KẾT NỐI MẠNG PLC BẰNG GIAO THỨC MODBUS TCP/IP VỚI S71200 SERVER VÀ CÁC S71200 CLIENT

Nguyễn Thành Đoàn[(1)], Nguyễn Phương Trà[(1)]

(1) Trường Đại học Thủ Dầu Một

Ngày nhận bài 17/03/2020; Ngày gửi phản biện 20/03/2010; Chấp nhận đăng 25/05/2020

Liên hệ email: doannt@tdmu.edu.vn

https://doi.org/10.37550/tdmu.VJS/2020.04.056

Tóm tắt

Với sự phát triển mạnh mẽ của việc điều khiển, truyền thông các thiết bị tự động qua mạng thì nhu cầu kết nối các thiết bị với nhau qua giao thức Moddbus TCP/IP rất cần thiết trong xí nghiệp, nhà máy trong các khu chế xuất và công nghiệp trên địa bàn tỉnh Bình Dương. Bài báo này trình bày phương pháp kết nối mạng giữa các PLC với nhau. S71200 làm Server và các S71200 làm các Client. Các PLC này trao đổi dữ liệu với nhau thông qua mạng truyền thông Modbus TCP/IP. Việc kết nối mạng giữa các PLC S71200 được thực hiện bằng cách sử dụng giao thức truyền Modbus TCP/IP . Cách thức truyền khai báo theo cấu trúc Modbus protocol gồm có địa chỉ, giao thực tuyền, số lượng các khối dữ liệu truyền và nhận thông qua cáp mạng RJ45. Thực hiện truyền khối dữ liệu đọc và ghi giữa 2 PLC S71200 với chương trình phần mềm Tia Portal V14, kết nối máy tính để giám sát thông số truyền. Số lượng đọc từ PLC S71200 Server là 10 byte (5 word đọc) và ghi từ PLC S71200 Client là 10 byte (5 word ghi). Nghiên cứu này cung cấp giải pháp tối ưu trong truyền thông mạng công nghiệp trong thực tế và áp dụng cho đào tạo với hiệu quả cao. Tốc độ truyền nhanh và chi phí thấp theo chuẩn Modbus TCP/IP. Có thể được ứng dụng truyền dữ liệu mạng nội bộ các thiết bị điều khiển trong các xí nghiệp, công nghiệp.

***Từ khóa**: mạng PLC, điều khiển, kết nối, thiết bị*

Abstracts

CONNECTING A PLC NETWORK WITH MODBUS TCP/IP PROTOCOL WITH S71200 SERVER AND S71200 CLIENT

With the strong development of automatic control and communication of equipment over the network, the need to connect devices together via Modbus TCP/IP protocol is essential in enterprises and factories in export processing and industrial zones in Binh Duong province. This paper presents the method of network connection between PLCs together. S71200 is the server and the S71200 is the client. These PLCs exchange data with each other via Modbus TCP/IP communication network. The network connection between the S71200 PLCs is made to use the Modbus TCP/IP communication protocol. The methods of transmission according to the Modbus protocol structure include the address, the interface, the number of blocks of data transmitted and received via the RJ45

network cable. Transmission of reading and writing data blocks between 2 S7 S7 1200s with Tia Portal V14 software program, connecting computers to monitor transmission parameters. The number of reading from PLC S71200 Server is 10 bytes (5 word read) and writing from PLC S71200 Client is 10 bytes (5 word write). This study provides an optimal solution in real network industrial communications and applies to training with high efficiency. Fast transmission speed and low cost according to Modbus TCP/IP standard. Can be applied intranet data transmission device control in enterprises, industry.

1. Đặt vấn đề

Trong một nhà máy rộng lớn có nhiều phân xưởng sản xuất. Nhu cầu muốn thu thập dữ liệu sản xuất hàng ngày là cần thiết, như số sản phẩm đã sản xuất, số sản phẩm lỗi từng xưởng, và xưởng nào đã đạt mục tiêu, xưởng nào cần tăng ca sản xuất cho đủ chỉ tiêu theo hợp đồng… Muốn làm được điều này một cách tự động hóa thì các thiết bị điều khiển phải kết nối mạng với nhau.

