Các hệ thống Tin học Công nghiệp
(Industrial Information Systems)

Lưu hành nội bộ

By Bùi Quốc Anh,
Hanoi University of Technology
Computer Engineering Department
Website: http://www.it-hut.edu.vn/~anhbq
Email: anhbq@it-hut.edu.vn

Mục đích - Yêu cầu

- **Mục đích: Cho học viên/ sinh viên nắm được:**
  - Cấu trúc và hoạt động của các hệ thống thông tin công nghiệp: SCADA, OCS, DCS...
  - Các hệ thống nhúng, các họ Vi điều khiển và xây dựng các ứng dụng lẻ.
  - Mô hình liên kết, truyền tin trong công nghiệp, các giao thức
  - PLC và lập trình với các ngôn ngữ của PLC
  - Hệ điều hành, lập trình/môi trường thời gian thực
- **Yêu cầu:**
  - Người học tham gia đầy đủ các buổi lên lớp lý thuyết, seminar và các buổi thực hành Lập trình PLC trên phòng thí nghiệm, đi tham quan/thực tập nhận thức.
  - Thực hiện các bài tập lớn, tham gia/trình bày seminar

Nội dung:

- Tổng quan hệ thống máy tính công nghiệp
- Mạng công nghiệp và các giao thức
- Embedded Systems: Vi điều khiển 51s, AVR-90, DSP240, 386EX
- Máy tính PC công nghiệp
- PLC và Hệ Siemens PLC S7-x00, ngôn ngữ lập trình Step 7 và WinCC Tool
- Hệ SCADA/ DCS/ QCS/ OCS...
- Tham quan Nhà máy/ Trung tâm TĐH A0, A1

Tài liệu tham khảo

- **Publications:**
  - Tự động hóa với Simatic S7-300, Prof. Phan Xuân Minh
  - Siemens Industrial Communication Networks
  - Siemens S7-200/ 300/ 400 Series User Manual...
- **Website/ pdf files:**
  - atmel.com; ti.com; modbus.org; scada.org...
- **Software/ Tools:**
  - WinCC, Citec, Advanced Builder, OOP, ...
  - Các hệ điều hành thời gian thực/nhúng - RTOS: WindowsCE, T-Engine, VxWorks, QNX...

Bài tập lớn (Không bắt buộc)

- Tìm hiểu và báo cáo các hệ thống:
  - Cấu trúc mạng truyền tải - phân phối điện Miền Bắc và Hệ thống SCADA A1;
  - Hệ DCS một số nhà máy như Phả lại 2 Thermo Power Plant, Hoàng thạch 2 Cement Mill, Bãi Bằng Paper Mill, ...
- RTOS/Protocol:
  - Realtime (http://www.eventhelix.com/)
  - Xd Hard Real Time OS cho các hệ nhúng.
  - Multi Point/multidrop;

Bài tập lớn (Không bắt buộc)

- Khai thác các RTOSes: cài đặt, lập trình ưd + IO, đánh giá, real time..., gồm:
  - WindowsCE (www.windows/imbedded/)
  - VxWorks (www.xs4all.nl/~borkhuis/vxworks/vxworks.html)
  - QNX...
- Tham gia các đề tài của gv/ bộmôn/ khoa/ trường có tính ứng dụng - Industry Oriented IT;
- Thiết kế, lắp ráp, lập trình các thiết bị cụ thể.

Ch 1.
Tổng quan về các hệ thống máy tính công nghiệp

Ch. 1 Tổng quan các hệ thống Máy tính công nghiệp

1.1. Khái niệm: Là các Mạng máy tính có độ tin cậy cao, gắn liền với đối tượng công nghệ, cho phép liên kết mạng ở nhiều cấp độ khác nhau để điều khiển quá trình và quản trị thông tin sản xuất.

Địa chỉ ứng dụng: trong các Nhà máy, các hệ Phát - Truyền tải - Phân phối điện, các nhà máy sản xuất thép, cement, phân bón, hệ thông tin Điều khiển giao thông, Hệ thống thăm dò khai thác dầu-khí, trong các lĩnh vực An ninh - Quốc phòng và Hàng không - Vũ trụ...

- **Các Hệ thống thiết bị và mạng:**
  - SCADA - Supervisory Control And Data Acquistion Systems,
  - DCS - Distributed Control System,
  - QCS/OCS - Quality [Open] Control System,
  - DAS - Data Acquisition System,
  - PLC - Robot ...

- **Lịch sử - phát triển:**
  - 1960s: Hệ thống điều khiển công nghiệp trên cơ sở Relays/ Contactors, cồng kềnh, độ chính xác kém, không tập trung, việc bảo dưỡng, xác định lỗi khó khăn... năng suất/ chất lượng kém.
  - 1970s: Xuất hiện PLC - Bộ điều khiển Logic khả trình, chủ yếu thực hiện các hàm logic, delay, bộ đếm... để thay thế cho các bộ điều khiển các dây chuyền sản xuất, thay đổi cấu trúc linh hoạt hơn nhưng chưa có tính tập trung hóa cao, số thiết bị được gắn kết với nhau ít, dbase mức thấp.
  - 1990s: Xuất hiện các hệ SCADA/ DCS trên cơ sở mạng LAN mạnh, các công cụ quản trị số liệu, các máy tính và hệ thống truyền tin tốt... nâng cao tính mềm dẻo cho sản xuất, nâng cao chất lượng, năng suất... giải phóng sức lao động cho công nhân.
  - Từ 1995: Mạng Internet phổ biến: các mô hình 'remote': training, installing, service, commissioning, upgrading...

– **Vietnam:** Hoàng thạch Cement Mill (1980s - QCX), Bãi bằng Pulp & Paper Mill (1997 - QCS) của ABB, SCADA điều độ lưới điện quốc gia - A0 và các miền A1/ A2/ A3 cùng các điều độ địa phương - HN, HCM... (1995 - nay)... và tất cả các N/m mới đầu tư, nâng cấp sau 1990 như Hòa bình Hydro Power Plan, Phú mỹ/ Bà rịa/ Phả lại... Thermo Power Plans (OCS), Rolling Mills, Cement Mills...

– Xu hướng phát triển hiện nay: Tự động dựa trên máy tính - PC based Automation, tích hợp với PLC... như dây chuyền sản xuất - lắp ráp BMW, Coca-cola, tầu sân bay USS Truman...

- **Phân biệt các hệ thống:**
  - SCADA:
    - Trên cơ sở hệ truyền thông mạnh, tốc độ cao, khoảng cách xa trải trên diện rộng lớn hàng trăm hoặc hàng ngàn km, có các lệnh kết nối qua vệ tinh, máy thu phát vi ba, cáp quang hoặc ISDN...
    - Ví dụ: các hệ điều độ sản xuất, truyền tải và phân phối điện lực Quốc gia, các khu vực Miền Bắc, Miền Nam, Miền Trung, Cty Điện lực Hà nội, Sài gòn, hệ Khai thác và Dẫn khí đồng hành Dinh cố...
    - Thường các hệ này ít điều khiển (tuy vẫn có chức năng ĐK)
  - DCS/OCS/QCS:
    - Hệ Đo lường - Điều khiển - Bảo vệ tập trung trong các nhà máy, xí nghiệp, số điểm công nghệ lên đến vài ngàn điểm
    - Khoảng cách gần, max là 10 km
    - Truyền tin trên các đường truyền mạng/giao thức công nghiệp
    - Có tính thời thực cao cho điều khiển và bảo vệ
  - DAS:
    - Hệ Đo lường - Điều khiển - Bảo vệ tập trung trong các dây chuyền xí nghiệp nhỏ lẻ, qui mô đơn giản

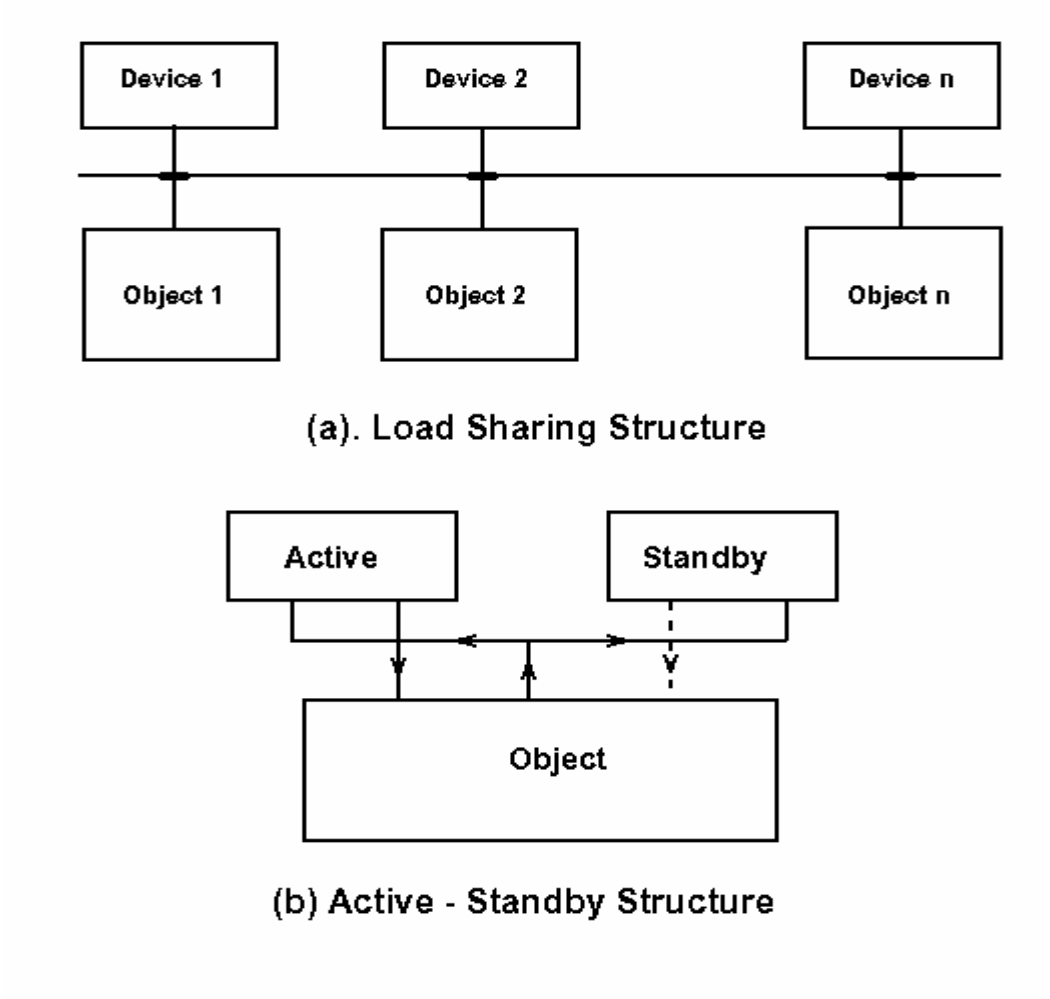
Ch 1. Tổng quan Hệ thống máy tính Công nghiệp

1.2. Đặc điểm Các hệ thống Máy tính công nghiệp:

- Ghép nối trực tiếp với đối tượng công nghệ và xử lý thông tin trong thời gian thực,
- Truyền tin trong khoảng cách xa (km.. Mm)
- Thường được liên kết thành mạng với các giao thức riêng, các giao thức hướng công nghiệp, đã được đơn giản hóa và chuẩn hóa mức độ cao
- Độ tin cậy cao, chống nhiễu tốt, chống treo (Watch Dog Timer/ Chien de Garde). Hoạt động được trong môi trường khắc nghiệt: Out door, độ ẩm cao, bụi, rung sóc, chịu được va đập...
- Hot services (hot pluggible/swap)

- Tính linh hoạt cao, dễ mở rộng, nâng cấp, khai báo đơn giản,
- Dễ dàng chuẩn đoán/ xác định sự cố nhờ có cơ chế (thiết bị và giao thức) để đo lường các thông tin vật lý của thiết bị (t, RH, ...)
- **Nguyên tắc hoạt động** theo kiểu chu kỳ quét lặp lại (scan loop), thay đổi các tham số của chương trình mà không cần (không được) dừng hệ thống,
- Các công cụ phát triển: dễ sử dụng, hướng đối tượng, thân thiện
- Nâng cao độ tin cậy: dùng các cơ chế Song hành (duplication), Dự phòng (redundancy) cho các máy chủ, máy in sự kiện, thiết bị sao lưu... và các đường truyền tin.

- **Nâng cao độ tin cậy:**
  - Cơ chế Song hành (duplication):
    - Cho các Hệ thiết bị như máy tính chủ, đường truyền LAN, các modules, nguồn cung cấp...
    - Các thiết bị song hành cùng thực hiện công việc chung - Load sharing. Nếu thiết bị thự (i) có sự có, các thiết bị còn lại thực hiện phần việc của TB (i)
    - Thường có Thiết bị Master hay Supervisor để giám sát việc thi hành của các thiết bị song hành
  - Cơ chế Dự phòng (Redundancy):
    - Dự phòng nguội.
    - Dự phòng nóng (Active-Standby): 2 thiết bị cùng thực hiện chức năng như nhau về update CSDL Công nghiệp, cùng tính toán cho điều khiển ra, nhưng chỉ có Tbị Active đưa tín hiệu ra
  - Watch Dog/ Chien de Garde:



Hình 101. Song hành và dự phòng

Ch 1. Tổng quan Hệ thống máy tính Công nghiệp

1.3. Cấu trúc mạng:

Mô hình mạng công nghiệp thường bao gồm 3 Layers: Field, Process Control (Master) và Supervisory/Management Levels: hình 101

- Field Level: Là các đối tượng gắn liền với quá trình công nghệ, thường được điều khiển bởi các máy tính công nghiệp, các hệ Vi điều khiển hay các bộ PLC nhỏ. Đường truyền thường dạng Point to Point hoặc Multi Point.
- Process Control/ Master Level: Kết nối, tập trung hóa các điểm công nghệ thông qua các module truyền tin, có data base. Thiết bị thông thường là các máy tính PC công nghiệp hoặc các PLC mạnh.
- Supervisory Management/ Operator Level: thường dùng Industrial Ethernet để đặt các thông số sản xuất, giám sát quá trình, quản trị cơ sở dữ liệu sx, qlý thiết bị, ql sự cố. Giống như mạng máy tính bình thường, có thể nối internet cho các dịch vụ remote (installing, training, service, update...)

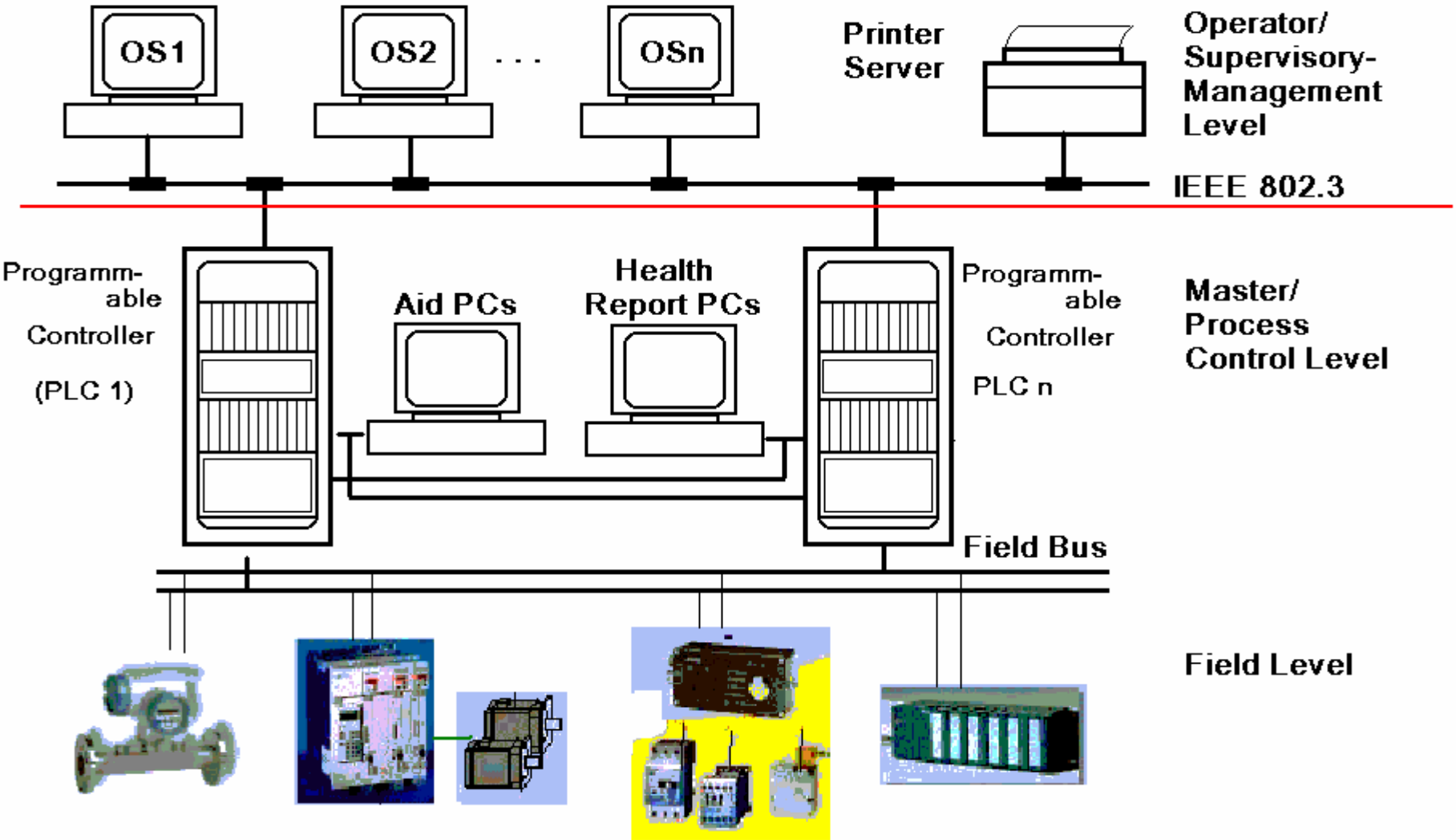


Fig. 102. 3 Level Industrial Computer Network

1.3.1. Field Level:

- Nói chung, chúng đều là các thiết bị thông minh (computerized devices như Vi điều khiển, iPC), có các cổng truyền tin RS232/ RS422/ RS485 hoặc đường truyền nguồn dòng điện có cách ly quang học:
  - Các thiết bị đo gắn với các quá trình sản xuất/ đối tượng công nghệ: Máy đo lưu lượng, nhiệt độ, áp suất, tốc độ quay...,
  - Các thiết bị điều khiển/ cơ cấu chấp hành: Motor, Valve, Contactor...,
- Các hệ điều khiển mạng CN cấp thấp hơn, điều khiển bởi những bộ PLC/PC (Field Controller) cho một nhóm thiết bị, như mạng AS-i của Siemens, MODBUS của Schneider
- Được tập trung hóa, đánh địa chỉ trên một bus chuẩn, (như Profibus của Siemens) để trao đổi thông tin với tầng trên
- Các transducers, sensors thông minh...

1.3.2. Master/ Process Control Level:

- Là các **PC công nghiệp (iPC), PLC** và các máy tính kỹ thuật (Aid/Health).
- **Các Cty sản xuất PLC:**
  - Siemens Automation Simatic, S5/S7 series;
  - Allen Bradley, a Rockwell Company, AB Master series;
  - GE-Fanuc, a GE Company, Master Logic 90 series;
  - ABB Automation, Master Piece Series;
  - Omron; ...
- **Cấu trúc các thiết bị PLC** thường chia thành các module chức năng, được gắn trên giá đỡ (RACK):
  - CPU + Power supply Module có cổng nối bộ lập trình (Programmer)
  - [Expansion Memory Module (Flash, SRAM, DRAM, BBRAM)]
  - Digital Input Module (mức áp dc/ac, cách ly...)

- Digital Output Module (relay, transistor, triac..., Relay/Opto Isolated)
- Analog Input Module (u, i, cách ly...)
- Analog Output Module (u, i)
- Timer/ Counter Module (kHz, đếm xung, đo tốc độ, chiều dài)
- Communication Module: (RS232/485; Ethernet IEEE 802.x)
- 2/3 D Positioner Module (định vị 2/ 3 chiều)
- Interface Module - dùng để mở rộng thêm các Module khác
- Function Modules: các chức năng điều khiển PID, Servo/ Step Motors,...

• **Bus:** thường dùng các
- Bus chuẩn công nghiệp để nối với với các tầng dưới,
- Ethernet IEEE 802.x để kết nối giữa các tủ PLC và nối với tầng trên.

- **Health Repport & Aid (Development System) PCs :**
  - Health Report PC: Nối với các điểm đo thô (các tầng Transporrt Oriented Protocols), hoặc các thông số vận hành của các máy chủ, các tủ PLC để cho các chuyên gia (masters) bảo dưỡng và sửa chữa.
  - Aid/ Development System Computers:
    - Chứa Ctr nguồn (system/application) trong PLC, chương trình dịch và tool - LOADER, DEBUGGER, SIMULATOR... để nạp và chạy thử PLCs.
    - Dùng cho các chuyên gia sửa chữa/ thay đổi/ nâng cấp phần mềm thay đổi các tham số đo lường/điều khiển (đôi khi được hiểu là data base) trong PLC,
    - Khai báo thêm các điểm công nghệ mới, xóa bỏ 1 điểm đã có (1 data base);
    - Có công cụ DEBUG để cho phép Test, Run, Stop, Break cho từng đối tượng

1.3.3. Supervisor (Operator/Management) Level

- Dùng để giao tiếp với người vận hành, các chuyên gia công nghệ (Điện, Lò, Cement, Giấy, cán thép...) để điều khiển quá trình sản xuất
- Mạng máy tính IEEE 802.3, 100 Mbps, Giao thức TCP/IP
  Các máy tính mạnh, song hành (Sun, DEC Alpha, IBM AS400/ RS6000/Netfinity...):
  - Máy tính quản lý quá trình sản xuất, giao tiếp với người vận hành (MMI)
  - Máy tính CSDL, lưu số liệu, điều khiển việc sao lưu
  - Máy tính Đào tạo, phát triển
  - Máy tính Truyền tin (gateway) nối với các tầng cao hơn
  - Event Printers ...
  - Kết nối tầng dưới (Down Stream) với các module Ethernet Adaptor của PLC, iPC

1.4. Hoạt động và các phần mềm:

1.4.1. Field Level: có thể là

• Dựa trên các hệ nhúng - Embedded System, các hệ vi điều khiển, các thiết bị transducer thông minh, hay các cơ cấu chấp hành thông minh... có các chương trình vận hành riêng. Một số được gọi là RTU - Remote Terminal Unit

• Các Field Controllers: các PLC qui mô trung bình và nhỏ (mini & mid range: S5-90/100/115; S7-200/300), có các module lập trình.

• Các Transducers/Transmitters, thông tin ra là các dòng điện, điện áp đã được chuẩn hóa:

- ✓ U_{OUT} = 0..10V
- ✓ I_{OUT} = 0..20mA hoặc 4..20 mA

• Có thể được tổ chức thành nhóm: mạng AS-i hoặc RTU

1.4.2. Master Level:

- Các máy tính kỹ thuật (Health/Aids/Depvelopment...):

  Hệ điều hành: WinNT/ UNIX/DOS/BASIC...

