

## TỰ ĐỘNG HÓA PLC S7 – 1200 VÀ TIA PORTAL

### 1.TỔNG QUAN VỀ PLC S7-1200

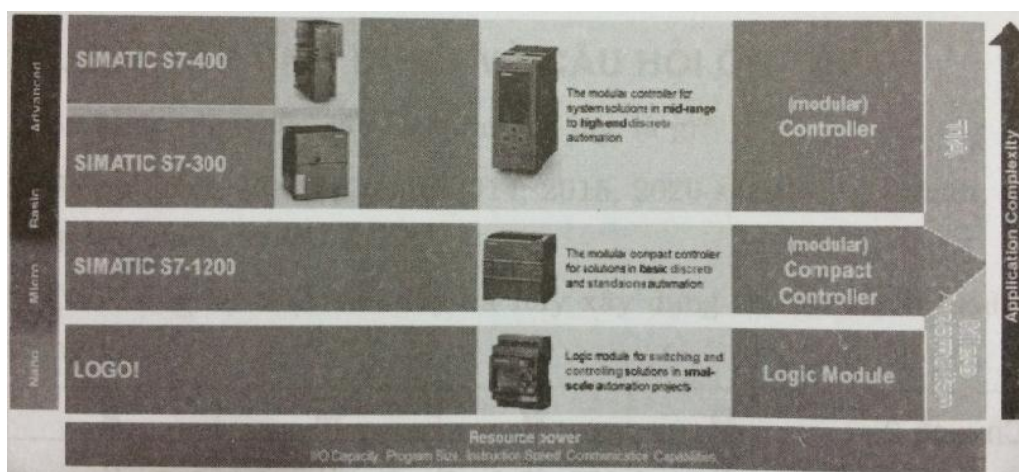
#### 1.1.Tổng quan về PLC S7-1200

##### 1.1.1.Sự lựa chọn cho hệ thống nhỏ và vừa

Bộ điều khiển PLC S7-1200, được sử dụng với sự linh động và khả năng mở rộng phù hợp đối với hệ thống tự động hóa nhỏ và vừa tương ứng với người dung cần.

Thiết kế nhỏ gọn, cấu hình linh động, hỗ trợ mạnh mẽ về tập lệnh đã làm cho PLC S7-1200 trở thành một giải pháp hoàn hảo trong việc điều khiển, chọn lựa phù hợp đối với nhiều ứng dụng khác nhau.

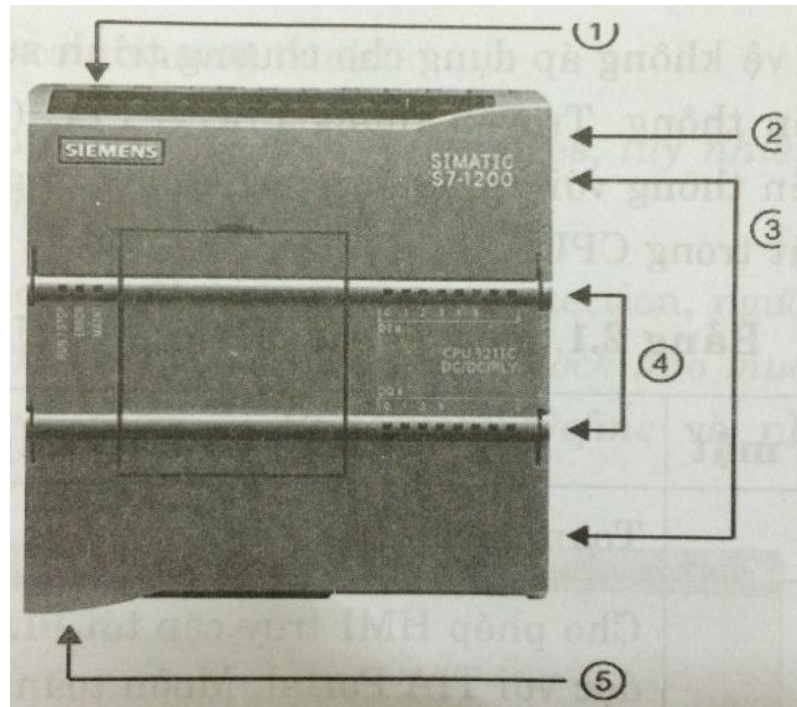
Để có thể làm rõ hơn vấn đề chúng ta muốn nói tới, tác giả sử dụng hình ảnh sau đây để minh họa chi tiết về vị trí, vai trò của PLC S7-1200 được siemens giới thiệu.



