

# Modbus RTU Protocol

## Modbus RTU protocol:

CWT device default slave id is 32, it 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

For example, read 4 channels of Di, slave id=32

Master sends: 20 01 03 E8 00 04 BB 08

RTU responds: 20 01 01 02 DA 75

the explanation of master request command:

Message description	Number of bytes	Message	Explanation
slave id	1	20H	slave id = 32
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
CRC CHECK	2	BB08H	

RTU responds:

Message description	Number of byte	Message	Explanation
slave id	1	20H	slave id = 32
function code	1	01H	Read Coil Status
number of bytes	1	01H	The number of data bytes to follow
data	1	02H	02H = 00000010 (BIN) corresponds to status of Di0 to Di3 Mean Di1 is close
CRC CHECK	2	DA75H	

## 2. Read digital output

**Fox example, read 4 channels of Do, slave id=32**

Master sends: 20 01 04 4C 00 04 FB 9F

RTU responds: 20 01 01 03 1B B5

the explanation of master request command:

Message description	Number of bytes	Message	Explanation
slave id	1	20H	slave id = 32
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
CRC CHECK	2	FB9FH	

RTU responds:

Message description	Number of bytes	Message	Explanation
slave id	1	20H	slave id = 32
function code	1	01H	Read Coil Status
number of bytes	1	01H	The number of data bytes to follow
data	1	03H	03H=00000011(Bin) corresponds to status of Di0 to Di3 Mean Di0 and Di1 are close
CRC CHECK	2	1BB5H	

## 3. Write digital output

**Fox example, write 4 channels of Do slave id=32:**

Master sends: 20 0F 04 4C 00 04 01 0B AC CF

Module responds: 20 0F 04 4C 00 04 92 5E

the explanation of master send command:

Message description	Number of bytes	Message	Explanation
slave id	1	20H	slave id =32
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
CRC CHECK	2	ACCFH	

RTU responds:

Message description	Number of bytes	Message	Explanation
slave id	1	20H	slave id =32
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
CRC CHECK	2	925EH	

## 4. Read analog input

**Fox example, read 4 channels of Ai, slave id=32:**

Master sends: 20 03 03 E8 00 08 C2 CD

Module responds: 20 03 10 3F 14 41 3C 14 12 41 5B CE D9 41 7A 91 D1 41 45 2B 36

the explanation of master request command:

Message description	Number of bytes	Message	Explanation
slave id	1	20H	slave id =32
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 Ai3
CRC CHECK	2	C2CDH	

RTU responds:

Message description	Number of bytes	Message	Explanation
slave id	1	20H	slave id = 32
function code	1	03H	read holding register

number of bytes	1	10H	16 bytes
data	16	3F14H 415BH	Channel 0=11.7654
		413CH CED9H	Channel 1=13.6924
		1412H 417AH	Channel 2=15.6755
		91D1H 4145H	Channel 3=12.3481
CRC CHECK	2	2B36H	

## 5. Read temperature input

**For example, read 4 channels of Ti, slave id=32:**

Master sends: 20 03 05 DC 00 08 83 8B

Module responds: 20 03 10 FA 44 41 4D 27 A1 42 19 13 A9 41 33 02 41 41 BF 5D 30

the explanation of master request command:

Message description	Number of bytes	Message	Explanation
slave id	1	20H	slave id =32
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
CRC CHECK	2	838BH	

RTU responds:

Message description	Number of bytes	Message	Explanation
slave id	1	20H	slave id = 32
function code	1	03H	read holding register
number of bytes	1	10H	16 bytes
data	16	FA44H 414DH	Channel 0: 12.8736
		27A1H 4219H	Channel 1: 38.2887
		13A9H 4133H	Channel 2: 11.1923
		0241H 41BFH	Channel 3: 23.8761
CRC CHECK	2	5D30H	