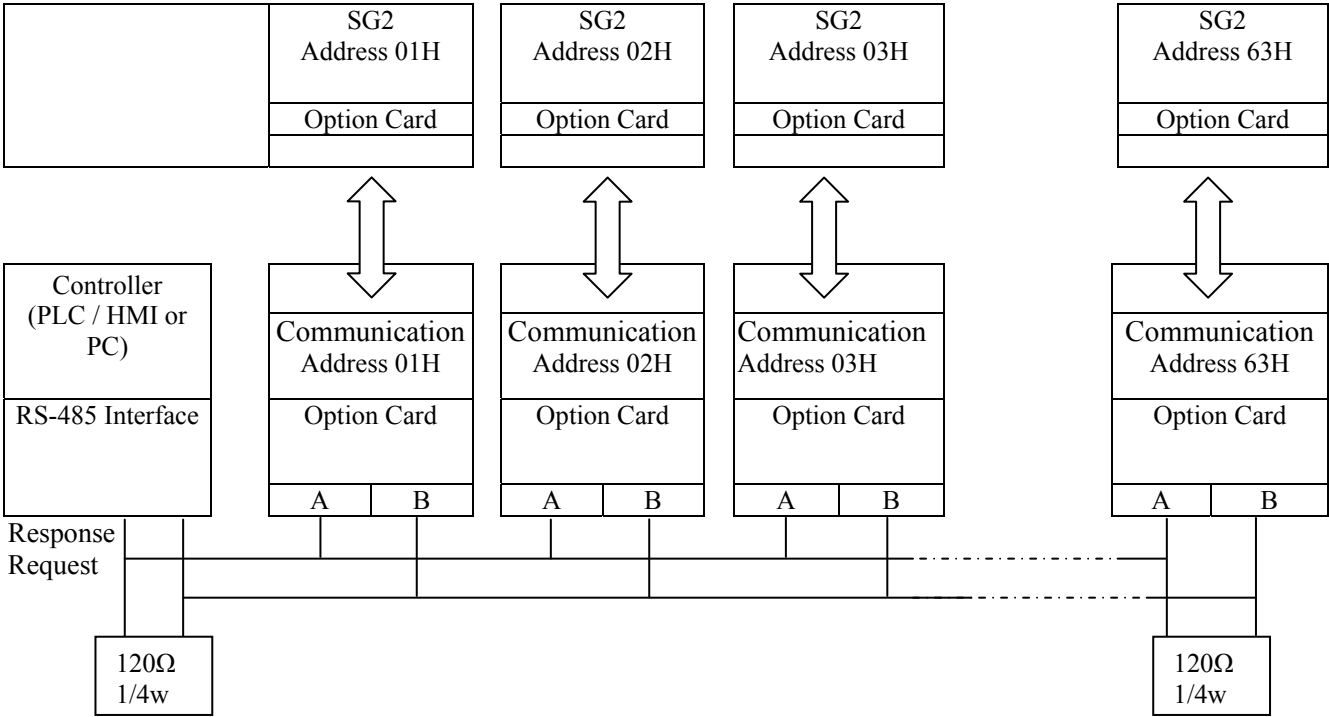
European Headquarters: Westlink Commercial Park Oranmore Co. Galway Ireland
 +353 91 792444 Fax +353 91 792445 www.bb-europe.com orders@bb-europe.com support@bb-europe.com

1. Communication Data Frame

SG2 series PLC can be communication controlled by the PC or other controller with the communication protocol, Modbus RTU mode, RS-485.

Baud Rate : 4800, 9600, 19200, 38400, 57600
 Stop Bit : 2 bit
 Parity : 1bit (stop 1 bit)
 Frame Length Maximum: 64 bytes

1.1 Hardware Installation



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

1.2 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	1 byte
Function Code	1 byte
Data	N byte
CRC16 Check	2 byte
Signal Interval	Signal Interval

** The interval should be maintained at 500ms between command signal and request. If command is write-function-preset-value, the interval should be maintained at 1000ms ;

1.3 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)

1.4 Function Code
 03H: Read the register contents
 06H: Write a WORD to register
 08H: Loop test
 10H: Write several data to register
 (complex number register write)



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 (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 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.

