

Giải pháp Mạng truyền thông Modbus với SIMATIC PLC S7



- 1 Giới thiệu về mạng truyền thông Modbus
- 2 Lựa chọn thiết bị Modbus với PLC S7 - 1200/300/1500
- 3 Cấu hình truyền thông Modbus RTU
- 4 Cấu hình truyền thông Modbus TCP/IP
- 5 Thực hành



- 1 **Giới thiệu về mạng truyền thông Modbus**
- 2 Lựa chọn thiết bị Modbus với PLC S7 - 1200/300/1500
- 3 Cấu hình truyền thông Modbus RTU
- 4 Cấu hình truyền thông Modbus TCP/IP
- 5 Thực hành

Các hệ thống mạng truyền thông công nghiệp

SIEMENS
Ingenuity for life



CC-Línk IE

sercos
the automation bus

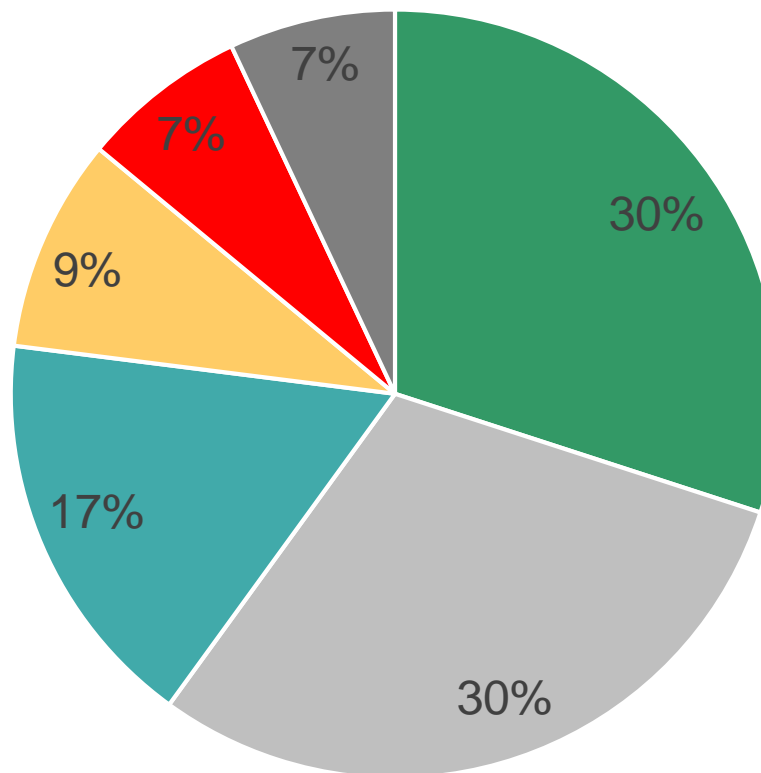
EtherCAT®



ETHERNET
POWERLINK



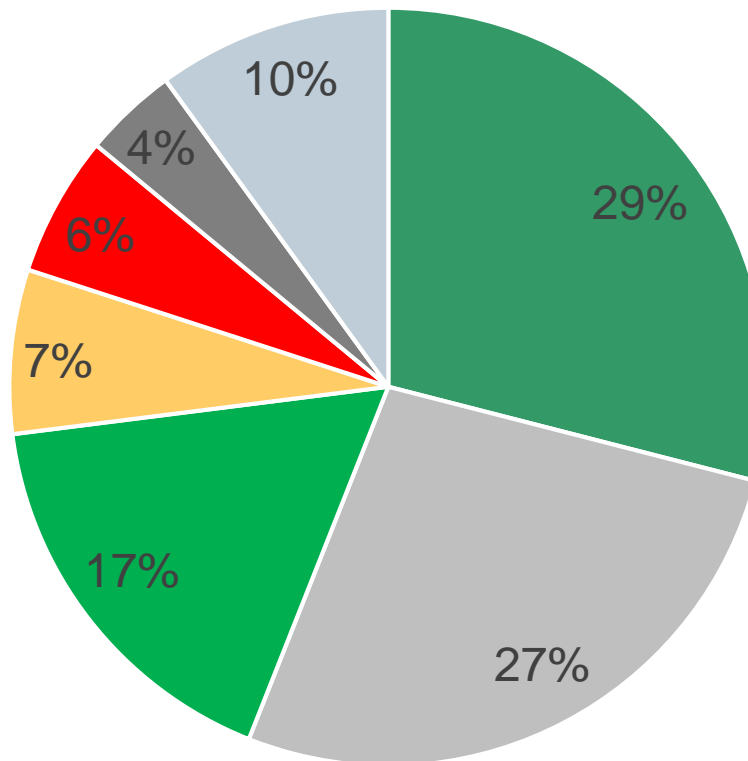
Thống kê về mạng truyền thông công nghiệp



