ACB – OCR A-type MODBUS Protocol

1. Introduction

MODBUS RTU protocol

2. Physical Layer

⊙ Communication port : RS485
⊙ Asynchronous format : One character consists of 10bit.
(1 start bit + 8 data bits + 1 stop bit)
⊙ Baud rate : 9600, 19200, 38400 bps (Adjustable from OCR)
⊙ Data Bits : 8 bits
⊙ Parity : No parity
⊙ Stop Bits : 1 bits
⊙ It has the communication method of Master-Slave, Master only can carry out a request action, and Slave sends the requested data received from Master or responses to the requested performance.

3 Data Link Layer

⊙ If Master sends the request frame to Slave, Slave sends back the response frame.
Each frame is separated by its dead time.

The general mode for sending/receiving frame is as follows:

DESCRIPTION	SIZE
SLAVE ADDRESS	1 byte
FUNCTION CODE	1 byte
DATA	N byte
CRC	2 byte
DEAD TIME	3.5 bytes transmission time

Master	Request		Response	Slave
Slave address	Device Address		Device Address	Slave Address
Definition of Slave action	Function Code		Function Code	Echo or MSB=1
Additional information to perform requested actions from Slave	Data		Data	Requested data or Exception code
CRC	Error check		Error check	CRC

⊙ SLAVE ADDRESS
Valid slave device address range : 0~247 decimal
Actually used slave device address range : 1~247 decimal
In case the slave device address of frame where Master requests to Slave is in the range of zero, it means that Master device is broadcasting to all slaves.
When Master requests to Slave, transmit address field after filling it out with corresponding address.
When Slave responses to Master, transmit address field after filling it out with Slave address.

⊙ FUNCTION CODE
Valid range : 1~255
normal : 1~127, error : 129 ~ 255(normal + 0x80)
It defines the action that Master can request to Slave.
Slave inputs the following information.
In case of normal response : Echo the function code value of request as it is.
In case of exception response : Fill out the function code value of request after setting MSB as 1.

⊙ DATA
Register address

The amount of item to handle
Byte quantity of actual data

⊙ **CRC**
It is used for Error checking method.
CRC-16

CRC Generation Function

```
unsigned short CRC16(puchMsg, usDataLen)
   unsigned char *puchMsg ; /* message to calculate CRC upon */
   unsigned short usDataLen ; /* quantity of bytes in message */
{
   unsigned char uchCRCHi = 0xFF ; /* high byte of CRC initialized */
   unsigned char uchCRCLo = 0xFF ; /* low byte of CRC initialized */
   unsigned uIndex ; /* will index into CRC lookup table */

   while (usDataLen—) /* pass through message buffer */
   {
      uIndex = uchCRCHi ^ *puchMsgg++ ; /* calculate the CRC */
      uchCRCHi = uchCRCLo ^ auchCRCHi[uIndex} ;
      uchCRCLo = auchCRCLo[uIndex] ;
   }

   return (uchCRCHi << 8 | uchCRCLo) ;
}
```

⊙ DEAD TIME
Frame is finished when it has a silent interval more than 3.5 charter time after receiving the final character.

MODBUS Exception Codes

code	Name
0x01	ILLEGAL FUNCTION
0x02	ILLEGAL DATA ADDRESS
0x03	ILLEGAL DATA VALUE
0x04	SLAVE DEVICE FAILURE
0x10	No Data of Event/Fault record
0x11	SBO TIME OUT (time-out set about 5 sec.)
0x12	ILLEGAL ADU LENGTH
0x13	LOCAL MODE

※ Exception Code Names in yellow box will only be actually executed in SUSOL ACB OCR.