Hiện nay việc điều khiển tự động hóa thường sử dụng các thiết bị điều khiển PLC. Đối với các hệ thống lớn thường sử dụng nhiều PLC, mỗi PLC thường thực hiện một nhiệm vụ riêng trong nhiều nhiệm vụ được yêu cầu từ sản xuất. Để hệ thống phối hợp làm việc một cách chặt chẽ thì chúng ta phải kết nối các thiết bị này lại và tiến hành trao đổi dữ liệu với nhau. Việc nối mạng giữa các PLC có nhiều giao thức khác nhau như CCLinks, Profibus, Profinet, Ethernet, DeviceNet, ControlNet.

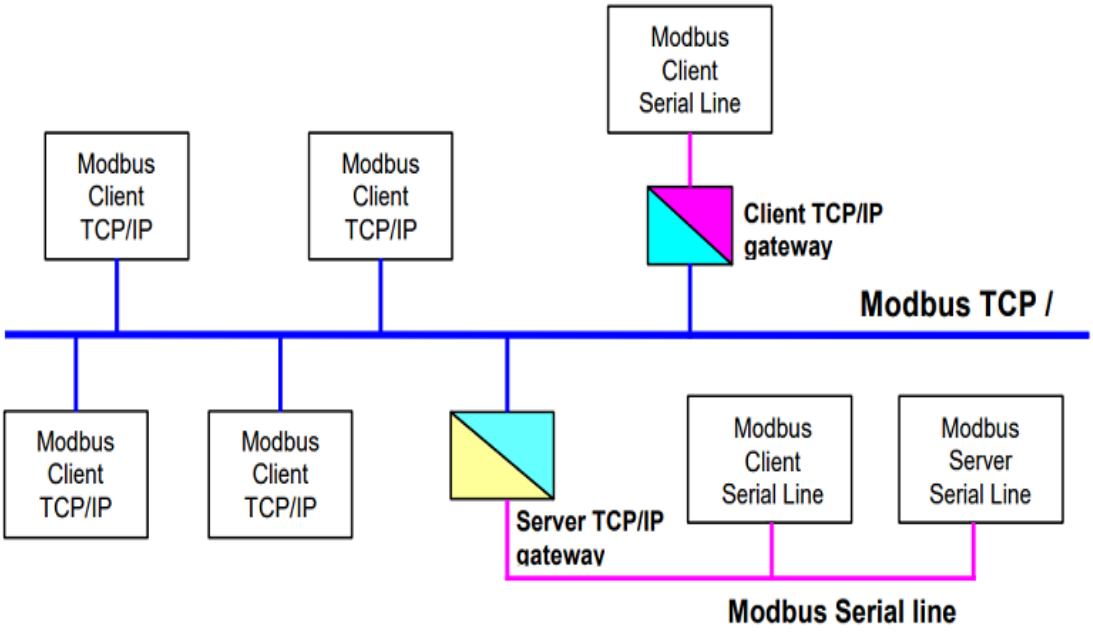
Đã có rất nhiều nghiên cứu về việc truyền thông kết nối mạng PLC, nhưng mỗi nghiên cứu đều tồn tại những điểm cần khắc phục như Morris, Vaughn và Dandass, (2012) hay Sideng, Zhengming, Yingchao và Shuping (2008) đã nghiên cứu chuẩn Modbus RTU có nhược điểm là chi phí cho thiết bị đầu cuối cao và thị trường hiện nay ít thiết bị tích hợp module Modbus RTU và tốc độ truyền chậm hơn chuẩn Modbus TCP. Jee, Edison, Rao và Cern (2003) đã sử dụng chuẩn giao tiếp Profibus để truyền thông giữa các PLC. Nhưng hiện nay chuẩn này ít sử dụng rộng rãi và cũng ít thiết bị hỗ trợ chuẩn truyền thông theo giao thức này. Jee, Edison, Rao, Cern (2003) sử dụng chuẩn giao tiếp CClink. Đây là chuẩn giao tiếp chưa phổ biến rộng và chỉ hạn chế một số nhà sản xuất thiết bị theo chuẩn riêng của mình. Mỗi giao thức có kiểu truyền và nhận dữ liệu khác nhau với chi phí cũng chênh lệch khá nhiều. Một giao thức truyền thông đảm bảo tốc độ khá cao và chi phí thấp, dễ sử dụng đó là Modbus TCP/IP. Về cơ bản giống như Modbus RTU, nhưng khác nhau ở chỗ giao chuẩn giao tiếp đó là Modbus TCP/IP sử dụng cáp mạng RJ45 thay vì RS485.