Hình 1.1.Vị trí của các PLC S7 sắp xếp theo ứng dụng

CPU của PLC S7-1200 được kết hợp với 1 vi xử lý, một bộ nguồn tích hợp, các tín hiệu đầu vào/ra, thiết kế theo nền tảng Profinet, các bộ đếm/phát xung tốc độ cao tích hợp trên than, điều khiển vị trí ( motion control ), và ngõ vào analog đã làm cho PLC S7-1200 trở thành bộ điều khiển nhỏ gọn nhưng mạnh mẽ. Sau khi download chương trình xuống CPU vẫn lưu giữ những logic cần thiết để theo dõi và kiểm soát các thiết bị thông tin trong ứng dụng của người lập trình. CPU giám sát ngõ vào và những thay đổi của ngõ ra theo logic trong chương trình người dung, có thể bao gồm các phép toán logic của đại số Boolean, những bộ đếm, bộ định thì, các phép toán phức tạp, và những giao tiếp truyền thông với những thiết bị thông minh khác.

PLC S7-1200 được tích hợp sẵn một cổng Profinet để truyền thông mạng Profinet. Ngoài ra, PLC S7-1200 có thể truyền thông Profibus, GPRS, RS485 hoặc RS232 thông qua các module mở rộng.



- 1, Nguồn cấp PS
- 2, Thẻ nhớ MMC
- 3, Kết nối với các module mở rộng
- 4, Đèn Led hiển thị I/O trên board
- 5, Kết nối Profinet

### ***1.1.2.Chế độ bảo mật của PLC S7-1200***

Một số tính năng bảo mật giúp bảo vệ truy cập vào CPU và chương trình điều khiển.

#### ***1.1.2.1.Chế độ bảo mật về quyền truy cập vào CPU và khối hàm***

CPU cung cấp các cấp độ bảo mật để hạn chế truy cập vào các chức năng cụ thể. Khi người dùng cấu hình mức độ bảo mật và mật khẩu cho CPU, người dùng có thể giới hạn các chức năng và vùng nhớ truy cập mà không dùng tới mật khẩu.

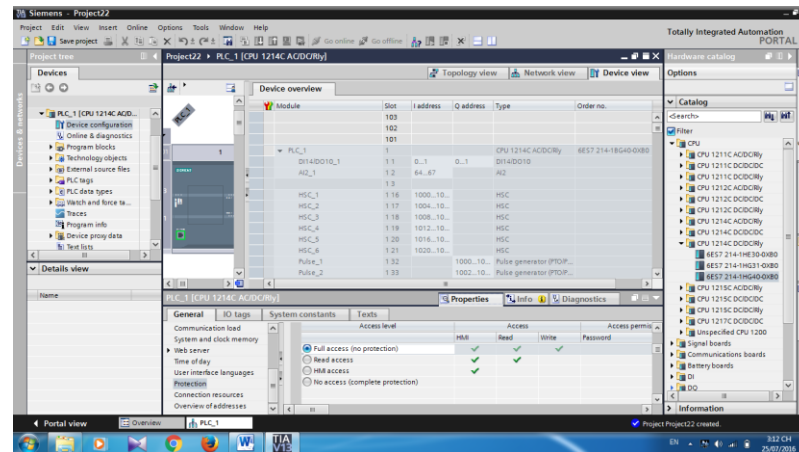
Mỗi cấp độ cho phép những chức năng nhất định để có thể truy cập mà không cần mật khẩu. Chế độ mặc định của CPU là được toàn quyền truy cập và không có mật khẩu bảo vệ. Để hạn chế quyền truy cập vào CPU, người dùng cần cấu hình thuộc tính “Protection” và mật khẩu bảo mật.

Mật khẩu bảo vệ không áp dụng cho chương trình sử dụng các chức năng về truyền thông. Truyền thông PLC – PLC (sử dụng những tập lệnh truyền thông với các khối hàm) không bị giới hạn bởi các chế độ bảo mật trong CPU.

**Bảng 1.1.Mức độ bảo mật của CPU**

Cấp độ bảo mật	Mức độ truy cập
Full access	Toàn quyền truy cập
Read access	Cho phép HMI truy cập tới PLC và chỉ được đọc với TIA Portal. Muốn toàn quyền truy cập phải có password.
HMI access	Chỉ cho phép HMI truy cập tới PLC. Muốn toàn quyền truy cập phải có password.
No access	Bảo mật hoàn toàn kể cả với HMI. Muốn toàn quyền truy cập phải có password.

Để cấu hình cho chế độ bảo mật và đặt mật khẩu, người dùng có thể thực hiện theo các bước sau: Device configuration → Chọn CPU → Properties → Protection và lựa chế độ bảo mật muốn dùng và đánh mật khẩu (password) sử dụng vào.