  Ứng dụng dùng các ngôn ngữ lập trình thông dụng: C/ C++/ASM.

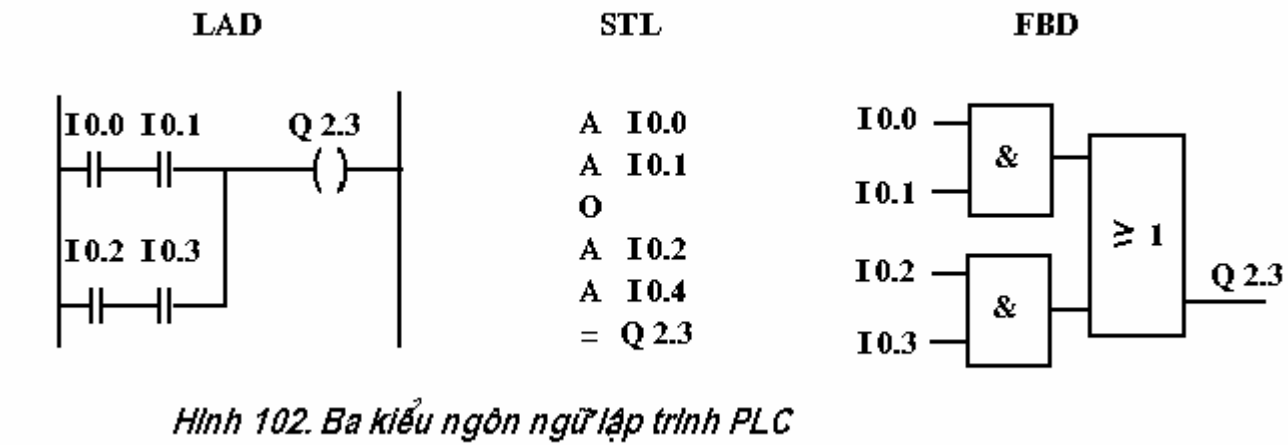
  - Các Hệ PLC cấu hình mạnh (Hi performance: S5-135/ S7-400

  - Chương trình điều hành PLC: do các hãng công nghệ TĐ

  - Chương trình ứng dụng:

  + Ngôn ngữ: hướng đối tượng, dễ học,

  + Kiểu LADder/ StaTement List và Functional Block Diagram (H. 102),



Hình 102. Ba kiểu ngôn ngữ lập trình PLC

- Chương trình dịch: Interpreter để cho phép chương trình đo lường - điều khiển hệ thống vẫn hoạt động trong khi thay đổi các tham số, cấu hình các module chương trình.
- Chương trình ứng dụng và số liệu được thiết kế sẵn kiểu module và database, dễ triển khai, dễ chỉnh sửa tại hiện trường: Input data base, Output data base... của các điểm công nghệ.

– **Hoạt động:**

• Thực hiện kiểu quét chương trình (hình 102), tốc độ quét phụ thuộc vào độ lớn chương trình.

  • Đọc các giá trị vào (Digi/Ana/Comm/Timer...)

  • Update vào cơ sở dữ liệu

  • Tính toán ra quyết định điều khiển

  • Đưa các tín hiệu ra

  • Kiểm tra các trạng thái nội bộ

• Chương trình được chia thành nhiều Function Block, có thể Enable hay Disable từng block trong quá trình hoạt động

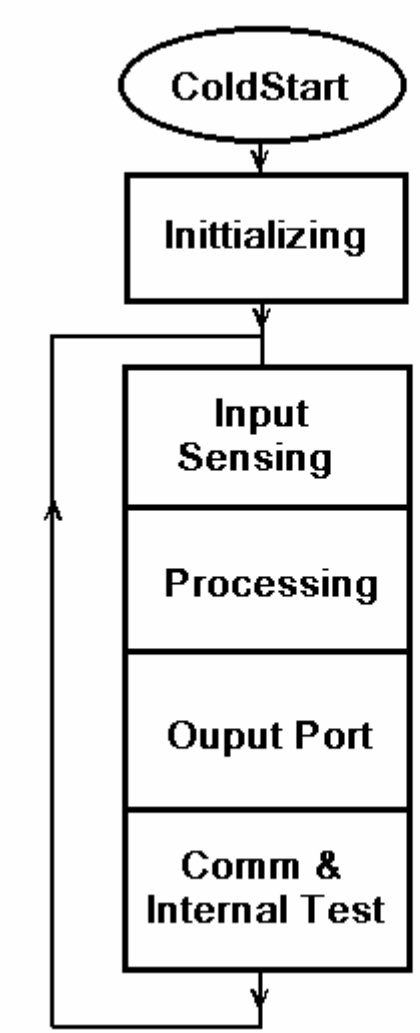


Fig 103. PLC Scan Loop

- Data base: Một số hãng thiết kế data base cho riêng mình như MasterPiece của ABB, Habitat của Alstom T&D. Mỗi điểm đo lường/điều khiển công nghệ được coi là 1 data base element.
- Bus và giao thức là chuẩn công nghiệp về truyền nối tiếp, do các hãng đưa ra phù hợp với các tiêu chuẩn IEC... IEEE... ví dụ mục sau.

- **Ví dụ** data base: số đo theo thời gian (Time stamp data base): là một bộ các số liệu (record) liên quan đến điểm đo đó, được hiểu như các fields như:
  - Tên/mã điểm đo,
  - Đơn vị/ thứ nguyên đo,
  - Hệ số hiệu chỉnh tuyến tính (ax + b) hoặc phi truyến (hàm đại số hoặc giải tích),
  - Range: min - max,
  - Alarm Levels: Low/Hi Alarm
  - E-Stop: Low/Hi Emergency stop
  - Thời gian update - interval hay thích nghi
  - Độ phân ly để update
  - Độc lập hay phụ thuộc (vector), Liên kết của số liệu
  - Historical Events (Fault - Value, Time...)
  - ...

1.4.3. Operator Level: Là mạng máy tính cục bộ LAN, chuẩn IEEE 802.x, giao thức TCP/IP

- Có các máy tính như các servers, hệ điều hành UNIX hoặc WinNT, các server này thường chạy song hành:
  - Server ứng dụng - hướng tới đối tượng là các quá trình công nghệ, được xây dựng bằng các ngôn ngữ/ ứng dụng chuyên cho SCADA như CITEC, WINCC (Siemens)...:
  - Server cho các hệ cơ sở dữ liệu ONLINE
  - Server cho các hệ CSDL OFFLINE, Historical Data base và các các thiết bị sao lưu tốt.
  - Có khả năng tái tạo lại các tính huống, các sự kiện hay sự cố
  - Server để đào tạo, để mô phỏng các quá trình, các sự cố có thể xảy ra và đưa ra kịch bản để xử lý.
  - Cổng nối với mạng cấp trên (gate way) như internet/ cáp quang để cho phép trao đổi số liệu và đặc biệt nối với nhà cung cấp để nhận được các dịch vụ đào tạo, cài đặt và maintenance từ xa.

- **1.5. Case study 1: PC3 - SCADA/EMS**
- **1.5.1. Sơ đồ Phát - Truyền tải - Phân phối điện năng Miền Trung - PC3.**

  Xem hình 104,

- **1.5.2. Hệ SCADA Điều độ lưới điện miền Trung:**

Hình 105.

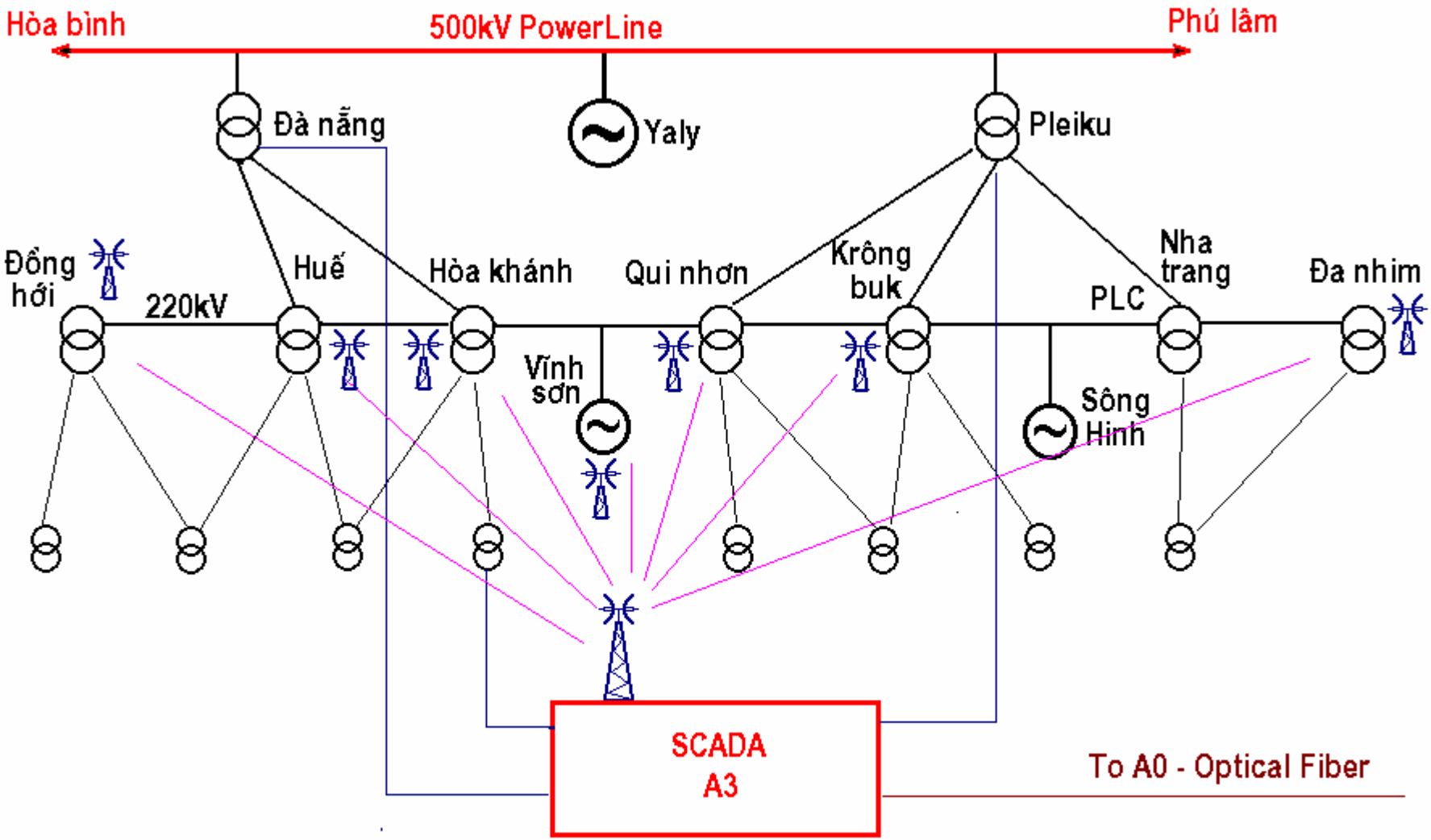


Fig 104. Vietnam Central Region (PC3) Hi-Voltage Transmission Lines and Communication Network

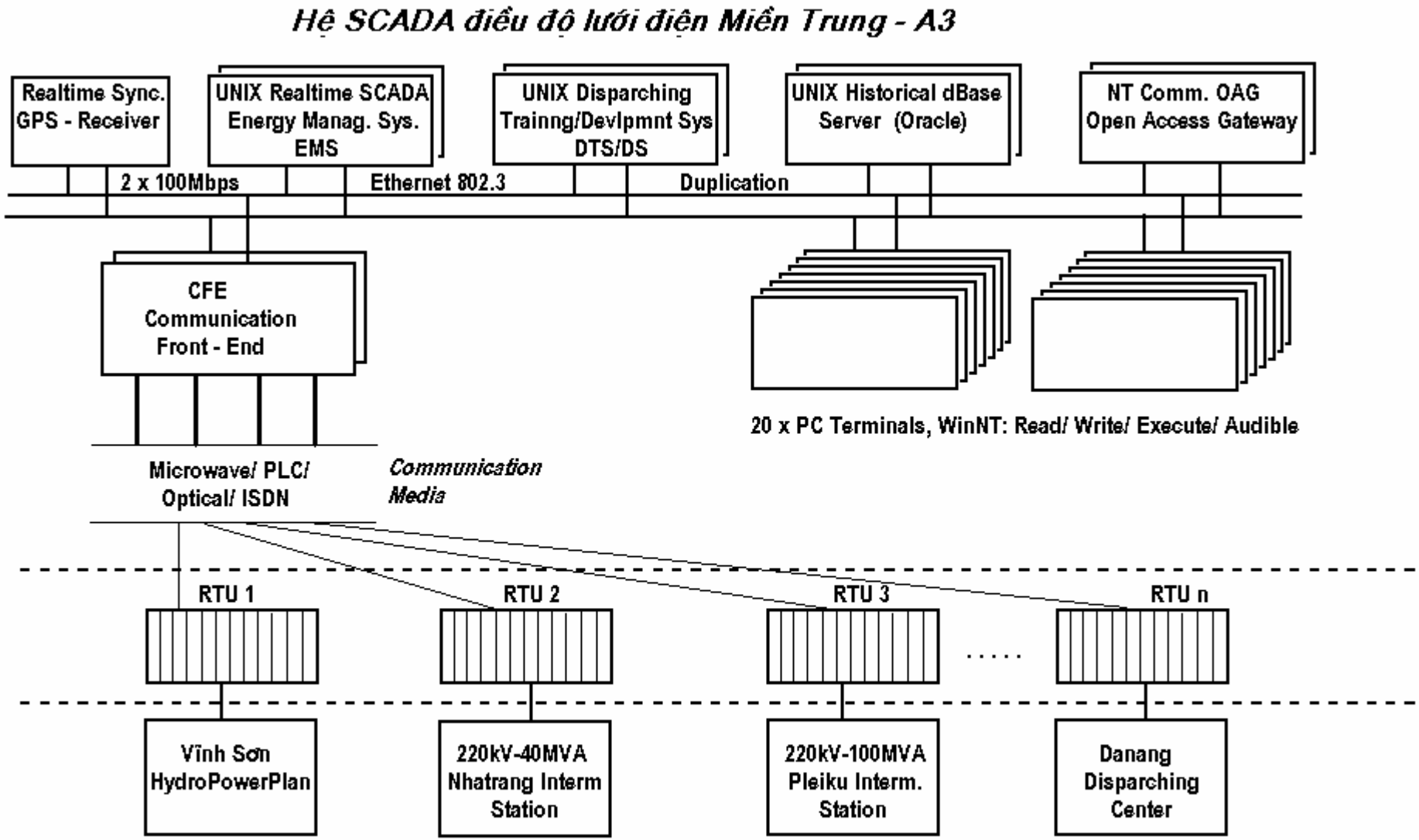


Fig. 105. Vietnam Central Region SCADA/EMS - A3

1.5.2.1. Đặc điểm Lưới điện và Hệ SCADA Điều độ:

- Lưới điện cao áp Miền Trung là 1 hệ thống các mạng 500, 220 và 110kV, trải khắp hàng ngàn km, từ Quảng bình đến Nha trang - Đa nhim.
- Có 2 trạm 500kV/220kV tại Đà nẵng và Pleiku,
- Gần 10 trạm 220kV/110kV trải dài khắp miền trung và khu vực Tây nguyên, nối thành mạch vòng khép kín.
- Hàng chục trạm 110kV...
- Tại mỗi trạm có RTUs là thiết bị kiểu PLC, để thu thập các số liệu của trạm: 3 điện áp thanh cái, 3 dòng điện sơ cấp, 3 dòng điện thứ cấp, 2 dòng điện zero, trạng thái các máy cắt, trạng thái các nấc biến áp, tần số, công suất tác dụng P và công suất phản kháng Q, các số đo tự dùng, các số đo của nguồn dc...

- Hệ thống truyền thông mạnh trên cơ sở 4 loại hình truyền thông (song hành): OF, Microwave, PLC và ISDN.
- Hệ thống do Hãng Alstom T&D, Pháp thiết kế, lắp đặt và ph/tr phần mềm trên cơ sở thiết bị hợp chuẩn của nhiều nhà cung cấp khác.

1.5.2.2. Cấu trúc hệ thống: Chia thành 3 lớp chính: Mạng LAN, các RTUs và các thiết bị đo lường - điều khiển tại các trạm:

① Mạng LAN Ethernet 802.3, 100Mbps, gồm 8 máy tính server, chia thành 4 nhóm chức năng (duplication), đặt tại trung tâm TĐH A3, Đà nẵng:

- RealTime EMS Servers, 2 máy tính DEC Alpha, UNIX, song hành, làm nhiệm vụ chính của hệ SCADA: đo lường, điều khiển, tính toán trào lưu công suất...

- DTS/DS Servers: Dec alpha, UNIX, song hành, làm nhiệm vụ mô phỏng, đào tạo và phát triển phần mềm (thêm bớt các trạm, hiệu chỉnh tham số cho các CSDL...)
- HIS Servers, DEC Alpha, UNIX: OFFLINE Database, gồm 2 x 6 HDD RAID 5; 12 MO Drivers để lưu số liệu trong vòng 2 năm
- Comm OAG, Open Access Gateway, DEC Alpha, WinNT: dùng để nối lên Internet và cáp quang nối A0, Trung tâm Điều độ HTĐ Quốc gia, Hà nội.
  - Data base 2 side A3 và A0
  - Protocol converter: IEC 870-x <==> ICCP (Inter Control Center Protocol),

- GPS dùng để thu thập thời gian thực từ vệ tính để chuẩn thời gian giữa các Trạm, giữa các điều độ miền và điều độ A0
- CFE, SUN, OS: OPEN VMS, Communication Front-End Processing : dùng để truyền thông với các trạm điện bằng 4 loại Adaptor: Cáp quang OF, Vi ba (microwave), PLC (PowerLineCarrier) và [ISDN]:
  - V24, 4800 bps
  - Concentrator,
  - Protocol converter: IEC 870-5 <==> TCP/IP
  - Buffer (HDDs)
  - 4 Cards x 16 path, mỗi path quản lý nhiều điểm (Multi drop),
  - Time synchronizing.

- 20 PC Terminals, WinNT, có chức năng MMI, cho 4 cấp users: Read/ Write/ Execute/ Audible
- ② RTUs tại các trạm, là các thiết bị kiểu PLC (Programmable [Logic] Controller):
- CPU board hãng Microsol, Ireland, CPU 68020, 1MB EPROM, 8 MB SRAM
- Communication: V24/V28, IEC 870-5
- Cấu trúc và hoạt động theo kiểu database IN/OUT (database driven)
- IN/OUT Cards:
  - Analog In: 64 channels/card, 4 card/RTU max, 0..20mA, Isolated, time resolution: 6ms
  - Digital IN/OUT Cards: 64 channels/card; 4 cards/RTU,
  - Hi speed counters: đo đếm công suất/ năng lượng
  - Power supply: Accu 48Vdc

③ Field Level: là các thiết bị chuyển đổi (transducers) từ dòng, áp, P, Q, f... thành các tín hiệu dòng điện (0..20mA) hoặc xung

1.5.2.3. Các phần mềm hệ thống và ứng dụng:

① Phần mềm trên các máy chủ:

- Hệ điều hành: UNIX - DEC và WinNT

- **Ứng dụng:**

- Phần mềm TOPOLOGY, đánh giá hệ thống lưới,
- SCANNER: thu thập số liệu, đánh giá số liệu
- Tính toán trào lưu công suất POWER FLOW,
- OPTIMAL PowerFlow,
- Economical Dispatching,
- Dự báo sự cố và hướng giải quyết,
- Sa thải phụ tải - Load Shedding,
- Dự báo phụ tải: mưa, nắng, lễ tết, mùa...

- Điều khiển OLTC (On Load Tap Changer)
- Work Order/ Scheduler,
- Supervisor for comm: Change Over, chuyển giữa 2 đường dây để phát hiện sự cố,
- Historical Reconstruction: 2s
- AGC: Automatic Generator Controlling,
- ....

- ONLINE Database: Habitat, ALSTOM T&D
  - Real time, đồng đều về thời gian,
  - Kết hợp mô hình quan hệ và mô hình cây,
  - Duplication, Online integration,
  - Limit: 150 RTU, 15k Analog, 25 k Digital data base.
  - ....
- OFFLINE Database Oracle: Copy và chuyển đổi từ Habitat sang Oracle, (Open)...

② RTU Software:

- Qui ước database cho mỗi điểm đo, điều khiển.
- Thu thập số liệu, chuyển đổi thành số đo vật lý hiện thị tại chỗ
- Tác động bảo vệ khi có sự cố
- Đóng gói số liệu, gửi lên trung tâm khi có yêu cầu.
- ...