2. Tổng quan về Modbus

Lịch sử phát triển: Modbus là một giao thức truyền thông nối tiếp ban đầu được Modicon (nay là Schneider Electric) xuất hiện năm 1979. Dùng để sử dụng với các bộ điều khiển logic lập trình (PLC). Modbus đã trở thành một giao thức truyền thông tiêu

chuẩn thực tế và hiện là phương tiện phổ biến để kết nối các thiết bị điện tử công nghiệp. Modbus phổ biến trong môi trường công nghiệp vì nó được phổ biến công khai và miễn phí bản quyền . Nó được phát triển cho các ứng dụng công nghiệp, tương đối dễ triển khai và bảo trì so với các tiêu chuẩn khác. Đơn giản trong việc thiết lập kích thước định dạng của dữ liệu được truyền. Modbus sử dụng 2 chuẩn giao tiếp RS485 và RJ45. Modbus cho phép giao tiếp giữa nhiều thiết bị được kết nối với cùng một mạng. Ví dụ, một hệ thống đo nhiệt độ và độ ẩm được truyền kết quả đến máy tính . Modbus thường được sử dụng để kết nối máy tính giám sát với thiết bị đầu cuối từ xa (RTU) trong các hệ thống điều khiển giám sát và thu thập dữ liệu (SCADA). Có thể lập trình bằng nhiều ngôn ngữ khác nhau như Ladder, SCL, FBD hay GRAPH. Sử dụng chương trình này điều khiển rơle (đầu ra vật lý một bit được gọi là cuộn dây) và đầu vào vật lý một bit được gọi là đầu vào riêng biệt hoặc tiếp điểm. Việc phát triển và cập nhật các giao thức Modbus đã được Tổ chức Modbus quản lý kể từ tháng 4 năm 2004. Từ khi Schneider Electric chuyển giao quyền cho tổ chức Modbus. Tổ chức này là tạo ra một hiệp hội của người dùng và nhà cung cấp các thiết bị tuân thủ chuẩn Modbus hỗ trợ người dùng và nhà sản xuất sử dụng công nghệ truyền theo chuẩn này.

Cách thức truyền: Một hệ thống giao tiếp qua MODBUS TCP/IP có thể bao gồm các loại thiết bị khác nhau như: (1) Thiết bị máy khách và máy chủ MODBUS TCP/IP được kết nối với mạng TCP/IP; (2) Các thiết bị kết nối như cầu nối, bộ định tuyến hoặc cổng để kết nối giữa mạng TCP/IP; (3) mạng con nối tiếp cho phép kết nối các thiết bị đầu cuối, máy khách và máy chủ nối tiếp qua giao thức MODBUS qua cáp RS 485 hay RJ45.



Hình 1. *Cấu trúc chung của mạng Modbus TCP/IP*

Truyền Bit và các thanh ghi 16 bit có địa chỉ như bảng 1.

Bảng 1. *Địa chỉ thanh ghi/đọc khi truyền theo chuẩn Modbus TCP/IP*

Loại đối tượng	Truy cập	Kích thước	Không gian địa chỉ
Ngõ ra số	Đọc viết	1 bit	00001 - 09999
Ngõ vào số	Chỉ đọc	1 bit	10001 - 19999
Thanh ghi đầu vào	Chỉ đọc	16 bit	30001 - 39999
Thanh ghi đọc/ghi	Đọc viết	16 bit	40001 - 49999

Modbus TCP/IP là biến thể của RTU sử dụng địa chỉ IP. Khung truyền như bảng 2.

