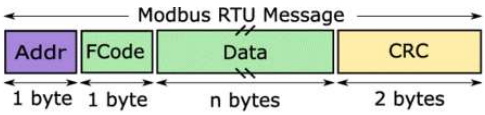
TÌM HIỂU VỀ TRUYỀN THÔNG MODBUS TCP/IP CỦA PLC S7-1200

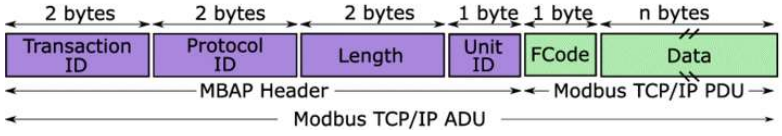
BY: TAPIT / ON: 14/07/2022 / IN: UNCATEGORIZED

TRUYỀN THÔNG MODBUS TCP/IP

1. Tổng quan Modbus TCP/IP và Modbus RTU.

Hai chuẩn truyền thông công nghiệp được sử dụng phổ biến hiện nay với hai khung truyền gói tin khác nhau:





1.1. Modbus RTU.

- Gói tin của Modbus RTU được mã hóa theo hệ nhị phân.
- Modbus RTU là giao thức lý tưởng đối với RS232 hoặc RS485.
- Tốc độ truyền và khoảng cách truyền theo chuẩn RS232 và RS485.
- Tốc độ Baud từ 1200 – 115200 bps. Tốc độ phổ biến nhất là 9600 hoặc 19200 baud.

XEM THÊM CÁC BÀI VIẾT TỪ TAPIT

- GIAO TIẾP CẢM BIẾN NHẬN DẠNG VÂN TAY AS608 (Phần 2)
- HƯỚNG DẪN CÀI ĐẶT RASPBERRY PI KHÔNG CẦN MÀN HÌNH, BÀN PHÍM (Mới nhất 11/2022)
- GIAO TIẾP CẢM BIẾN NHẬN DẠNG VÂN TAY AS608 (Phần 1)
- Chuỗi bài viết đề tài "Giải pháp bảo mật cho thiết bị Datalogger" (P5)
- Chuỗi bài viết đề tài "Giải pháp bảo mật cho thiết bị Datalogger" (P4)

XEM THÊM CÁC CHỦ ĐỀ KHÁC

- GIỚI THIỆU
- HỌC TẬP
  - Khóa Vi điều khiển STM32
  - Khóa Internet of Thing
  - Khóa Lập trình Arduino
  - Khóa Ngôn ngữ lập trình C
  - Đào tạo theo nhu cầu
  - Kho tài liệu
- NGHIÊN CỨU

- Modbus RTU là protocol công nghiệp phổ biến nhất.
- Hoạt động dựa trên mô hình chủ – tớ Master – Slave. Master sẽ quyết định các yêu cầu đọc ghi cho Slave.

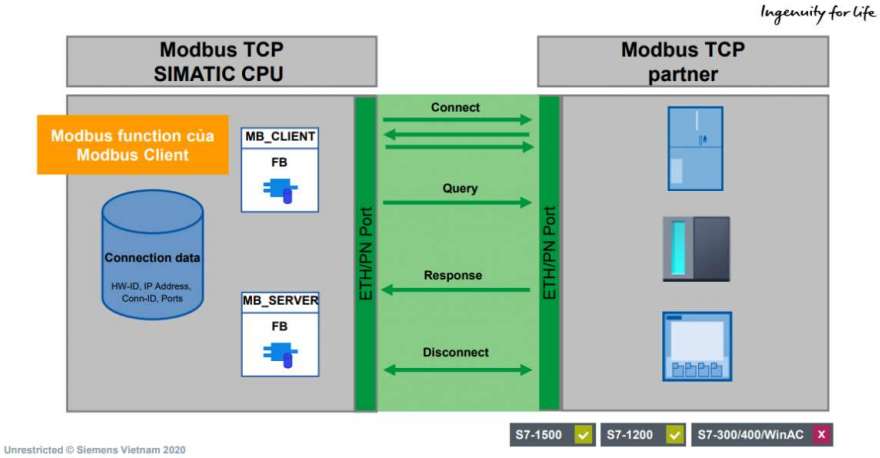
Parameter	RS-232	RS-485
Line configuration	Single-ended	Differential
Mode of operation	Simplex or full duplex	Simplex or half duplex
Maximum cable length	50 feet	4000 feet
Maximum data rate*	20 kbits/s	10 Mbits/s
Typical logic levels	±5 to ±15 V	±1.5 to ±6 V
Minimum receiver input impedance	3 to 7 kΩ	12 kΩ
Receiver sensitivity	±3 V	±200 mV

