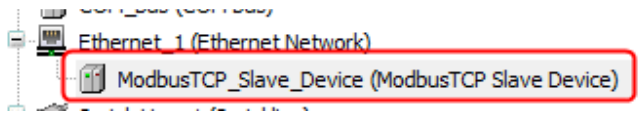# ModbusTCP Slave Device explanation

Background

For PLC with Ethernet port in SoMachine software, we can add "ModbusTCP Slave Device" in Ethernet：

However, many users do not know: what's the meaning of"ModbusTCP Slave Device"; what's the difference with Modbus TCP server; what's the advantage to use it; and how to use it.

Explanation

The Modbus TCP Slave device creates a specific I/O area on the controller, accessible through Modbus/TCP protocol. The I/O mapping of this area is:

Variable	Mapping	Channel	Address	Type	Default Value	Unit	Description
⊟ 🏷		Inputs	%IW5	ARRAY [0...9] OF WORD			Modbus Holding Registers
⊞ 🏷 iwModbusTCT_Sla...		Inputs[0]	%IW5	WORD			
⊞ 🏷 iwModbusTCT_Sla...		Inputs[1]	%IW6	WORD			
⊞ 🏷 iwModbusTCT_Sla...		Inputs[2]	%IW7	WORD			
⊞ 🏷 iwModbusTCT_Sla...		Inputs[3]	%IW8	WORD			
⊞ 🏷 iwModbusTCT_Sla...		Inputs[4]	%IW9	WORD			
⊞ 🏷 iwModbusTCT_Sla...		Inputs[5]	%IW10	WORD			
⊞ 🏷 iwModbusTCT_Sla...		Inputs[6]	%IW11	WORD			
⊞ 🏷 iwModbusTCT_Sla...		Inputs[7]	%IW12	WORD			
⊞ 🏷 iwModbusTCT_Sla...		Inputs[8]	%IW13	WORD			
⊞ 🏷 iwModbusTCT_Sla...		Inputs[9]	%IW14	WORD			
⊟ 🏷		Outputs	%QW2	ARRAY [0...9] OF WORD			Modbus Input Registers
⊞ 🏷 qwModbusTCP_Sl...		Outputs[0]	%QW2	WORD			
⊞ 🏷 qwModbusTCP_Sl...		Outputs[1]	%QW3	WORD			
⊞ 🏷 qwModbusTCP_Sl...		Outputs[2]	%QW4	WORD			
⊞ 🏷 qwModbusTCP_Sl...		Outputs[3]	%QW5	WORD			
⊞ 🏷 qwModbusTCP_Sl...		Outputs[4]	%QW6	WORD			
⊞ 🏷 qwModbusTCP_Sl...		Outputs[5]	%QW7	WORD			
⊞ 🏷 qwModbusTCP_Sl...		Outputs[6]	%QW8	WORD			
⊞ 🏷 qwModbusTCP_Sl...		Outputs[7]	%QW9	WORD			
⊞ 🏷 qwModbusTCP_Sl...		Outputs[8]	%QW10	WORD			
⊞ 🏷 qwModbusTCP_Sl...		Outputs[9]	%QW11	WORD			

It is used when an external I/O scanner (Master) needs to access the %IW and %QW objects of the controller. %IW area can be only written and read by Master, and Slave device can only read them. %QW area can be only written by Slave, and Master can only read them.
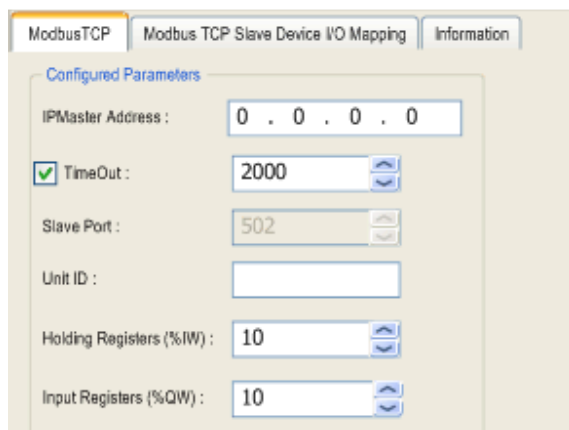
From I/O scanner (Master) point of view,
- The corresponding address for %IW area are %MW0~%MW(n-1);
- The corresponding address for %QW area are %MWn~%MW(n+m-1) .

n= %IW quantity, m=%QW quantity. The quantity of %IW and %QW are 2~40 words for each.

Note: Actual %MW address of slave device cannot be visited.

Configuration of Modbus TCP Slave device

When PLC configure Modbus TCP Slave device, in the following configuration page:

IPMaster Address: it can be 0.0.0.0. When IP address of the Modbus Master is configured, the connection will never be closed on this address.

Timeout: The timeout applies to the IP Master Address unless if the address is 0.0.0.0. The timeout duration associated to the privileged connection allows you to check if the controller is polled by the privileged Master. If no Modbus request is received within the timeout duration, the diagnostic information i_byMasterIpLost is set to 1 (TRUE).

Unit ID: This ID (1~247) should be same the unit ID setting in Modbus TCP I/O scanner. If not same, the PLC will work as a standard Modbus TCP server!

Holding Registers (%IW): Number of registers in the input assembly (2...40 words)

Input Registers (%QW): Number of registers in the output assembly (2...40 words)

Modbus TCP Slave device serves as a gateway between %MW0~%MW(n+m-1) in I/O scanner and the %IW and %QW area in the PLC via Unit ID.

Modbus requests that attempt to access registers above n+m-1 are answered by the 02 - ILLEGAL DATA ADDRESS exception code.

Compare with Modbus TCP server

Modbus TCP server	Modbus TCP slave device
Only configure IP address	Need to configure parameters and I/O mapping
For Modbus TCP client, all %MW address of server can be R/W.	For I/O scanner, only %IW area (2~40 words) can be R/W, %QW area (2~40 words) are read only, and actual %MW address of slave device cannot be visited.
No need to configure "Unit ID"	Unit ID (1~247) should be same the unit ID setting in Modbus TCP I/O scanner.
No visualized list for communicated address.	Have a clear and visualized interface to monitor all communicated variables.
The connection to one client may be closed when more than 8 connections are needed.	The connection to the Master client is never forcefully closed, when IPMaster Address is configured.

Advantages and disadvantages

The main advantage of using a Modbus TCP Slave device is that the controller objects are gathered, which allows to have a clear and easy configuration interface for PLC as a slave device.

The TCP Slave device also has the capability to define a privileged Modbus client application, whose connection is never forcefully closed (the regular Modbus server connections may be closed when more than 8 connections are needed).

The PLC can simultaneously works as Modbus TCP Slave device and standard Modbus TCP server without interference.

As the configuration of the %IW and %QW is limited to 40 words it is often not sufficient – most applications have much more words to be communicated to a Mobus TCP client station.