■ PROFINET ■ Ethernet/IP ■ Modbus TCP ■ Ethernet-Powerlink ■ EtherCAT ■ Others

Source: IMS Research "The World Market for Industrial Ethernet" – 2013 Edition

Thống kê về mạng truyền thông công nghiệp



■ PROFINET ■ EtherNet/IP ■ Ethernet TCP/IP ■ Modbus TCP ■ EtherCAT ■ CC-Link IE ■ Others

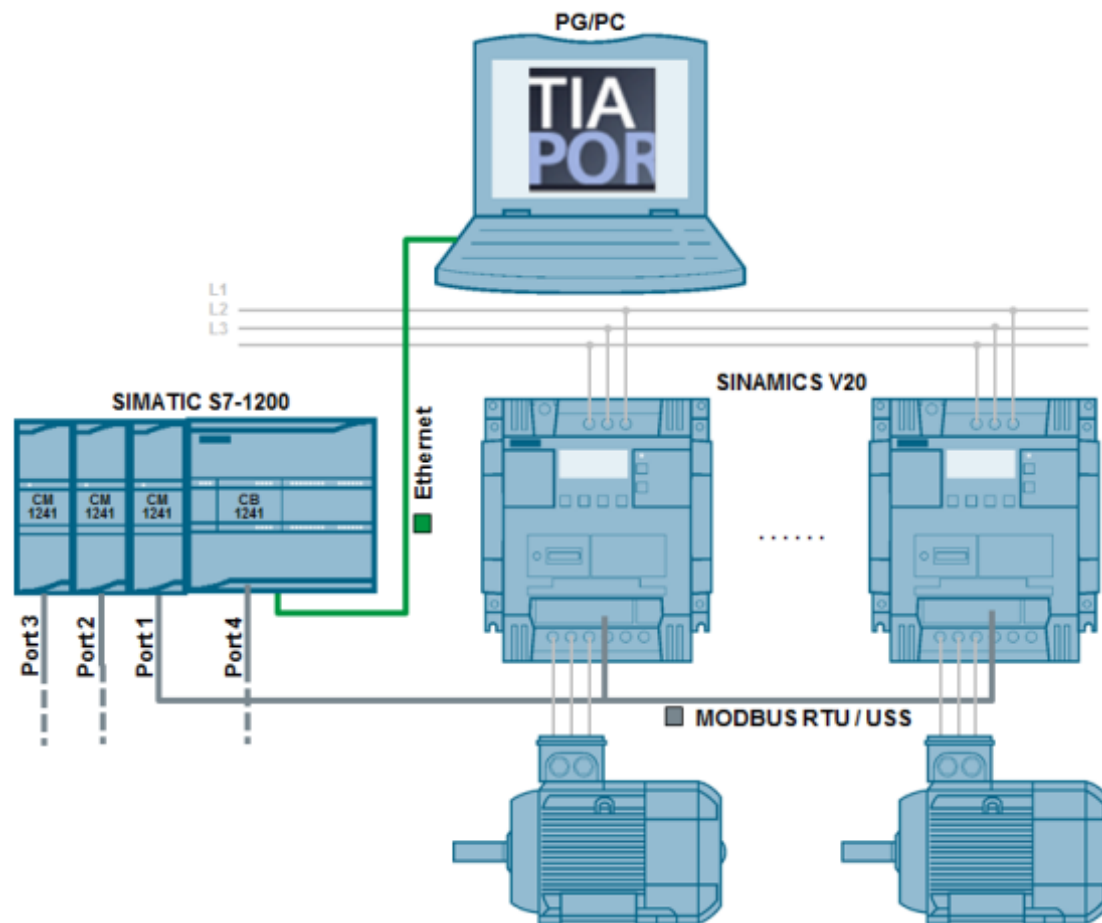
Source: HIS Markit | Technology (Informa Tech 2019)

Giới thiệu về mạng truyền thông Modbus



- Modbus do Modicon phát triển năm 1979
- Phương tiện truyền thông với nhiều thiết bị thông qua một cặp dây xoắn đơn.
- Tiêu chuẩn thông dụng trong ngành tự động hóa và là giao thức Protocol miễn phí.
- Modbus là một hệ thống hoạt động với **Master – Slaver**.

Giới thiệu về mạng truyền thông Modbus



- **Master** được kết nối với một hoặc nhiều Slaver
- **Master** thường là PLC, PC, DCS
- **Slaver** thường là các thiết bị trường, cảm biến đo lường, biến tần...
- **Master** có thể kết nối tới 247 Slaver

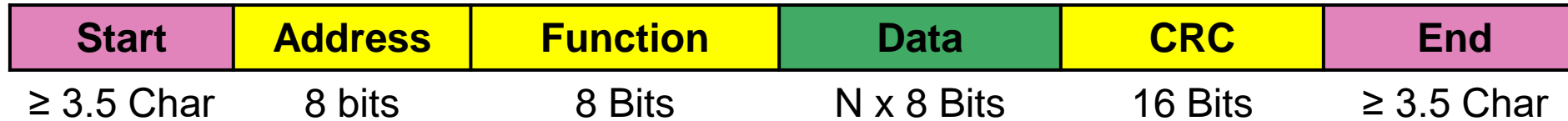
Các giao thức truyền thông Modbus

Có 3 giao thức truyền thông Modbus phổ biến được sử dụng nhiều nhất là:

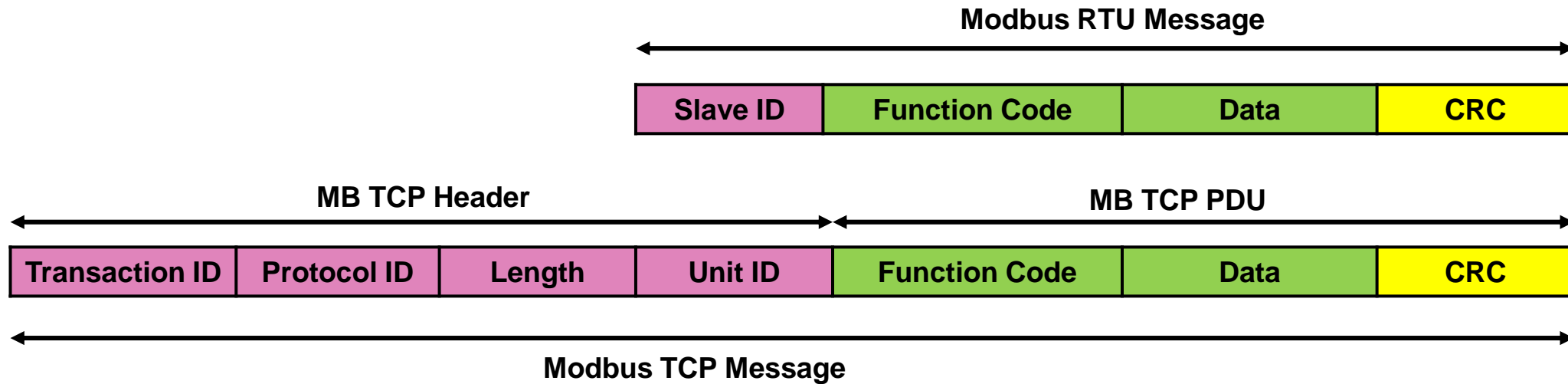
- Modbus ASCII
- Modbus RTU
- Modbus TCP/IP

Start	Address	Function	Data	LRC Check	End
1 Char	2 Chars	2 Chars	N Chars	2 Chars	2 Chars CRLF

- Gói tin của Modbus ASCII mã hóa theo hexa, sử dụng đặc tính ASCII 4 bit.
- Modbus ASCII chậm nhất trong số 3 loại protocol.
- Thích hợp khi kết nối bằng modem điện thoại hay kết nối sử dụng sóng radio do ASCII.



- Gói tin của Modbus RTU được mã hóa theo hệ nhị phân.
- Modbus RTU là giao thức lý tưởng đối với RS 232 hoặc RS485
- Tốc độ baud từ 1200 – 115200 bps . Tốc độ phổ biến nhất là 9600 hoặc 19200 baud.
- Modbus RTU là protocol công nghiệp phổ biến nhất.



- Là giao thức Modbus phát dựa trên nền tảng Industrial Ethernet.
- Các kết nối thay Master – Slaver bằng Client – Server.
- Dữ liệu Modbus được tóm lược đơn giản trong một gói tin TCP/IP.



- 1 Giới thiệu về mạng truyền thông Modbus
- 2 **Lựa chọn thiết bị Modbus với PLC S7 - 1200/300/1500**
- 3 Cấu hình truyền thông Modbus RTU
- 4 Cấu hình truyền thông Modbus TCP/IP
- 5 Thực hành

Hỏi đáp



- 1 Giới thiệu về mạng truyền thông Modbus
- 2 Lựa chọn thiết bị Modbus với PLC S7 - 1200/300/1500
- 3 **Cấu hình truyền thông Modbus RTU**
- 4 Cấu hình truyền thông Modbus TCP/IP
- 5 Thực hành

Nguyên tắc truyền thông của Modbus RTU



Gói tin của Modbus master truyền/gửi đi:

- Địa chỉ slave
- Mã chức năng hay Modbus function code
- Địa chỉ thanh ghi (Input, Output, thanh ghi Holding)
- Kiểm tra lỗi

Địa chỉ của các thiết bị Modbus từ 0 – 247.