1.2. Modbus TCP.

- Giao thức Modbus phát triển dựa trên nền tảng của Industrial Ethernet.
- Các kết nối thay thế master – Slave bằng Client – Server. Khi áp dụng mô hình Client – Server thì Client sẽ gửi lệnh đọc hoặc ghi tới Server.
- Dữ liệu Modbus được tóm lược đơn giản trong một gói tin TCP/IP.
- Khả năng tương thích với nhiều hệ điều hành và phần cứng.
- Khả năng mở rộng cao, TCP/IP như là một mô hình có để định tuyến, thông qua địa chỉ IP để xác định đường dẫn hiệu quả.

2. Giao thức Modbus TCP/IP.

2.1. Mô hình kết nối.



Mô hình kết nối giữa PLC và thiết bị đầu cuối bằng chuẩn Modbus TCP/IP và giao tiếp với nhau bằng mô hình Server và Client.

2.2. Các function và thanh ghi.

2.2.1. Thanh ghi.

Địa chỉ	Kích thước	Mô tả
0xxxx	1bit	Đọc viết ngõ đầu ra số.

- CHIA SẺ
  - Hệ thống nhúng (Các chia sẻ về hệ thống nhúng: vi điều khiển, máy tính nhúng, các ứng dụng.)
    - Vi điều khiển (Tài liệu hướng dẫn, các ví dụ, đề tài ứng dụng của các dòng vi điều khiển ARM, MSP, PIC, Arduino.)
      - Arduino Board (Tài liệu hướng dẫn, thực hành với các board Arduino)
      - Vi điều khiển MSP430 (Tài liệu tham khảo, hướng dẫn, ví dụ, đề tài sử dụng vi điều khiển MSP430)
      - Vi điều khiển lõi ARM (Các vi điều khiển lõi ARM như STM32, TivaC)
    - Máy tính nhúng (Các máy tính nhúng Raspberry, BeagleBone Black)
  - Internet of Things (Các tài liệu, hướng dẫn về thiết bị cảm biến, giao thức truyền nhận, server, ứng dụng của Internet of Things.)
    - WiFi ESP8266 và ESP32
    - 3G/4G/5G
    - IoT Cloud Platform
    - Bluetooth (Chia sẻ các kiến thức, hướng dẫn về Bluetooth Low Energy và Bluetooth Mesh. Kết nối cộng đồng nghiên cứu Bluetooth tại Việt Nam.)
    - LPWAN
  - Trí tuệ nhân tạo
  - Thiết kế phần cứng (Thiết kế phần cứng bao gồm thiết kế mạch in PCB, thiết kế vỏ hộp, CNC, in 3D)
    - Thiết kế PCB (Thiết kế mạch trên Altium, đặt mạch công nghiệp)
    - Thiết kế 3D (Thiết kế mẫu thử, chi tiết, vỏ hộp sản phẩm,)
  - Ngôn ngữ lập trình C/C++
  - Kỹ năng thiết yếu
- SỰ KIỆN

1xxxx	1bit	Đọc ngõ vào số
3xxxx	16bit	Đọc thanh ghi đầu vào
4xxxx	16bit	Đọc và viết thanh ghi.