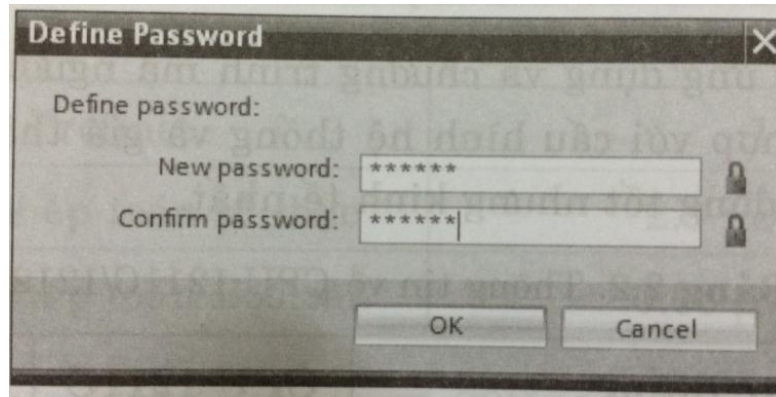


#### 1.1.2.2.Chế độ Know – how Protection

Chế độ Know – how protection cho phép người dùng ngăn chặn những truy cập trái phép vào các khối hàm, khối tổ chức OB, FB, FC, DB. Người dùng có thể tạo những password riêng lẻ để giới hạn truy cập tới các khối hàm. Nếu không có password thì người dùng chỉ có thể đọc những thông tin như sau:

- Tiêu đề khối, comment, và thuộc tính của khối hàm.
- Thông tin về các tham số vào/ra (IN, OUT, IN\_OUT, Return)
- Cấu trúc của chương trình
- Tag toàn cục trong cross references, tuy nhiên các tag cục bộ sẽ bị ẩn không quan sát được

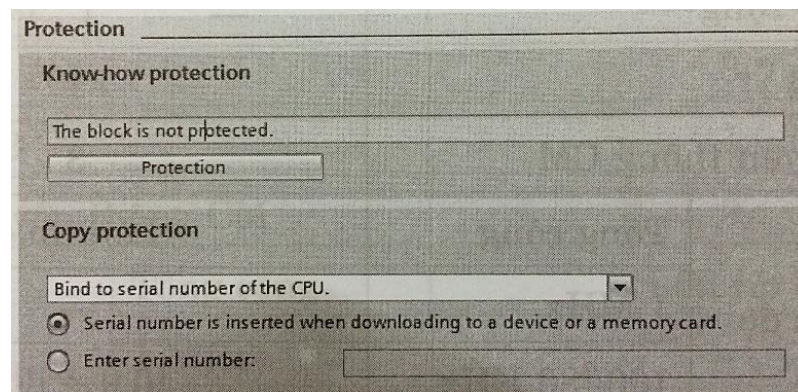
Để cấu hình cho chế độ Know – how protection, người dùng có thể thực hiện theo các bước sau: Chọn block nào muốn bảo mật → Properties → Protection → Protection → Define và nhập password muốn đặt.



### ***1.1.2.3. Chế độ Copy Protection***

Thêm một tính năng về bảo mật cho phép người dùng ẩn (blind) các khối chương trình sử dụng vào thẻ nhớ hoặc CPU. Tính năng này đặc biệt hữu ích cho việc bảo vệ sở hữu trí tuệ của người lập trình. Chức năng Copy Protection có thể áp dụng cho các khối OB, FB và FC.

Để cấu hình cho chế độ Copy Protection, người dùng có thể thực hiện theo các bước sau: Chọn block nào muốn bảo mật → Properties → protection → Copy Protection. Chọn chế độ ẩn vào thẻ nhớ hoặc CPU.



Sau đó chọn chế độ Copy Protection và nhập số serial của thẻ nhớ và CPU khi download xuống CPU hoặc thẻ nhớ.

**Chú ý:** Chế độ bảo mật/password là chế độ nhạy cảm do đó người dùng cần chú ý khi sử dụng những chế độ này.

### 1.1.3. Một số dòng CPU S7-1200 thông dụng

Hiện nay, PLC S7-1200 có nhiều dòng CPU khác nhau như: CPU 1211C, CPU 1212C, CPU 1214C, CPU 1215C, CPU 1217C và đồng thời người dùng có nhiều sự lựa chọn với các nguồn điện áp AC/DC, tín hiệu đầu vào/ra relay/DC ...

Tuy nhiên, tùy ứng dụng và chương trình mà người dùng lựa chọn CPU cho phù hợp với cấu hình hệ thống và giá thành để làm cho hệ thống hoạt động tốt nhưng kinh tế nhất.