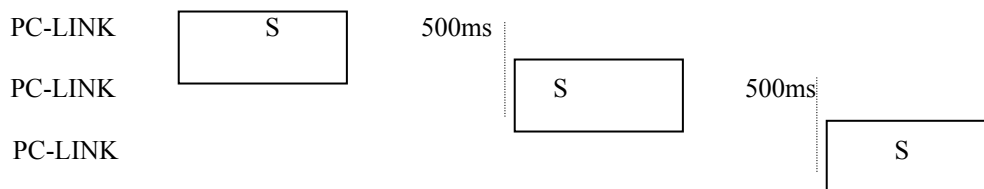
- **CRC Calculation Application Program**

```

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

```

2.2 Time-Out (500ms) & Retry (max. : 2 times)



Attention : When writing SG2-Special-Function-Block's preset value, the TIME-OUT value is 1000ms ;
 (When SG2 time-out or detect checksum error, or SG2 response error code = checksum error, PC-LINK retry maximum two times, and if two times after still error, then display "Communication error")

Attached : When Modbus Communication Module response an error information, waiting a resetting-time (Modbus transfer 64bytes data time); If baud rate is 4800bps, the time is 147ms; if baud rate is 9600bps, the time is 73ms; if baud rate is 19200bps, the time is 37ms; if the baud rate is 38400bps, the time is 18ms; if baud rate is 57600bps, the time is 12ms;



International Headquarters: 707 Dayton Road PO Box 1040 Ottawa, IL 61350 USA
 815-433-5100 Fax 433-5104 www.bb-elec.com orders@bb-elec.com support@bb-elec.com

European Headquarters: Westlink Commercial Park Oranmore Co. Galway Ireland
 +353 91 792444 Fax +353 91 792445 www.bb-europe.com orders@bb-europe.com support@bb-europe.com

3. Command

3.1 03H Read Register

PC → PLC

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

PLC→PC(OK)

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

PLC→PC(ERROR)

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

3.2 06H Write Single Register

PC → PLC

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

PLC→PC(OK)

Address	01H
Function Code	06H
*Register Address	High 01H
Address	Low 02H
Write Data	High 17H
Write Data	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

3.3 08H Loop Back Check

The check code checking the transmission of the signal between MASTER and SLAVE could be discretionary.

PC → PLC

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

PLC→PC(OK)

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

PLC→PC(ERROR)

SLAVE Address	01H
Function Code	88H
Exception Code	20H
CRC-16	High 47H
CRC-16	Low D8H

3.4 10H Write Multiple Registers

PC → PLC

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

PLC→PC(ERROR)

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



International Headquarters: 707 Dayton Road PO Box 1040 Ottawa, IL 61350 USA
815-433-5100 Fax 433-5104 www.bb-elec.com orders@bb-elec.com support@bb-elec.com

European Headquarters: Westlink Commercial Park Oranmore Co. Galway Ireland
+353 91 792444 Fax +353 91 792445 www.bb-europe.com orders@bb-europe.com support@bb-europe.com

3.4 Exception Code

Under communication linking, the controller responses the Exception Code and send Function Code AND 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	Reserved
53	Reserved
54	Data value over rang
55	SG2 set error (I/O NUMBER set error)
56	EXT communication module --SG2 don't connected
57	Reserved
58	Reserved
59	EXT communication module --SG2 communication data error



International Headquarters: 707 Dayton Road PO Box 1040 Ottawa, IL 61350 USA
815-433-5100 Fax 433-5104 www.bb-elec.com orders@bb-elec.com support@bb-elec.com

European Headquarters: Westlink Commercial Park Oranmore Co. Galway Ireland
+353 91 792444 Fax +353 91 792445 www.bb-europe.com orders@bb-europe.com support@bb-europe.com

4.0 Register Address

4.1 (00xxH) Coil Status Address

Register Address	Data Length	Command	Content															
			F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
0000H	1	03H 06H 10H	-	RF	RE	RD	RC	RB	RA	R9	R8	R7	R6	R5	R4	R3	R2	R1
0001H	1		-	GF	GE	GD	GC	GB	GA	G9	G8	G7	G6	G5	G4	G3	G2	G1
0002H	1		-	TF	TE	TD	TC	TB	TA	T9	T8	T7	T6	T5	T4	T3	T2	T1
0003H	1		-	CF	CE	CD	CC	CB	CA	C9	C8	C7	C6	C5	C4	C3	C2	C1
0004H	1		-	MF	ME	MD	MC	MB	MA	M9	M8	M7	M6	M5	M4	M3	M2	M1
0005H	1		-	-	-	-	IC	IB	IA	I9	I8	I7	I6	I5	I4	I3	I2	I1
0006H	1		-	-	-	-	XC	XB	XA	X9	X8	X7	X6	X5	X4	X3	X2	X1
0007H	1		-	-	-	-	-	-	-	-	Q8	Q7	Q6	Q5	Q4	Q3	Q2	Q1
0008H	1		-	-	-	-	YC	YB	YA	Y9	Y8	Y7	Y6	Y5	Y4	Y3	Y2	Y1
0009H	1		-	NF	NE	ND	NC	NB	NA	N9	N8	N7	N6	N5	N4	N3	N2	N1

Attention: Command writing II Cor XI C is invalid;

4.2 (01xxH) Control Register Address

Register Address	Data Length	Command	Content																					
			F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0						
0100H	1	03H 06H 10H	ID NO. Run/Stop	-												-	-	-	-	-	-	-	-	SI
				S=0STOP S=1RUN																				