Mã chức năng của Modbus

Mã chức năng	Chức năng
01	Đọc Bit ngõ ra
02	Đọc Bit ngõ vào
03	Đọc thanh ghi Holding
04	Đọc Word ngõ vào
05	Ghi vào Bit ngõ ra
06	Ghi vào thanh ghi Holding
...	
...	
...	
xx	255 mã chức năng, phụ thuộc vào thiết bị

Địa chỉ Modbus

Địa chỉ Modbus	Kiểu thực thi	Định dạng thanh ghi/ Vùng nhớ
00001 – 09999	Đọc hoặc ghi	Bit ngõ ra (Q)
10001 – 19999	Chỉ đọc	Bit ngõ vào (I)
30001 – 39999	Chỉ đọc	Đọc Word ngõ vào (IW)
40001 – 49999	Đọc hoặc viết	Thanh ghi Holding (Register)

Địa chỉ Modbus = Thanh ghi thiết bị + Offset

Lựa chọn Offset:

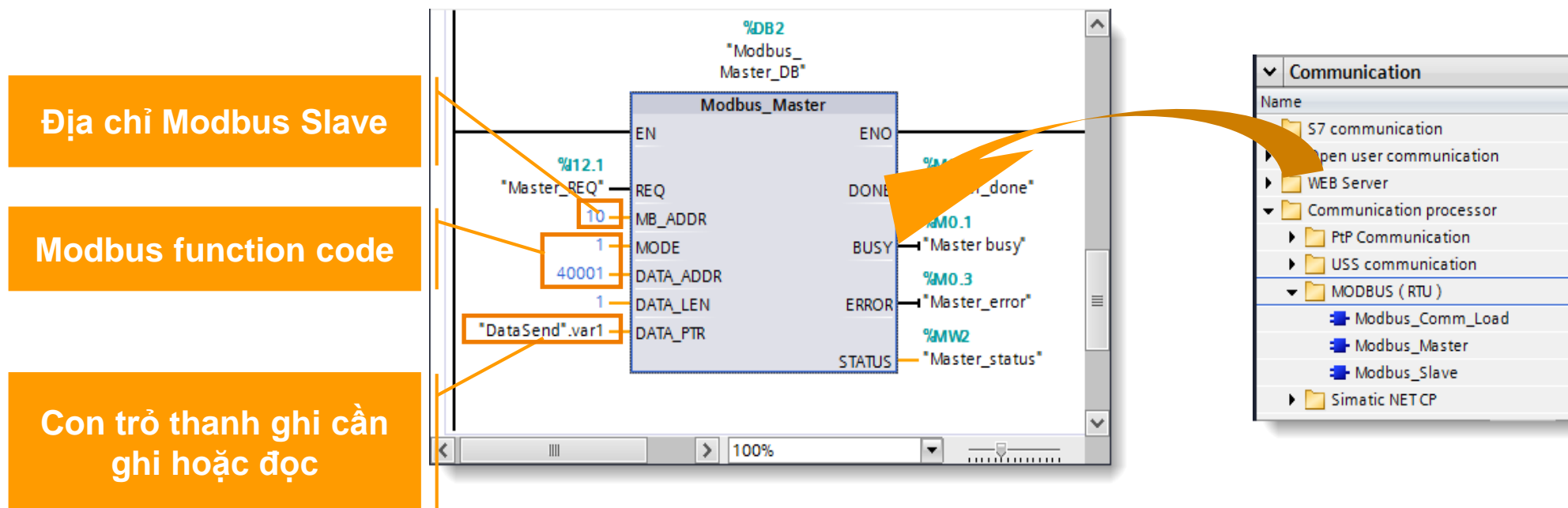
- 40000 hoặc 40001
- 400000 hoặc 400001

Thiết kế Modbus RTU trong STEP 7 V1x

Chọn giao thức Modbus trong thuộc tính Properties của module CM

The image illustrates the configuration of a Modbus RTU network in STEP 7 V1x. The top window, titled 'ModbusRTU > Devices & networks', shows a network topology with two PLCs (PLC_1 and PLC_2) connected via a PN/IE_1 interface. A yellow circle with the number 1 highlights the connection line. The bottom window, titled 'CM PtP RS232 HF_1 [CM PtP RS232 HF]', shows the 'Properties' dialog for the communication module. A yellow circle with the number 2 highlights the 'Protocol' dropdown menu, which is set to 'Modbus'. The 'Hardware catalog' window on the right shows the selection path: Catalog > Filter > Controllers > SIMATIC S7-1500 > CPU > Communication modules > PROFIBUS > Point-to-Point > CM PtP RS232 HF, with the specific module '6ES7 541-1AD00-0AB0' selected.

