Chapter 12 Modbus Communication

12.1 General

Modbus is a serial and asynchronous communication protocol. Modbus protocol is a general language applied to PLC and other controlling units. This protocol has defined an information structure which can be identified and used by a controlling unit regardless of whatever network they are transmitted.

You can read reference books or ask for the details of MODBUS from manufactures.

Modbus protocol does not require a special interface while a typical physical interface is RS485.

NOTE: The AC10 cannot be a Modbus master.

12.2 Modbus Protocol

12.2.1 Transmission mode

Format

ASCII mode

Start	Address	Function	Data				LRC check		End	
: (0X3A)	Inverter Address	Function Code	Data Length	Data 1	… …	Data N	High-order byte of LRC	Low-order byte of LRC	Return (0X0D)	Line Feed (0X0A)

RTU mode

Start	Address	Function	Data	CRC check		End
T1-T2-T3-T4	Inverter Address	Function Code	N data	Low-order byte of CRC	High-order byte of CRC	T1-T2-T3-T4

12.2.2 ASCII Mode (F901=1)

In ASCII mode, one Byte (hexadecimal format) is expressed by two ASCII characters.

For example, 31H (hexadecimal data) includes two ASCII characters'3(33H)','1(31H)'.

Common characters, ASCII characters are shown in the following table:

Characters	'0'	'1'	'2'	'3'	'4'	'5'	'6'	'7'
ASCII Code	30H	31H	32H	33H	34H	35H	36H	37H
Characters	'8'	'9'	'A'	'B'	'C'	'D'	'E'	'F'
ASCII Code	38H	39H	41H	42H	43H	44H	45H	46H

12.2.3 RTU Mode (F901=2)

In RTU mode, one Byte is expressed by hexadecimal format. For example, 31H is delivered to data packet.

12.3 Baud rate F904

Setting range: 1200, 2400, 4800, 9600, 19200, 38400, 57600

12.4 Frame structure:

ASCII mode

Byte	Function
1	Start Bit (Low Level)
7	Data Bit
0/1	Parity Check Bit (None for this bit in case of no checking. Otherwise 1 bit)
1/2	Stop Bit (1 bit in case of checking, otherwise 2 bits)

RTU mode

Byte	Function
1	Start Bit (Low Level)
8	Data Bit
0/1	Parity Check Bit (None for this bit in case of no checking. Otherwise 1 bit)
1/2	Stop Bit (1 bit in case of checking, otherwise 2 bits)

12.5 Error Check

12.5.1 ASCII mode

Longitudinal Redundancy Check (LRC): It is performed on the ASCII message field contents excluding the 'colon' character that begins the message, and excluding the CRLF pair at the end of the message.

The LRC is calculated by adding together successive 8–bit bytes of the message, discarding any carries, and then two's complementing the result.

A procedure for generating an LRC is:

1. Add all bytes in the message, excluding the starting 'colon' and ending CRLF. Add them into an 8–bit field, so that carries will be discarded.

2. Subtract the final field value from FF hex (all 1's), to produce the ones–complement.

3. Add 1 to produce the twos–complement.

12.5.2 RTU Mode

Cyclical Redundancy Check (CRC): The CRC field is two bytes, containing a 16–bit binary value.

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, and the parity bit, do not apply to the CRC.

A procedure for generating a CRC-16 is:

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 high–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 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.

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

12.5.3 Protocol Converter

It is easy to turn a RTU command into an ASCII command followed by the lists:

1. Use the LRC replacing the CRC.
2. Transform each byte in RTU command into a corresponding two byte ASCII. For example: transform 0x03 into 0x30, 0x33 (ASCII code for 0 and ASCII code for 3).
3. Add a 'colon' (:) character (ASCII 3A hex) at the beginning of the message.
4. End with a 'carriage return – line feed' (CRLF) pair (ASCII 0D and 0A hex).

So we will introduce RTU Mode in followed part. If you use ASCII mode, you can use the up lists to convert.

12.6 Command Type & Format

The listing below shows the function codes.

Code	Name	Description
03	Read Holding Registers	Read the binary contents of holding registers in the slave. (Less than 10 registers at a time)
06	Write Single Register	Preset a value into holding register

12.6.1 Address and meaning

The part introduces inverter running, inverter status and related parameters setting.

Description of rules of function codes parameters address:

i) Use the function code as parameter address

General Series:

High-order byte: 01~0A (hexadecimal)

Low-order byte: 00~50 (max range) (hexadecimal) Function code range of each partition is not the same. For the specific range refer to manual.

