8.3 Modbus Protocol Communication

8.3.1 Introduction

MASTER-K120S built-in communication supports Modbus, the Modicon product's communication protocol. It supports ASCII mode, using ASCII data and RTU mode using Hex data. Function code used in Modbus is supported by instruction and especially function code 01, 02, 03, 04, 05, 06, 15 and 16. Refer to "Modicon Modbus Protocol Reference Guide"

8.3.2 Basic Specification

1) ASCII mode

(1) It communicates, using ASCII data.

(2) Each frame uses ': (colon : H3A)', for header, CRLF (Carriage Return-Line Feed : H0D H0A), for tail.

(3) It allows Max. 1 second interval between characters.

(4) It checks errors, using LRC.

(5) Frame structure (ASCII data)

Item	Header	Address	Function code	Data	LRC	Tail(CR/LF)
Size	1 byte	2 bytes	2 bytes	n bytes	2 bytes	2 bytes

2) RTU mode

(1) It communicates, using hex data.

(2) There's no header and tail. It starts with address and finishes frame with CRC.

(3) It has at least 3.5 character times between two frames.

(4) It ignores the current frame when 1.5 character times elapse between characters.

(5) It checks errors, using 16 bit CRC.

(6) Frame structure (hex data).

Item	Address	Function code	Data	CRC
Size	1 byte	1 bytes	n bytes	2 bytes

REMARK

1) The size constituting 1 letter is 1 character. So 1 character is 8 bits that is 1 byte.

2) 1 character time means the time lapsed for sending 1 character.

Ex) Calculation of 1 character time at 1200 bps.

1200 bps means that it takes 1 second to send 1200 bits. To send 1 bit, 1 sec/1200 bits = 0.83 ms.

Therefore 1 character time is 0.83ms * 8 bits = 6.64ms.

3) 584, 984 A/B/X executes frame division, using intervals of more than 1 sec without LRC in processing internally.

3) Address area

(1) Setting range is available from 1 to 247, but MASTER-K120S supports from 0 to 31.

(2) Address 0 is used for broadcast address. Broadcast address is all slave device recognize and respond to like the self-address, which can't be supported by MASTER-K120S.

4) Function code area

(1) MASTER-K120S supports only 01, 02, 03, 04, 05, 06, 15, and 16 among Modicon products' function codes.

(2) If the response format is confirm+(ACK), it uses the same function code.

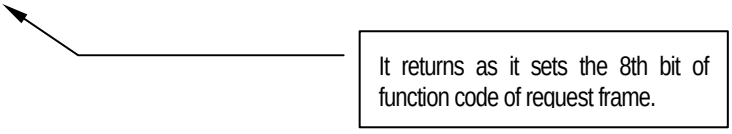
(3) If the response format is confirm-(NCK), it returns as it sets the 8th bit of function code as 1.

Ex) If function code is 03, (we write here only function code part. Because only function codes are different.)

[Request] 0000 0011 (H03)

[Confirm+] 0000 0011 (H03)

[Confirm-] 1000 0011 (H83)



5) Data area

(1) It sends data, using ASCII data(ASCII mode) or hex (RTU mode).

(2) Data is changed according to each function code.

(3) Response frame uses data area as response data or error code.

6) LRC Check/CRC Check area

(1) LRC (Longitudinal Redundancy Check) : It works in ASCII mode. It takes 2' complement from sum of frame except header or tail to change into ASCII code,

(2) CRC (Cyclical Redundancy Check): It works in RTU mode. It uses 2-byte CRC check rules.

REMARK

1) All numerical data can use hexadecimal, decimal, and binary type. If we convert decimal 7 and 10 into each type:

Hexadecimal : H07, H0A or 16#07, 16#0A

Decimal : 7, 10

Binary : 2#0111, 2#1010

7) Function code types and memory mapping

Code	Function code name	Modicon PLC Data address	Remark
01	Read Coil Status	0XXXX(bit-output)	Read bits
02	Read Input Status	1XXXX(bit-input)	Read bits
03	Read Holding Registers	4XXXX(word-output)	Read words
04	Read Input Registers	3XXXX(word-input)	Read words
05	Force Single Coil	0XXXX(bit-output)	Write bit
06	Preset Single Register	4XXXX(word-output)	Write word
15	Force Multiple Coils	0XXXX(bit-output)	Write bits
16	Preset Multiple Registers	4XXXX(word-output)	Write words