1.6. Case study 2: Siemens Industrial Communication Networks - SINEC

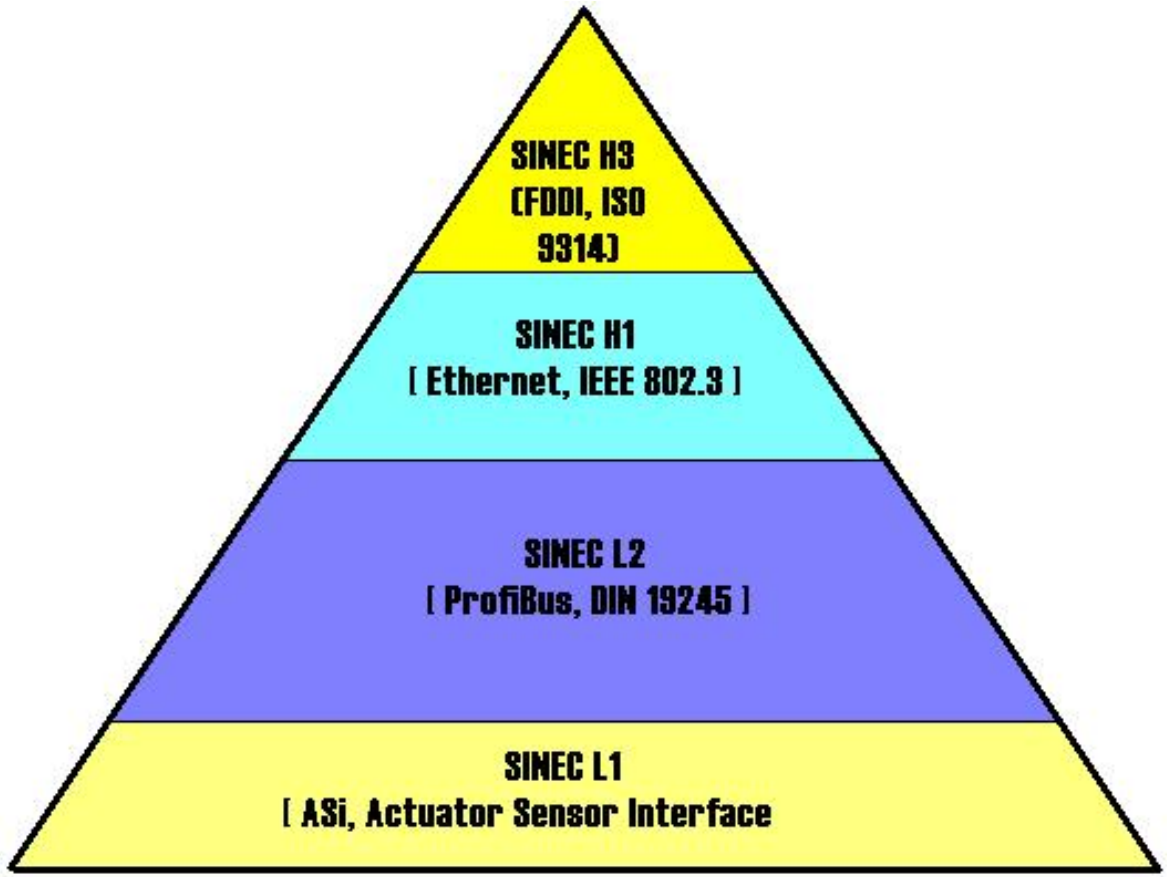
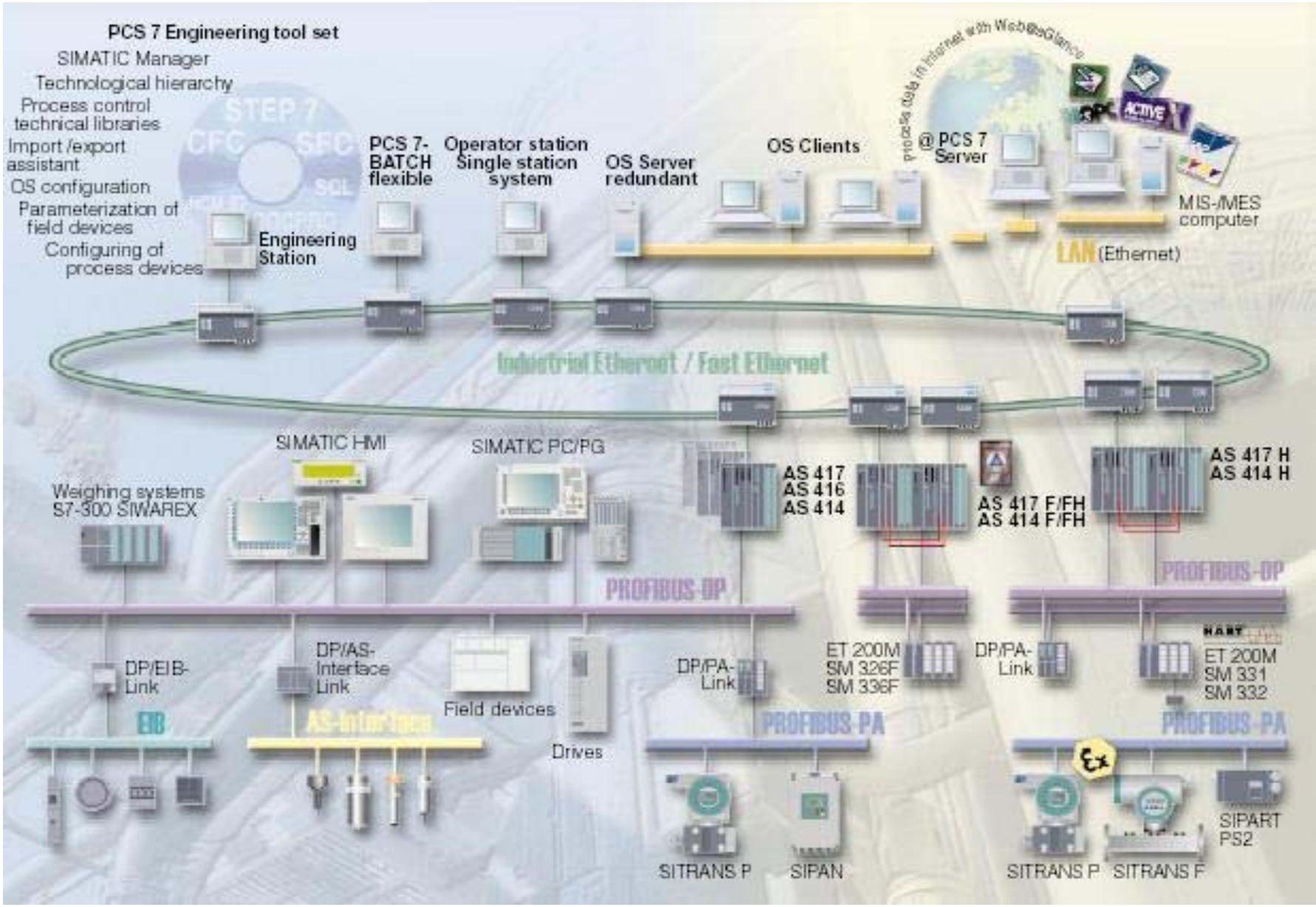


FIG. 106. SINEC NETWORK CONCEPT


PCS 7 Engineering tool set
SIMATIC Manager
Technological hierarchy
Process control technical libraries
Import /export assistant
OS configuration
Parameterization of field devices
Configuring of process devices
Engineering Station
PCS 7-BATCH flexible
Operator station Single station system
OS Server redundant
OS Clients
@ PCS 7 Server
MIS-/MES computer
LAN (Ethernet)
Industrial Ethernet / Fast Ethernet
SIMATIC HMI
SIMATIC PC/PG
Weighing systems S7-300 SIWAREX
AS 417
AS 416
AS 414
AS 417 F/FH
AS 414 F/FH
AS 417 H
AS 414 H
PROFIBUS-DP
DP/EIB-Link
DP/AS-Interface Link
Field devices
Drives
DP/PA-Link
ET 200M
SM 326F
SM 336F
DP/PA-Link
ET 200M
SM 331
SM 332
HART
PROFIBUS-PA
PROFIBUS-PA
SITRANS P
SIPAN
SITRANS P
SITRANS F
SIPART PS2

1.6. Case study: Siemens Industrial Communication Networks - SINEC

1.6.1. K/n: Địa chỉ ứng dụng:

Lĩnh vực tự động hóa trong sản xuất, công nghiệp:

- Automobile industry,
- Chemical industry,
- Power generation,
- Food industry,
- Paper industry,
- Transportation systems,
- Water and sewage treatment,
- Mechanical engineering ...

1.6. Case study: Siemens Industrial Communication Networks - SINEC

1.6.2. Cấu trúc:

1.6.2.1. SINEC H3: *Top speed at top level*

- Backbone network based on the FDDI standard, có thẻ trao đổi thông tin với các mạng khác ở xa, bảo mật và chống nhiễu tốt.
- FDDI: Fiber distributed data interface - chuẩn ISO 9314
- 100Mbps, ring upto 100 km
- Double ring redundancy,
- 500 network nodes,

1.6.2.2. SINEC H1:*Accepted basis at the Field Level*

- Ethernet Based Industrial Standard:
  - Triaxial/ Twisted pair/ Optic Cable
  - 1024 Nodes, 4.3 km Optical, 1.5km Electrical
  - IEEE 802.3, 10/100Mbps
- MAP/MMS (Manufacturing Automation Protocol/Message Specification) over Ethernet,
- Access Modes: CSMA/CD (CarrierSenseMultipleAccess/CollisionDectection)
- Dùng để ghép nối với nhiều thiết bị: PLC hay PG/PC. Có 2 Options để lựa chọn phù hợp:
  - SINEC H1-MAP:Phù hợp với chuẩn quốc tế MMS User Interface - ISO 9506, được dùng rộng rãi, đặc biệt công nghiệp chế tạo Ôtô
  - SINEC H1-TF (Technological Function):
  - Cung cấp TF dùng các dịch vụ MMS dựa trên AP (Automation Protocol - Siemens)

- Được chấp nhận và dùng nhiều ở châu Âu. Kết nối với SIMATIC, H1-TF có các dịch vụ đơn giản nhằm tối ưu hóa thông lượng cho hệ thống.
- Dùng được nhiều giao thức trên mạng này: Novell, TCP/IP có thể chạy song song với các ứng dụng SINEC H1.
- Với module interface của SINEC H1, có thể dùng nhiều protocols đồng thời trên mạng, có sự chuyển đổi (transition) đơn giản giữa mạng sản xuất và mạng hành chính trong Cty.

1.6.2.3. SINEC L2: *Communication at Field Level*

- Siemens Profibus, 127 nodes, 23.8/9.6 km - Optic/electrical
- So sánh Fieldbus với kiểu Point to Point
- Các đặc điểm chính:
  - Dải rộng các thiết bị và các ứng dụng
  - Đã dược chuẩn hóa theo các chuẩn của DIN, ISO và các tổ chức Qtế khác.
  - Giảm chi phí lắp đặt và vận hành

- Nhiều nhà sản xuất/ khách hàng đã dùng nên dễ dàng lực chọn và thờin gian ngắn.
- PROFIBUS là chuẩn bus đầu tiên đáp ứng được các y/c trên đây - chuẩn DIN 19 245.
- Giao tiếp tốc độ cao với các thiết bị tại hiện trường (các Distributed I/O Stations/ devices), 9.6 - 1500 kbps
- Topology: Line, Tree, Star, ring
- Access Mode: Token passing underlying Master/Slave
- Protocols:
  - SINEC L2-FMS - Fieldbus Mesage Specification:Cấp các dịch vụ người dùng có cấu trúc (giống như MMS) cho các các modules - như SIMATIC PLCs hay PCs (10 đến 15)
  - SINEC L2-DP - Distributed IOs: Là Giao diện người dùng để nối các thiết bị (ET200 Station, Valves...)
  - SINEC L2-TF và SINEC L2-S7
- Kết nối đơn giản giữa các PLCs trong hệ SIMATIC
- Có thể dùng cáp điện hoặc cáp quang

1.6.2.4. SINEC S1 (AS-i): *Communication at Field Level*

- Của nhiều Hãng, thành chuẩn quốc tế IEC TG 17B
- Nối trực tiếp giữa các sensor, cơ cấu chấp hành đơn giản với PLC/PG/PCs
- Lượng tin tức nhỏ với các lệnh ON/OFF...
- 100m, có thể dùng chung cáp tín hiệu và nguồn cung cấp, cáp thường
- Access Mode: Master/Slave
- 5ms for 31 slaves - line/ tree

Chapter 2

Industrial Communications and Networking

- Giới thiệu một số mô hình/chuẩn truyền tin trong công nghiệp:
- Chuẩn truyền tin V24/V28 (RS-232C, RS-485 và RS-422), I2C...
- Các bus tiêu biểu: Profibus, CAN, Modbus, AS-I…
- Các giao thức: ProfiBus, MODBUS và IEC 870-5

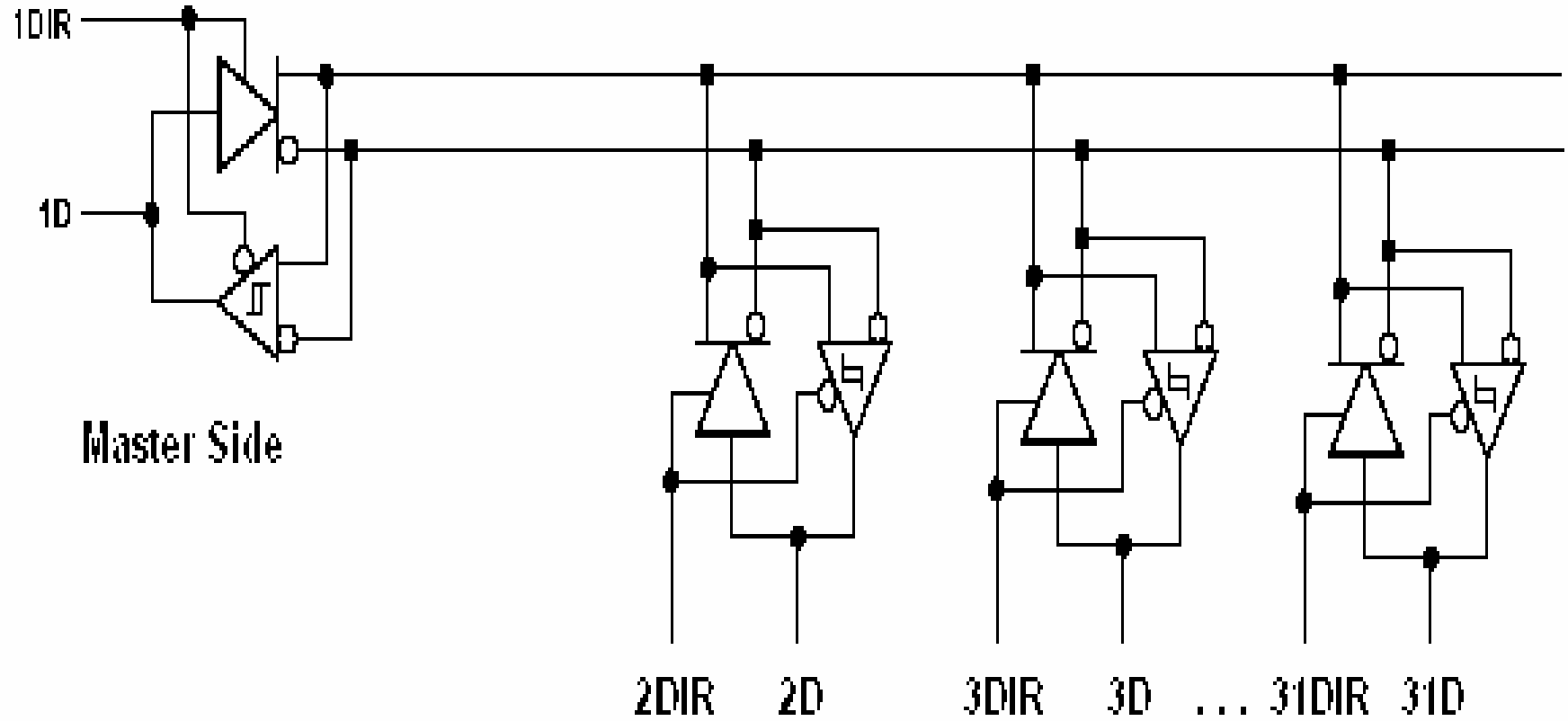
2.1. Khái niệm về truyền tin trong môi trường công nghiệp (TTCN):

- Khái niệm:
  - Là mạng máy tính với số nodes và phạm vi địa lý hạn chế, thông tin trên mạng là các số đo, các trạng thái và các lệnh điều khiển, gắn với các quá trình thực, với độ tin cậy cao, khả năng chịu nhiễu tốt
  - Có khả năng kết nối với các mạng máy tính thông thường để khai thác được các đặc tính ưu việt về remote và database.
  - Topologies: Daisy chain, Ring, Bus, Star, Tree

- Giao thức: (Kỹ thuật ghép nối) thường dùng các giao thức các tầng phía thiết bị (Transport Oriented Protocols)
- Bảo toàn thông tin – trong mô hình OSI, lớp 2:
  - Phân loại lỗi:
    - Lỗi không phát hiện được
    - Phát hiện được nhưng không sửa được và
    - Phát hiện và sửa được
  - Phân tích và đánh giá lỗi: Chech sum, CRC, Parity...
  - Đánh giá theo:
    - Xác xuất xuất hiện,
    - Thời gian xuất hiện,
    - Theo điều kiện môi trường,
    - Theo tác động của đối tượng...

- Parity: cho từng byte/character
- Parity kép: cho 1 packet. Tính Parity và XOR dọc theo gói tin => phát hiện lỗi và sửa lỗi nếu xác suất nhỏ
- CRC: phần cứng, vi mạch
- Check sum: phần mềm

- Các chuẩn truyền thông tin:
  - TIA/EIA (Electronics/Telecommunication Industry Association), mô hình DTE và DCE, các chuẩn qui định vật lý của tín hiệu như:
    - Complete Interface Standards: TIA/EIA 232-F, TIA/EIA 530-A [561]...
    - Electrical Only Standards: EIA 422, EIA 485...
    - Signal Quality Standards…
- Tín hiệu:
  - Single End, RS232
  - Differential, RS 422/485, MultiDrop, Hình 201

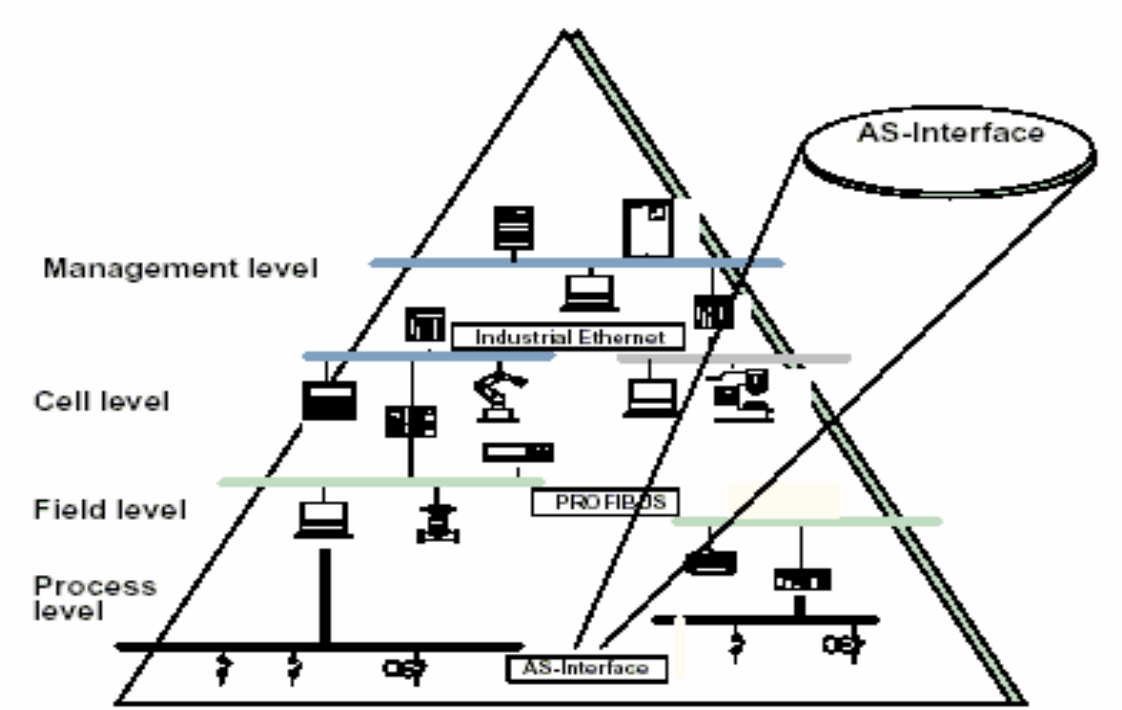


Hình 201. Mạng RS 485 với các drivers/receivers

2.2. Standard Buses:

2.2.1. AS-i bus:

- Actuator Sensor Interface
- Các (11) hãng Châu Âu hợp tác phát triển



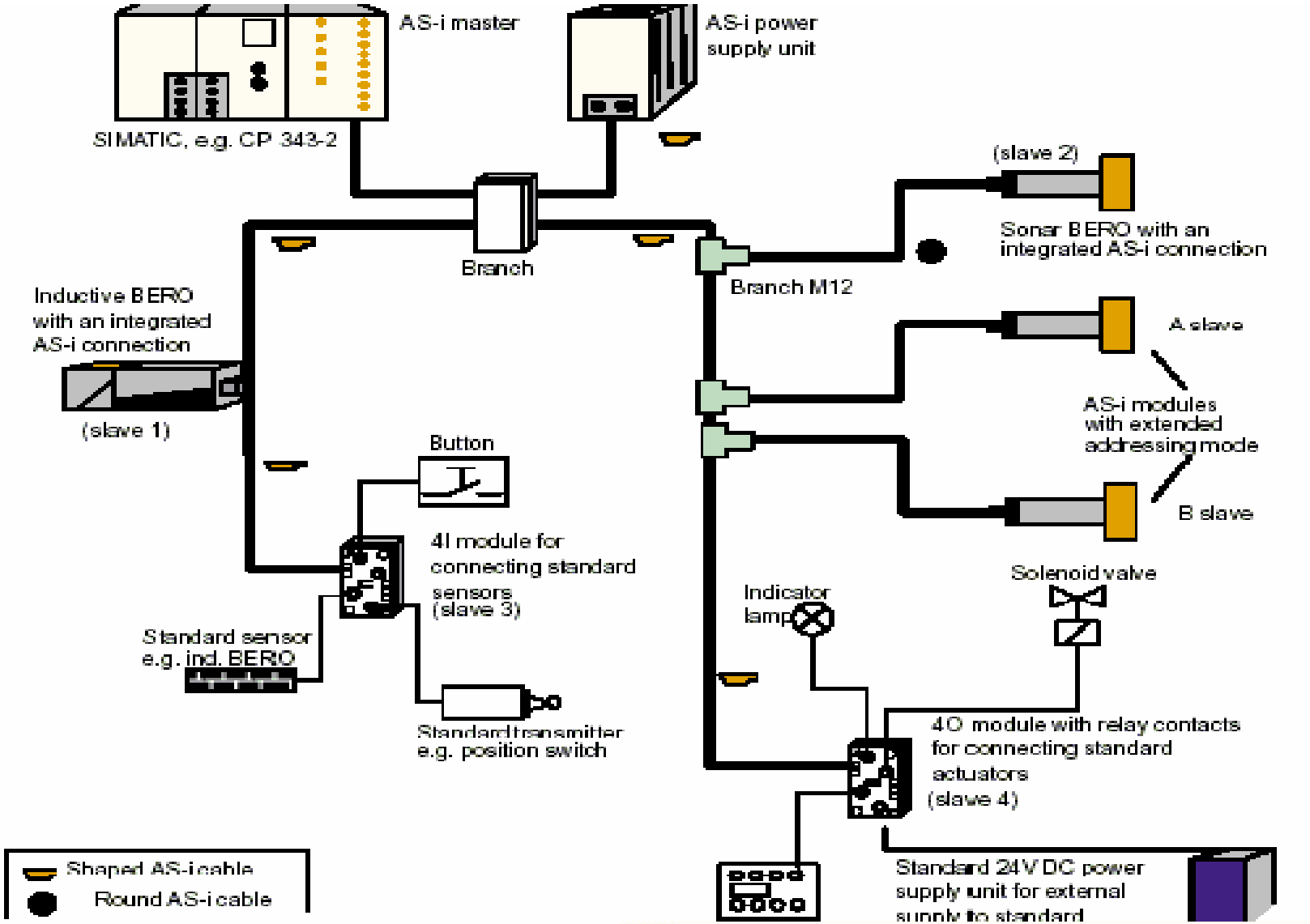
Hình 202. Ví trí AS-I bus trong hệ thống mạng CN

2.2.1.1. Khái niệm mạng AS-i:

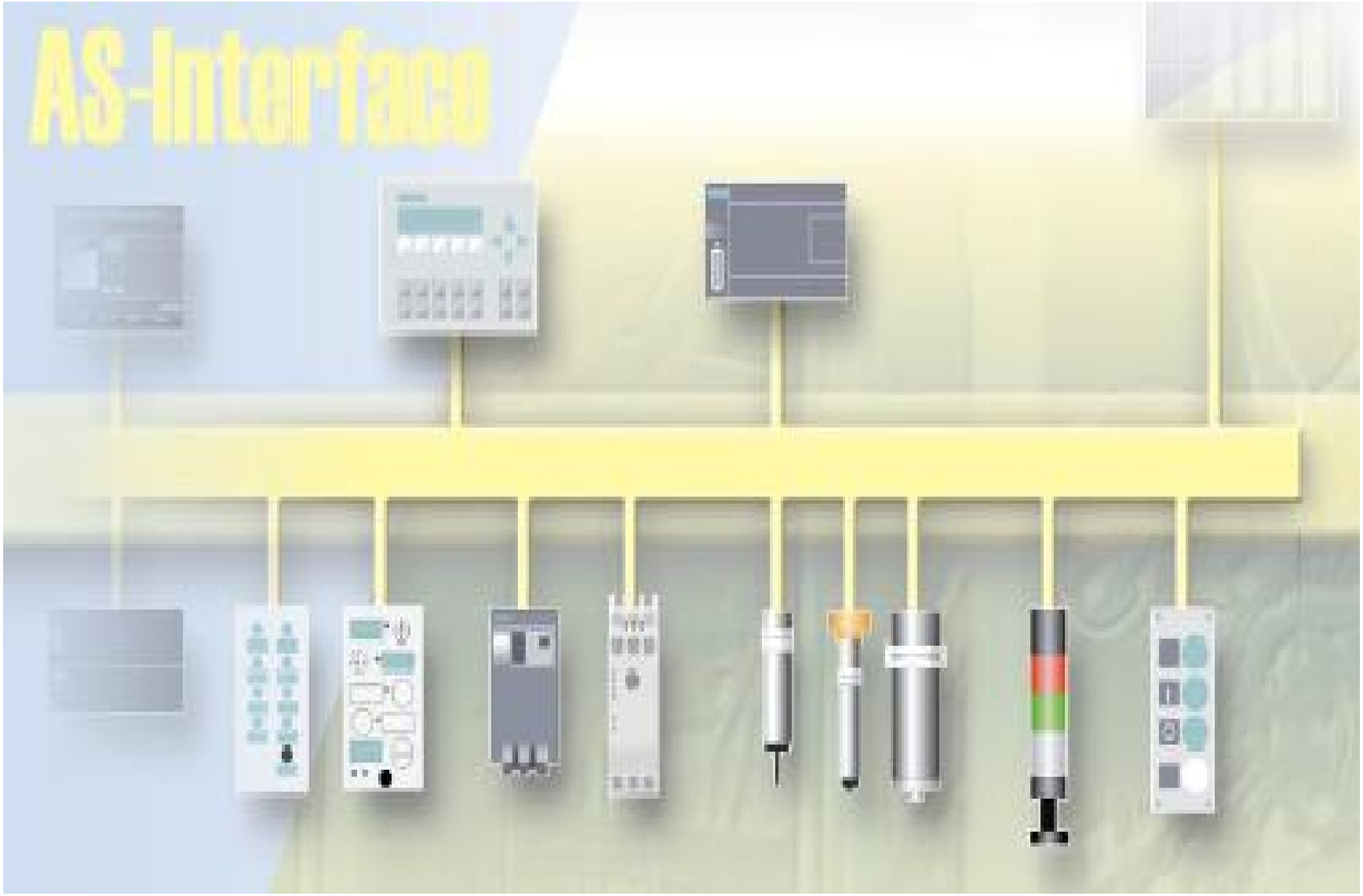
- AS-i (Actuator/Sensor Interface) là giao diện kết nối các cảm biến và cơ cấu chấp hành ở tầng thấp nhất (field level) trong một hệ thống tự động.