For example: parameter address of F114 is 010E (hexadecimal).

parameter address of F201 is 0201 (hexadecimal).

Note: in this situation, it allows to read six function codes and write only one function code.

Some function codes can only be checked but cannot be modified; some function codes can neither be checked nor be modified; some function codes cannot be modified in run state; some function codes cannot be modified both in stop and run state.

In case parameters of all function codes are changed, the effective range, unit and related instructions refer to user manual for related series of inverters. Otherwise, unexpected results may occur.

ii) Use different parameters as parameter address

(The above address and parameters descriptions are in hexadecimal format, for example, the decimal digit 4096 is represented by hexadecimal 1000).

12.6.2 Running Status Parameters

Parameters Address	Parameter Description（read only）
1000	Output frequency
1001	Output voltage
1002	Output current
1003	Pole numbers/ control mode, high-order byte is pole numbers, low-order byte is control mode.
1004	Bus voltage
1005 ----AC10	Drive ratio/inverter status High-order byte is drive ratio, low-order byte is inverter status Inverter status: 0X00: Standby mode 0X01: Forward running 0X02: Reverse running 0X04: Over-current (OC) 0X05: DC over-current (OE) 0X06: Input Phase loss (PF1) 0X07: Frequency Over-load (OL1) 0X08: Under-voltage (LU) 0X09: Overheat (OH) 0X0A: Motor overload (OL2) 0X0B: Interference (Err) 0X0C: LL 0X0D: External Malfunction (ESP) 0X0E: Err1 0X0F: Err2 0X10: Err3 0X11: Err4 0X12: OC1 0X13: PF0 0X14: Analog disconnected protection (AErr) 0X19: PID parameters are set incorrectly (Err5) 0X2D: Communication timeout (CE) 0X2E: Flycatching fault (FL) 0X31: Watchdog fault (Err6)
1006	The percent of output torque
1007	Inverter radiator temperature
1008	PID given value
1009	PID feedback value

Reading parameter address	Function	Remarks
100A	Read integer power value	The integer power value is read by PC.
100B	DI terminal status	DI1~DI8—bit0~bit7
100C	Terminal output status	bit0-OUT1 bit2-fault relay
100D	AI1	0~4095 read input analog digital value
100E	AI2	0~4095 read input analog digital value
1010	Reserved	
1011	Reserved	
1012	Reserved	
1013	Present-stage speed value 0000 : no function 0001 : stage speed 1 0010 : stage speed 2 0011 : stage speed 3 0100 : stage speed 4 0101 : stage speed 5 0110 : stage speed 6 0111 : stage speed 7 1000 : stage speed 8 1001 : stage speed 9 1010 : stage speed 10 1011 : stage speed 11 1100 : stage speed 12 1101 : stage speed 13 1110 : stage speed 14 1111 : stage speed 15	Monitoring in which stage speed inverter is. (Valid when F500 = 1 or F500 = 2)
1014	Reserved	
1015	AO1 （0~100.00）	Monitoring analog output percent
1016	AO2 （0~100.00）	Monitoring analog output percent
1017	Current speed	Monitoring current speed.
1018	Read accurate power value	Correct the power to 1 decimal place.

12.6.3 Control commands

Parameters Address	Parameters Description（write only）
2000	Command meaning: 0001：Forward running (no parameters） 0002：Reverse running（no parameters） 0003：Deceleration stop 0004：Free stop 0005：Forward jogging start 0006：Forward jogging stop 0007：Fault reset 000A: Forward jogging stop

	000B: Reverse jogging stop
2001	Lock parameters 0001：Unlock System (remote control locked） 0002：Lock remote control (any remote control commands are not valid before unlocking） 0003: RAM and EEprom are permitted to be written. 0004: Only RAM is permitted to be written, EEprom is prohibited being written.

Writing parameter address	Function	Remarks
2002	AO1output percent is set by PC/PLC. Setting range: 0~1000	F431=7 AO1 token output analog is controlled by PC/PLC.
2003	AO2 output percent is set by PC/PLC. Setting range: 0~1000	F432=7 AO2 token output analog is controlled by PC/PLC.
2004	Reserved	
2005	Multi-function output terminal DO1	1 means token output is true. 0 means token output is false.
2006	Multi-function output terminal DO2	
2007	Relay output terminal	

12.6.4 Illegal Response When Reading Parameters

Command Description	Function	Data
Slave parameters response	The highest-order byte changes into 1.	Command meaning: 0001: Illegal function code 0002: Illegal address 0003: Illegal data 0004: Slave fault note 2

Note 2: Illegal response 0004 appears below two cases:

Do not reset inverter when inverter is in the malfunction state.