4.3 (02XXH) Current Value Address

Register Address	Data Length	Command	Content		Note
0200H	1H	03H	Timer1		
0201H	1H		Timer2		
0202H	1H		Timer3		
...		
020EH	1H		TimerF		
0210H	2H	03H	CNT1		*1
0211H	2H		CNT2		
....		
021EH	2H		CNTF		
			RTC current value		
0220H	4H	03H, 10H	CURRENT YEAR		CURRENT MOON
			CURRENT DAY		CURRENT WEEK
			CURRENT HOUR		CURRENT MINUTE
			CURRENT SECOND		00
			ANALOG 1		
0230	1H	03H	A1 VALUE H		A1 VALUE L
0231	1H		A2_VALUE_H		A2_VALUE_L
0232	1H		A3 VALUE H		A3 VALUE L
0233	1H		A4 VALUE H		A4 VALUE L
0234	1H		A5 VALUE H		A5 VALUE L
0235	1H		A6 VALUE H		A6 VALUE L
0236	1H		A7 VALUE H		A7 VALUE L
0237	1H		A8 VALUE H		A8 VALUE L
PWM					
0260H	3H	03H	00		PWM RUN NUM
			PW H		PW L
			PT H		PT L



International Headquarters: 707 Dayton Road PO Box 1040 Ottawa, IL 61350 USA
815-433-5100 Fax 433-5104 www.bb-elec.com orders@bb-elec.com support@bb-elec.com

European Headquarters: Westlink Commercial Park Oranmore Co. Galway Ireland
+353 91 792444 Fax +353 91 792445 www.bb-europe.com orders@bb-europe.com support@bb-europe.com

4.4 (04XXH) Preset Value Address

Register Address	Data Length	Command	Content	Note
TMR				
0400H	1H	03H 10H	Timer1	
0401H	1H		Timer2	
0402H	1H		Timer3	
...	
040EH	1H		TimerF	
COUNTER				
0410H	5H	03H 10H	CNT1	*2
0411H	5H		CNT2	
....	
041EH	5H		CNTF	
RTC				
0420H	3H	03H 10H	RTC1	*3
0421H	3H		RTC2	
...	
042EH	3H		RTCF	
ANALOG				
0430H	1H	03H 10H	ANALOG 1	
0431H	1H		ANALOG 2	
...	
043EH	1H		ANALOG F	
PWM				
0460H	10H		PWM	*4



International Headquarters: 707 Dayton Road PO Box 1040 Ottawa, IL 61350 USA
815-433-5100 Fax 433-5104 www.bb-elec.com orders@bb-elec.com support@bb-elec.com

European Headquarters: Westlink Commercial Park Oranmore Co. Galway Ireland
+353 91 792444 Fax +353 91 792445 www.bb-europe.com orders@bb-europe.com support@bb-europe.com

5.0 Notes

5.1 Note 1: Counter Current Value

High Bytes	Low Bytes
C current V M	C current V L
00	C current V H

5.2 Note 2: Counter Preset Value

	High Bytes	Low Bytes
COUNTER MOD 1~7	C PRESET V M	C PRESET V L
	00	C PRESET V H
	00	00
	00	00
	00	00
COUNTER MOD8	FIX TIM H	FIX TIM L
	C ON PRESET V M	C ON PRESET V L
	00	C_ON_PRESET_V_H
	C_OFF_PRESET_V_M	C_OFF_PRESET_V_L
	00	C_OFF_PRESET_V_H

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

5.3 Note 3: RTC Preset Value

	High Bytes	Low Bytes
RTC MOD1	Turn on week	Turn off week
RTC MOD2	Turn on time (hour)	Turn on time (min)
	Turn off time (hour)	Turn off time (min)
RTC MOD3	Turn on year	Turn off year
	Turn on month	Turn on day
	Turn off month	Turn off day

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

	High Bytes	Low Bytes
1	PW1 H	PW1 L
2	PT1 H	PT1 L
3	PW2 H	PW2 L
4	PT2 H	PT2 L
5	PW3 H	PW3 L
6	PT3 H	PT3 L
7	PW4 H	PW4 L
8	PT4 H	PT4 L
9	PW5 H	PW5 L
10	PT5 H	PT5 L
11	PW6 H	PW6 L
12	PT6 H	PT6 L
13	PW7 H	PW7 L
14	PT7 H	PT7 L
15	PW8 H	PW8 L
16	PT8 H	PT8 L

PW: Pulse Width Value(00000~32767)

PT: Period Value(00001~32767)



International Headquarters: 707 Dayton Road PO Box 1040 Ottawa, IL 61350 USA
815-433-5100 Fax 433-5104 www.bb-elec.com orders@bb-elec.com support@bb-elec.com

European Headquarters: Westlink Commercial Park Oranmore Co. Galway Ireland
+353 91 792444 Fax +353 91 792445 www.bb-europe.com orders@bb-europe.com support@bb-europe.com