Bảng 2. *Cấu trúc định dạng kiểu truyền dữ liệu Modbus TCP/IP*

Tên	Độ dài (byte)	Chức năng
Mã định danh giao thức	2	Để đồng bộ giữa dữ liệu của máy chủ và máy khách
Xác định giao thức	2	Số 11 cho Modbus/TCP
Trường chiều dài	2	Số byte còn lại trong khung truyền
Địa chỉ Client	1	Địa chỉ Client (0 đến 255)
Mã chức năng	1	Mã chức năng dùng để phân biệt nhiều đường truyền khác nhau
Byte dữ liệu	*n*	Dữ liệu dưới dạng phản hồi hoặc lệnh

- Mã định danh giao thức: Nó được sử dụng để ghép nối các thiết bị máy chủ MODBUS và máy tớ trong việc lấy dữ liệu và phản hồi trên đường truyền theo yêu cầu.
- Xác định giao thức : Nó được sử dụng để ghép kênh trong hệ thống. Giao thức MODBUS được xác định bởi giá trị 11.
- Trường chiều dài: Trường độ dài là số byte của các khối dữ liệu cần truyền, bao gồm Mã nhận dạng đơn vị và trường dữ liệu.
- Địa chỉ Client: Sử dụng để khai báo các máy tớ (Client) trên đường truyền có nhiều thiết bị
- Mã chức năng hay định danh đơn vị: Trường này được sử dụng cho mục đích định tuyến trong hệ thống. Nó thường được sử dụng để liên lạc với MODBUS Server và Client nối tiếp trong mạng MODBUS thông qua các cổng mạng Ethernet TCP-IP hoặc đường nối tiếp MODBUS RTU. Trường này được thiết lập bởi máy khách MODBUS trong yêu cầu đọc và ghi các giá trị trong với sự phản hồi của máy chủ.

Dưới đây là ví dụ về yêu cầu đọc và ghi dữ liệu theo chuẩn Modbus TCP cho nội dung các thanh ghi giữ liệu đầu ra tương tự từ # 40108 đến # 40110 từ thiết bị Client có địa chỉ 17.

00 01 00 00 00 15 15 00 00 6B 00 03

0001 : Mã định danh giao thức

0000 : Xác định giao thức

0006 : Độ dài tin nhắn (6 byte để theo dõi)

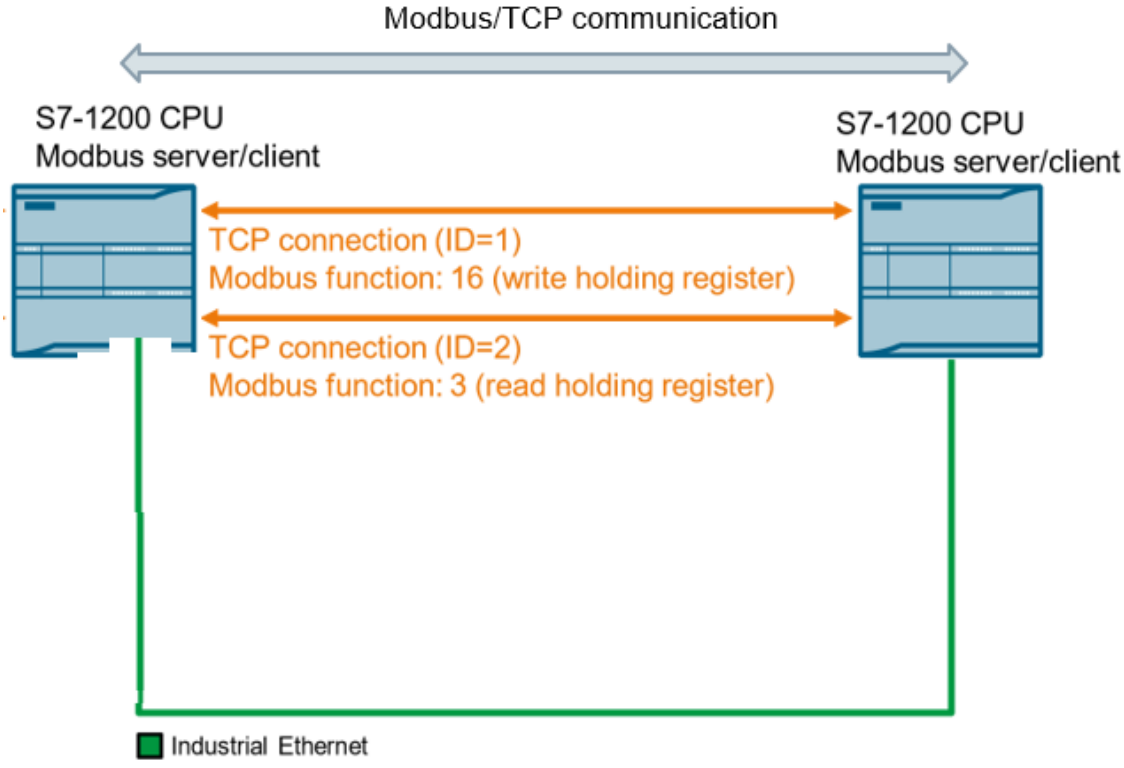
15 : Mã định danh đơn vị (17 = 0x15)