Function Code	Name	Property	Kind of switch	Register (DEC)	Format	Notes
0x03		R	Iu (x In)	40001	F001 Format	Position of rotary switch with decimal(Base 10) notation (1~9)
			tsd		F001 Format	Position of rotary switch with decimal(Base 10) notation (1~9)
			Ir (x Iu)	40002	F001 Format	Position of rotary switch with decimal(Base 10) notation (1~9)
			Ii		F001 Format	Position of rotary switch with decimal(Base 10) notation (1~9)
			tr	40003	F001 Format	Position of rotary switch with decimal(Base 10) notation (1~9)
			Ig		F001 Format	Position of rotary switch with decimal(Base 10) notation (1~9)
			Isd	40004	F001 Format	Position of rotary switch with decimal(Base 10) notation (1~9)
			tg		F001 Format	Position of rotary switch with decimal(Base 10) notation (1~9)
			Long time delay set current	40005	F002 Format	Indicates a value of Scaled current depends on ratings(A)
			Long time delay set time	40006	F002 Format	Long time delay operating time (msec) (@ Ir 600% time standard) (50, 1000, 2000, 4000, 8000, 12000, 16000, 20000
			Short time delay set current	40007	F002 Format	Indicates a value of Scaled current depends on ratings(A)
			short time delay set time	40008	F002 Format	Short time delay operating time (msec) ※ In case of I2t on, LSB sets as 1
			ground-fault set curre	40009	F002 Format	Indicates a value of Scaled current depends on ratings(A) ※Ref.1 Using as an external ground-fault setting current depends on DIP switch
			ground-fault set tim	40010	F002 Format	ground-fault operation time (msec) ※ In case of I2t on, LSB set 1 Using as an external ground-fault setting current depends on DIP switch
			Instantaneous delay set current	40011	F003 Format	Indicates a value of Scaled current depends on ratings(A
				40012		
			Event Buffer 1 (When the event position is vacant, it will fill up with 0xff).	40021	F006 Format	Indicates a value of Scaled current depends on ratings(A) ※ Indicates mA in case of external ground-fault
				40022		Trip types, Information on Trip phase
				40023	F007 Format	Event year (BCD code)
					F007 Format	Event month (BCD code)
				40024	F008 Format	Event day (BCD code)
					F007 Format	Event hour (BCD code)
				40025	F007 Format	Event minute (BCD code)
					F009 Format	Event second (BCD code)
			Event Buffer 10	40066	F006 Format	Indicates a value of Scaled current depends on ratings(A) ※ Indicates mA in case of external ground-fault
				40067		Trip types, Information on Trip phase
				40068	F007 Format	Event year (BCD code)
					F007 Format	Event month (BCD code)
				40069	F007 Format	Event day (BCD code
					F007 Format	Event hour (BCD code)
				40070	F007 Format	Event minute (BCD code)
					F007 Format	Event second (BCD code)
			Year	46001	F010 Format	year (BCD code
			Month	46002	F010 Format	month (BCD code)
			Day	46003	F010 Format	day (BCD code)
			Hour	46004	F010 Format	hour (BCD code)
			Minute	46005	F010 Format	minute (BCD code
			Second	46006	F010 Format	second (BCD code
			Milli Second	46007	F010 Format	1/1000 sec. (BCD code), Actually not used (always 0 msec send)
0x04	Read Input Reg	R Only	OCR Information	30001	F011 Format	DO state, battery state information
			dip switch inform.		F005 Format	Frequency setting, Thermal Memory using/not, 4Pole setting, CT ratings setting information
			OCR I/O inform.	30002	F012 Format	ZSI out, ZSI in, ZSI delay yes, ZSI delay no, remote in, CB Status
			Max current phase inform.		F004 Format	R phase-1, S phase-2, T phase-3, N phase-4
			R Phase	30003	F003 Format	Indicates a value of Scaled R-phase current depends on ratings(A)
				30004		