Thiết kế Modbus RTU Master trong STEP 7 V1x



Thiết kế Modbus RTU Master trong STEP 7 V1x



Hardware-ID

Modbus_Master_DB

Name	Data type	Offset
Compatibility_Mode	Bool	22.1
MB_DB	P2P_MB_BASE	24.0
S_PORT	Word	0.0
S_RESP_TO	Word	2.0
S_ICHAR_GAP	Word	4.0
S_RETRIES	Word	6.0
S_MB_CRC	Byte	8.0
Send_P2P	Send_P2P	
Receive_P2P	Receive_P2P	

Modbus_Comm_Load

EN, ENO, DONE, ERROR, STATUS

REQ, PORT, BAUD, PARITY, FLOW_CTRL, RTS_ON_DLY, RTS_OFF_DLY, RESP_TO

9600, 0, 0, 0, 0, 1000

%DB1 "Modbus_Comm_Load_DB"

%I2.0 "Tag_1"

276

PIDB2.DBX24.0 "Modbus_Master_DB".MB_DB

CM PtP RS232 HF_1 [CM PtP RS232 HF]

General, IO tags, Texts

Hardware identifier

Hardware identifier: 276

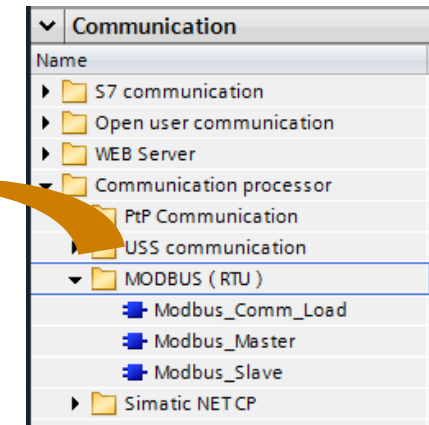
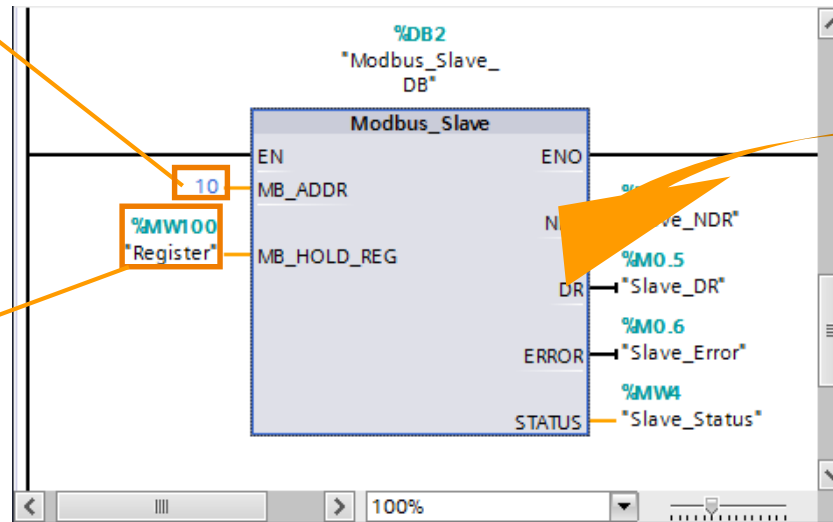
Communication

- S7 communication
- Open user communication
- WEB Server
- Communication processor
 - PtP Communication
 - USS communication
 - MODBUS (RTU)
 - Modbus_Comm_Load
 - Modbus_Master
 - Modbus_Slave
- Simatic NET CP

Thiết kế Modbus RTU Slave trong STEP 7 V1x

Địa chỉ Modbus Slave

Thanh ghi Pointer Modbus-Holding



Thiết kế Modbus RTU Slave trong STEP 7 V1x

Xem Hardware-ID trong
thuộc tính Properties

The screenshot illustrates the configuration of a Modbus RTU Slave in STEP 7 V1x. The main window shows the 'Modbus_Comm_Load' block with the following parameters:

- EN: %M0.0
- REQ: *Modbus_REQ*
- PORT: 276
- BAUD: 9600
- PARITY: 0
- FLOW_CTRL: 0
- RTS_ON_DLY: 0
- RTS_OFF_DLY: 0
- RESP_TO: 1000
- MB_DB: P#DB2.DBX24.0

The 'Properties' window for the 'Modbus_Comm_Load' block shows the 'Hardware identifier' set to 276. The 'Communication' tree on the right shows the project structure with 'MODBUS (RTU)' selected. The 'Modbus_Slave_DB' table is shown at the bottom left:

Name	Data type	Offset
Success_Count	Word	22.0
MB_DB	P2P_MB_BASE	24.0
S_PORT	Word	0.0
S_RESP_TO	Word	2.0
S_ICHAR_GAP	Word	4.0
S_RETRIES	Word	6.0
S_MB_CRC	Byte	8.0
SEND_P2P	Send_P2P	
RCV_P2P	Receive_P2P	



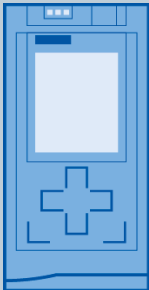

- 1 Giới thiệu về mạng truyền thông Modbus
- 2 Lựa chọn thiết bị Modbus với PLC S7 - 1200/300/1500
- 3 Cấu hình truyền thông Modbus RTU
- 4 **Cấu hình truyền thông Modbus TCP/IP**
- 5 Thực hành