03 : Mã chức năng (đọc các thanh ghi giữ đầu ra tương tự)

006B : Địa chỉ dữ liệu của thanh ghi đầu tiên được yêu cầu (40108 - 40001 offset = 107 = 0x6B)

3. Kết nối phần cứng giữa các PLC S71200 Server và Salve

3.1. Giới thiệu cấu trúc hệ thống



***Hình 2**. Tổng quan phần cứng kết nối PLC S7 1200*

Hệ thống sẽ truyền dữ liệu qua cáp RJ45 theo chuẩn MODBUS TCP/IP với chức năng ghi và đọc qua lại các thông số giữa PLC thông qua thiết bị kết nối mạng CSM 1277.

***Bảng 3**. Cài đặt địa chỉ truyền Master, Slave*

Parameter	S7-1200 (Client)	S7-1200 (Server)
Instruction	MB_CLIENT	MB_SERVER
Modbus function	16 (Write holding register)	
Connection number (ID)	1	
Connection type	0x0B (hex) = 11 (dec): TCP connection	
Connection setup	Active	Passive
Own IP address	192.168.0.3	192.168.0.2
IP address of the remote partner (remote IP address)	192.168.0.2	192.168.0.3
Local port	0: any port	502
Remote port	502	0: The "MB_SERVER" instruction is to accept connection requests from any remote connection partner.

Để truyền thông 2 PLC ta cài đặt các thông số như sau:

PLC S71200 Server ta dùng khối MB_SERVER với khai báo đọc thanh ghi (Mã 16), Loại kết nối là 11 (TCP/IP), đường truyền ID là 1. Kết nối Passive, địa chỉ là 192.168.0.2, kết nối với Client có IP là 192.168.0.3, Local port là 502, Remote port là 0.

PLC S71200 Client ta dùng khối MB_CLIENT với khai báo đọc thanh ghi (Mã 16), Loại kết nối là 11 (TCP/IP), đường truyền ID là 1, Kết nối active, địa chỉ là 192.168.0.3, kết nối với Server có IP là 192.168.0.2, Local port là 0, Remote port là 502.

3.2. Kết nối phần cứng

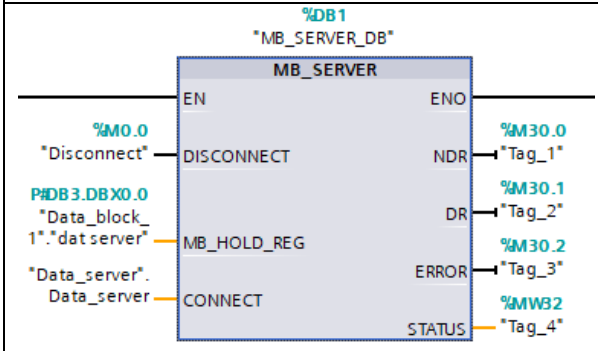
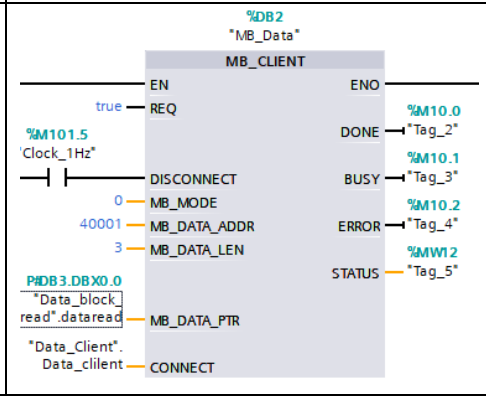
***Hình 3**. Kết nối phần cứng truyền thông PLC thực tế*