			S Phase	30005 30006	F003 Format	Indicates a value of Scaled S-phase current depends on ratings(A)
			T Phase	30007 30008	F003 Format	Indicates a value of Scaled T-phase current depends on ratings(A)
			N Phase	30009 30010	F003 Format	Indicates a value of Scaled N-phase current depends on ratings(A)
			Max current	30011 30012	F003 Format	Indicates a value of the Scaled highest current depends on ratings(A)
			IDMTL Format	30013	F013 Format	0x00-None(Thermal), 0x01-DT, 0x02-SIT(0.02), 0x08-VIT, 0x10-EIT
			OCR Inform. 2		F004 Format	If a bit-0 is 1, "Main Trip Device Fail"
			Firmware version	30014	F015 Format	OCR Firmware version Information

0x05	Write Single Coil	W Only	D0_01 ON Select	00001	F008 Format	DO 01 On select
			DO_01 ON OP	00002	F008 Format	DO 01 On Operation
			DO_01 OFF Select	00003	F008 Format	DO 01 Off select
			DO_01 OFF OP	00004	F008 Format	DO 01 Off Operation
			D0_02 ON Select	00005	F008 Format	DO 02 On select
			DO_02 ON OP	00006	F008 Format	DO 02 On Operation
			DO_02 OFF Select	00007	F008 Format	DO 02 Off select
			DO_02 OFF OP	00008	F008 Format	DO 02 Off Operation
			DO_03 ON Select	00009	F008 Format	DO 03 On select
			DO_03 ON OP	00010	F008 Format	DO 03 On Operation
			DO_03 OFF Select	00011	F008 Format	DO 03 Off select
			DO_03 OFF OP	00012	F008 Format	DO 03 Off Operation
0x10	Write Multiple Reg.	W	Year	46001	F010 Format	year (BCD code)
			Month	46002	F010 Format	month (BCD code)
			Day	46003	F010 Format	day (BCD code)
			Hour	46004	F010 Format	hour (BCD code)
			Minute	46005	F010 Format	minute (BCD code)
			Second	46006	F010 Format	second (BCD code
			Milli Second	46007	F010 Format	1/1000 sec. (BCD code), Actually not used (always 0 msec send)

F001
8bit unsigned Integer Format
F002
16bit unsigned Integer Format : Little Endian
F003
32bit unsigned Integer Format : Little Endian
F004
R-0x01, S-0x02, T-0x03, N-0x04
※ N Phase can not be bigger than R, S, T, hence data of 0x04 is actually not used.
The highest phase indicates 0 when under 5% of rated current flows at the R,S,T.
F005
bit7(0-60Hz, 1-50Hz), bit6(0-Thermal Memory disable, 1-enable)
bit5/4(00-dummy OCGR, 01-PTA, 10-external OCGR, 11-basic OCGR))
bit3~0(400, 630, 800, 1000, 1250, 1600, 2000, 2500, 3200, 4000, 5000, 6300)
F006
bit23~0 (24Bit unsigned integer Format : Little Endian)
bit24~27 (R-bit24 set, S-bit25 set, T-bit26 set, N-bit27 set)
bit28~31 (Long time delay-0, short time delay-1, instantaneous-2, ground-fault-3)
F007
8 bit unsigned Integer Format BCD Code
(ex: Value of 19 in Hex is 0x13, but in BCD Code it indicates 0x19.)
Indicates 24 hours mode, meaning that time indicates through 0~23.
(ex: day time 9H-0x09, night time 9H-0x21)
F008
F002 Format, 0xFF00 : ON/OFF
F009
BCD Code (the year after 2000 indicates with BCD code)
(ex: case of year 2006, 0x06 / case of year 2010, 0x10)
F010
16 bit unsigned Integer Format BCD code
F011

F001 Format

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
	No use	DO_3	DO_2	DO_1	No Use	No Use	Battery status	No Use
1		Close	Close	Close			Normal	
0		open	open	open			Low	

F012
F001 Format

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
	ZSI Output	ZSI Imput	ZSI state after trip	ZSI state after trip	Remote reset	CB Status	No Use	No Use
1	Active	Active	ZSI O	ZSI X	Active	Close		
0	Inactive	Inactive	No ZSI Trip		Inactive	Open		

F013 (only P/S Format)
0x00-None(Thermal), 0x01-DT, 0x02-SIT(0.02),
0x08-VIT, 0x10-EIT