Do not unlock inverter when inverter is in the locked state.

Additional Remarks

Expressions during communication process:

Parameter Values of Frequency＝actual value X 100

Parameter Values of Time=actual value X 10

Parameter Values of Current=actual value X 100

Parameter Values of Voltage=actual value X 1

Parameter Values of Power (100A)=actual value X 1

Parameter Values of Power (1018)=actual value X 10

Parameter Values of Drive Ratio=actual value X 100

Parameter Values of Version No. =actual value X 100

Instruction: Parameter value is the value sent in the data package. Actual value is the actual value of inverter. After PC/PLC receives the parameter value, it will divide the corresponding coefficient to get the actual value.

NOTE: Take no account of radix point of the data in the data package when PC/PLC transmits command to inverter. The valid value is range from 0 to 65535.

12.7 Function Codes Related to Communication

Function Code	Function Definition	Setting Rang	Mfr's Value
F200	Source of start command	0: Keypad command; 1: Terminal command; 2: Keypad＋Terminal; 3: MODBUS; 4: Keypad＋Terminal＋MODBUS	4
F201	Source of stop command	0: Keypad command; 1: Terminal command; 2: Keypad＋Terminal; 3: MODBUS; 4: Keypad＋Terminal＋MODBUS	4
F203	Main frequency source X	0: Digital setting memory; 1: External analog AI1; 2: External analog AI2; 3: Reserved 4: Stage speed control; 5: No memory by digital setting; 6:Reserved; 7: Reserved; 8: Reserved; 9: PID adjusting; 10: MODBUS	0
F900	Inverter Address	1~255	1
F901	Modbus Mode Selection	1: ASCII mode 2: RTU mode	1
F903	Parity Check	0: Invalid 1: Odd 2: Even	0
F904	Baud Rate(bps)	0: 1200 1: 2400 2: 4800 3: 9600 4: 19200 5: 38400 6: 57600	3
F905	Communication Timeout	0.0~3000.0	0.0

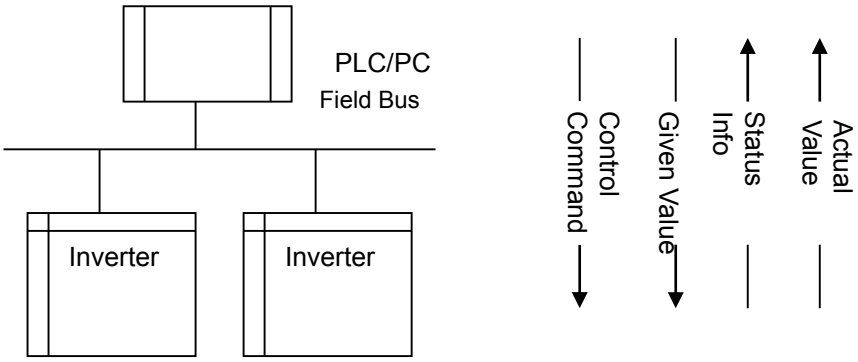
Set the functions code related to communication consonant with the PLC/PC communication parameters, when inverter communicates with PLC/PC.

12.8 Physical Interface

12.8.1 Interface instruction

The RS485 communication interface is located on the control terminals, marked A+ and B-

12.8.2 Structure of Field Bus



Connecting Diagram of Field Bus

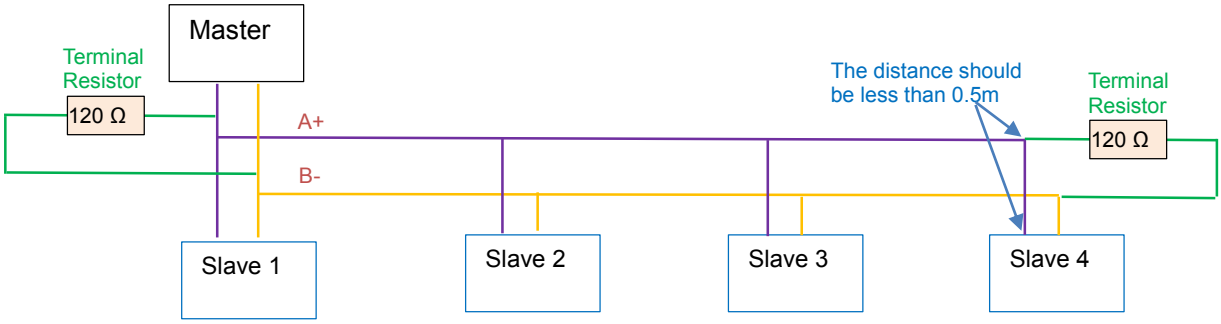
RS485 Half-duplex communication mode is adopted for AC10 series inverter. Daisy chain structure is adopted by 485 Bus-line. Do not use 'spur' lines or a star configuration. Reflect signals which are produced by spur lines or star configuration will interfere in 485 communications.