Hệ thống gồm Máy tính có cài đặt chương trình Tia Portal V14, 2 PLC S2 1200 CPU 1214 C DC/DC/DC và PLC S71200 1212C DC/DC/DC. Được kết nối mạng Modbus TCP/IP qua bộ chia mạng CSM 1277 của Siemens.

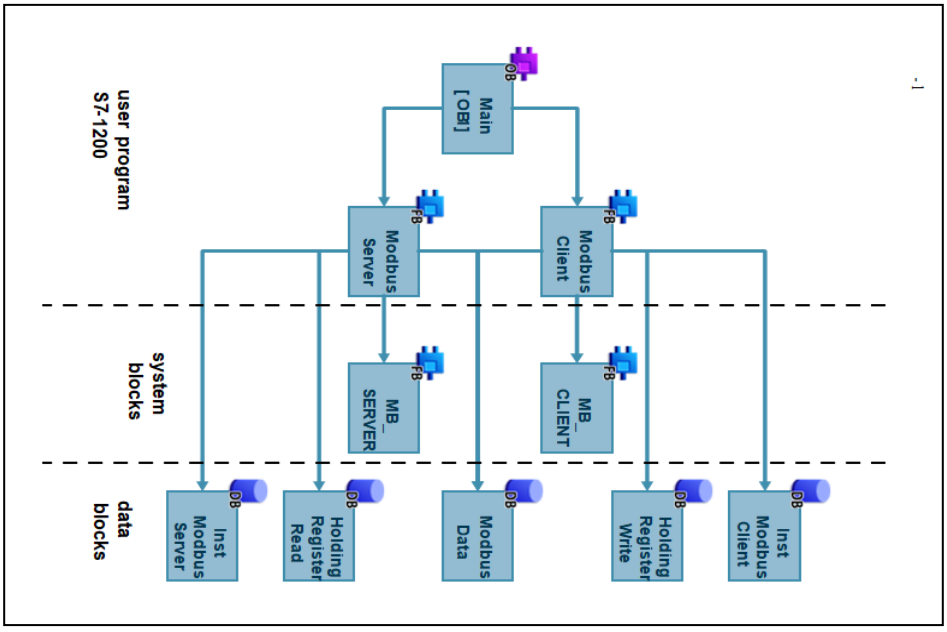
3.3. Chương trình phần mềm

Trong chương trình phần mềm lập trình Tia portal V14 của 2 CPU S7-1200, ta sử dụng các lệnh "MB_CLIENT" và "MB_SERVER". Sử dụng một kết nối Modbus/TCP với một ID duy nhất . Các lệnh "MB_CLIENT" và "MB_SERVER" được gọi mỗi lần với xung nhịp khác nhau để truyền và gửi dữ liệu. Các xung nhịp này phải lệch pha nhau để tránh xung đột trên đường truyền.

Bảng 4. *Kết nối dữ liệu hai khối MB_Server và MB_Client*

S7 1200 Server	S7 1200 Client
	

Lưu đồ truyền nhận dữ liệu:



Hình 4. *Sơ đồ truyền theo chuẩn Modbus TCP/IP*

https://doi.org/10.37550/tdmu.VJS/2020.04.056

Dạng dữ liệu của Server và client

Client	Server

Data_Client

Name	Data type	Start value
Static		
Data_clilent	TCON_IP_v4	
InterfaceId	HW_ANY	64
ID	CONN_OUC	5
ConnectionType	Byte	16#0B
ActiveEstablished	Bool	true
RemoteAddress	IP_V4	
ADDR	Array[1..4] of Byte	
ADDR[1]	Byte	192
ADDR[2]	Byte	168
ADDR[3]	Byte	0
ADDR[4]	Byte	3
RemotePort	UInt	502
LocalPort	UInt	0