2.2.1.2. Hoạt động của hệ thống mạng AS-i:

- Kiến trúc và các thông số hoạt động của mạng
  - ***AS-i*** *Mạng AS-i là mạng Single Master/ Multi Slaves*: Trong mạng AS-i chỉ có một master việc trao đổi dữ liệu với các slaves trong mạng, thông qua cơ chế polling các slave liên tiếp và chờ đợi trả lời.
  - *Topology của mạng*: Mạng AS-i có thể có dạng đường thẳng, hoặc dạng cây.



Hình 202a. Cấu trúc một mạng AS-i



Hình 203. Cấu trúc mạng AS-i

- *Thời gian vòng quét*: AS-i Master cần 5ms để trao đổi dữ liệu số với 31 nút mạng - polling, analog (12 bit sensor) cần 6 vòng quét - 30ms.
- *Tốc độ truyền thông*: Fixed 167Kbps
- *Thành phần nút mạng*: Mỗi nút mạng có thể là các sensor/actuator theo chuẩn AS-i, hoặc các AS-i I/O module cho phép kết nối nhiều nhất với 4 sensor/actuator nhị phân
- *Khoảng cách mạng*: Độ dài cáp truyền trong mạng AS-i là không lớn, khoảng cách tối đa 300m, với 2 repeater max. Lượng thông tin nhị phân không lớn.

- Chế độ địa chỉ:
  - Chế độ địa chỉ thông thường, 1 Master có thể quản lý 31 slaves (4I/4O), cho phép kết nối với 124 sensors/actuators.
  - Chế độ mở rộng (A/B), một master có thể quản lý 62 slaves (4I/3O), kết nối được với 186 actuator hoặc 248 sensor.
  - *Mỗi slave AS-i được gán một địa chỉ*, lưu trong EPROM của slave đó. Địa chỉ có thể được đặt do AS-i Master hoặc dùng một thiết bị đặt địa chỉ chuyên dụng (mỗi slave chỉ có thể được đặt địa chỉ 15 lần)

- Cơ chế giao tiếp:
  - AS-i hoạt động kiểu Master/Slave. Trong một chu kì quét bus, Master thực hiện trao đổi dữ liệu với mỗi slave một lần.
  - Master gửi message 14 bit (5 bit địa chỉ Slave và 5 bit thông tin - dữ liệu output hoặc mã gọi hàm), rồi chờ đợi slave trả lời.
  - Message trả lời của slave 7 bit [4 bit thông tin (dữ liệu đầu vào hoặc kết quả thực hiện hàm)].
  - Thời gian một chu kì bus phụ thuộc vào số lượng slave.
  - Master có thể gửi kèm một số thông báo khác. Có tất cả 9 loại messge,
    - 2 loại để truyền dữ liệu và tham số,
    - 2 loại để đặt địa chỉ cho slave,
    - 5 loại để nhận dạng và xác định trạng thái hoạt động của các slave.

- Cấu trúc message từ Master
  - 0-CB-A4-A3-A2-A1-A0-I4-I3-I2-I1-I0-P-1
    - Bit 0: đầu Message Bit 1: cuối Message
    - CB: Bit điều khiển P: Bit Parity
    - A4-A0: Slave Addr I4 - I0:to Slave
- Cấu trúc message của slave:
  - 0-S3-S2-S1-S0-P-1
    - Bit 0: đầu Mess. Bit 1: cuối Mess.
    - Bit S3-S0: to Master P: Bit Parity
- Kỹ thuật truyền:
  - Kỹ thuật mã hoá chọn dải tần số truyền, tự đồng bộ theo cơ chế APM (Alternate Pulse Modulation) cho phép loại nhiễu => có độ tin cậy cao.

- Kiểm soát lỗi:
  - Trong 1 chu kì bit 6μs (chu kì bus 5ms), tín hiệu trên đường truyền được receiver senses 16 lần. Theo phương pháp điều chế APM đã nói, trong mỗi chu kì bit phải có một hoặc hai xung và các xung kế tiếp phải đảo chiều. Như vậy chỉ có các tín hiệu có dạng này mới được nhận và giải mã, ngược lại sẽ được coi là nhiễu và sẽ bị loại bỏ.
  - Mỗi Mess. chiều dài cố định, có bit đầu, bit cuối và có khoảng thời gian nghỉ, => phát hiện tín hiệu sai lệch. Ngoài ra, các bit truyền còn có bit chẵn lẻ parity để phát hiện lỗi.

2.2.1.3. AS-i Devices

- ***AS-i cable:***
  - Kiểu riêng, để kết nối với các thiết bị mạng, không cần tách vỏ, bắt vít hoặc hàn.
  - Truyền được cả năng lượng và số liệu trên cùng một cáp 2 dây.
  - Không truyền được trong khoảng cách xa (tối đa 100 mét cần có 1 repeater)
  - Cũng có thể dùng bất kì cáp 2 dây thông thường có kích thước 2x1.5mm2 trong mạng AS-i, không cần vỏ chống nhiễu.

- Repeater/Extender
  - Repeater/ Extender: Prolongation, max 100m. Max 300m with 2 repeaters
- Nguồn cung cấp ở cả hai đầu của repeater
- Hai đường cáp AS-i của repeater được cách ly về điện với Extender
  - Mở rộng chiều dài mạng thêm được 100m.
  - Chỉ cần nguồn cung cấp ở phía không nối với Master.
- Cáp trực tiếp: không cách ly với Extender

- Power Supply Unit:
  - Nguồn cấp dc có độ ổn định, tin cậy cao cho mọi thiết bị mạng AS-i chuẩn và các sensor nối vào mạng.
  - Normal Actuators không lấy nguồn từ AS-i cable, mà thường được cấp nguồn riêng.
- Addressing Device:
  - Là thiết bị gán địa chỉ và chẩn đoán (offline).
  - Address: 1 đến 31 (hoặc 1A đến 31A) và Ext (1B đến 31B). Các thiết bị mới xuất xưởng có địa chỉ 0.
  - Các Master hỗ trợ chế độ địa chỉ mở rộng phải nối với các slave có chế độ địa chỉ mở rộng.
  - Trên một mạng không thể có hai thiết bị có cùng địa chỉ.
- AS-i Master: Phần sau

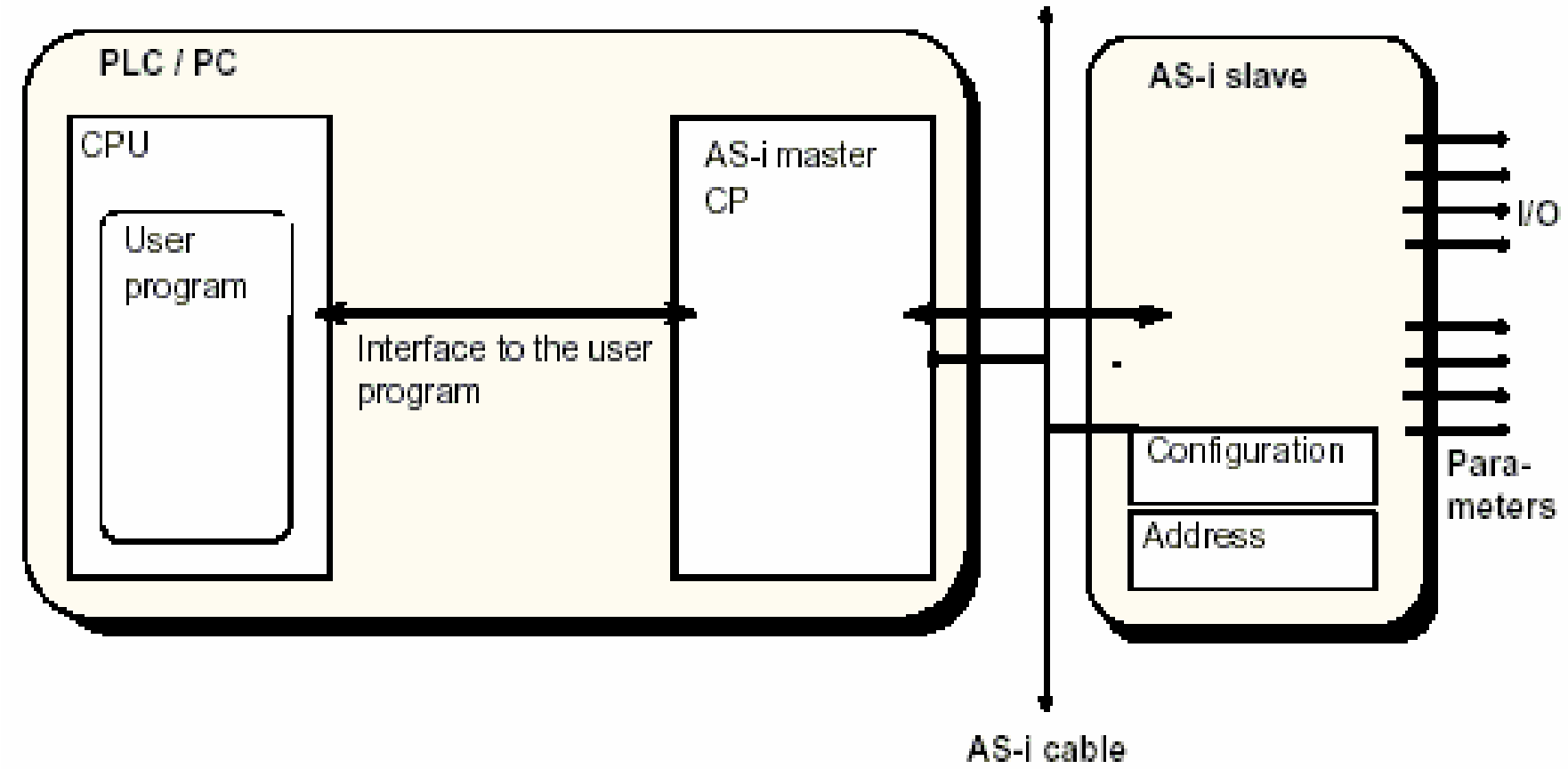
- AS-i Gateway:
  - AS-i Gateway (Distributed I/O) là các thiết bị cho phép nối mạng AS-i với các thiết bị ở mạng khác, cũng là một Master, đóng vai trò làm chủ đối với mạng AS-i bên dưới và là Slave của mạng trên (thường là PROFIBUS)
- I/O Module đặt tại hiện trường
  - Là các module ghép nối với các cơ cấu chấp hành và cảm biến nhị phân, được lắp đặt trực tiếp tại hiện trường
  - *Compact Module*: Module kết nối với các cơ cấu chấp hành và cảm biến làm việc trong môi trường khắc nghiệt

- Motor Starter và load branch:
  - Motor Starter: Thiết bị khởi động động cơ. Mọi cơ cấu động lực và kết nối mạng AS-i đều được tích hợp chỉ trong thiết bị này.
  - Load Branch: Thiết bị khởi động băng tải, được đặc trưng bởi 1 đầu vào, 2 đầu ra nối với thiết bị chấp hành.
- Proximity switch:
  - Dùng để nhận biết, đếm sản phẩm, được dùng trong các dây chuyền sản xuất. Gồm:
    - Cảm biến từ: BERO inductive proximity switch
    - Cảm biến siêu âm: Sonar-BERO ultrasonic proximity switch. Cảm biến từ và cảm biến siêu âm được dùng để phát hiện vật thể lớn với khoảng cách tương đối xa, như trong một dây chuyền rửa xe tự động...
    - Cảm biến quang: Opto-BERO photoeletric proximity switch

- Logic module LOGO:
  - Là thiết bị slave của mạng AS-i song xử lý được các phép logic, cho phép thực hiện một số quy trình tự động nhỏ, đơn giản.
- Một số thiết bị hỗ trợ như:
  - *Push button and indicator light:* Bộ nút bấm và đèn báo
  - *Counter module:* Module đếm
  - *Ground fault detection module:* Module kiểm tra lỗi nối đất
  - *Overvoltage protection module:* Module bảo vệ chống quá áp

Hình 204. Siemens LOGO!

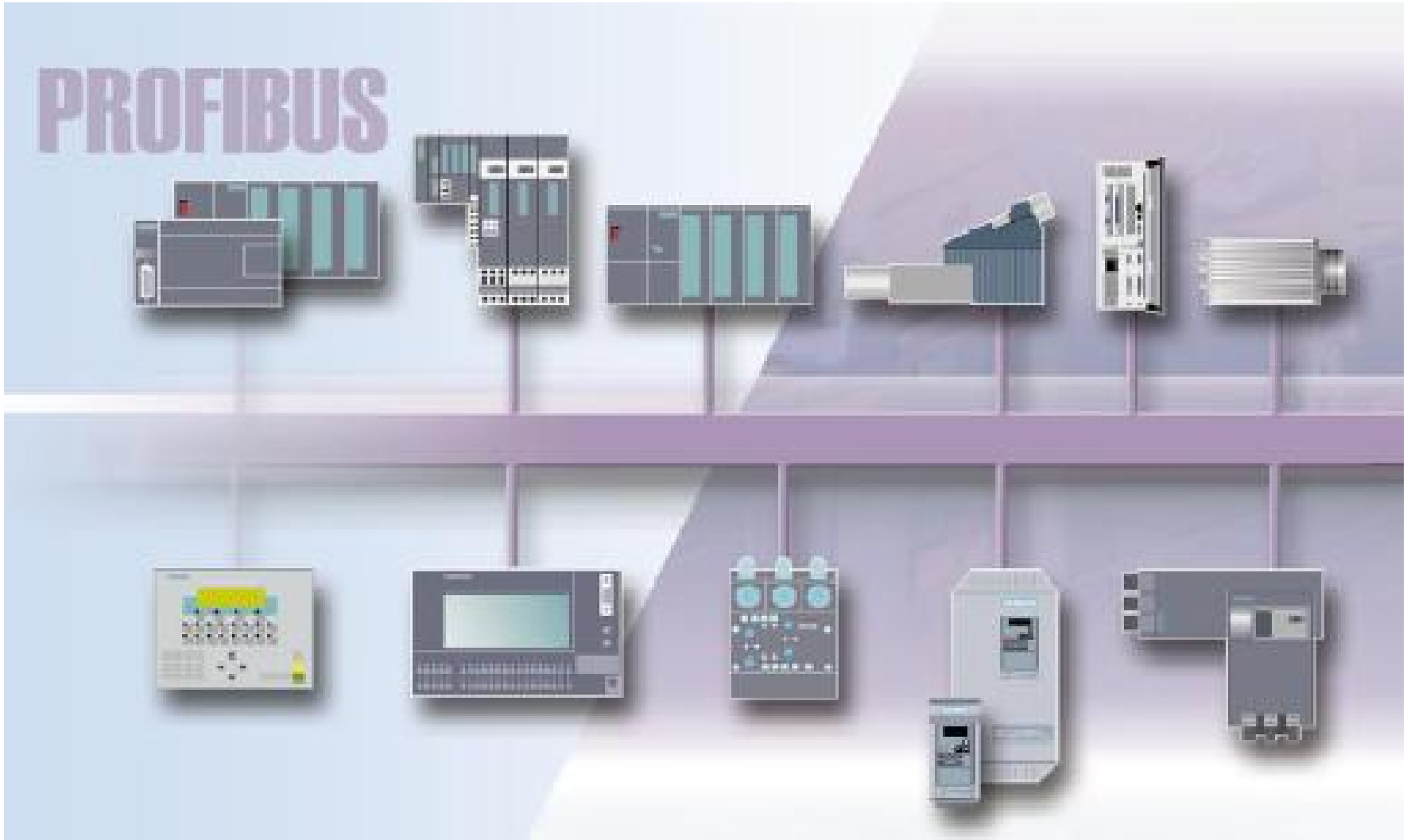
2.2.1.4. AS-i Masters:



Hình 205. AS-I Master

- Master:
  - Thiết bị truyền thông AS-i như CP243-2 (cho S7 200) và CP 342-2 (cho S7 300)
- Standard AS-i Master và Extended AS-i Master:
  - Extended AS-i Master: 62 Slave với chế độ địa chỉ mở rộng A/B, Standard AS-i Master chỉ hỗ trợ được 31 slave.
  - Nối mạng với Extended AS-i Master phải là các slave có chế độ địa chỉ mở rộng, nối mạng với Standard AS-i Master phải là các Standard Slaves.

2.2.2. Profibus:



Hình 206. Sơ đồ mạng Profibus

2.2.2.1. Khái niệm Mạng PROFIBUS:

- Mạng PROFIBUS (Process Field Bus) là mạng truyền thông tại hiện trường (cell and field area) theo chuẩn EN 50170-1-2, DIN 19245, kết nối các thiết bị vào ra phân tán (distributed I/O), các thiết bị truyền động (drives) với các bộ điều khiển khả trình, như PC hoặc SIMATIC S7.

2.2.2.2. Các giao thức PROFIBUS:

- **Bao gồm DP, PA, FMS và FDL.**

❑ *PROFIBUS DP (Decentralized Periphery)*

- Là giao diện chuẩn để trao đổi thông tin giữa trạm SIMATIC S7/M7/C7 với các thiết bị hiện trường phân tán (SIMATIC ET- 200), trong đó các DP Master và Slave trao đổi dữ liệu vào/ra ít, tốc độ cao.
- Khoảng cách truyền lớn và độ tin cậy cao.
- DP Slave: là thiết bị hiện trường tương thích với các module vào/ra được kết nối qua giao diện PROFIBUS DP (CP, IM) với bộ điều khiển trung tâm.
- Đ/v Chương trình điều khiển trung tâm, các thiết bị phân tán được đánh địa chỉ như các thiết bị trung tâm.

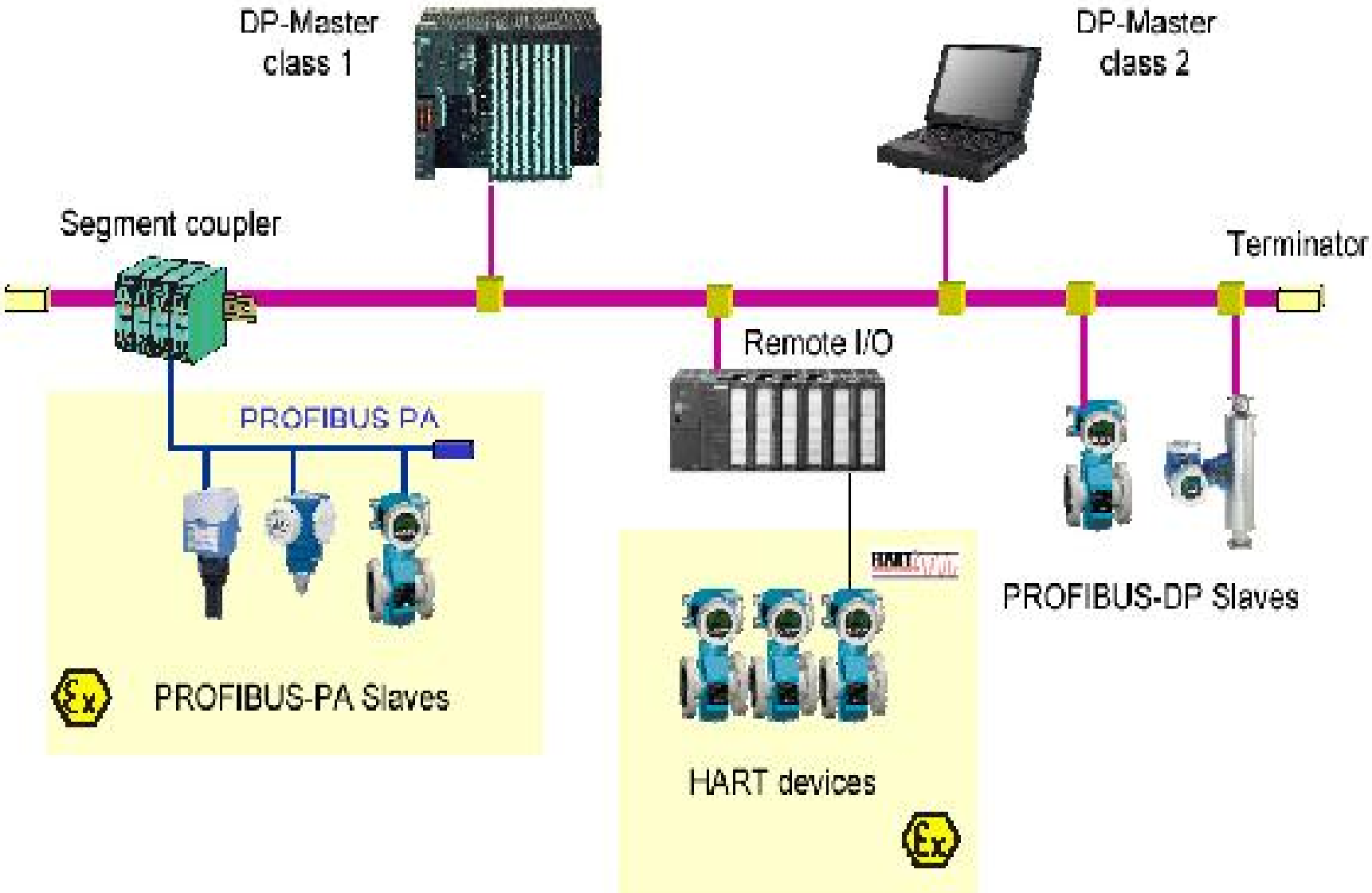
❑ *PROFIBUS PA (Process Automation)*

- IEC 61158 - 2, kết nối các thiết bị vận hành trong môi trường khắc nghiệt, đòi hỏi độ an toàn dữ liệu cao.
- Cho phép truyền dữ liệu và nguồn cấp trên cùng một đường truyền duy nhất.
- Topology: Star/ Line/ Tree.
- Tốc độ truyền: Fixed 31.25 kbps.
- Mạng PROFIBUS PA được kết nối với PROFIBUS DP qua các bộ chuyển đổi DP/PA Coupler hay DP/PA Link, trong đó DP/PA Coupler chỉ hoạt động như protocol Converter,
- Kết nối nhiều nhất 5 cơ cấu chấp hành, còn DP/PA Link hoạt động như một slave của mạng DP.