- MASTER-K120S Mapping

Bit area		Word area	
Address	Data area	Address	Data area
h0000	P area	h0000	P area
h1000	M area	h1000	M area
h2000	L area	h2000	L area
h3000	K area	h3000	K area
h4000	F area	h4000	F area
h5000	T area	h5000	T area(current value area)
h6000	C area	h6000	C area(current value area)
		h7000	S area
		h8000	D area

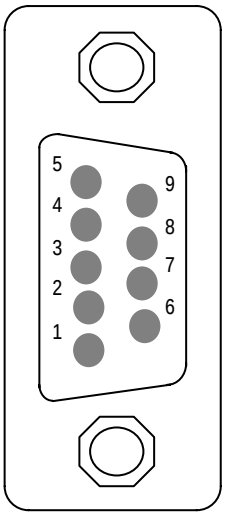
8) Modbus addressing rules

MASTER-K120S main unit starts its address from 0 and matches with 1 of Modicon products' data address. So MASTER-K120S's address n matches n+1 of Modicon products' address. This means that the output contact point 1 (0001) of Modicon products is marked as communication address 0 and the input contact point 1 (0001) of Modicon products is marked as communication address 0 in MASTER-K120S.

9) The size of using data

As for data size, MASTER-K120S main unit supports 128 bytes in ASCII mode and 256 bytes in RTU mode. The maximum size of the Modicon products is different from each other kind. So refer to "Modicon Modbus Protocol Reference Guide."

10) Map of wiring



Male Type

MASTER-K120S main unit Pin no.	Connecting no. and direction	Quantum (9PIN) Pin no.	Signal
1		1	CD
2		2	RXD
3		3	TXD
4		4	DTR
5		5	SG
6		6	DSR
7		7	RTS
8		8	CTS
9		9	

- Use RS-485 connector when using channel 2.

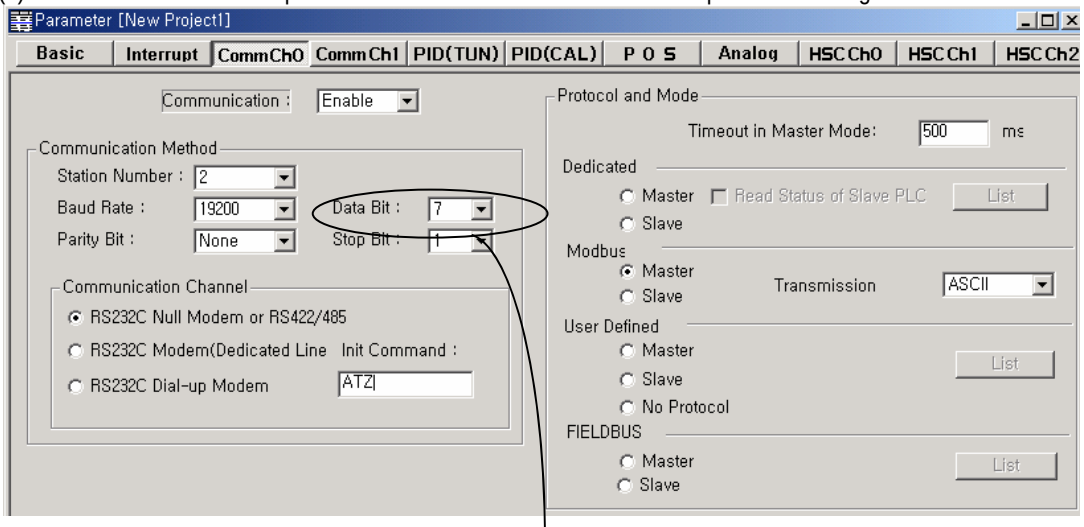
8.3.3 Parameters Setting

1) Setting communication parameter

(1) Open a new project file at KGLWIN.

- K120S should be selected in PLC types.
- Open a new project file for each of the master and the slave.

(2) Select a communication parameter at KGLWIN and double click to open the following window.



If communication mode is ASCII, Be sure to set 7bit

(3) Set the contents as follows.