F014 (bit 1 is only for P/S Format)

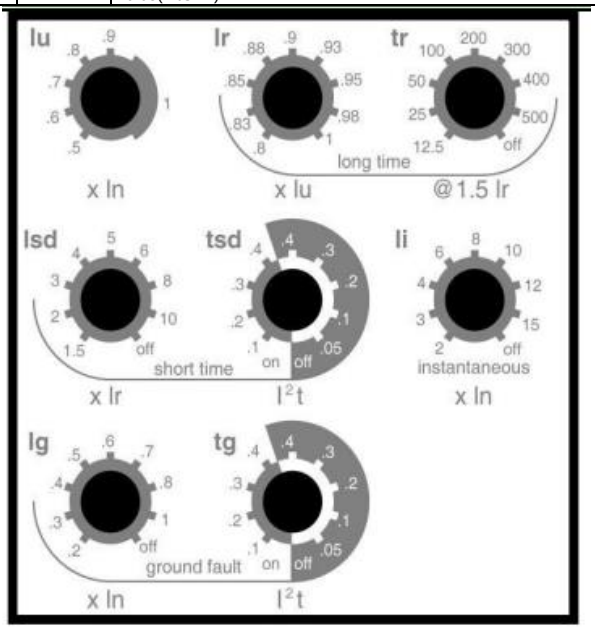
	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
	Unused	Unused	Unused	Unused	Unused	Unused	PTA Relay Status	MTD status
1							On	Fail
0							Off	normal

F015
BCD code assigned 4 bits
ex) case of 0.99a, 0x099a
case of 1.23b, 0x123b

※ Reference 1

In case of external ground-fault, the value for ground-fault setting current will be sent as "Current-value * 10."
For example, if it is 0.5A, the value will comes up with "5."
Also, if ground-fault setting time is set as "Alarm," the corresponding time vlaue of LSB comes up with setting value of 1. ex) In case of Alarm 140ms, value of 141 comes up.

Switch Types	Register Address	Address	Notes
Iu(x In)	40001	40000	1-0.5 / 2-0.6 / 3-0.7 / 4-0.8 / 5-0.9 / 6-1.0 / 7-1.0 / 8-1.0 / 9-1.0
tsd			1-0.1(I2tON) / 2-0.2(I2tON) / 3-0.3(I2tON) / 4-0.4(I2tON) / 5-0.4(I2tOFF) / 6-0.3(I2tOFF) / 7-0.2(I2tOFF) / 8-0.1(I2tOFF) / 9-0.05(I2tOFF
Ir_(x Iu)	40002	40001	1-0.8 / 2-0.83 / 3-0.85 / 4-0.88 / 5-0.9 / 6-0.93 / 7-0.95 / 8-0.98 / 9-1.0
Li			1-2 / 2-3 / 3-4 /4-6 / 5-8 / 6-10 / 7-12 / 8-15 / 9-OFF
tr	40003	40002	1-12.5 / 2-25 / 3-50 / 4-100 / 5-200 / 6-300 / 7-400 / 8-500 / 9-OFF
Ig			1-0.2 / 2-0.3 / 3-0.4 / 4-0.5 / 5-0.6 / 6-0.7 / 7-0.8 / 8-1 / 9-OFF
Isd	40004	40003	1-1.5 / 2-2 / 3-3 / 4-4 / 5-5 / 6-6 / 7-8 / 8-10 / 9-OFF
tg			1-0.1(I2tON) / 2-0.2(I2tON) / 3-0.3(I2tON) / 4-0.4(I2tON) / 5-0.4(I2tOFF) / 6-0.3(I2tOFF) / 7-0.2(I2tOFF) / 8-0.1(I2tOFF) / 9-0.05(I2tOFF)



Examples

(1) 03(0x03) Read Holding Registers

Example of a Request/response to read registers 40001 … 40004 from slave device 1