- ***ProFiBus FMS (Fieldbus Message Specification):***
  - Là giao thức chuẩn kiểu thông điệp, lượng thông tin lớn,
  - Truyền giữa các PLCs của các hãng khác nhau, trao đổi giữa SIMATIC S7/M7/C7 với PC.
  - Ưu điểm: Dữ liệu có cấu trúc được truyền đi ở một định dạng trung lập, không phụ thuộc thiết bị truyền (non-device specific format) và sau đó lại được chuyển đổi thành định dạng tương ứng thiết bị nhận (device-specific format) ở đầu kia.
  - PROFIBUS FMS và PROFIBUS DP sử dụng cùng một kĩ thuật truyền và cùng giao thức truy nhập bus, do đó có thể hoạt động đồng thời.

- ***PROFIBUS FDL (Fieldbus Data Link):***
  - Là giao thức truyền thông với các thiết bị tương thích các hệ S5 để trao đổi dữ liệu với các mạng con.

- Tổ chức mạng: dạng Master/Slave,
  - Master của mạng là các module truyền thông DP (như CP 342-5 - cho CPU S7 300)
  - Topology: Star, Tree, Line
  - Tín hiệu: vi sai, RS 485 hoặc Optic
  - Thời gian xử lý một vòng quét 1ms với tốc độ truyền là 12Mbps và 5ms với tốc độ truyền 1.5Mbps



Hình 207. Profibus

- Kết nối với mạng PROFIBUS DP qua các DP/PA Coupler hoặc DP/PA Link + Coupler (khi đó DP/PA Link là slave của mạng DP nhưng là Master của mạng PA)

- **Môi trường truyền:**
  - Cáp xoắn hai dây có bọc (trở kháng 150Ω)
  - Cáp xoắn có bọc + bảo vệ trong (đ/v PROFIBUS PA) cho môi trường khắc nghiệt, IEC 61158
  - Cáp quang: loại trừ được nhiễu điện, tổn hao năng lượng rất thấp. Cáp quang được chế tạo từ chất liệu nhựa hoặc thuỷ tinh, có thể sử dụng in/out door, khoảng cách >10km
  - Truyền không dây (InfraRed Technology): Số liệu được truyền thông qua Module ILM (Infrared Link Module) có khoảng cách truyền tối đa là 15m.

❑ Cơ chế truyền:

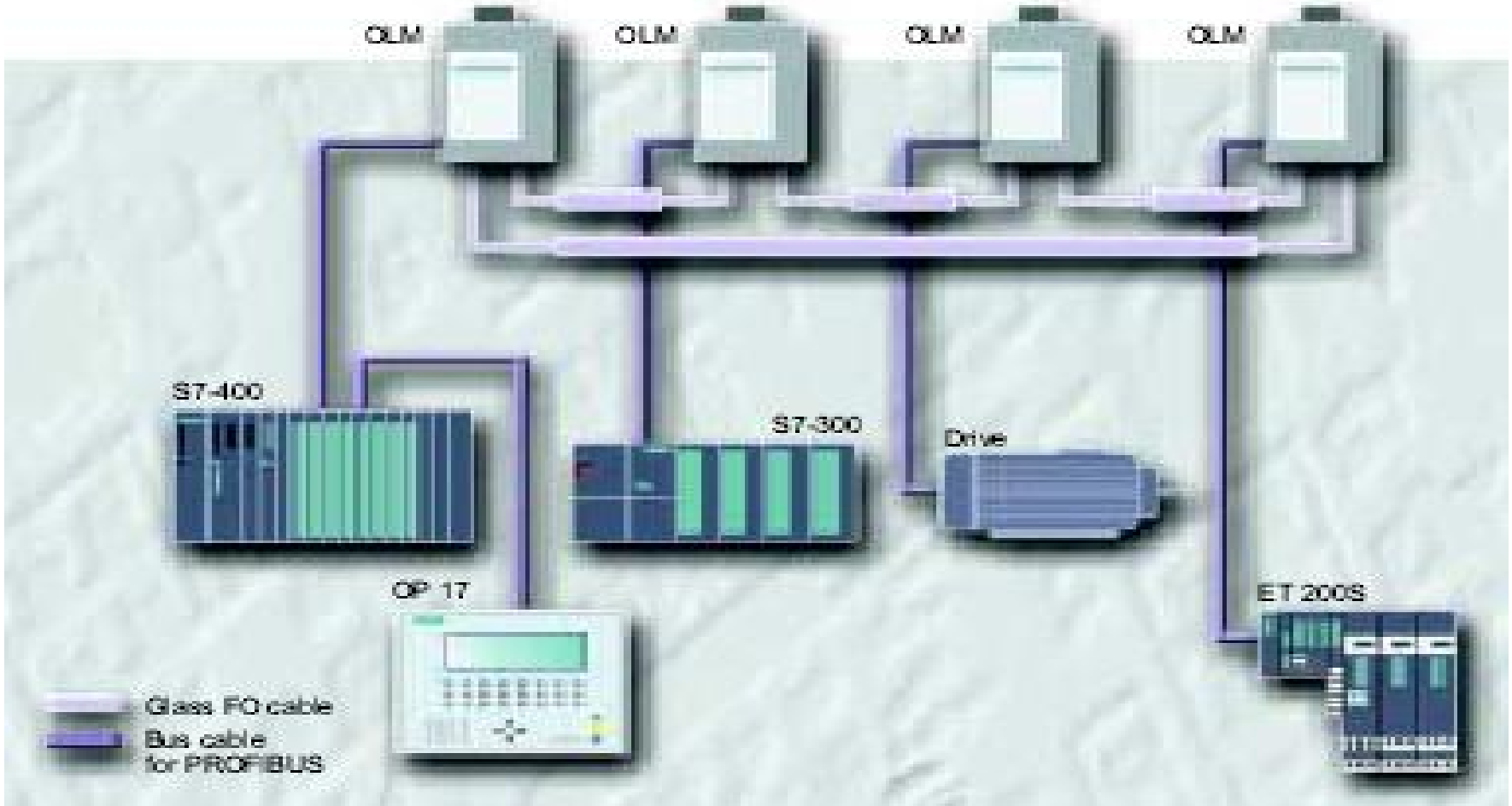
- ***Token Bus***
  - Nếu mạng nhiều active nodes (masters) tạo thành một mạng Token Ring logic với thứ tự xác định theo địa chỉ của node đó. Mỗi active node mạng tự nhận biết được các active node khác.
  - Quyền truy nhập: “Token” là một frame đặc biệt được truyền lần lượt giữa các active node trong mạng Token Ring.
  - 1 node nhận được token (được gắn địa chỉ trong token), nó có thể gửi các frame và chỉ được giữ token trong 1 khoảng thời gian xác định - token holding time) được kiểm soát bởi token timer. Khi Time Out, node mạng đó chỉ được quyền gửi đi một thông điệp dạng ưu tiên cao.

- Active node giữ token có kết nối tới các passive node để trao đổi dữ liệu với slave kiểu polling hoặc gửi dữ liệu đến slaves.
- Khi một active node nhận token mà không có yêu cầu trao đổi dữ liệu, nó chuyển token sang active node tiếp theo
- Các passive node không có token
- Các node có thể được thêm vào hay loại bỏ trong quá trình hoạt động

- ***Chế độ Master – Slave***
  - Nếu mạng có 1 active node và nhiều passive nodes, được gọi là hệ thống Master/Slave.
  - Chế độ truyền Master/Slave cho phép Master đánh địa chỉ cho Slaves.
  - Master trao đổi dữ liệu với Slave kiểu tuần tự, Master truyền xuống Slave thông số cấu hình/ các lệnh để trao đổi dữ liệu, điều khiển.
  - Slave gửi lên cho Master trạng thái, dữ liệu thu thập được và kết quả thực hiện các lệnh của Master.

2.2.2.3. Các dạng vật lý của ProFiBus:

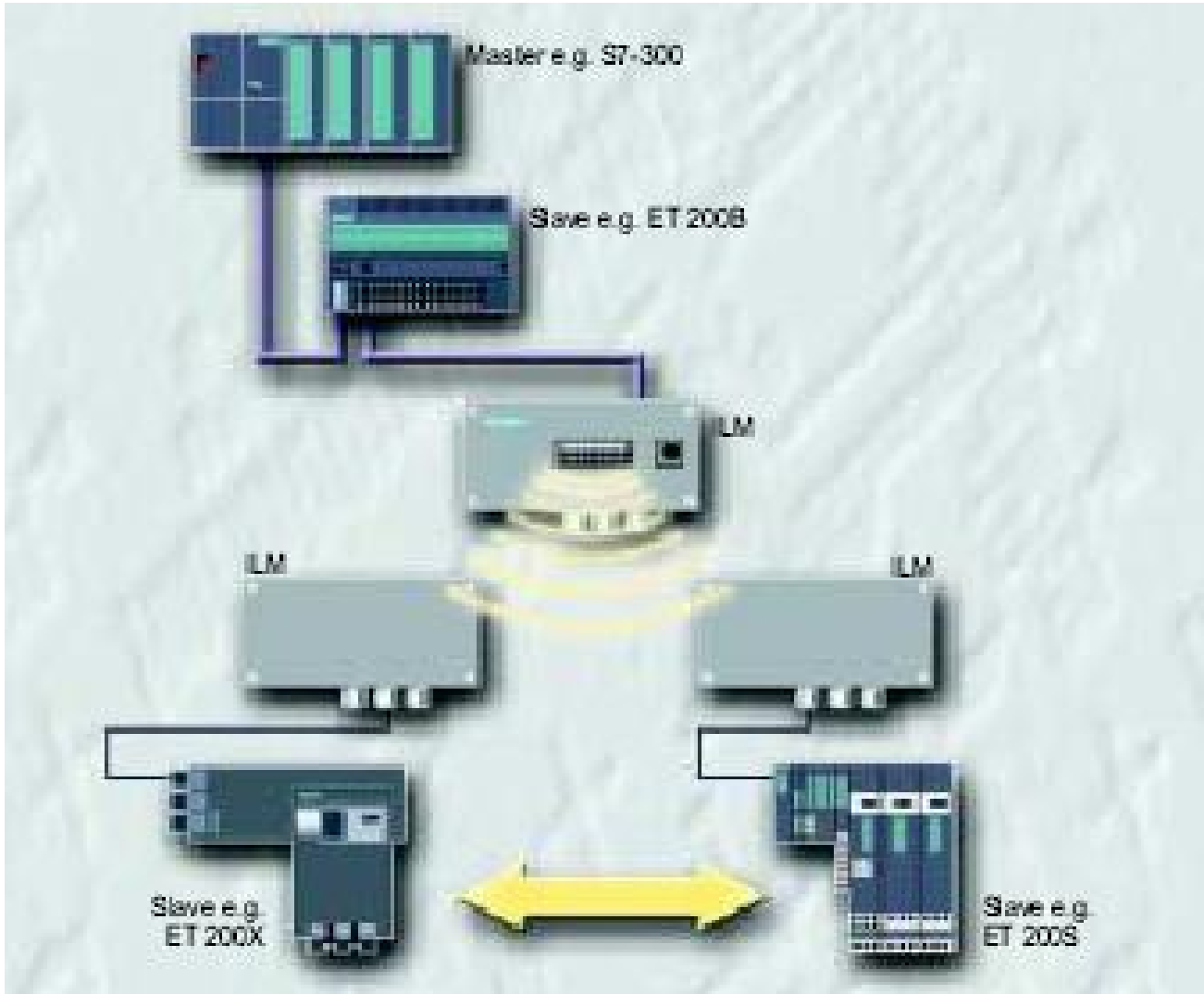
- ***Mạng cáp quang:***



Hình 208. mạng cáp quang của Profibus

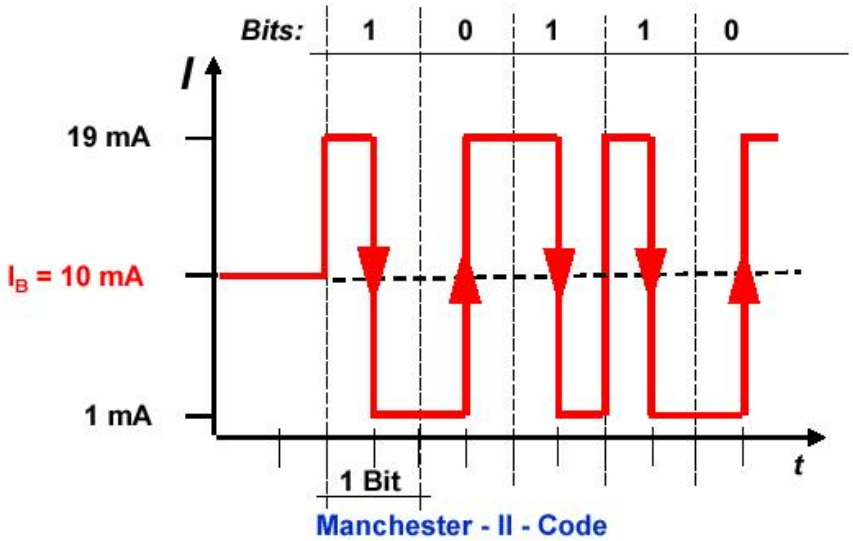
- Đặc điểm mạng cáp quang:
  - Chống được nhiễu điện - từ,
  - Thích hợp với các mạng có khoảng cách truyền lớn (khoảng cách truyền > 10km)
  - Cách ly (điện) với các thiết bị hiện trường
  - Mạng có thể có cấu trúc dạng bus, star hoặc dạng vòng
  - Tốc độ truyền từ 9.6Kbps tới 12Mbps
- Các thiết bị mạng cáp quang:
  - OBT (Optical Bus Terminal) được dùng để kết nối các thiết bị mạng hoặc các segment RS 485 không quá 31 node vào mạng cáp quang.
  - OML (Optical Link Module) cho phép thiết lập cấu hình mạng cáp quang, có 1 giao diện RS 485 và 1 hoặc 2 giao diện cáp quang.
  - Các loại cáp quang dùng cho OBT và OLM là khác nhau, có thể là cáp quang thuỷ tinh, cáp quang plastic, cáp PCF FOC, glass FOC

- *Mạng không dây:*
  - Module ILM được sử dụng để kết nối không dây các slave riêng lẻ hoặc slave segments, cho phép điều khiển và truyền thông với các thiết bị di động, max 1.5Mbps, 15m. Tia hồng ngoại dùng để truyền dữ liệu được phát trong dải +/- 10^0 so với trục thẳng.

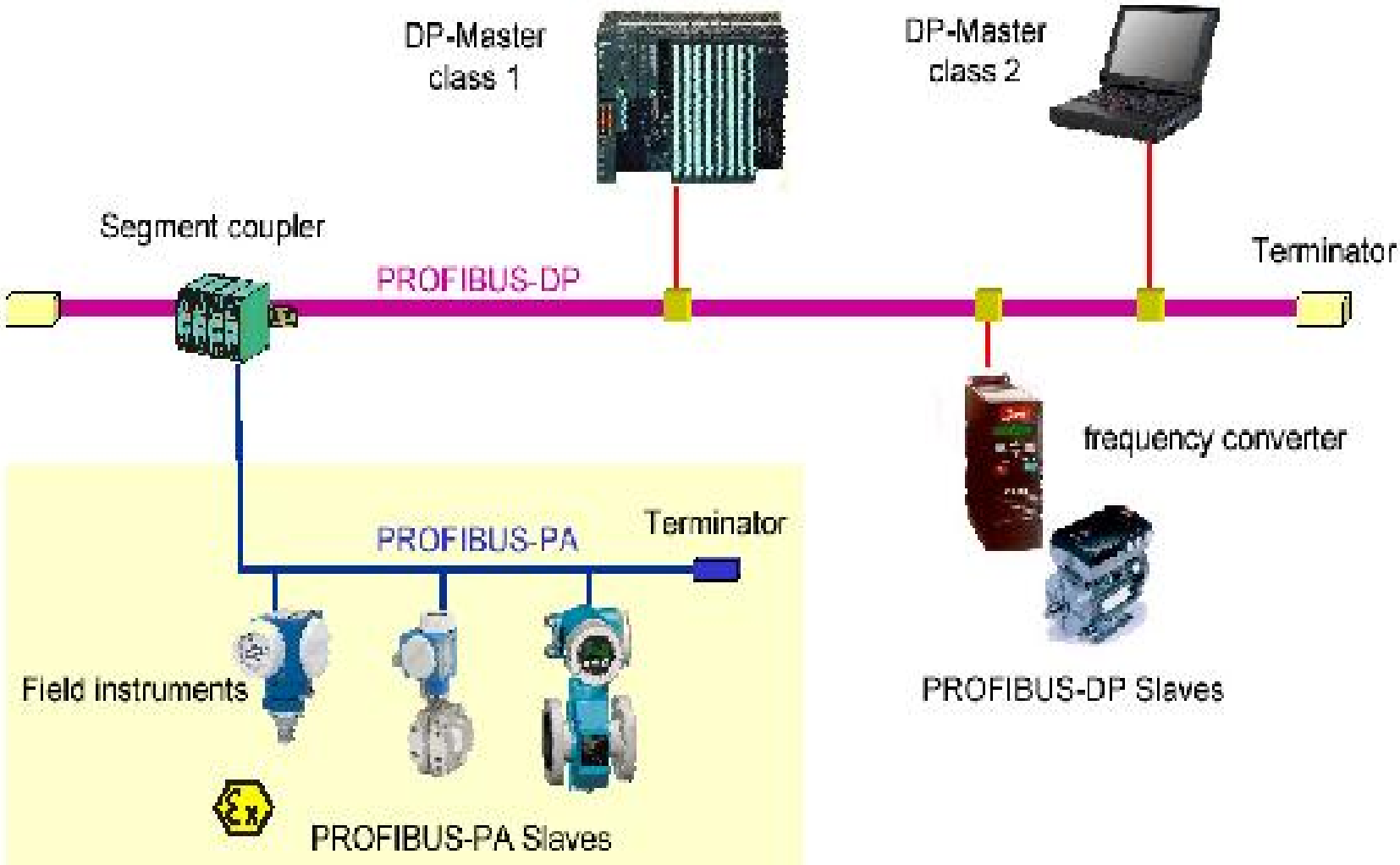


Hình 209. Wireless ProFiBus network

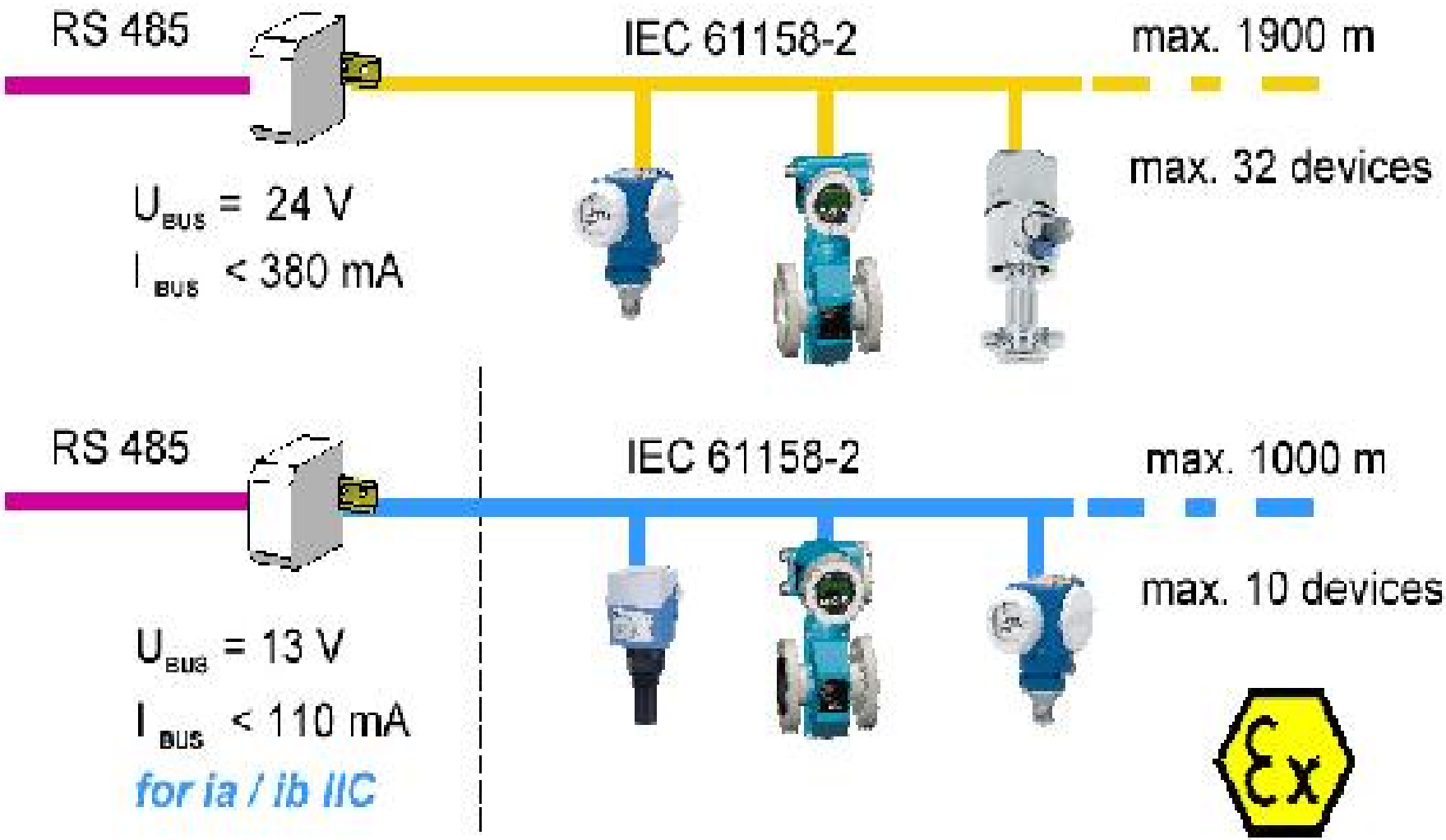
- PROFIBUS PA:
  - Tốt trong môi trường CN như bụi kim loại, n/độ axit cao, áp suất, tº cao...
  - Tốc độ truyền cố định, 31.25Kbps
  - Truyền tín hiệu và năng lượng (nguồn cấp) trên cùng một cáp 2 dây
  - Tín hiệu được mã hoá Manchester II