Item	Setting contents
Station No.	Set a number between 0 to 31 (Don't assign no. 0 as broadcasting station lest it may be a cause for mistaken operation)
Baud Rate	Set one from 1200, 2400, 4800, 9600, 19200, 38400, or 57600 bps.
Data Bit	Set 7 or 8. ASCII mode: Set as 7 bits. RTU mode: Set as 8 bits.
Parity Bit	Set as one of None, Even, or Odd.
Stop Bit	Set 1 or 2 bit(s). When parity bit is set: Set as 1 bit. When parity bit isn't set: Set as 2 bits.
Communication Channel	• RS232C Null Modem or RS422/485 : It's a communication channel for the communication, using MASTER-K120S main unit's built-in communication and Cnet I/F module (G7L-CUEC). • RS232C Modem (Dedicated Line) : It's to be selected for the communication, using an dedicated modem with Cnet I/F module (G7L-CUEB). • S232C Dial Up Modem : It's to be selected for the general communication connecting through the telephone line by dial up modem and Cnet I/F module (G7L-CUEB). • Note : Using Cnet I/F module (G7L-CUEB) supporting RS232C, RS232C dedicated or dial-up modem communication can be done, but not through Cnet I/F module (G7L-CUEC) supporting RS422/485.
Time out in Master Mode	• It's the time waiting a responding frame since the master MK80S main unit sends a request frame. • The default value is 500ms. • It must be set in consideration of the max. periodical time for sending/receiving of the master PLC. • If it's set smaller than the max. send/receive periodical time, it may cause communication error.
Modbus Master/ Slave	If it is set as the master, it's the subject in the communication system. If it's set as the slave, it only responds to the request frame of the master.
Transmission Mode	Select ASCII mode or RTU mode.

8.3.4 Instruction and example

1) MODBUS communication instruction(MODCOM)

MODCOM	MODBUS communication

Instruction	Available device											No. of steps	Flag		
	M	P	K	L	F	T	C	S	D	#D	integer		Error (F110)	Zero (F111)	Carry (F112)
Ch											○	7	○		
S1	○	○	○	○	○	○	○		○	○					
S2	○	○	○	○		○	○		○	○					
S3	○	○	○	○		○	○		○	○					

Flag

Error (F110)	Error flag turns on when designating area is over and the instruction isn't executed

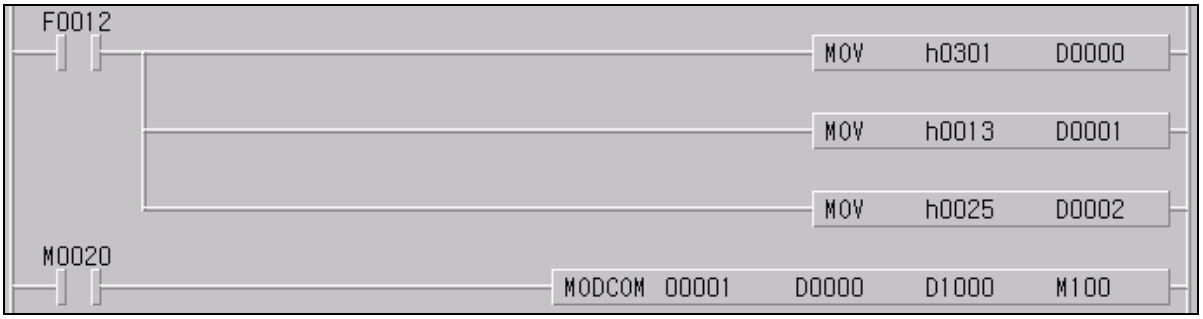
Designation

Ch	Designated communication channel
S1	Device which is registered communication parameter
S2	Device which stored communication data
S3	Device which stored communication status

■ MODCOM Ch S1 S2 S3

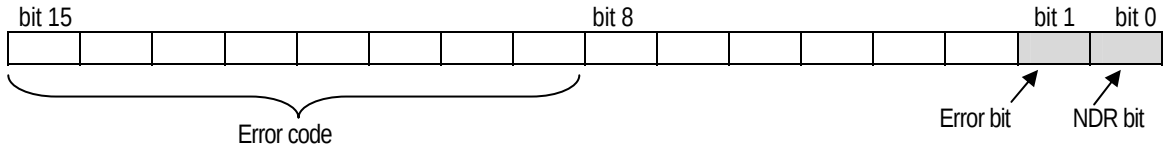
(1) Example program

- Designate slave station No. , function code,.address, No. of reading
- When input condition(M0020) turns on, MODBUS communication starts.
- Receiving data are stored D1000, and communication status is stored to M100



- When operates as slave, MASTER-K120S responses to master station without commands. And When operates as master, MASTER-K120S sends data in S1 with MODBUS protocol at rising edges of execution condition.