**Bảng 2.2.** Thông tin về CPU 1211C/1212C

Đặc điểm		CPU 1211C	CPU 1212C
Bộ nhớ chương trình	Work	50KB	50KB
	Load	1MB	
	Retentive	10KB	
I/O tích hợp	Digital	6DI/4DO	8DI/6DO
	Analog	2AI	
Process image	Input	1024 Byte	
	Output	1024 Byte	
Vùng nhớ M		4096 Byte	
Module mở rộng		-	2
SB, BB, CB <sup>(*)</sup>		1	
Module truyền thông CM		3	
Bộ đếm tốc độ cao	Tổng cộng	Lên tới 6	
	1MHz	-	
	100/ <sup>1</sup> 80 KHz	I0.0 – I0.5	
	30/ <sup>1</sup> 20 KHz	-	I0.6 – I0.7
Bộ phát xung PTO/PWM <sup>(2)</sup>	Tổng cộng	Lên tới 4	
	1MHz	-	
	100KHz	Q0.0 – Q0.3	
	20KHz		Q0.4 – Q0.5
Thẻ nhớ		Hỗ trợ	
Lưu trữ thời gian thực: 20 ngày/nhỏ nhất 12 ngày tại 40°C			
Tích hợp cổng Profinet		1	
Tốc độ xử lý phép toán số thực		2.3 μs/lệnh	
Tốc độ xử lý phép toán Boolean		0.08 μs/lệnh	



**Bảng 1.3.**Thông tin về CPU 1214C/1215C

Đặc điểm		CPU 1211C	CPU 1212C
Bộ nhớ chương trình	Work	100KB	100KB
	Load	4MB	
	Retentive	10KB	
I/O tích hợp	Analog	2AI	2AI/2AO
	Digital	14DI/10DO	
Process image	Input	1024 Byte	
	Output	1024 Byte	
Vùng nhớ M		8196 Byte	
Module mở rộng		8	
SB, BB, CB <sup>(*)</sup>		1	
Module truyền thông CM		3	
Bộ đếm tốc độ cao	Tổng cộng	Lên tới 6	
	1MHz	-	
	100/ <sup>1</sup> 80 KHz	I0.0 – I0.5	
	30/ <sup>1</sup> 20 KHz	I0.6 – I1.5	
Bộ phát xung PTO/PWM <sup>(2)</sup>	Tổng cộng	Lên tới 4	
	1MHz	-	
	100KHz	Q0.0 – Q0.3	
	20KHz	Q0.4 – Q1.1	
Thẻ nhớ		Hỗ trợ	
Lưu trữ thời gian thực: 20 ngày/nhỏ nhất 12 ngày tại 40°C			
Tích hợp cổng Profinet		1	
Tốc độ xử lý phép toán số thực		2.3 μs/lệnh	
Tốc độ xử lý phép toán Boolean		0.08 μs/lệnh	

Ghi chú:

- (\*) Signal board (SB), Battery board (B) và communication board (CB).
- 1-tốc độ xử lý HSC thấp khi sử dụng chế độ lệch pha 90°
- 2-Khi CPU với ngõ ra relay thì có thể mua SB gắn vào mở rộng để sử dụng chế độ phát xung.

#### **1.1.4.Khối hàm, bộ định thì, bộ đếm PLC S7-1200**

Trong mục này, chúng ta sẽ cùng tổng quan về số lượng, định dạng ... của những khối hàm, bộ định thì, bộ đếm được sử dụng trong PLC S7-120 thông qua bảng số liệu dưới đây.

**Bảng 1.4.**Khối hàm, bộ định thì, bộ đếm của PLC S7-1200

Thành phần		Miêu tả
Các Block	Kiểu	OB, FB, FC, DB
	Kích thước	-30 KB (CPU 1211C) -50KB (CPU 1212C) -64KB (CPU 1214C, CPU 1215C, CPU 1217C)
	Số lượng	Lên tới 1024
	Số lần gọi lồng các khối hàm	16 bắt đầu từ Main
	Giám sát	2 Block cùng lúc
Các khối OB	Main	Nhiều OB Main
	Khởi động	Nhiều OB khởi động
	Ngắt thời gian	4
	Ngắt chu kỳ	4
	Ngắt phần cứng	50
	Ngắt lỗi thời gian	1
	Ngắt chuẩn đoán lỗi	1
	Tháo/gắn module	1
	Lỗi rack hoặc station	1
	Time of day	Nhiều OB Time of day
	Status	1
	Update	1
	Profile	1
	Kiểu	IEC
	Số lượng	Phụ thuộc bộ nhớ
	Lưu trữ	Lưu trong DB, 16byte
	Kiểu	IEC
	Số lượng	Phụ thuộc bộ nhớ
	Lưu trữ	Phụ thuộc cấu trúc DB. -SInt, UInt: 3byte -Int, UInt: 6byte -Dint, UDInt: 12byte

## **1.2.MODULE phần cứng của PLC S7-1200**

Để tìm hiểu kỹ hơn về PLC S7-1200 chúng ta cùng tìm hiểu chi tiết hơn về những module phần cứng mà PLC S7-120 hỗ trợ đến người dùng. Để từ đó, người dùng có những lựa chọn về sản phẩm phù hợp với ứng dụng theo yêu cầu khách hàng.