Hình 210. Manchester II Code



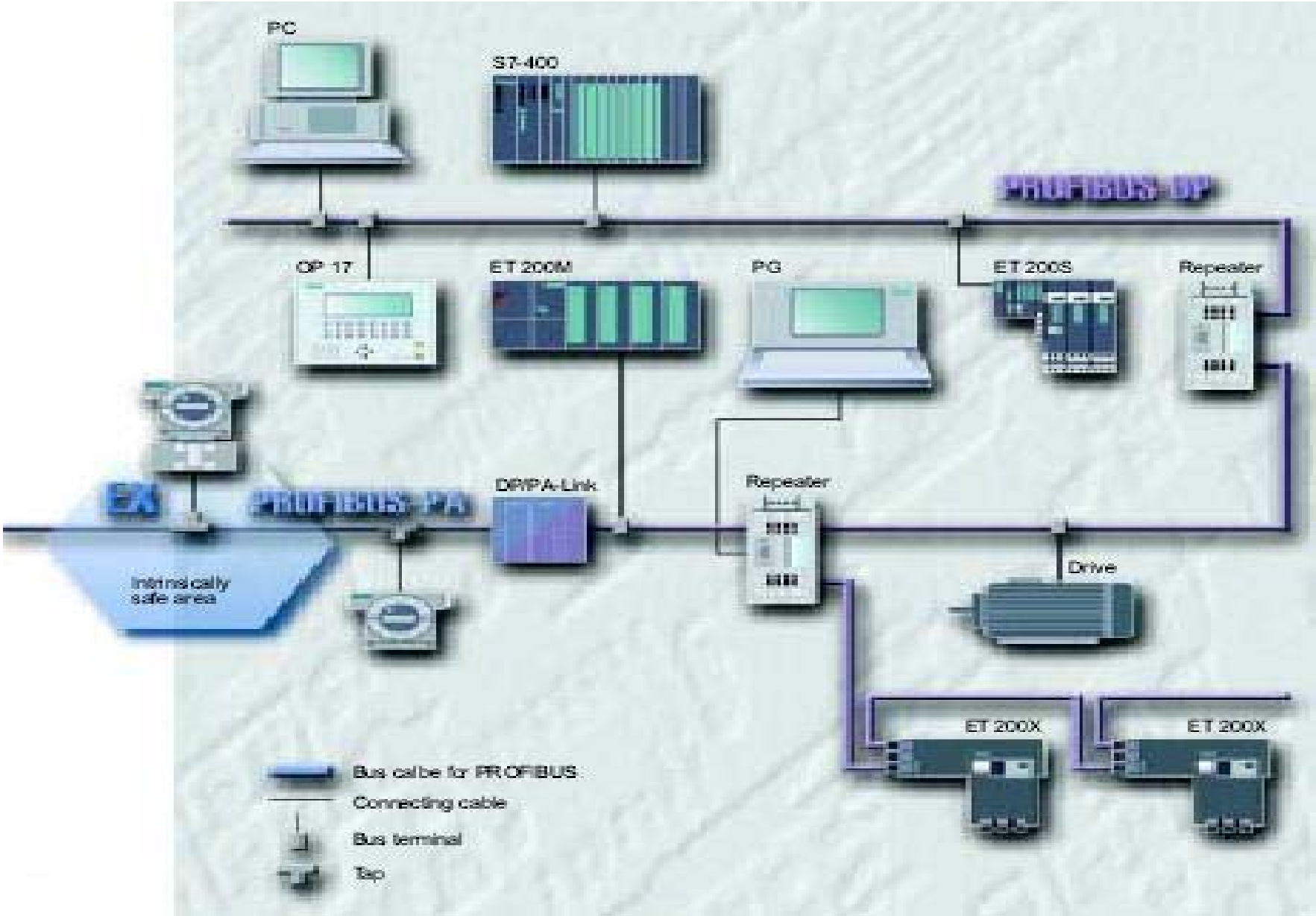
Hình 211. Profibus PA Network



Hình 212. Quan hệ Khoảng cách – U/I của PA

- Các thiết bị mạng PROFIBUS PA:
  - Nhiều loại T/b cho các ứng dụng khác nhau (w/wo Ex)
  - Cable: nhựa PVC chống cháy, điện áp trên cáp không quá 100V.
  - Split T Connector: để kết nối thiết bị slave PA vào đường PROFIBUS PA chung
  - DP/PA Link: được ghép nối với DP/PA. Tốc độ truyền thông PA: 31.25Kbps, tốc độ DP khi có DP/PA Link có thể lên tới 12Mbps.
  - 1 DP/PA Link có thể ghép nối với tối đa 5 DP/PA coupler.
  - DP/PA coupler chuyển đổi format 11bit/char (Async) => 8bit/char (Sync) và đổi tốc độ truyền.
  - DP/PA coupler cấp nguồn cho các thiết bị hiện trường và giới hạn dòng tối đa trên mạch. Môi trường nguy hiểm (Ex version) dòng giới hạn là 90mA, trong môi trường bình thường (non-Ex version) là 400mA.

- Mạng tín hiệu điện:
  - **RS 485:**
    - RS 485: tín hiệu áp vi sai, khoảng cách >1 km trên đường cáp xoắn 2 dây có vỏ bọc.
    - Cáp truyền trong mạng được chia thành các segment có trở kháng không đổi.
    - Các thiết bị được nối vào mạng (node mạng) qua bus terminal với tap line hoặc bus connector (thiết bị kết nối/giắc cắm)
    - Có tối đa 32 node mạng trên một segment.
    - Các đoạn được kết nối với nhau bởi các repeater. Có thể có tối đa 9 repeater trong một network.
    - Các cable terminator phải được cấp nguồn trước khi được kích hoạt. Bus connector và bus terminal được cấp nguồn bởi thiết bị DTE gắn vào nó, còn repeater, terminator, ILM có nguồn riêng.



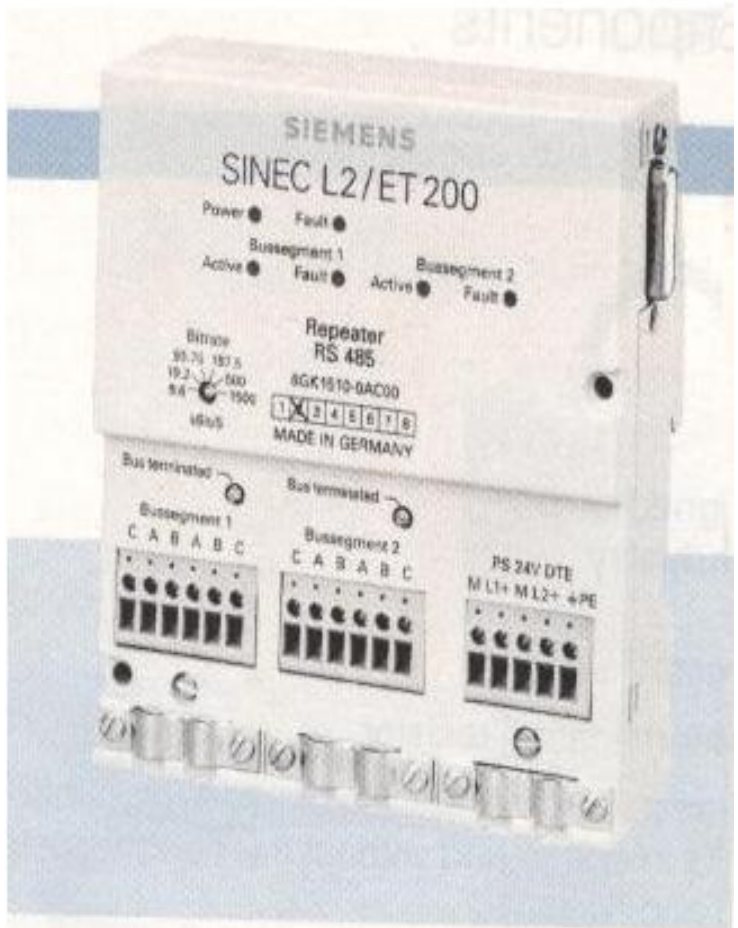
Hình 213: Sơ đồ PROFIBUS - RS 485 sử dụng repeater

- Có cấu trúc mở, linh động với các bus terminal, bus connector, repeater cho phép dễ dàng gắn các thiết bị mạng, mở rộng mạng hay thay đổi cấu hình mạng.
- Đường truyền vi sai cho phép các thiết bị có thể dừng hoạt động (deactivated) mà không hề làm ảnh hưởng đến hoạt động của mạng
- Lắp đơn giản, không cần kiến thức chuyên môn sâu
- Khoảng cách giảm, tốc độ truyền tăng lên
- Cần có thiết bị bảo vệ chống sét khi lắp đặt ngoài trời

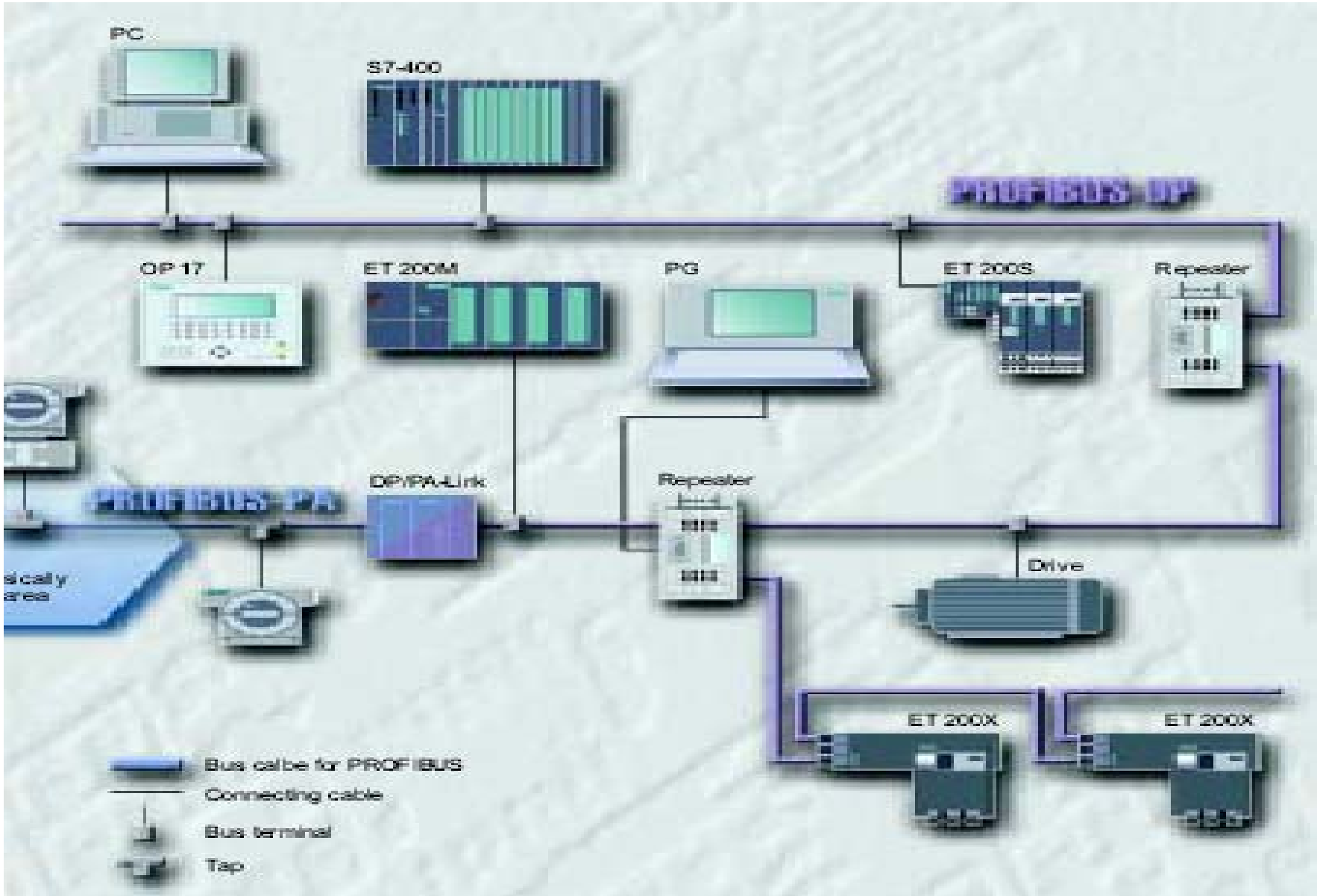
- Cấu hình mạng: Dạng bus, cấu trúc tự do, dùng repeater
- Môi trường: Cáp xoắn 2 dây có vỏ bọc
- Chiều dài mạng và tốc độ: 1000m - 187.5 Kbps
  400m – 500 Kbps
  200m – 1.5 Mbps
  100m – 12 Mbps
- Số Repeater max: 9
- Số node trong một segment max: 32
  trong một network: 127
- Tốc độ truyền: 9.6 kbps, 19.2, 45.45, 93.75, 187.5, 1.5 Mbps, 3, 6 và 12 Mbps

❑ Mạng PROFIBUS DP

- **Mô hình mạng PROFIBUS DP:**
  - ***PROFIBUS DP (Distributed I/O)*** là giao diện chuẩn để trao đổi dữ liệu vào ra giữa các trạm SIMATIC S7/M7/C7 với các thiết bị hiện trường phân tán như SIMATIC ET 200, trong đó các DP Master và DP Slave trao đổi một khối lượng nhỏ dữ liệu vào/ra một cỏch tuần tự với tốc độ cao.



Hình 213b. Simatic ET200



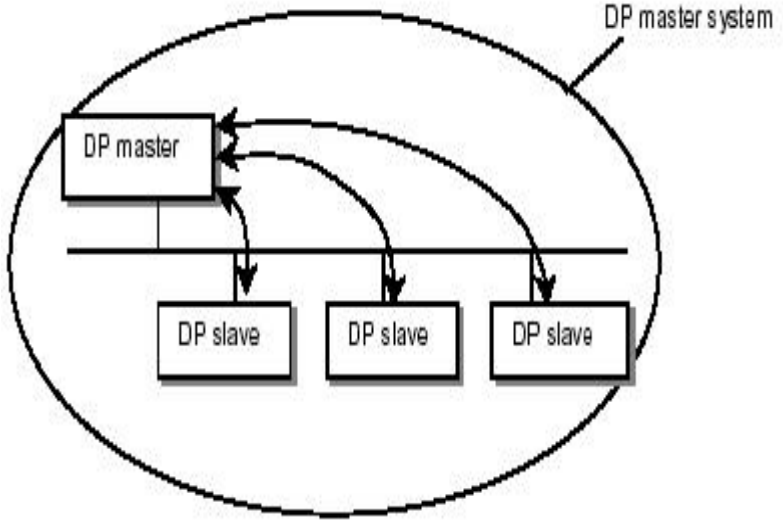
Hình 213c. Mạng Profibus DP

- **Ghép nối PLC SIMATIC S7:**
  - Chương trình ứng dụng PLC SIMATIC S7 điều khiển và kiểm soát quá trình truyền thông trên mạng PROFIBUS bằng các khối chương trình FC (cho S7-300) và SFC (cho S7-400). Các FC thực hiện các chức năng sau:
    - Chuyển dữ liệu ra từ vùng nhớ của PLC (process image, bit memory, data block) tới các thiết bị hiện trường
    - Đọc dữ liệu vào từ thiết bị hiện trường tới vùng nhớ xác định của PLC
    - Thực hiện công việc giám sát và chẩn đoán

- **Các trạm làm việc trong hệ PROFIBUS DP:**
  - DP Master (class 1): thiết bị thực hiện các tác vụ điều khiển
  - DP Slaves: các thiết bị hiện trường, nhận lệnh từ Master và gửi dữ liệu về master
  - DP Master (class 2 – tuỳ chọn): thiết bị lập trình, chuẩn đoán hoặc quản lý

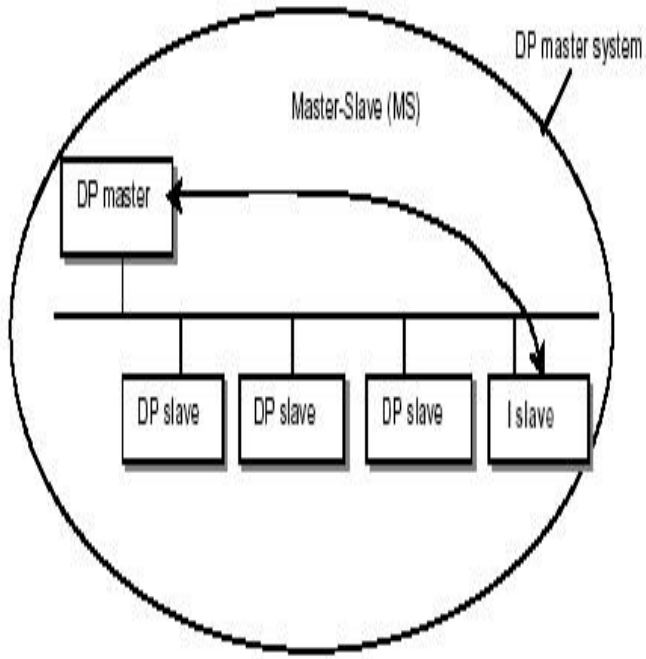
Các dạng truyền thông trong mạng DP

- *Đặt cấu hình Modular/ Compact DP Slaves* (Trao đổi dữ liệu Slave <=> Master)
  - Trong cơ chế này, DP Master polling lần lượt các slave, gửi và nhận dữ liệu với slave đó. Địa chỉ vào/ra của các slave được đánh tự động khi đặt cấu hình mạng



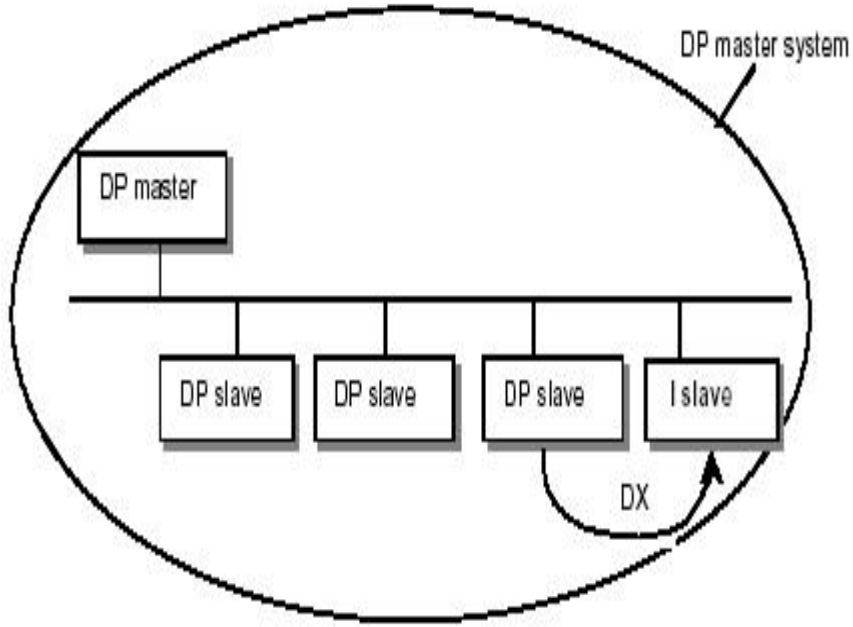
Hình 214. Trao đổi dữ liệu DP Master – Slave (a)

- *Đặt cấu hình với Intelligent DP Slave* (Trao đổi dữ liệu trực tiếp Slave <> Master)
  - I-Slave là các thiết bị có khả năng thao tác độc lập và tự xử lý số liệu với các cơ cấu chấp hành gắn với nó trước khi gửi số liệu về master (như CPU S7, Drives...).
  - Master không trực tiếp truy nhập các I/O module gắn với I-slave, mà chỉ truy nhập vào vùng địa chỉ của CPU của I-slave. Do đó, địa chỉ của các I/O module do I-slave quản lý, được đặt trong khi khai báo cấu hình mạng cho DP I-slave.



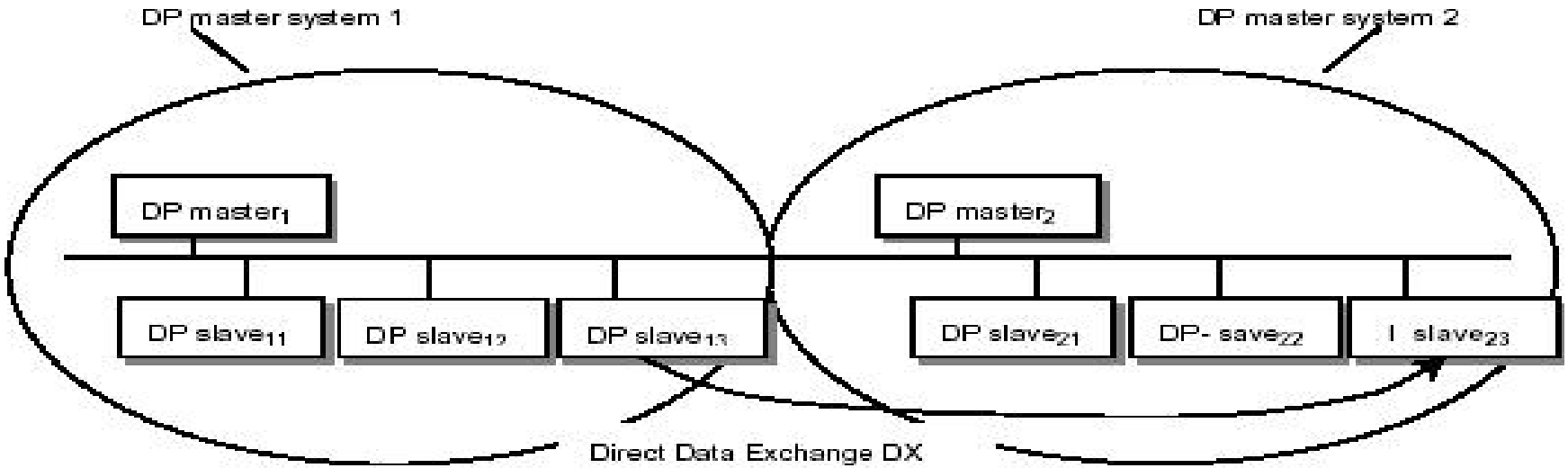
Hình 215. Trao đổi dữ liệu ISlave – Master (b)

- Trao đổi dữ liệu trực tiếp Slave > Islave
  - Các DP Slave có thể trao đổi dữ liệu trực tiếp với các Intelligent slave với tốc độ cao mà không qua master.