- S3 format is as below.



- NDR : when the communication ends normally, this bit turns on during 1 scan.
- Error bit : when communication error occurs, this bit turns on during 1 scan. At that time error code stores bit 8 ~ bit 15.
- Error code is as follow

Code	Error type	Meaning
01	Illegal Function	Error in inputting function code in instruction.
02	Illegal Address	Error of exceeding the area limit of reading/writing on the slave station.
03	Illegal Data Value	Error when the data value to be read from or write on the slave station isn't allowed.
04	Slave Device Failure	Error status of the slave station.
05	Acknowledge	It's a responding code of the slave station for the master station to prevent the master station time-out error, when request command processing takes time. The master station marks an error code and waits for a certain time without making any second request.
06	Slave Device Busy	Error when request command processing takes too much time. The master should request again.
07	Time Out	Error when exceeds the time limit of the communication parameter as it communicates.
08	Number Error	Errors when data is 0 or more than 256 bytes
09	Parameter Error	Error of setting parameters (mode, master/ slave)
10	Station Error	Error when the station number of itself and the station number set by the S1 of instruction are the same.

Remark

-. In MASTER-K120S series, the 'MODBUS' command which has been used in MK80S series can be used.
In this case, communication channel is fixed to channel 0.

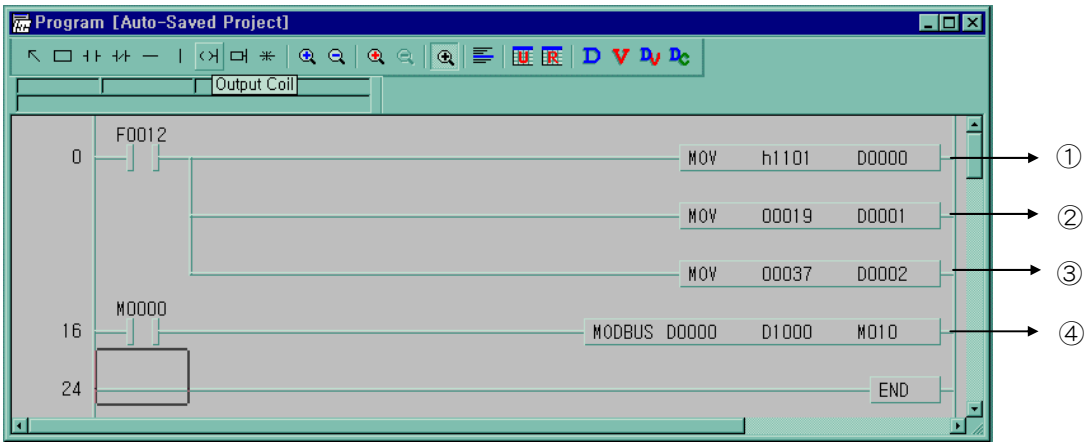
2) Example program 1

It's supposed that MASTER-K120S main unit is the master and it reads Coil Status of the station no. 17, a Modicon product. The master reads status of the Coil 00020 ~ 00056 of the slave station no. 17. The Coil of the slave station is supposed to be as follows and the data that are read is saved in D1000

Coil	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40
Status	X	X	X	1	1	0	1	1	0	0	0	0	1	1	1	0	1	0	1	1
Hex	1				B				0				E				B			
Coil	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20
Status	0	0	1	0	0	1	1	0	1	0	1	1	1	1	0	0	1	1	0	1
Hex	2				6				B				C				D			

- The status of Coil 57, 58, 59 are redundancy.
- Data is sent starting from the low bit by byte unit. If the deficient bit of a byte is filled with 0. An example of sending the above data is as Following example 1.