### **1.2.1.Module xử lý trung tâm CPU**

Module xử lý trung tâm CPU chứa vi xử lý, hệ điều hành, bộ nhớ, các bộ định thì, bộ đếm, cổng truyền thông Profinet ... module lưu trữ chương trình người dùng trong bộ nhớ của nó. Ngoài ra, module CPU có thể tích hợp một vài cổng vào/ra số, analog tùy thuộc vào mã hàng (order number).

CPU S7-120 hỗ trợ các protocol như TCP/IP, ISO-on-TCP, S7 communication. Đồng thời, CPU tích hợp những tập lệnh hỗ trợ cho truyền thông như: USS, Modbus RTU, S7 communication 'T-Send/T-Receive' hay Freeport ...

Cổng Profinet tích hợp cho phép CPU có thể kết nối với HMI, máy tính lập trình, hay những PLC S7 thông qua Profinet.

### **1.2.2.Module tín hiệu SM**

Module AI: module đọc analog với các loại tín hiệu khác nhau như dòng  $4 \div 20$  mA (theo cách đấu 2 dây và 4 dây), đọc tín hiệu điện áp  $0 \div 10$  VDC, đọc tín hiệu RTD, TC ...

Module AI/AO: module đọc/xuất analog

Module AO: module xuất tín hiệu analog

Module DI: module đọc tín hiệu digital

Module DI/DO: module đọc/xuất tín hiệu digital

### **1.2.3.Module xử lý truyền thông**

Module truyền thông được gắn bên trái CPU và được ký hiệu là CM 1241 CP 124x. Tối đa chỉ có thể gắn được 3 module mở rộng về truyền thông.

#### **1.2.3.1.Module xử lý truyền thông CM 1241**

Module truyền thông CM 1241 hỗ trợ các protocol theo các tiêu chuẩn như:

- Truyền thông ASCII: được sử dụng để giao tiếp với những hệ thống của bên thứ 3 (third – party systems) để truyền những giao thức protocol đơn giản như kiểm tra các ký tự đầu và cuối hoặc kiểm tra các thông số của khối dữ liệu.
- Truyền thông Modbus: được sử dụng truyền thông theo tiêu chuẩn Modbus RTU.

Modbus Master: có thể giao thức với PLC S7 là master.

Modbus Slave: có thể giao thức với PLC S7 là slave, không cho phép trao đổi dữ liệu giữa slave với slave trong truyền thông.



- Truyền thông USS Driver: lệnh cho phép kết nối USS với Driver. Các Driver. Các Driver có thể trao đổi dữ liệu theo chuẩn RS485, trong truyền thông cho phép điều khiển Driver cũng như đọc và ghi các thông số cần thiết.

- Truyền thông Point – to – point: kết nối nối đa điểm được sử dụng theo truyền thông trao đổi dữ liệu nối tiếp. Truyền thông đa điểm được ứng dụng trong hệ thống tự động hóa Simatic S7 và những hệ thống tự động hóa khác để liên kết với máy in, điều khiển robot, máy scan, đọc mã vạch ...

- Truyền thông Profibus: được sử dụng với tiêu chuẩn profibus DP hỗ trợ DPV1, có thể sử dụng làm master hoặc slave tùy thuộc vào ứng dụng mà module sử dụng.

- Module hỗ trợ AS – I Master.

#### *1.2.3.2.Module xử lý truyền thông CP 124x*

Module xử lý truyền thông CP 123x hỗ trợ những chuẩn truyền thông về GPRS/GSM, Messages/Email, DNP3, SNMP, Teleservice ...

- Module CP 1242 – 7: Hỗ trợ kết nối PLC S7 – 1200 với GPRS/GSM.

- Module CP 1243 – 1: Hỗ trợ kết nối PLC S7 – 1200 với Messages/ Email, DNP3, SNMP, Redundancy ...

#### *1.2.4.Module nguồn cung cấp Power module*

Module nguồn Power module cung cấp nguồn hoạt động cho các module phần cứng kết nối với CPU. Tên viết tắt của module nguồn S7 – 1200 là PM 1207.

Module nguồn PM 1207 yêu cầu áp cung cấp đầu vào là 120/230 VAC và ngõ ra là 24 VDC / 2,5 A được thiết lập riêng dành cho S7 – 1200 và không cần cấu hình trong phần cứng.