Data_server

Name	Data type	Start value
Static		
Data_server	TCON_IP_v4	
InterfaceId	HW_ANY	64
ID	CONN_OUC	5
ConnectionType	Byte	16#0B
ActiveEstablished	Bool	false
RemoteAddress	IP_V4	
ADDR	Array[1..4] of Byte	
ADDR[1]	Byte	192
ADDR[2]	Byte	168
ADDR[3]	Byte	0
ADDR[4]	Byte	2
RemotePort	UInt	0
LocalPort	UInt	502

***Hình 5**. Thông số cài đặt các khối dữ liệu các PLC S7 1200.*

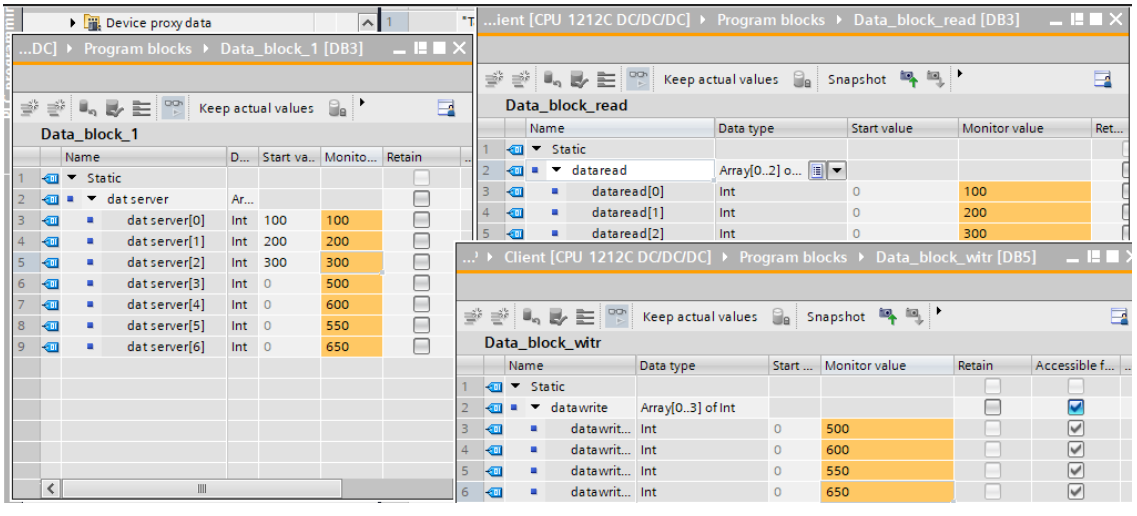
Sau khi biên dịch (Compile) thì tiến hành download từng CPU. Để tránh bị lỗi chúng ta phải định dạng đúng dạng dữ liệu (Data Type) của từng vùng nhớ bit, byte, word, Dword…. Để kết nối, chúng ta tạo các khối dữ liệu (DB) và định dạng thành mảng (Array) gồm nhiều word. Trong đó chúng ta chi thành các word chỉ đọc và các word chỉ ghi. Khi đọc và ghi thanh ghi word, chúng ta chỉ cần trỏ vào thanh ghi đầu tiên (Data pointer). Ví dụ đọc và ghi các thanh ghi 16 bit bắt đầu từ 40001 thì ta chia ra như sau:

10 word đầu để đọc ta trỏ và thanh ghi word có địa chỉ từ 40001 đến 40010.

10 word còn lại để ghi ta trỏ vào thanh ghi word bắt đầu từ 4011 đến 4020.