Example 1) CD B2 0E 1B



① It designates slave station and function code (No. of station : h11(17) , function code : h01)

② Address setting

- Address '0' at MODBUS protocol means address '1' actually .So if you want to designate address '20' , write address '19'

③ Reading number setting (Reading number is 37 from 20 to 56.)

④ This is MODBUS Communication instruction.

- Data is sent starting from the low bit by byte unit. If the deficient bit of a byte is filled with 0. An example of sending the above data is as follows.
- The data transmission starts lower byte. The remnant part of byte is filled with '0'

⑤ Stored data at D1000,D1001,D1002 are :

Device	Stored data
D1000	h CD 6B
D1001	h B2 CE
D1002	h 00 1B

3) Example program 2

It's supposed that MASTER-K120S main unit is the master and it reads Coil Status of the station no. 17, a Modicon product.

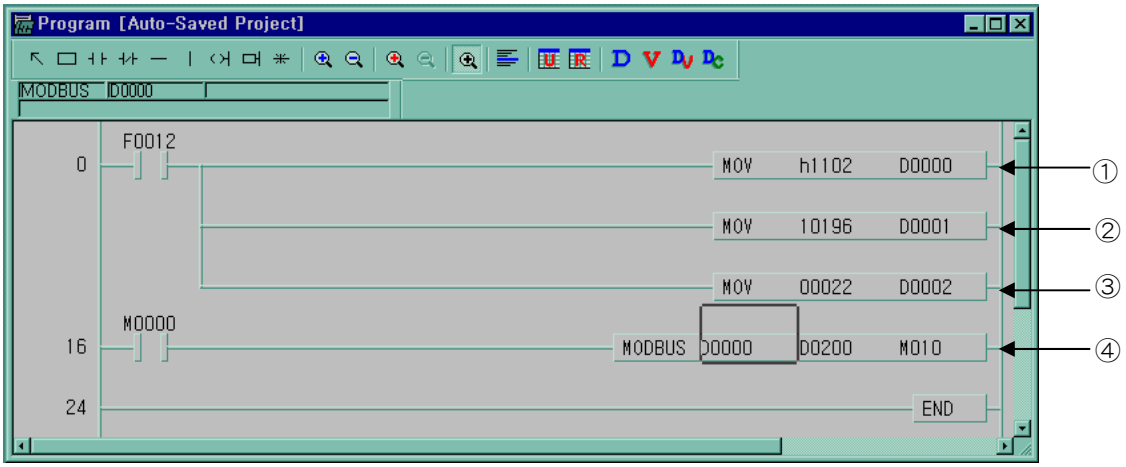
The master reads status of the input contact 10197 ~ 10218 of the slave station no. 17.

The input contact of the slave station is supposed to be as follows and the data that are read is saved in M015.

Input	10220	10219	10218	10217	10216	10215	10214	10213	10212	10211	10210	10209
Status	X	X	1	1	0	1	0	1	1	1	0	1
Hex	3				5				D			
Input	10208	10207	10206	10205	10204	10203	10202	10201	10200	10199	10198	10197
Status	1	0	1	1	1	0	1	0	1	1	0	0
Hex	B				A				C			

- The status of input contact 10219,10220 are redundancy.
- Data is sent starting from the low bit by byte unit. If the deficient bit of a byte is filled with 0. An example of sending the above data is as follows.

Example 2) AC DB 35



① : It designates slave station and function code (No. of station : h11(17) , function code : h02)

② : Address setting

Address '0' at MODBUS protocol means address '1' actually .So if you want to designate address '10197' , write address '10196'

③ : Reading number setting (Reading number is 22 from 10197 to 10220.)

④ : This is MODBUS Communication instruction.