Đặc điểm

- Modbus TCP là một giao thức mở
- Truyền thông Modbus TCP có thể được cấu hình hoặc lập trình thông qua các kết nối:
 - PROFINET
 - ETHERNET
- Các tham số kết nối được gán thông qua một cấu trúc (SDT)
 - TCON_IP_v4
 - TCON_Configured
- Modbus TCP chiếm các tài nguyên truyền thông với OUC Communication Resources
- Modbus TCP sử dụng “well-known” port 502

SIMATIC PLC S7 – 1200/1500 với Modbus TCP



S7-1200/1500		MODBUS TCP	
	CPU	CP	✓
		CM	✓
		ETH	✓
		PN	✓
		PN	✓

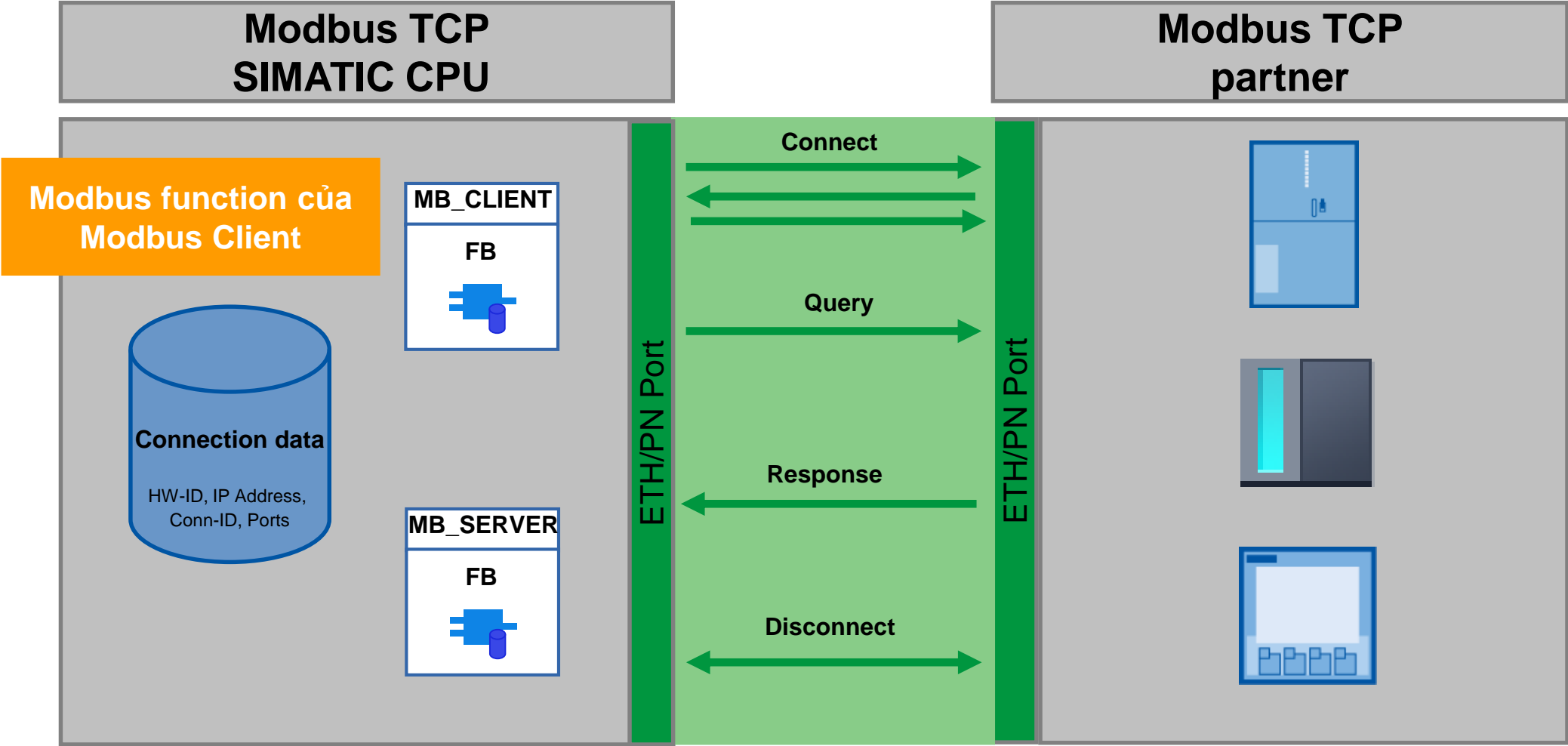
MB_CLIENT	
EN	ENO
REQ	DONE
DISCONNECT	BUSY
MB_MODE	ERROR
MB_DATA_ADDR	STATUS
MB_DATA_LEN	
MB_DATA_PTR	
CONNECT	

MB_SERVER	
EN	ENO
DISCONNECT	NDR
CONNECT	DR
MB_HOLD_REG	ERROR
	STATUS

Hỗ trợ cho phần cứng sản xuất từ ngày 01.07.2013 tới nay

S7-1500	✓	S7-1200	✓	S7-300/400/WinAC	✗
---------	---	---------	---	------------------	---