Note that for the same time in half-duplex connection; only one inverter can have communication with PC/PLC. Should two or more than two inverters upload data at the same time, then bus competition will occur, which will not only lead to communication failure, but higher current to certain elements as well.

12.9 Grounding and Terminal

Terminal resistance of 120 Ω will be adopted for terminal of RS485 network, to diminish the reflection of signals. Terminal resistance shall not be used for intermediate network.

No direct grounding shall be allowed for any point of RS485 network. All the equipment in the network shall be well grounded via their own grounding terminal. Please note that grounding wires will not form closed loop in any case.



Connecting Diagram of Terminal Resistance

Check the drive capacity of PC/PLC and the distance between PC/PLC and inverter when wiring. Add a repeaters if drive capacity is not enough.

All wiring connections for installation shall have to be made when the inverter is disconnected from power supply.

12.9.1 Examples

Example1: In RTU mode, change acc time (F114) to 10.0s in NO.01 inverter.

Query

Address	Function	Register Address Hi	Register Address Lo	Preset Data Hi	Preset Data Lo	CRC Lo	CRC Hi
01	06	01	0E	00	64	E8	1E

Function code F114 Value: 10.0S

Normal Response

Address	Function	Register Address Hi	Register Address Lo	Response Data Hi	Response Data Lo	CRC Lo	CRC Hi
01	06	01	0E	00	64	E8	1E

Function code F114 Normal Response

Abnormal Response

Address	Function	Abnormal code	CRC Lo	CRC Hi
01	86	04	43	A3

The max value of function code is 1. Slave fault

Example 2：Read output frequency, output voltage, output current and current rotate speed from N0.2 inverter.

Host Query

Address	Function	First Register Address Hi	First Register Address Lo	Register count Hi	Register count L0	CRC Lo	CRC Hi
02	03	10	00	00	04	40	FA

Communication Parameters Address 1000H

Slave Response：

Address	Function	Byte Count	Data Hi	Data Lo	Data Hi	Data Lo	Data Hi	Data Lo	Data Hi	Data Lo	Crc Lo	Crc Hi
02	03	08	13	88	01	90	00	3C	02	00	82	F6

Output Frequency Output Voltage Output Current Numbers of Pole Pairs Control Mode

NO.2 Inverter's output frequency is 50.00Hz, output voltage is 380V, output current is 0.6A, numbers of pole pairs are 2 and control mode keypad control.

Example 3： No.1 Inverter runs forwardly.

Host Query:

Address	Function	Register Hi	Register Lo	Write status Hi	Write status Lo	CRC Lo	CRC Hi
01	06	20	00	00	01	43	CA

Communication parameters address 2000H **Forward running**

Slave Normal Response:

Address	Function	Register Hi	Register Lo	Write status Hi	Write status Lo	CRC Lo	CRC Hi
01	06	20	00	00	01	43	CA

Normal Response

Slave Abnormal Response:

Address	Function	Abnormal Code	CRC Lo	CRC Hi
01	86	01	83	A0

The max value of function code is 1. Illegal function code (assumption)

Example 4: Read the value of F113, F114 from NO.2 inverter

Host Query：

Address	Function	Register Address Hi	Register Address Lo	Register Count Hi	Register Count L0	CRC Lo	CRC Hi
02	03	01	0D	00	02	54	07

Communication Parameter Address F10DH Numbers of Read Registers

Slave Normal Response:

Address	Function	Byte count	The first parameters status Hi	The first parameters status Lo	The second parameters status Hi	The second parameters status Lo	CRC Lo	CRC Hi
02	03	04	03	E8	00	78	49	61

The actual value is 10.00. The actual value is 12.00.

Slave Abnormal Response：

Address	Function Code	Abnormal Code	CRC Lo	CRC Hi
02	83	08	B0	F6

The max value of function code is 1. Parity check fault