2.2.2. Mã hàm được sử dụng trong PLC (Funtion Code).

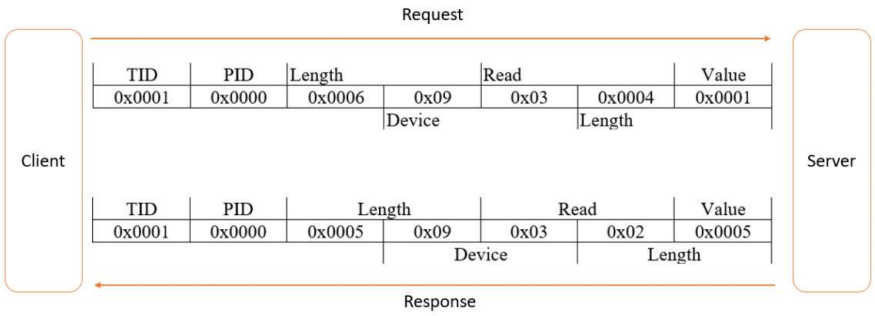
MODE	MB_DATA_ADDR	MB_DATA_LEN	Modbus function	Function and data type
0	1 to 9,999	1 to 2,000	01	Read 1 to 2,000 output bits on the remote address 0 to 9,998
0	10,001 to 19,999	1 to 2,000	02	Read 1 to 2,000 input bits on the remote address 0 to 9,998
0	· 40,001 to 49,999 · 400,001 to 465,535	1 to 125	03	· Read 1 to 125 holding registers on the remote address 0 to 9,998 · Read 1 to 125 holding registers on the remote address 0 to 65,534
0	30,001 to 39,999	1 to 125	04	Read 1 to 125 input words on the remote address 0 to 9,998
1	1 to 9,999	1	05	Write 1 output bit on the remote address 0 to 9,998
1	· 40,001 to 49,999 · 400,001 to 465,535	1	06	· Write 1 holding register on the remote address 0 to 9,998 · Write 1 holding register on the remote address 0 to 65,534
1	1 to 9,999	2 to 1,968	15	Write 2 to 1,968 output bits on the remote address 0 to 9,998
1	· 40,001 to 49,999 · 400,001 to 465,535	2 to 123	16	· Write 2 to 123 holding registers on the remote address 0 to 9,998 · Write 2 to 123 holding registers on the remote address 0 to 65,534
2	1 to 9,999	1 to 1,968	15	Write 1 to 1,968 output bits on the

				remote address 0 to 9,998
2	· 40,001 to 49,999 · 400,001 to 465,535	1 to 123	16	· Write 1 to 123 holding registers on the remote address 0 to 9,998 · Write 1 to 123 holding registers on the remote address 0 to 65,534
11	The MB_DATA_ADDR and MB_DATA_LEN parameters are not evaluated when this function is executed.		11	Read status word and event counter of the server: · The status word reflects the the processing status (0 – not processing, 0xFFFF – processing). · The event counter is incremented when the Modbus request was executed successfully. If an error occurred during execution of a Modbus function, a message is sent by the server, but the event counter is not incremented.
80	–	1	08	Check the server status with the diagnostic code 0x0000 (return loop test – the server sends the request back): · 1 WORD per call
81	–	1	08	Reset the event counter of the server with the diagnostic code 0x000A: · 1 WORD per call
101	0 to 65,535	1 to 2,000	01	Read 1 to 2,000 output bits on the remote address 0 to 65,535
102	0 to 65,535	1 to 2,000	02	Read 1 to 2,000 input bits on the remote address 0 to 65,535

103	0 to 65,535	1 to 125	03	Read 1 to 125 holding registers on the remote address 0 to 65,535
104	0 to 65,535	1 to 125	04	Read 1 to 125 input words on the remote address 0 to 65,535
105	0 to 65,535	1	05	Write 1 output bit on the remote address 0 to 65,535
106	0 to 65,535	1	06	Write 1 holding register on the remote address 0 to 65,535
115	0 to 65,535	1 to 1,968	15	Write 1 to 1,968 output bits on the remote address 0 to 65,535
116	0 to 65,535	1 to 123	16	Write 1 to 123 holding registers on the remote address 0 to 65,535

2.3. Frame truyền của chuẩn truyền thông.

- Cấu trúc định dạng kiểu truyền dữ liệu Modbus TCP/IP.