Nguyên tắc truyền thông của Modbus TCP



S7-1500



S7-1200



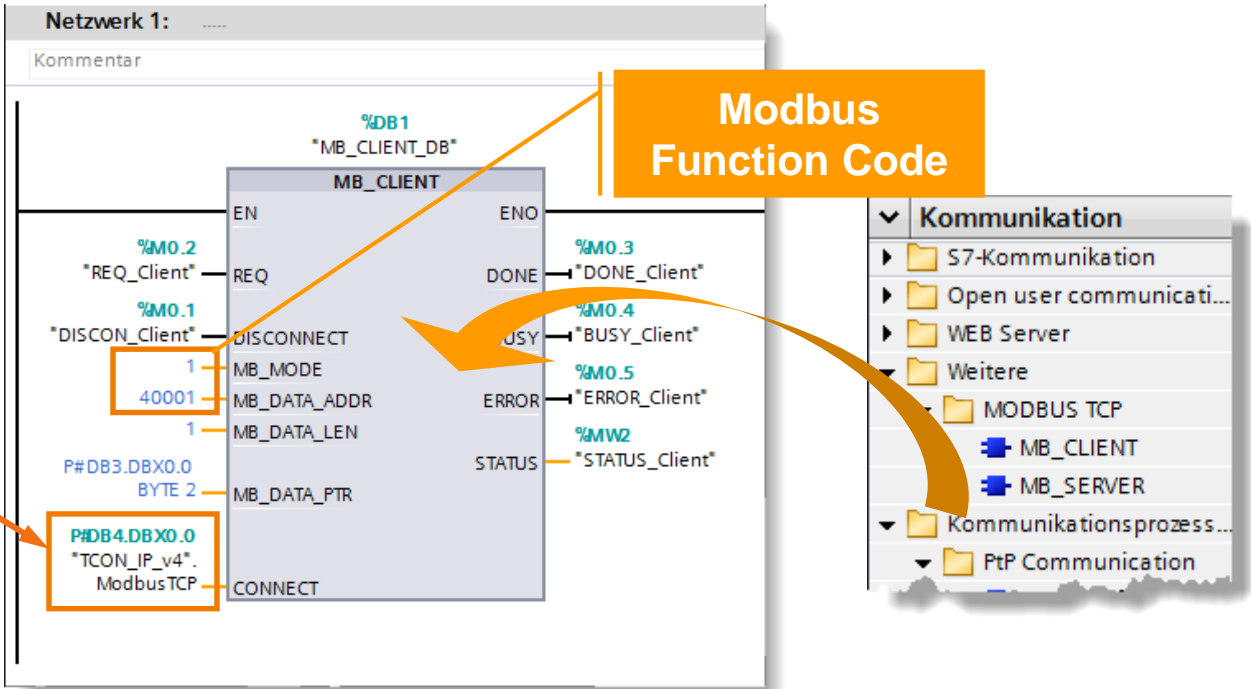
S7-300/400/WinAC



Modbus TCP Client

Phụ thuộc vào kiểu kết nối, các tham số được gán với một cấu trúc

TCON_IP_v4_Client				
	Name	Datentyp	Offset	Startwert
1	Static			
2	ModbusTCP	TCON_IP_v4	0.0	
3	Interfaceld	HW_ANY	0.0	64
4	ID	CONN_OUC	2.0	1
5	ConnectionType	Byte	4.0	16#0B
6	ActiveEstablished	Bool	5.0	true
7	RemoteAddress	IP_V4	6.0	
8	ADDR	array [1..4] o...	0.0	
9	ADDR[1]	Byte	0.0	192
10	ADDR[2]	Byte	1.0	168
11	ADDR[3]	Byte	2.0	0
12	ADDR[4]	Byte	3.0	11
13	RemotePort	UInt	10.0	502
14	LocalPort	UInt	12.0	2000