4. Thử nghiệm và kết quả

Sau khi tải chương trình ta tiến hành chạy và cho truyền dữ liệu ta có kết quả như sau:



***Hình 6**. Kết quả khi truyền dữ liệu giữa các PLC S7 1200*

PLC Client đọc về 3 word đầu tiên dataread (0), dataread (1), dataread (2) của PLC Server datserver (0), datserver (1), datserver (2) có giá trị lần lượt là 100, 200, 300 và sau đó ghi về 4 word datawrite (0), datawrite (1), datawrite (2), datawrite (3) có giá trị lần lượt là 500, 600, 550, 650 và 4 word dataserver (3), dataserver (4), dataserver (5), dataserver (6),

5. Kết luận

Sau khi nghiên cứu phần cứng và phần mềm nhóm tác giả đã tiến hành lắp đặt kết nối và lập trình để truyền thông giữa các PLC với nhau qua mạng truyền thông Modbus TCP/IP. Kết quả là các PLC đã giao tiếp được với nhau, cụ thể là đã đọc và ghi dữ liệu qua lại giữa PLC Server S71200 CPU 1214C DC/DC/DC và PLC Client S7 1200C DC/DC/DC. So với các nghiên cứu trước đó thì bài báo này đã đưa ra phương pháp kết nối dữ liệu giữa các PLC với nhau theo chuẩn phổ biến nhất và chi phí thấp nhất. Chuẩn này được hỗ trợ bởi hầu hết các nhà sản xuất thiết bị, thuận lợi trong việc kết nối, cài đặt và lập trình, đường truyền ổn định và có thể truyền với khoản cách xa. Đây là ứng dụng rất cần thiết trong công nghiệp tự động hóa quá trình và đào tạo mạng truyền thông công nghiệp.

TÀI LIỆU THAM KHẢO

[1] Trần Văn Hiếu (2019). *Thiết kế hệ thống mạng truyền thông công nghiệp với Tia Portal*. NXB Khoa học Kỹ thuật.

[2] Trần Văn Hiếu (2019). *Lập trình S71200 với Tia Portal*. NXB Khoa học Kỹ thuật.

[3] D. T. Robinson (2017). *Modbus Monitoring for Networked Control Systems of Cyber-Defensive Architecture*. Howard University.

[4] W. You and H. Ge (2019). Design and Implementation of Modbus Protocol for Intelligent Building Security. IEEE 19th International Conference on Communication Technology (ICCT), 2019, pp. 420-423: IEEE.

[5] G. Pavlou, K. McCarthy, S. Bhatti, and G. Knight (1995). "The OSIMIS Platform: Making OSI Management Simple". Integrated Network Management IV: Proceedings of the fourth international symposium on integrated network management, 1995, A. S. Sethi, Y. Raynaud, and F. Faure-Vincent, Eds. Boston, MA: Springer US, 1995, pp. 480-493.

[6] Z. Luo, F. Zuo, Y. Jiang, J. Gao, X. Jiao, and J. Sun (2019). "Polar: Function Code Aware Fuzz Testing of ICS Protocol". ACM Transactions on Embedded Computing Systems (TECS), vol. 18, no. 5s, pp. 1-22.

[7] L. G. Z. Xinjian (2005). "How to Improve RS485 Communication Reliability in Measure and Control System". Chinese Journal of Scientific Instrument, p. S1.

[8] V. A. Kumar (1995). "Overcoming data corruption in RS485 communication". International Conference on Electromagnetic Interference and Compatibility (INCEMIC), 1995, pp. 9-12: IEEE.

[9] K. Chen, Z. Jin, and H. Chen (2016). "Effect of common-mode interference on communication performance of a motor drive system". IEEE Vehicle Power and Propulsion Conference (VPPC), 2016, pp. 1-6: IEEE.

[10] Jee, G., Edison, C., Rao, R. D., & Cern, Y. (2003). Demonstration of the technical viability of PLC systems on medium-and low-voltage lines in the United States. *IEEE Communications Magazine, 41*(5), 108-112.

[11] Morris, T., Vaughn, R., & Dandass, Y. (2012). *A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems.* Paper presented at the 2012 45th Hawaii International Conference on System Sciences.

[12] Sideng, H., Zhengming, Z., Yingchao, Z., & Shuping, W. (2008). *A novel Modbus RTU-based communication system for adjustable speed drives.* Paper presented at the 2008 IEEE Vehicle Power and Propulsion Conference.