#### *1.2.5.Các module đặc biệt và Board tín hiệu*

##### *1.2.5.1.Module I/O link*

Module được sử dụng có thể kết nối lên tới 4 thiết bị I/O – kink phù hợp với đặc tính kỹ thuật I/O – link V1.1. Các thông số của I/O – link có thể cấu hình phần mềm Port Configuration Tool (PCT) V3.2 hoặc phiên bản cao hơn.

##### *1.2.5.2.Module cân SIWAREX*

Module cân Siwres WP231 là module cân đa năng cho tất cả các ứng dụng cân đơn giản, phức tạp hay ứng dụng trong đo lực ... Module nhỏ gọn dễ dàng lắp đặt với PLC S7 – 1200 và có thể hoạt động độc lập mà không cần PLC S7 – 1200.

Module cân Siwares WP1 có thể kết nối trực tiếp với PLC S7 thông qua Ethernet (Modbus TCP/IP ) và RS485 ( Modbus RTU ). Đồng thời, module có thể hoạt động với những PLC hoặc thiết bị của các hãng tự động hóa khác.

#### *1.2.5.3.Module CANopen*

Để mở rộng tính năng kết nối, giao tiếp truyền thông với các thiết bị của nhiều hãng, Siemens phát triển module CM CANopen cho PLC S7 – 1200, cho phép cấu hình với cả hai chế độ Master và slave.

#### *1.2.5.4.Sing Board*

Sing Board được cắm phía trên than CPU để có thể mở rộng thêm DI/DO, AI/AO, Pin backup ( Battery board ) dữ liệu về thời gian thực, mở rộng truyền thông với RS485 ( Communications boards )

### **1.3.Vùng nhớ, địa chỉ và kiểu dữ liệu trong PLC S7 -1200**

#### **1.3.1.Vùng nhớ chương trình PLC S7 – 1200**

CPU hỗ trợ những vùng nhớ để lưu trữ chương trình người dùng, dữ liệu và cấu hình hệ thống như sau:

- Load memory: Không mất đi ( non – volatile ) và được sử dụng để lưu trữ chương trình người dùng, dữ liệu và cấu hình PLC. Khi một project được download xuống PLC, nó được lưu đầu tiên tại vùng nhớ Load memory. Vùng nhớ này nằm trong thẻ nhớ MMC (nếu có) hoặc nằm trên CPU. Người dùng có thể tăng dung lượng vùng nhớ bằng thẻ MMC.
- Work memory: Vùng nhớ sẽ bị mất dữ liệu khi CPU mất điện. Trong quá trình hoạt động, CPU có thể copy một số phần, chức năng của project từ vùng nhớ Load memory sang vùng nhớ Work memory để thực hiện.
- Retentive memory: là vùng nhớ được sử dụng để lưu trữ lại những dữ liệu cần thiết, mong muốn khi CPU mất điện hoàn toàn.

#### **1.3.2.Thẻ nhớ MMC**

Một lựa chọn khác để lưu trữ chương trình người dùng giống như những vùng nhớ được nói ở trên, đó là sử dụng Simatic MMC để lưu trữ chương trình người dùng hoặc transfer chương trình người dùng. Nếu người dùng sử dụng thẻ nhớ MMC, CPU sẽ chạy chương trình từ thẻ nhớ chứ không phải trên vùng nhớ của CPU.

Thẻ nhớ Simatic MMC được sử dụng như một thẻ nhớ chương trình, một thẻ transfer, lưu trữ dữ liệu data log hoặc sử dụng để nâng cấp firmware cho CPU.

- Khi muốn download chương trình xuống nhiều CPU giống nhau và cùng một project. Việc sử dụng phần mềm làm tốn kém thời gian ... thì việc sử dụng simatic MMC với chức năng là thẻ transfer giúp cho hiệu quả hơn rất nhiều. Người dùng chỉ cần cắm thẻ nhớ MMC và đợi transfer xong và lấy thẻ nhớ ra.

- Dùng thẻ nhớ với chức năng thẻ nhớ chương trình thì tất cả những chức năng CPU hoạt động sẽ được load từ thẻ nhớ.

- Ngoài ra, thẻ MMC cũng có thể sử dụng để lưu trữ thông tin về data log, mở rộng vùng nhớ lưu trữ cho Web server, hoặc có thể sử dụng để nâng cấp firmware cho CPU ( Ví dụ từ V1.0 lên V2.0, V2.0 lên V2.3 ... ).

### 2.3.3. Kiểu dữ liệu của S7 – 1200

Kiểu dữ liệu hỗ trợ cho PLC S7-1200 sẽ được giải thích cách định dạng dữ liệu và kích thước dữ liệu thông qua bảng 2.5.