Request	
Field Name	(Hex)
Slave Address	0x01
Function	0x03
Starting Address Hi	0x00
Starting Address Lo	0x00
Quantity of Inputs Hi	0x00
Quantity of Inputs Lo	0x04
CRC Lo	0x44
CRC Hi	0x09

Response	
Field Name	(Hex)
Slave Address	0x01
Function	0x03
Byte Count	0x08
Register value Lo(40001)	0x01
Register value Hi (40001)	0x02
Register value Lo(40002)	0x05
Register value Hi (40002)	0x06
Register value Lo(40003)	0x07
Register value Hi (40003)	0x03
Register value Lo(40004)	0x04
Register value Hi (40004)	0x08
CRC Lo	0x0D
CRC Hi	0xFC

(2) 04(0x04) Read Input Registers

Example of a Request/response to read registers 30001 … 30007 from slave device 1

Request	
Field Name	(Hex)
Slave Address	0x01
Function	0x04
Starting Address Hi	0x00
Starting Address Lo	0x00
Quantity of Inputs Hi	0x00
Quantity of Inputs Lo	0x07
CRC Lo	0xB1
CRC Hi	0xC8

Response		
Field Name	(Hex)	
Slave Address	0x01	
Function	0x04	
Byte Count	0x0E	
Register value Lo(30001)	0x00	-> 0x78
Register value Hi (30001)	0x00	-> 0x56
Register value Lo(30002)	0x00	-> 0x34
Register value Hi (30002)	0x00	-> 0x12
Register value Lo(30003)	0x00	
Register value Hi (30003)	0x00	
Register value Lo(30004)	0x00	
Register value Hi (30004)	0x00	-> 0x34
Register value Lo(30005)	0x00	-> 0x12
Register value Hi (30005)	0x00	
Register value Lo(30006)	0x00	
Register value Hi (30006)	0x04	
Register value Lo(30007)	0x00	
Register value Hi (30007)	0x00	
CRC Lo	0xEC	
CRC Hi	0xE6	

In case of
4 Byte Data
of 0x12345678

In case of 2 Byte Data

of 0x1234

(3) 05(0x05) Write Single Coil

Example of a Request/response to force coil 1 ON in slave device 1

Request	
Field Name	(Hex)
Slave Address	0x01
Function	0x05
Starting Address Hi	0x00
Starting Address Lo	0x00
Force Data Hi	0xFF
Force Data Lo	0x00
CRC Lo	0x8C
CRC Hi	0x3A

⟷

Response	
Field Name	(Hex)
Slave Address	0x01
Function	0x05
Starting Address Hi	0x00
Starting Address Lo	0x00
Force Data Hi	0xFF
Force Data Lo	0x00
CRC Lo	0x8C
CRC Hi	0x3A

(4) 16(0x10) Write Multiple Registers

TimeSync : 2006. Oct. 26th. 19H. 53M. 01S. 001msec
Consider as an Exception, if the full data(14 byte count) for the TimeSync could not be written.
Example of a Request/response to preset 7 registers starting at 46001 in slave device 1

Request	
Field Name	(Hex)
Slave Address	0x01
Function	0x10
Starting Address Hi	0x17
Starting Address Lo	0x70
Quantity of Inputs Hi	0x00
Quantity of Inputs Lo	0x07
Byte Count	0x44
Data Hi	0x0E
Data Lo	0x06
Data Hi	0x00
Data Lo	0x10
Data Hi	0x00
Data Lo	0x26
Data Hi	0x00
Data Lo	0x19
Data Hi	0x00
Data Lo	0x53
Data Hi	0x00
Data Lo	0x01
Data Hi	0x00
Data Lo	0x01
Data Hi	0x3C
Data Lo	0x49

⟷

Response	
Field Name	(Hex)
Slave Address	0x01
Function	0x10
Starting Address Hi	0x17
Starting Address Lo	0x70
Number of Registers Hi	0x00
Number of Registers Lo	0x07
CRC Lo	0x85
CRC Hi	0xA4