Ví dụ 1: Ghi giá trị từ Client lên Server dữ liệu cho phép gửi 6 thanh ghi (MB_DATA_LEN), thanh ghi bắt đầu 40001, tổng dữ liệu request (MB_DATA_PTR) là 12 thanh ghi.

Frame Client gửi lên Server:

36 28 00 00 00 13 63 10 9C 41 00 06 0C 00 01 00 02 00 03 00 00 00 00 00 00

Trong đó:

- **36 27**: mã định danh giao thức Transaction ID.
- **00 00**: mã xác định giao thức Protocol ID.
- **00 06**: độ dài tin nhắn.
- **63** : địa chỉ ID thiết bị (ID là 99).
- **10** : Funtion 16 mode 116.
- **9C 41**: Địa chỉ thanh ghi bắt đầu (40001) ở mục MB_DATA_ADDR.
- **00 06**: Số lượng thanh ghi được phép ghi (MB_DATA_LEN).

- **0C** : Độ dài dữ liệu gửi (6 thanh ghi, mỗi thanh ghi 2 byte, tổng độ dài gửi là 12 byte).
- **00 01 00 02 00 03 00 00 00 00 00 00**: dữ liệu.

Frame phản hồi từ Server:

36 27 00 00 00 06 63 10 9C 41 00 06

Trong đó:

- **36 27**: mã định danh giao thức Transaction ID.
- **00 00**: mã xác định giao thức Protocol ID.
- **00 06**: độ dài tin nhắn.
- **63** : địa chỉ ID thiết bị (ID là 99).
- **10** : Funtion 16 mode 116.
- **9C 41**: Địa chỉ thanh ghi bắt đầu (40001) ở mục MB_DATA_ADDR.
- **00 06**: Số lượng thanh ghi được phép ghi (MB_DATA_LEN).

Ví dụ 2: Client đọc giá trị từ Server với 5 thanh ghi, thanh ghi bắt đầu là 40000.

Frame Client gửi lên Server:

01 A5 00 00 00 0D 63 03 9C 40 00 05

Trong đó:

- **01 A5**: mã định danh giao thức Transaction ID.
- **00 00**: mã xác định giao thức Protocol ID.
- **00 0D**: độ dài tin nhắn.
- **63** : địa chỉ ID thiết bị (ID là 99).
- **03** : Funtion 3 mode 103.
- **9C 40**: Địa chỉ thanh ghi bắt đầu (40000) ở mục MB_DATA_ADDR.
- **00 05**: Số lượng thanh ghi được phép ghi (MB_DATA_LEN).

Frame Server phản hồi:

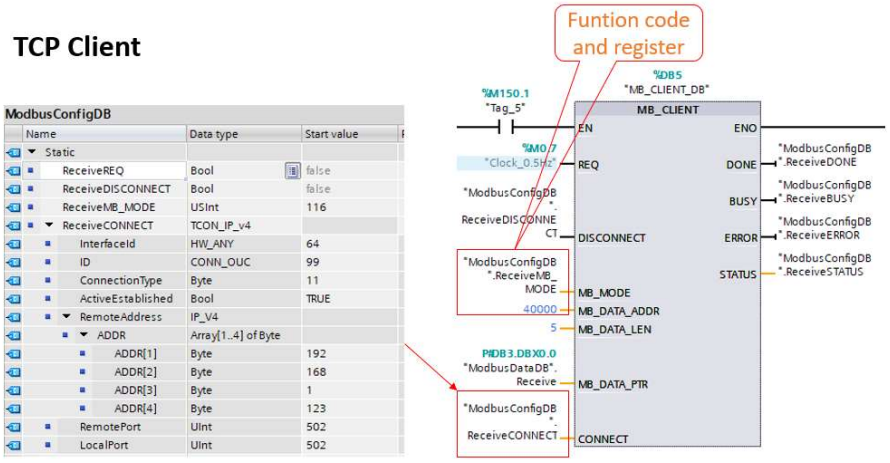
01 A6 00 00 00 06 63 03 0A 00 0C 00 7B 00 02 00 02 00 22