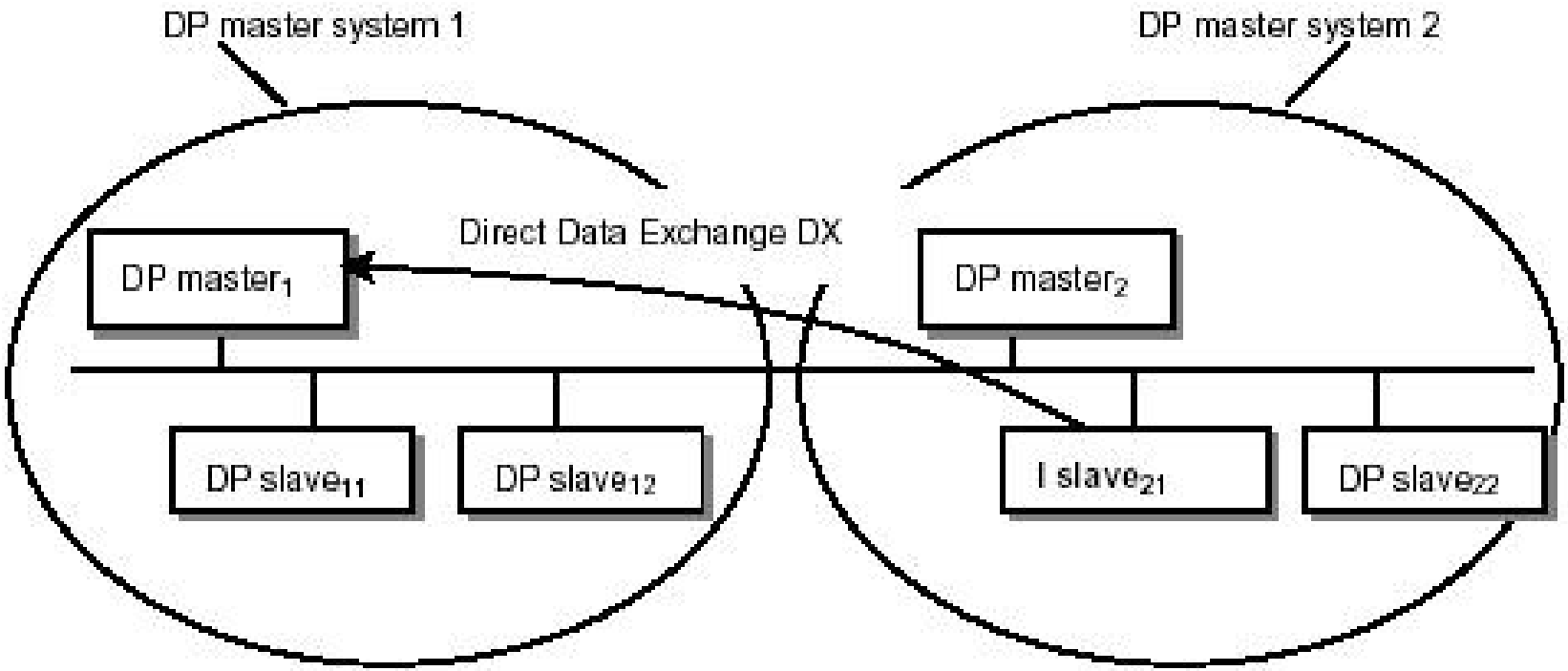
Hình 216. Trao đổi dữ liệu Slave-Islave (c)

- Trao đổi dữ liệu qua 2 trạm: trực tiếp Slave => Islave
  - Các intelligent slave có thể đọc dữ liệu từ các slave với tốc độ cao, cả các slave cùng hay khác master với i-slave đó.



Hình 217. Direct data XCGH (d)

- *Trao đổi dữ liệu giữa 2 trạm Master* (Trao đổi dữ liệu trực tiếp Slave => Master)
  - Trong chế độ này, dữ liệu từ các slave hay i-slave có thể được master này hay master khác trên cùng mạng PROFIBUS DP truy nhập.
  - Cơ chế này được gọi là " chia sẻ đầu vào" vì dữ liệu được sử dụng chéo giữa các hệ thống PROFIBUS DP.



Hình 218. Trao đổi số liệu (e)

2.2.2.4. Hoạt động của Mạng Profibus

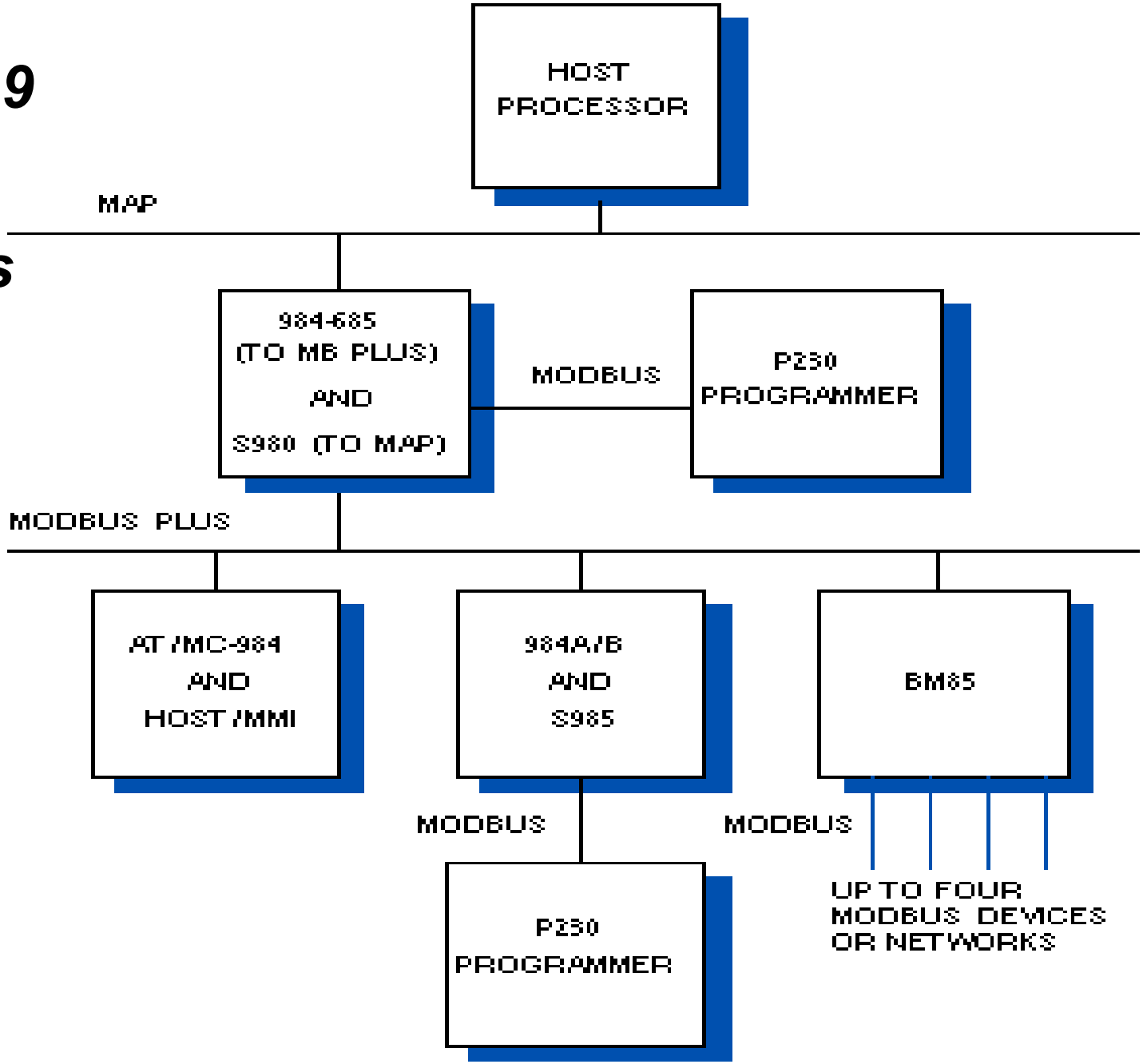
- DP Master
- Profibus CP
- DP Master và DP Slave
- CPU Cycle & DP Polling Cycle

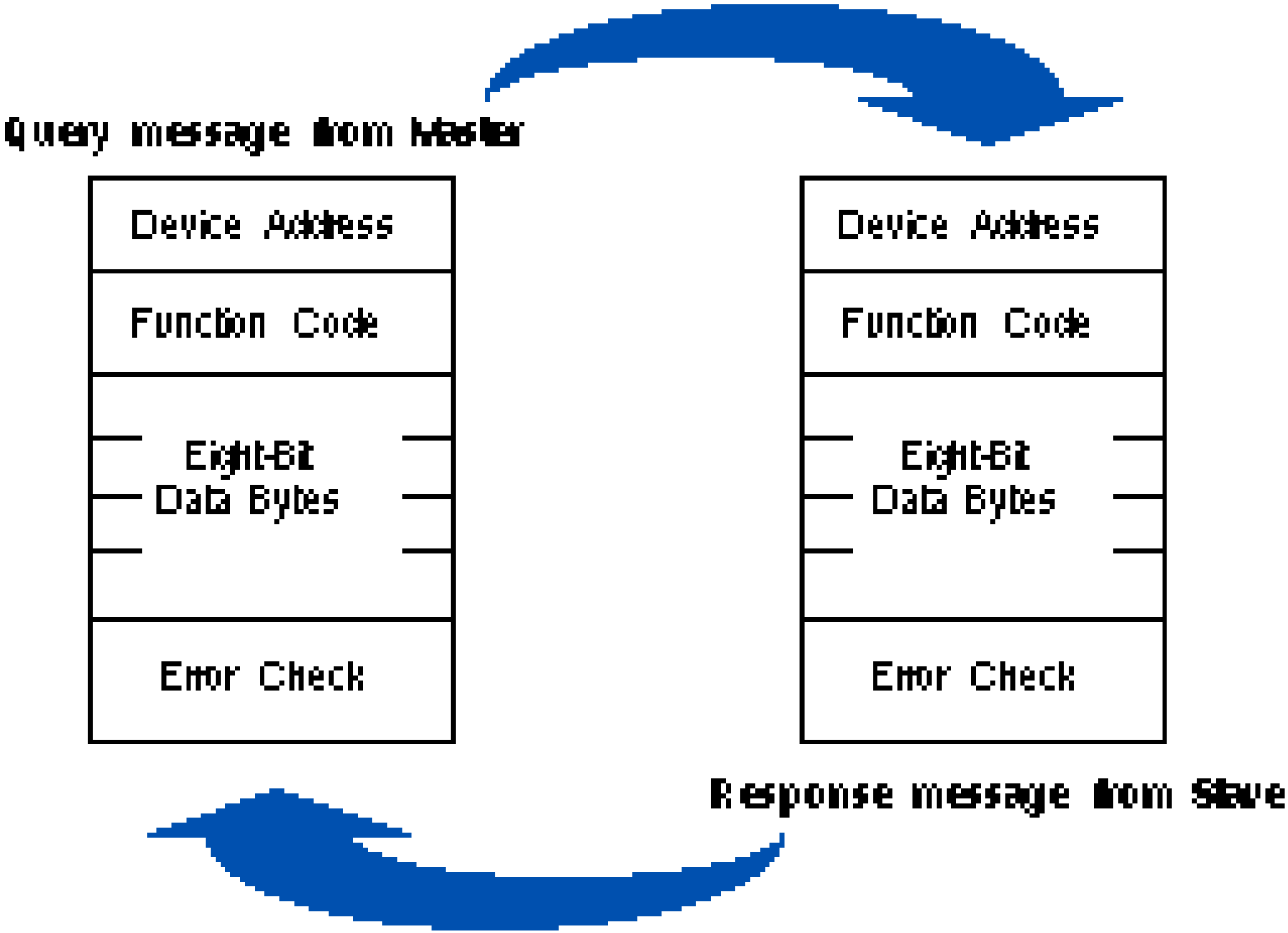
2.3. MODBUS Protocol:

- Là Giao thức chuẩn cho các đường truyền mạng cấp thấp (cả RS232/485/422) do Modicon/ AEG/ Schneider Automation
- Thường dùng trong các PLC, các computerized sensor, các drives, trong các hệ SCADA, DCS… Nhiều hãng dùng
- Có các qui ước trao đổi lệnh, dữ liệu, diagnostics
- Truyền thông mức thấp (232/485), gồm standard modbus và trên các giao thức khác: TCP/IP, MAP, …
- Master/Slave:
  - Master: Command (query message)
  - Slave: Response message

Hình 219

Sơ đồ Modbus





Hình 220. Kịch bản MODBUS

- Device Address: gồm 247 slaves, Địa chỉ 0 là Broadcast
- Function code
- 8bit data bytes, tùy số lượng
- CRC Error checking
- Characters: 7/8 bit data, PE or Non
- ASCII/ RTU modes:
  - ASCII: breaking down 1 byte = 2 ASCII characters: 7, [PE/ PO], 1[2]
  - RTU: binary character: 8,[PE/PO], 1[2]

With Parity Checking

Start	1	2	3	4	5	6	7	Par	Stop

Without Parity Checking

Start	1	2	3	4	5	6	7	Stop	Stop

With Parity Checking

Start	1	2	3	4	5	6	7	8	Par	Stop

Without Parity Checking

Start	1	2	3	4	5	6	7	8	Stop	Stop

Hình 221. MODBUS Format of Frames

- Format of packet:

Hình 222. MODBUS Packet

- ASCII format
  - Functions: Read Reg, Fetch Event-log, Diagnostic, Preset Reg…

START	ADDRESS	FUNCTION	DATA	LRC CHECK	END
1 CHAR :	2 CHARS	2 CHARS	n CHARS	2 CHARS	2 CHARS CRLF

- RTU format:
  - start: 4 space chr
  - Time out: 1,5 char time
  - End(n)⇔start(n+1)

START	ADDRESS	FUNCTION	DATA	CRC CHECK	END
T1-T2-T3-T4	8 BITS	8 BITS	n X 8 BITS	16 BITS	T1-T2-T3-T4

2.4. IEC 870-5-101 Protocol

❑ 2.4.1. Giới thiệu chung về IEC 870-5-101.

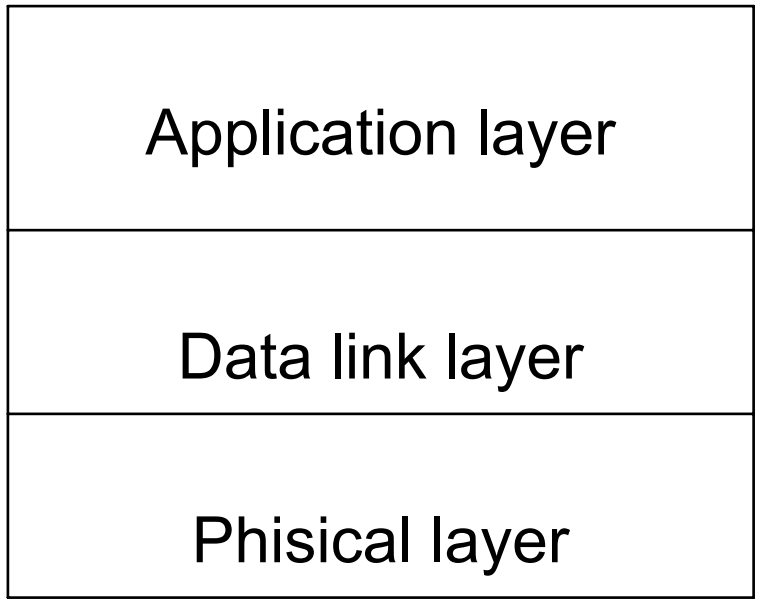
- Giao thức IEC 870-5 do tổ chức IEC (International Electrotechnical Commission)Technical Committee 57 cho các lĩnh vực telecontrol, teleprotection và telecommunication của các hệ thống năng lượng. Có 5 tài liệu đặc tả về chuẩn giao thức này:
- IEC 870-5-1 (Transmission Frame Formats)
- IEC 870-5-2 (Data Link Transmission Services)
- IEC 870-5-3 (General Structure Of Application Data)
- IEC 870-5-4 (Definition And Coding Of Information Elements)
- IEC 870-5-5 (Basic Application Functions)

- Giao thức IEC 870-5-101 cho các ứng dụng có sử dụng các RTU điều khiển xa, các định nghĩa và đặc tả của giao thức này được lựa chọn từ 5 tài liệu trên.
- Là giao thức truyền thông giữa các thiết bị đầu cuối (RTU) và hệ thống trung tâm (Central Station).
- Thông tin theo hướng từ thiết bị đầu cuối (RTU) tới Central Station thường là các thông số đo RTU thu thập từ các thiết bị vật lí (như tần số, điện áp, dòng điện, công suất…) và
- thông tin theo hướng ngược lại thường là các lệnh điều khiển hoạt động thiết bị vật lí.

- **Một số định nghĩa:**
  - Controlling Station: Trạm điều khiển hoạt động toàn bộ hệ thống.
  - Controlled Station: Các trạm cấp dưới hoặc thiết bị thu thập số liệu RTU.
  - Unbalanced Mode: Là chế độ hoạt động mà chỉ có Controlling Station khởi đầu một phiên truyền nhận.
  - Balanced Mode: Là chế độ hoạt động mà tất cả các trạm đều có thể khởi đầu một phiên truyền nhận.

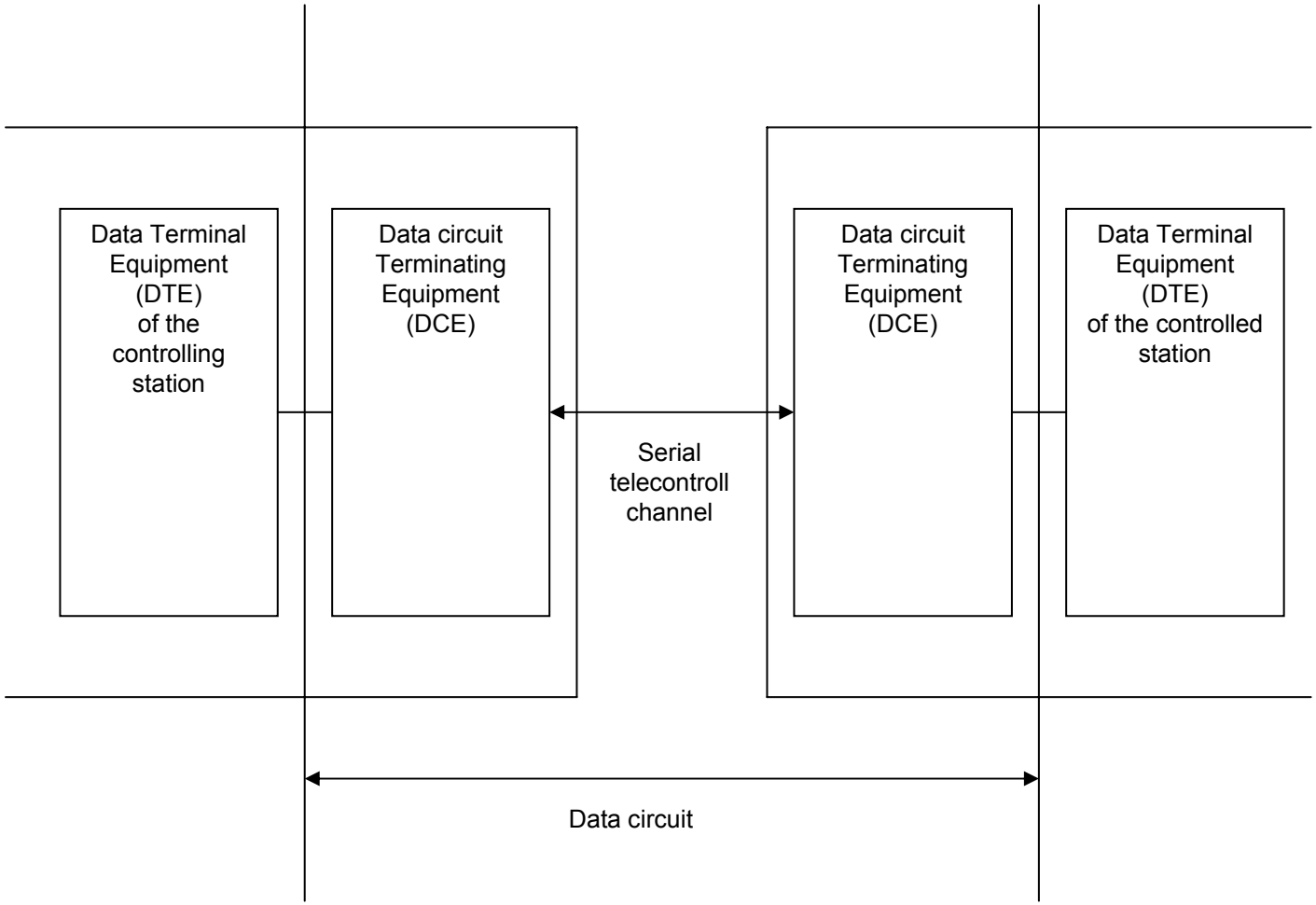
2.4.2. Cấu trúc giao thức

- Giao thức đưa ra mô hình phân lớp mạng bao gồm 3 lớp:
  - Application layer
  - Data link layer
  - Physical layer



Hình 223.
IEC 780
Layers

Phisical Layer:



Hình 224. IEC Physical Layers

Link layer:

- Cung cấp các thủ tục truyền thông, sử dụng trường điều khiển và trường địa chỉ.
- Liên kết giữa các trạm có thể được thực hiện theo chế độ truyền thông unbalanced /balanced mode.
- Nếu sự liên kết giữa trạm điều khiển trung tâm và các trạm khác chia sẻ cùng một đường truyền thì chế độ hoạt động phải là unbalanced mode.