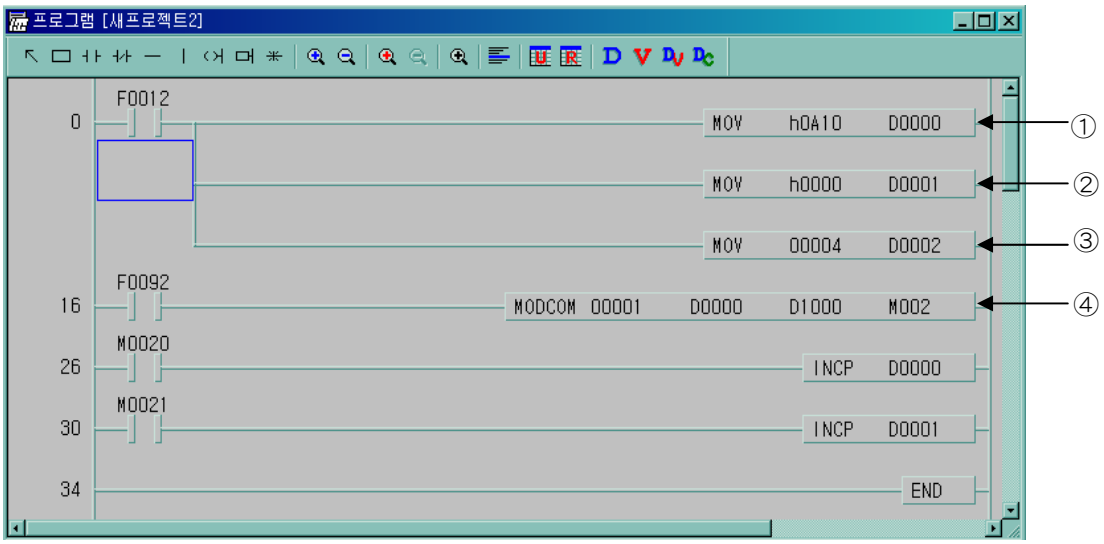
The data transmission starts lower byte. The remnant part of byte is filled with '0'

⑤ Stored data at D200,D201 are :

Device	Stored data
D200	h AC DB
D201	h 00 35

4) Example program 3

The master writes data D1000 ~ D1003 to contact 40000 of the slave station no. 10.



① : It designates slave station and function code (No. of station : h0A(10) , function code : h10)

② : Address setting

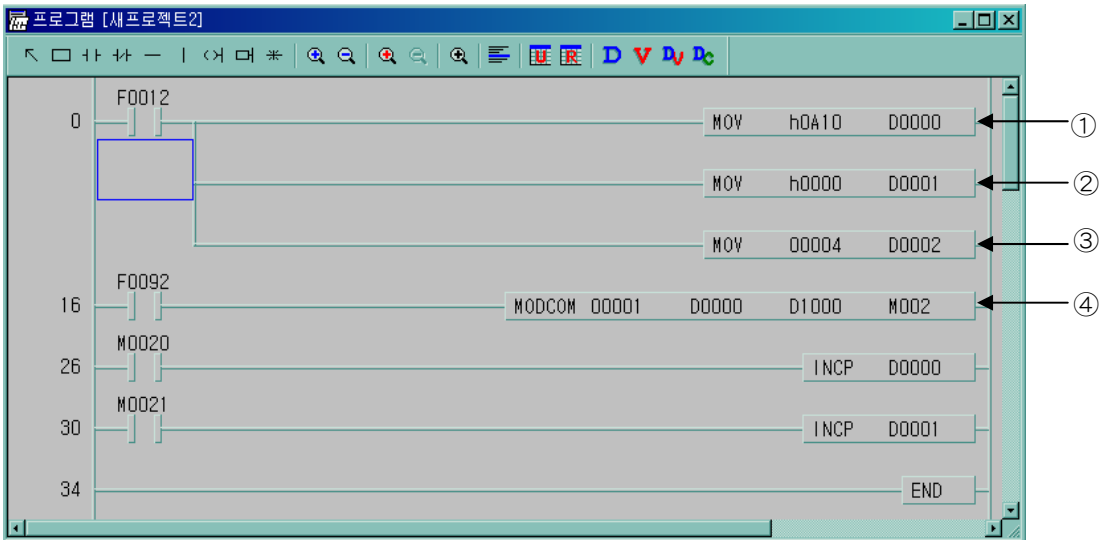
Address '0' of function code '16' at MODBUS protocol means address '40000' actually.

③ : Writing number setting (Writing number is 4)

④ : This is MODBUS Communication instruction.

5) Example program 4

The master writes data in D1000 to contact 40000 of the slave station no. 10.



① : It designates slave station and function code (No. of station : h0A(10) , function code : h06)

② : Address setting

Address '0' of function code '16' at MODBUS protocol means address '40000' actually.

③ : Writing number setting (Writing number is 1)

④ : This is MODBUS Communication instruction.