S7-1500



S7-1200



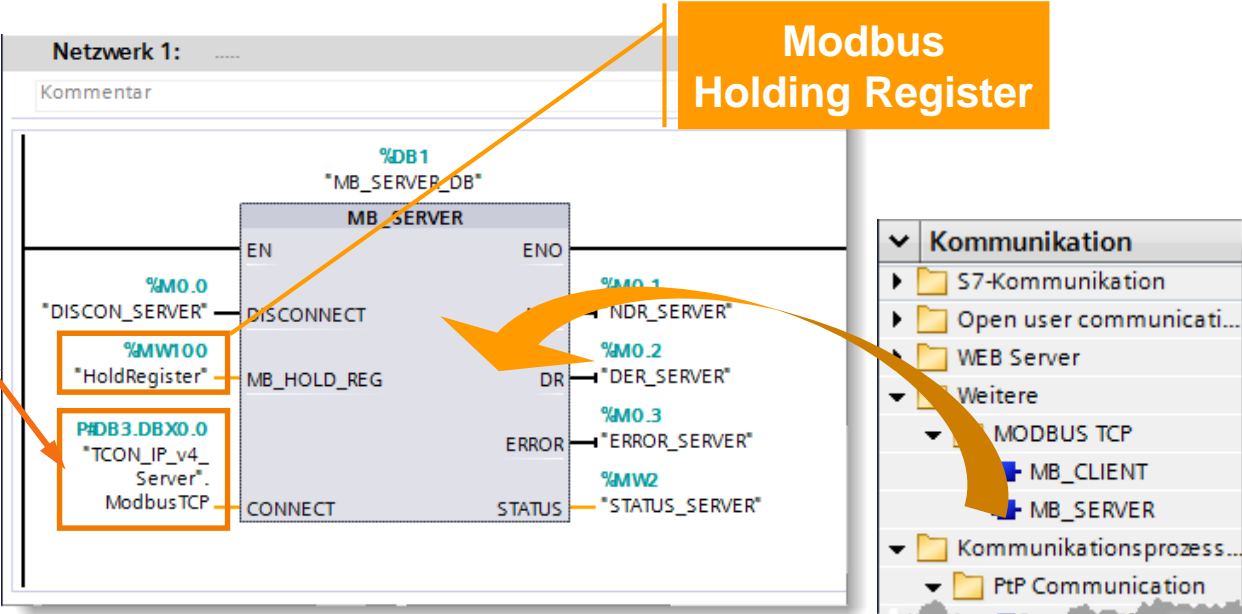
S7-300/400/WinAC



Modbus TCP Server

Phụ thuộc vào kiểu kết nối, các tham số được gán với một cấu trúc

TCON_IP_v4_Server				
	Name	Datentyp	Offset	Startwert
1	Static			
2	ModbusTCP	TCON_IP_v4	0.0	
3	Interfaceld	HW_ANY	0.0	64
4	ID	CONN_OUC	2.0	1
5	ConnectionType	Byte	4.0	16#0B
6	ActiveEstablished	Bool	5.0	false
7	RemoteAddress	IP_V4	6.0	
8	ADDR	array [1..4] of Byte	0.0	
9	ADDR[1]	Byte	0.0	16#C0
10	ADDR[2]	Byte	1.0	16#A8
11	ADDR[3]	Byte	2.0	16#00
12	ADDR[4]	Byte	3.0	16#0A
13	RemotePort	UInt	10.0	2000
14	LocalPort	UInt	12.0	502



S7-1500



S7-1200



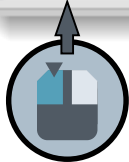
S7-300/400/WinAC



Thực hiện chuẩn đoán Modbus TCP



Go online Go offline



Trạng thái kết nối

Network overview	Connections	I/O communication	VPN
Local connection name		Local end point	
Programmed open user communication_192.168.0.11_1		Client	
Programming device connection_192.168.0.196_1		Client	
Programmed open user communication_192.168.0.10_1		Server	
Programming device connection_192.168.0.196_2		Server	

Connection resources

	Station resources						Module resources	
	Reserved			Dynamic			CPU 1516-3 PN/DP (R0/S1)	
	Maximum	Configured	Used	Configured	Used		Configured	Used
Maximum number of resources:	10	10	246	246	128	128		
PG communication:	4	-	1	-	0	-	1	
HMI communication:	4	0	0	0	0	0	0	
OP communication:	0	-	0	0	0	0	0	
Open user communication:	0	-	-	0	1	0	1	
Web communication:	2	-	0	-	0	-	0	
Other communication:	0	-	-	-	0	-	0	
Total resources used:	0	1	0	1	0	2		
Available resources:	10	9	246	245	128	126		

Modbus TCP chiếm tài nguyên của OUC communication

Connection address details

Local	Partner
End point: Client	192.168.0.11
Interface: Client(Slot1)/PROFINET interface_1	
Subnet: E261-0000-0001	
Address: 192.168.0.10	192.168.0.11
Port: 2000	502
<input checked="" type="checkbox"/> Active connection establishment	

Chi tiết về kết nối như IP-Active partner, Addresses, Ports



- 1 Giới thiệu về mạng truyền thông Modbus
- 2 Lựa chọn thiết bị Modbus với PLC S7 - 1200/300/1500
- 3 Cấu hình truyền thông Modbus RTU
- 4 Cấu hình truyền thông Modbus TCP/IP
- 5 Thực hành

Hỏi đáp

Để tìm hiểu thêm hoặc cần trợ giúp, xin vui lòng liên hệ:



Automation Forum Siemens Việt Nam



Siemens Training Center – SITRAIN

Cảm ơn sự quan tâm theo dõi!

SIEMENS
Ingenuity for life



Trần Văn Hiếu

Quản lý Trung tâm Đào tạo Công nghiệp Số SITRAIN

Ban Công nghiệp Số, Siemens Việt Nam

Email: tran-van.hieu@siemens.com

www.siemens.com.vn

www.facebook.com/Siemens.Vietnam