**Bảng 2.5.** Kiểu dữ liệu của PLC S7-1200

Kiểu dữ liệu	Miêu tả
Bit và chuỗi Bit	<ul style="list-style-type: none"><li>• Bool gồm một bit đơn</li><li>• Byte gồm 8 bit</li><li>• Word gồm 16 bit</li><li>• Dword gồm 32 bit</li></ul>
Integer	<ul style="list-style-type: none"><li>• USInt ( số integer không dấu 8 bit )</li><li>• SInt ( số integer có dấu 8 bit )</li><li>• UInt ( số integer không dấu 16 bit )</li><li>• Int ( số integer có dấu 16 bit )</li><li>• UDInt ( số integer không dấu 32 bit )</li><li>• Dint ( số integer có dấu 32 bit )</li></ul>
Số thực – Real	<ul style="list-style-type: none"><li>• Real – số thực dấu chấm động 32 bit</li><li>• LReal – số thực dấu chấm động 64 bit</li></ul>
Data and time	<ul style="list-style-type: none"><li>• Data là kiểu dữ liệu 16 bit chỉ số ngày có tầm từ D#1990-1-1 đến D#2168-12-31<ul style="list-style-type: none"><li>• DTL ( data and time long ) bao gồm dữ liệu với 12 byte lưu giữ thông tin về ngày, tháng, năm.<ul style="list-style-type: none"><li>• Year (UInt): 1970 → 2554</li><li>• Month (UInt) : 1 → 12</li><li>• Day (UInt): 1 → 31</li><li>• Weekday (UInt): 1 → 7 (1 là chủ nhật )</li><li>• Hours (UInt): 0 → 59</li><li>• Seconds (UInt): 0 → 59</li><li>• Nanoseconds (UDInt): 0 → 999999999</li></ul></li><li>• Time là kiểu dữ liệu 32 bit được miêu tả theo chuẩn IEC time tầm giá trị lên đến T#24D20H31M23S647MS<ul style="list-style-type: none"><li>• TOD (time of day) là kiểu dữ liệu 32 bit có tầm giá trị từ TOD#0:0:0:0 đến TOD#23:59:59:999.</li></ul></li></ul></li></ul>
Char và Sting	<ul style="list-style-type: none"><li>• Char là kiểu dữ liệu ký tự với 8 bit</li><li>• Sting là kiểu dữ liệu chuỗi lên tới 254 char</li></ul>
Array và Structure	<ul style="list-style-type: none"><li>• Array là kiểu dữ liệu mảng bao gồm nhiều thành phần đơn giống nhau về kiểu dữ liệu. Mảng có thể tạo trong giao diện interface của OB, FB, FC, DB.<ul style="list-style-type: none"><li>• Struct là kiểu dữ liệu định dạng theo cấu trúc thành phần có thể bao gồm nhiều kiểu dữ liệu khác nhau.</li></ul></li></ul>

PLC data types	PLC Data types hay còn gọi là UDT là dạng dữ liệu cấu trúc có thể định nghĩa bởi người dùng.
Pointer	Pointer hay con trỏ sử dụng để định địa chỉ gián tiếp.
BCD <sup>(*)</sup>	<ul style="list-style-type: none"> <li>• BCD 16 có giá trị từ -999 → 999</li> <li>• BCD32 có giá trị từ -9999999 → 9999999.</li> </ul>

**Ghi chú:** <sup>(\*)</sup> BCD không phải kiểu dữ liệu, tuy nhiên được đưa vào vì liên quan tới việc đến việc chuyển đổi dữ liệu sau này.

#### 1.3.4. Vùng nhớ địa chỉ

Step 7 Basic V1x của Tia Portal hỗ trợ cho việc lập trình bằng tag nhớ (Symbolic). Người dùng có thể tạo tag nhớ hay Symbolic (tên gọi nhớ) cho các địa chỉ dữ liệu cần dùng, không phân biệt vùng nhớ toàn cục (global) hay vùng nhớ cục bộ (local). Để truy xuất các Tag nhớ trong chương trình chỉ cần gọi tên của Tag cho các tham số của lệnh.

Để hiểu rõ hơn về cấu trúc CPU và địa chỉ vùng nhớ, chúng ta sẽ đi tìm hiểu sâu hơn về địa chỉ trực tiếp (absolute) là nền tảng cho việc sử dụng các Tag nhớ của PLC.