Trong đó:

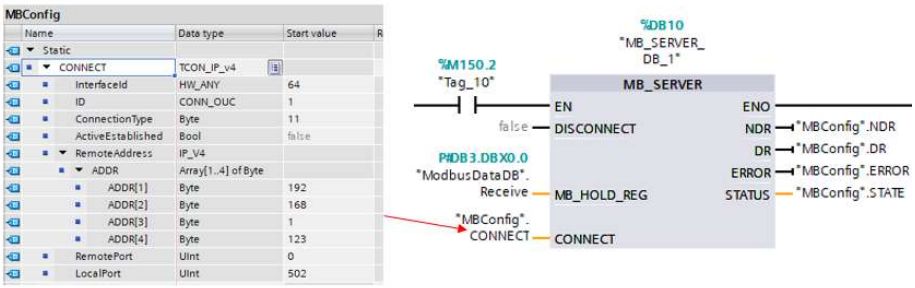
- **01 A6**: mã định danh giao thức Transaction ID.
- **00 00**: mã xác định giao thức Protocol ID.
- **00 0D**: độ dài tin nhắn.
- **63** : địa chỉ ID thiết bị (ID là 99).
- **03** : Funtion 3 mode 103.
- **0A** : Độ dài dữ liệu (5 thanh ghi, mỗi thanh ghi 2 byte, tổng là 10 byte).
- **00 0C 00 7B 00 02 00 02 00 22**: dữ liệu Server phản hồi.
- Các lệnh được sử dụng truyền thông trong PLC.

2.4 Cấu hình PLC S7-1200 trong TIA Portal

TCP Client



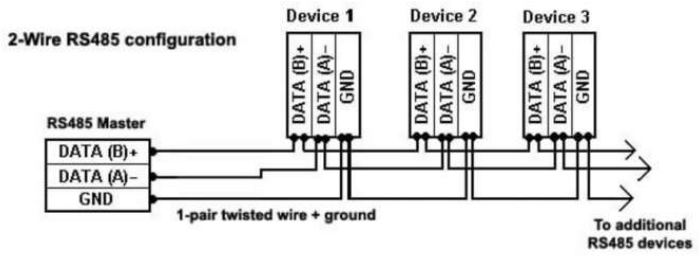
TCP Server



3. Kết luận

Ở trên là bài chia sẻ về chi tiết của giao thức modbus TCP/IP của PLC S7-1200, hi vọng bài viết sẽ mang lại kiến thức cho những ai chưa rõ về giao thức này, hoặc có thể tự thực hành để nắm rõ hơn về nó. Biết đâu sau này bạn có dịp tiếp cận nó thì sẽ dễ dàng hơn sao. Trong bài viết nếu có gì sai sót, hãy báo mình biết để điều chỉnh kịp thời nhé. Chúc bạn may mắn và thành công,

Bài viết về **modbus RTU** đã từng post trước:



TRUYỀN THÔNG GIAO TIẾP GIỮA PLC VÀ ARDUINO QUA RS485 MODBUS

Bài viết này sẽ hướng dẫn cách giao tiếp giữa PLC S7-1200 và Arduino qua truyền thông Rs485. Qua bài viết này các bạn có thể sử dụng vi điều khiển bất kỳ để lập trình truyền thông Rs485 với PLC hoặc module giao tiếp rs485 bất kỳ, khi bạn nắm được nguyên lý giao tiếp.Continue Reading

TAPIT

TÀI LIỆU THAM KHẢO

https://www.youtube.com/watch?v=6qLv_J2Dk1s

https://www.youtube.com/watch?v=Y0Xx_iGn4hQ

Modbus TCP Client Trên PLC S7 1200 / 1500 | Industrial Communication

Tấn Lĩnh – Thành Trung
ATOMA Technology

Previous Post: Thiết kế phần cứng thực nghiệm nhà thông minh sử dụng điện toán đám mây IoT
Next Post: Sử dụng Watchdog Timer trong Arduino