Modbus TCP Protocol

Modbus RTU protocol：

IP address of RTU can be set by config tool

IO port register map:

IO Port		PLC address	Hex address	Function code	Data type	Property
Digital Input	Di0	11001	03E8	01	UINT16	R
	Di1	11002	03E9			
	Di2	11003	03EA			
	…….	…….	……			
	Din	11001+n	03E8+n			
Digital Output	Do0	11101	044C	01/05	UINT16	R/W
	Do1	11102	044D			
	Do2	11103	044E			
	……	……				
	Don	11101+n	044C+n			
Analog Input	Ai0	41001~41002	03E8~03E9	03	Float32	R
	Ai1	41003~41004	03EA~03EB			
	Ai2	41005~41006	03EC~03ED			
	……	……	……			
	Ain	(41001+2n) ~ (41001+2n+1)	(03E8+2n) ~ (03E8+2n+1)			
Temperature Input	Ti0	41501~41502	05DC~05DD	03	Float32	R
	Ti1	41503~41504	05DE~05DF			
	Ti2	41505~41506	05E0~05E1			
	……	……	……			
	Tin	(41501+2n) ~ (41501+2n+1)	(05DC+2n) ~ (05DC +2n+1)			

1. Read digital input

Fox example, read 4 channels of Di, slave id=1

Master sends: 05 7A 00 00 00 06 01 01 03 E8 00 04

RTU responds: 05 7A 00 00 00 04 01 01 01 01

the explanation of master request command:

Message description	Number of bytes	Message	Explanation
Header	5	05 7A 00 00 00	
following bytes	1	06	
slave id	1	01H	slave id = 1
function code	1	01H	Read Coil Status
start address	2	03E8H	Read register start from 11001
number of points	2	0004H	Read 4 registers (11001-11004) corresponds to Di0 to Di3

RTU responds：

Message description	Number of byte	Message	Explanation
Header	5	05 7A 00 00 00	
following bytes	1	04	
slave id	1	01H	slave id = 1
function code	1	01H	Read Coil Status
number of bytes	1	01H	The number of data bytes to follow
data	1	01H	01H = 00000001 (BIN) corresponds to status of Di0 to Di3 Mean Di0 is close

2. Read digital output

Fox example, read 4 channels of Do, slave id=1

Master sends: 05 CA 00 00 00 06 01 01 04 4C 00 04

RTU responds: 05 CA 00 00 00 04 01 01 01 09

the explanation of master request command:

Message description	Number of bytes	Message	Explanation
Header	5	05 CA 00 00 00	
following bytes	1	06	
slave id	1	01H	slave id = 1
function code	1	01H	Read Coil Status
start address	2	044CH	Read register start from 11101
number of points	2	0004H	Read 4 registers (11101-11104) corresponds to Do0 to Do3

RTU responds：

Message description	Number of bytes	Message	Explanation
Header	5	05 CA 00 00 00	
following bytes	1	04	
slave id	1	01H	slave id = 1
function code	1	01H	Read Coil Status
number of bytes	1	01H	The number of data bytes to follow
data	1	09H	09H=00001001(Bin) corresponds to status of Di0 to Di3 Mean Di0 and Di3 are close

3. Write digital output

Fox example, write 4 channels of Do slave id=1:

Master sends: 0C E5 00 00 00 08 01 0F 04 4C 00 04 01 0B

Module responds: 0C E5 00 00 00 06 01 0F 04 4C 00 04

the explanation of master send command:

Message description	Number of bytes	Message	Explanation
Header	5	0C E5 00 00 00	
following bytes	1	08	
slave id	1	01H	slave id =1
function code	1	0FH	write multiple coil
start address	2	044CH	write register start from 11101
number of points	2	0004H	write 4 registers (11101-11104) corresponds to Do0 to Do3
number of data bytes	1	01H	write 1 byte
data	1	0BH	0BH = 0 0 0 0 1 0 1 1 (bin) Mean close Do0, Do1, Do3 and open Do2

RTU responds：

Message description	Number of bytes	Message	Explanation
Header	5	0C E5 00 00 00	
following bytes	1	06	
slave id	1	01H	slave id = 1
function code	1	0FH	write multiple coil
start address	2	044CH	write register start from 11101
number of points	2	0004H	write 4 registers (11101-11104) corresponds to Do0 to Do3

4. Read analog input

Fox example, read 4 channels of Ai, slave id=1：

Master sends: 06 A9 00 00 00 06 01 03 03 E8 00 08

Module responds: 06 A9 00 00 00 13 01 03 10 3E 42 41 4C F8 Al 41 5F F0 07 41 31 3E 42 41 7E

the explanation of master request command:

Message description	Number of bytes	Message	Explanation
Header	5	06 A9 00 00 00	
following bytes	1	06	
slave id	1	01H	slave id = 1
function code	1	03H	read holding register
start address	2	03E8H	read register start from 41001
number of points	2	0008H	Read 8 registers (41001-41008) corresponds to Ai0 to Ai7

RTU responds：

Message description	Number of bytes	Message	Explanation
Header	5	06 A9 00 00 00	
following bytes	1	13H	
slave id	1	01H	slave id = 1
function code	1	03H	read holding register
number of bytes	1	10H	16 bytes
data	16	3E42H 414CH	Channel 0=12.7655
		F8A1H 415FH	Channel 1=13.9982
		F007H 4131H	Channel 2=11.1211
		3E42H 417FH	Channel 3=15.9527

5. Read temperature input

Fox example, read 4 channels of Ti, slave id=1：

Master sends: 06 57 00 00 00 06 01 03 05 DC 00 08
Module responds: 06 57 00 00 00 13 01 03 10 64 C3 41 43 62 4E 41 63 2B 36 41 9A 31 90 41 6E

the explanation of master request command:

Message description	Number of bytes	Message	Explanation
Header	5	06 57 00 00 00	
following bytes	1	06H	
slave id	1	01H	slave id =1
function code	1	03H	read holding register
start address	2	05DCH	read register start from 41501
number of points	2	0008H	Read 8 registers (41501-41508) corresponds to Ti0 to Ti3

RTU responds：

Message description	Number of bytes	Message	Explanation
Header	5	06 57 00 00 00	
following bytes	1	13H	
slave id	1	01H	slave id = 1
function code	1	03H	read holding register
number of bytes	1	10H	16bytes
data	16	64C3H 4143H	Channel 0: 12.2121
		624EH 4163H	Channel 1: 14.2115
		2B36H 419AH	Channel 2: 19.2711
		3190H 416EH	Channel 3: 14.8871