- Vùng nhớ toàn cục – Global memory: CPU cung cấp những vùng nhớ toàn cục như: I (input), Q(output), vùng nhớ nội M (memory). Những vùng nhớ toàn cục có thể được truy xuất ở tất cả các khối.
- Khối dữ liệu DB: Cũng là vùng nhớ toàn cục. Ngoài ra vùng nhớ DB nếu được sử dụng với chức năng Instance DB để lưu trữ chỉ định cho FB và cấu trúc bởi các tham số của FB.
- Vùng nhớ tạm – Temp ( hay vùng nhớ Local): Vùng dữ liệu cục bộ được sử dụng trong các khối chương trình OB, FC, FB. Vùng nhớ L được sử dụng cho các biến tạm (temp) và trao đổi dữ liệu của biến hình thức với những khối chương trình gọi nó. Nội dung của một khối dữ liệu trong miền nhớ này sẽ bị xóa khi kết thúc chương trình.

Vùng nhớ I, Q của PLC S7-1200 có thể truy xuất dưới dạng process image. Để có thể truy xuất trực tiếp và ngay lập tức với ngõ vào/ra vật lý, có thể thêm “:P”. Ví dụ như: I0.0:P, Q0.0:P.

Chế độ Forcing chỉ có thể ứng dụng cho các tín hiệu vào/ra vật lý (Ix.y:P, Qx.y:P).

**Bảng 2.6.**Bảng phân loại vùng nhớ PLC S7-1200

Vùng nhớ	Miêu tả
Process image I	Được copy dữ liệu từ tín hiệu ngõ vào vật lý khi bắt đầu quét chương trình.
Ngõ vào vật lý Ix.y:P	Đọc địa chỉ ngay lập tức từ ngõ vào của CPU, SB, SM. Có thể dùng chế độ Force với ngõ vào vật lý.
Process image Q	Chuyển dữ liệu tới tín hiệu ngõ ra vật lý khi bắt đầu quét chương trình.
Ngõ ra vật lý Qx.y:P	Xuất trực tiếp tới ngõ ra ngay lập tức tới ngõ ra vật lý của CPU, SB, SM. Có thể dùng chế độ Force với ngõ vào vật lý.
Vùng nhớ nội M	Lưu trữ dữ liệu/tham số trước khi đưa ra ngoại vi. Có thể cài đặt để sử dụng chức năng Retentive memory đối với vùng nhớ này.
Vùng nhớ tạm Local memory	Vùng nhớ được sử dụng để lưu trữ tạm thời trong các khối OB, FB, FC. Dữ liệu sẽ mất khi ngừng gọi khối.
Khối dữ liệu DB	Được sử dụng theo định dạng vùng nhớ toàn cục, hoặc lưu trữ dữ liệu và tham số cho khối hàm FB. Có thể cài đặt để sử dụng chức năng Retentive meory đối với vùng nhớ này.

## 2.4. Phần mềm và ngôn ngữ lập trình PLC S7-1200

### 2.4.1. Phần mềm lập trình PLC S7-1200

Năm 2009, Siemens giới thiệu PLC S7-1200 cùng với phần mềm lập trình Tia Portal V10.5 tích hợp sẵn Step 7 Basic, lập trình cho PLC S7-1200 và WinCC Basic lập trình cho màn hình KTP.

Từ năm 2010 đến nay, Siemens không ngừng cải tiến và nâng cấp phần mềm Tia Portal V10.5 lên tới Tia Portal V13. Hiện nay phần mềm Tia Portal không chỉ lập trình cho các bộ Controller mà còn có thể thiết kế giao diện HMI, SCADA và cấu hình cho Driver của Siemens. Tuy nhiên, trong nội dung này chúng ta chỉ trình bày và tìm hiểu về PLC S7-1200 và phần mềm Step 7 Basic V1x của Tia Portal để lập trình cho PLC S7-1200.

### 2.4.2. Ngôn ngữ lập trình PLC S7-1200

Với dòng sản phẩm PLC S7-1200 ứng dụng cho hệ thống nhỏ và vừa, Siemens phát triển và ưu tiên hỗ trợ cho 3 ngôn ngữ lập trình chính, đó là: LAD, FBD và SCL.

- LAD – Ladder: Đây là ngôn ngữ lập trình dựa theo sơ đồ mạch. Nó đơn giản, dễ hiểu, dễ chỉnh sửa và tiện lợi.
- FBD – Function Block Diagram: Đây là ngôn ngữ lập trình dựa theo đại số Bool.

- SCL – Structure Language Control: Đây là ngôn ngữ lập trình theo dạng text và là ngôn ngữ trình cấp cao sử dụng dựa trên nền Pascal phát triển. Ngôn ngữ lập trình SCL có thể coi là ngôn ngữ hướng tới đối tượng cho PLC, vì nó gần gũi với tư duy người dùng.

Khi viết code cho một khối hàm nào đó ( OB, FB, FC ) thì người dùng có thể sử dụng 1 trong 3 ngôn ngữ trên để có thể lập trình.