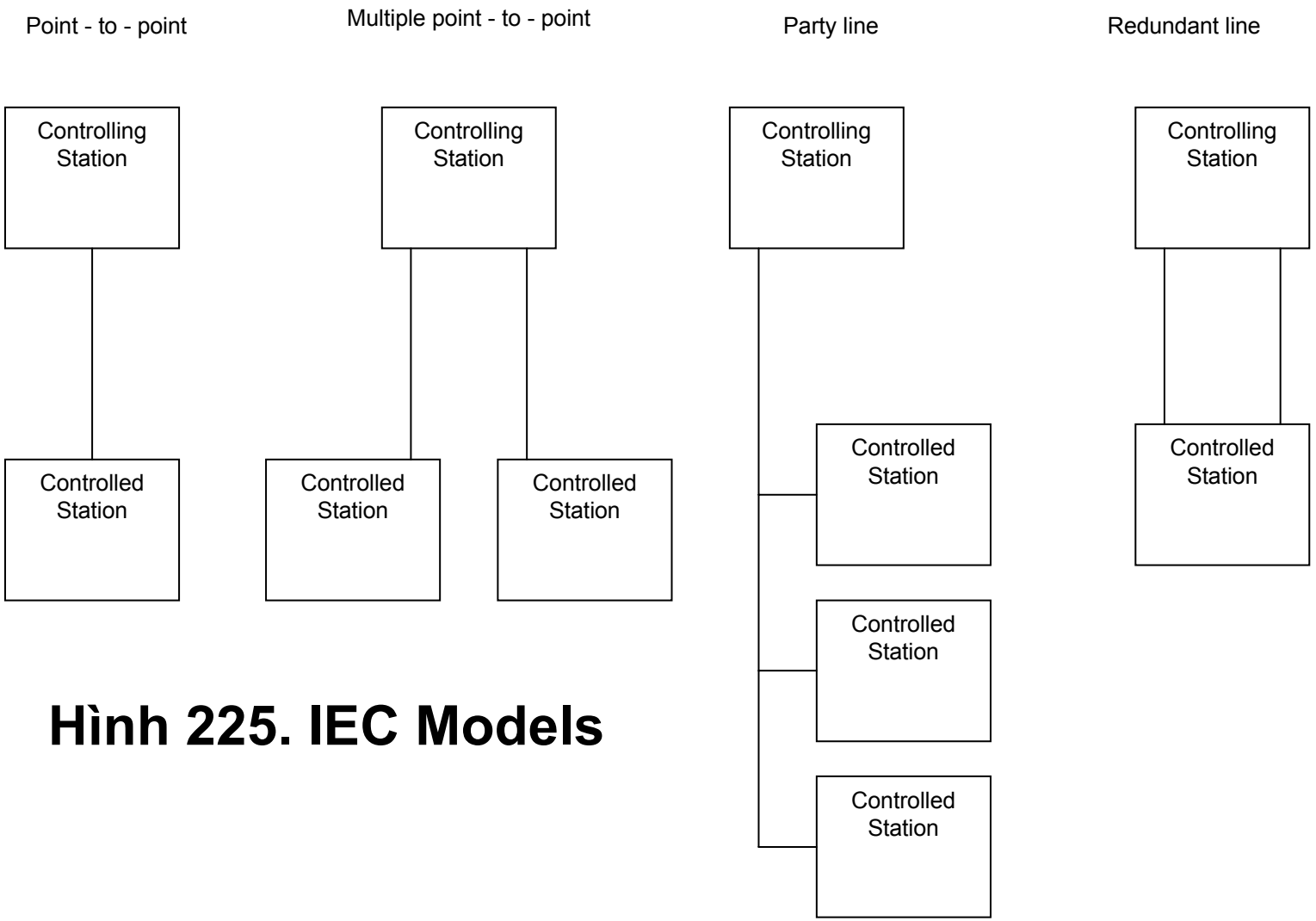
Application layer

- Application Service Data Units (ASDU): là cấu trúc dữ liệu trên từng ứng dụng.
- Các ASDU thực chất là 1 frame có chứa số liệu hay lệnh điều khiển.

2.4.3. Các đặc tả về truyền thông

- Các đặc tả này định nghĩa cấu hình mạng, định dạng chuẩn kí tự và các luật truyền thông.
- *Cấu hình mạng:* bao gồm các dạng sau:
  - Point - to – point, *figures @ next page*
  - Multiple point - to - point
  - Party line
  - Redundant line

Hình 2.2 Các mô hình mạng của giao thức IEC 870-5-101



Hình 225. IEC Models

- Character format: 1 Start bit, 1 Stop bit, 1 Parity bit (even) và 8 Data bits
- Transmission rules:
  - Đường truyền rỗi là mức nhị phân 1.
  - Mỗi kí tự có một bit khởi đầu (binary = 0), 8 bit thông tin, một bit parity (chẵn) và một bit stop(binary = 1).
  - Không được có khoảng thời gian rỗi trên đường truyền giữa các kí tự trong cùng một frame.
  - Khoảng thời gian xác định lỗi giữa các frame cho phép nhỏ nhất là 33 bit (3 kí tự)
  - Các kí tự dữ liệu được kết thúc bởi 8 bits checksum (CS). Checksum được thực hiện trên toàn bộ các byte mang dữ liệu.
  - Phía nhận thực hiện kiểm tra:
  - Các bít không mạng tin/char: bit start, bit stop và parity bit.
  - Đối với mỗi frame: kí tự start, độ dài (2 bytes trong frame có độ dài không cố định), check sum của frame và kí tự kết thúc

2.4.4 Định dạng frame dữ liệu

- Giao thức IEC 870-5-101 sử dụng ba định dạng frame
  - Frame có độ dài thay đổi
  - Frame có độ dài cố định
  - Frame chỉ có một kí tự

Frame có độ dài thay đổi

Start 68H
L
L
Start 68H
C
A
A
Link/ user data
…
…
…
…
Check sum
End 16H

Frame có độ dài cố định

Start 10H
C
A
Check sum
End 16H

Frame chỉ có một kí tự

E5H

L: Số byte, gồm cả điều khiển và địa chỉ.

C: Trường điều khiển (Control field).

A: Trường địa chỉ (Address field) là địa chỉ cho lớp Datalink.

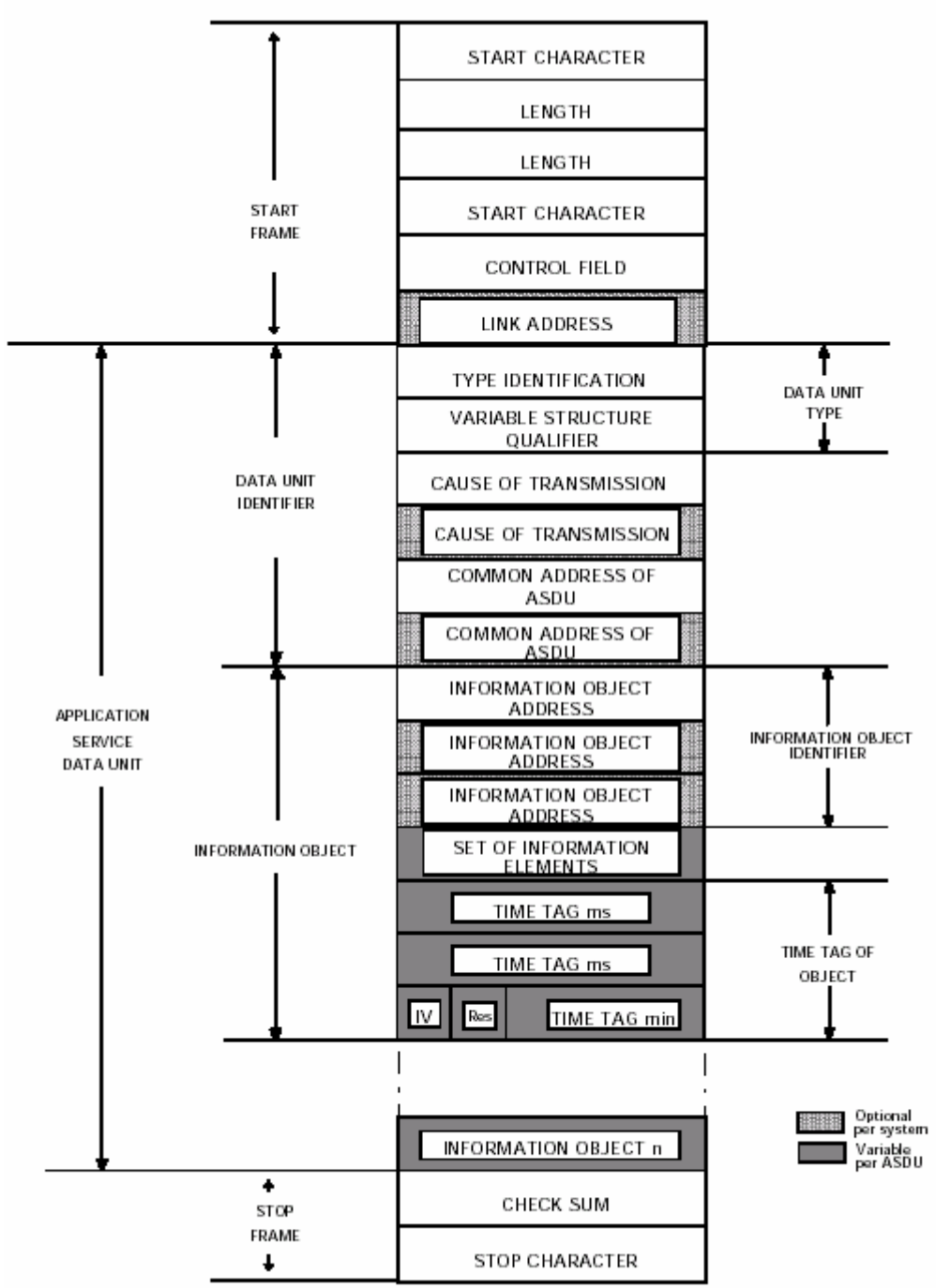
Hình 226. IEC 780-5 Frames

- Frame có độ dài thay đổi: truyền dữ liệu giữa controlling và controlled station.
- Frame có độ dài cố định: dùng cho các dịch vụ của link layer.
- Frame chỉ có một kí tự: xác nhận các hoạt động như đồng bộ thời gian, yêu cầu dữ liệu...

❑ *Cấu trúc dữ liệu*

- IEC 870-5-101 định nghĩa: Các Application Service Data Unit (ASDU) chứa thông tin truyền thông giữa các trạm. Các ASDU được định nghĩa là các frame dữ liệu có độ dài không cố định. Định dạng của frame:
- **Khởi đầu frame:**
  - 1 byte START CHARACTER
  - 2 byte FRAME LENGTH
  - 1 byte START CHARACTER
  - 1 byte LINK ADDRESS
- **Kết thúc frame:**
  - 1 byte CHECKSUM
  - 1 byte STOP CHARCTER

Hình 226. Formats of Application Service Data Unit



- Mỗi ASDU bao gồm hai phần:
  - DATA UNIT IDENTIFIER:
    - 1 byte TYPE IDENTIFICATION,
    - 1 byte VARIABLE STRUCTURE QUALIFIER,
    - 1 hay 2 byte CAUSE OF TRANSMISSION,
    - 1 hay 2 byte COMMON ADDRESS OF ASDU
  - INFORMATION OBJECT:
    - Nếu ASDU được truyền từ Controlled Station theo yêu cầu số liệu từ Controlling Station thì ASDU thông tin các đối tượng có thể kèm theo thẻ thời gian.
    - Nếu ASDU được truyền từ Controlling Station thì thông tin được chứa là thời gian nếu là lệnh đồng bộ thời gian hay là trạng thái trong lệnh điều khiển...

2.4.5. Command set and Scenario

- Command set:
  - Station initialisation: Khởi tạo các trạm.
  - Data acquisition by polling: Thu thập số liệu kiểu polling
  - Cyclic data transmission: Truyền dữ liệu có tính chu kì.
  - Acquisition of events: Thu thập sự kiện.
  - General interrogation: Thủ tục để Controlling Station cập nhật các Controlled Station, thực hiện sau khi khởi tạo.
  - Clock synchronisation: đồng bộ thời gian.
  - Command transmission: Truyền lệnh điều khiển.
  - Transmission of integrated totals: Thu thập giá trị đếm xung.
  - Parameter loading: Nạp tham số cho Controlled Station.
  - Test procedure: Thủ tục kiểm tra sự kết nối giữa các trạm.
  - File transfer: Truyền file.
  - Acquisition of transmission delay: Xác định độ trễ đường truyền.

A Case Study: Acquisition of events

- Các sự kiện xảy ra được lưu trữ trong buffer của Controlled Station cho các sự kiện xảy ra nhanh hơn so với tốc độ truyền thông. Khi Controlling Station hỏi Controlled Station yêu cầu các sự kiện thì có hai khả năng xảy ra: không có sự kiện trong buffer và có sự kiện trong buffer của Controlled Station.
  - Trường hợp không có sự kiện trong buffer: Controlled Station trả lời NACK dưới dạng message chỉ có một kí tự (05H) hay hay một frame có độ dài cố định (fixes frame) mang thông điệp "Requested data not available".
  - Trường hợp có sự kiện trong buffer: Controlled Station trả lời bằng một fixed frame NACK nhưng bit trạng thái = 1 báo hiệu cho Controlling Station có sự kiện. Controlling gửi message "Request user data class 1" yêu cầu và Controlled trả bằng một ASDU chứa sự kiện, ASDU này có thể chứa toàn bộ hoặc một vài sự kiện của Controlled Station.

Chapter 3
INTRODUCTION of EMBEDDED SYSTEMS

3.1. What is an Embedded System?

- Electronic devices that incorporate a computer (usually a microprocessor) within their implementation.
- A computer is used in such devices primarily as a means to simplify the system design and to provide flexibility.
- Often the user of the device is not even aware that a computer is present.

Aerospace	Navigation systems, automatic landing systems, flight attitude controls, engine controls, space exploration (e.g., the Mars Pathfinder).
Automotive	Fuel injection control, passenger environmental controls, anti-lock braking systems, air bag controls, GPS mapping.
Children's Toys	Nintendo's "Game Boy", Mattel's "My Interactive Pooh", Tiger Electronic's "Furby".
Communi-cations	Satellites; network routers, switches, hubs.

Computer Peripherals	Printers, scanners, keyboards, displays, modems, hard disk drives, CD-ROM drives, USB Mem sticks.
Home	Dishwashers, Microwave Ovens, VCRs, televisions, stereos, fire/security alarm systems, lawn sprinkler controls, thermostats, cameras, clock radios, answering machines.
Industrial	Elevator controls, surveillance systems, robots.
Instrumen-tation	Data collection, oscilloscopes, signal generators, signal analyzers, power supplies.

Medical	Imaging systems (e.g., XRAY, MRI, and ultrasound), patient monitors, heart pacers.
Office Automation	FAX machines, copiers, telephones, cash registers.
Personal	Personal Digital Assistants (PDAs), pagers, cell phones, wrist watches, video games, portable MP3 players, GPS.

Embedded Rules!

- Embedded processors account for 100% of worldwide microprocessor production!
- Embedded:desktop = 100:1
- 2003: #embedded processors in the home estimated at 70-80.

Design Goal: Reliability

- Mission Critical
- Life-Threatening
- 24/7/365
- Can’t reboot!

Design Goal: Performance

- Multitasking and Scheduling
- Optimized I/O ➔ Assembly Language
- Limits, Inaccuracies of Fixed Precision

Design Goal: Cost

- Consumer Market: Minimize Manufacturing Cost.
- Fast Time to Market Required
- No chance for future modification.

What is a Real-Time System?

- Real-time systems process events.
- Events occurring on external inputs cause other events to occur as outputs.
- Minimizing response time is usually a primary objective, or otherwise the entire system may fail to operate properly.

Hard/Soft Real-Time Systems

- Soft Real-Time System
  - Compute output response as fast as possible, but no specific deadlines that must be met.

- Hard Real-Time System
  - Output response must be computed by specified deadline or system fails.

Multi-Tasking and Concurrency

- Most real-time systems are also embedded systems w/several inputs and outputs and multiple events occurring independently.
- Separating tasks simplifies programming, but requires somehow switching back and forth among the three task (*multi-tasking*).
- *Concurrency* is the appearance of simultaneous execution of multiple tasks.

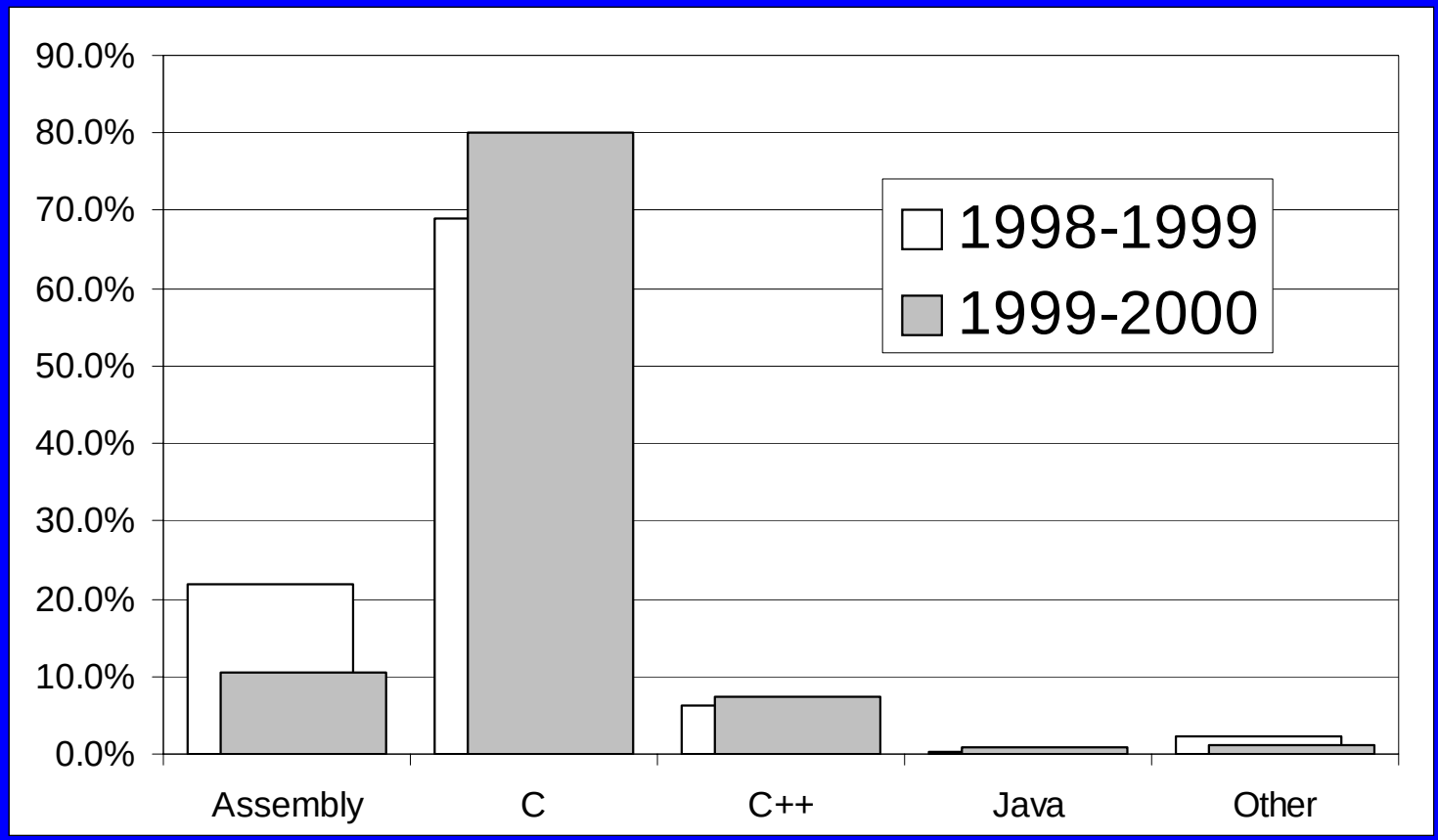
Three Concurrent Tasks Within a Programmable Thermostat

```
/* Monitor Temperature */
do forever {
        measure temp ;
        if (temp < setting)
                start furnace ;
        else if (temp >
                setting + delta)
                stop furnace ;
}
```

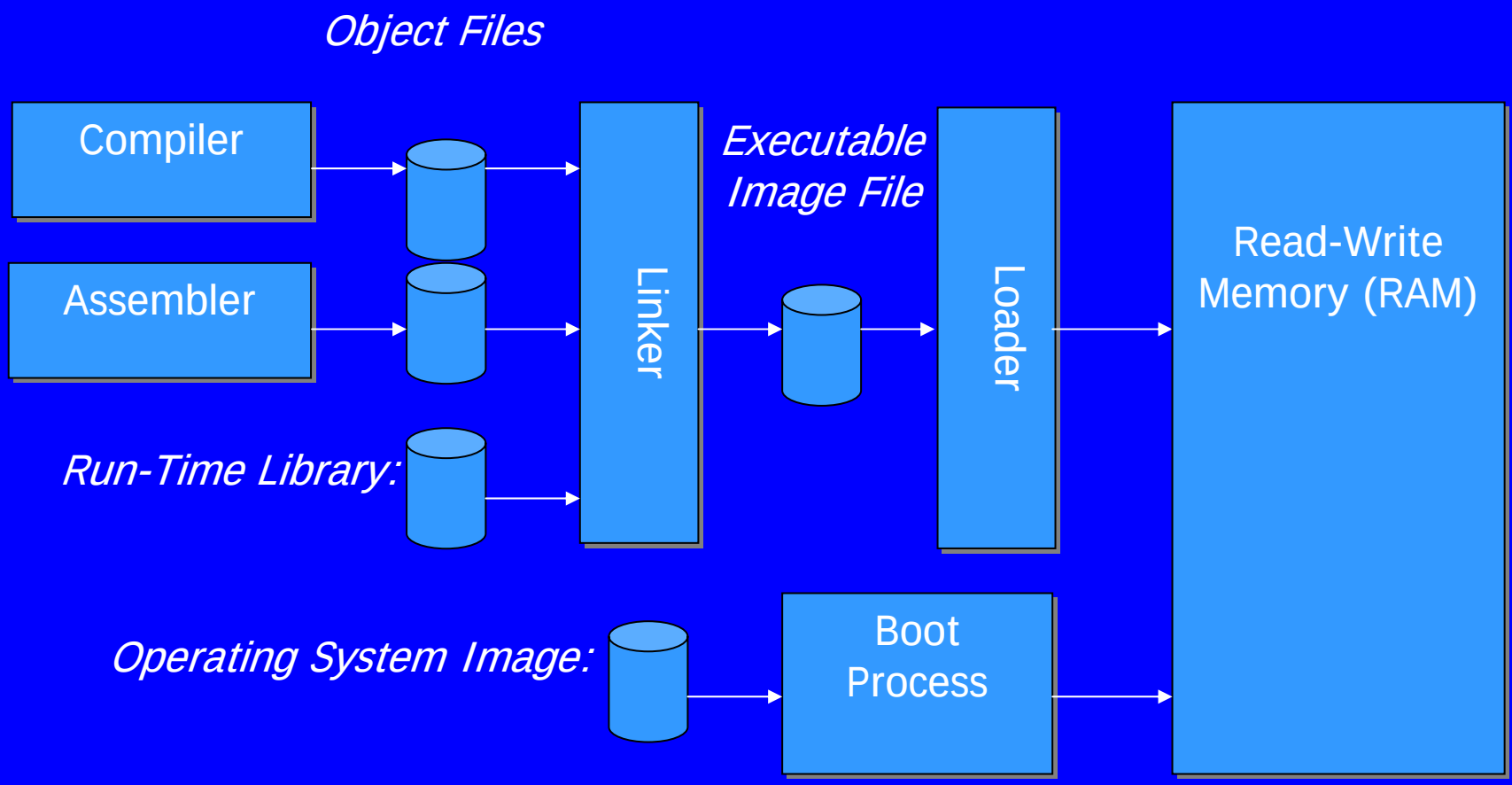
```
/* Monitor Time of Day */
do forever {
        measure time ;
        if (6:00am)
                setting = 72°F ;
        else if (11:00pm)
                setting = 60°F ;
}
```

```
/* Monitor Keypad */
do forever {
        check keypad ;
        if (raise temp)
                setting++ ;
        else if (lower temp)
                setting-- ;
}
```

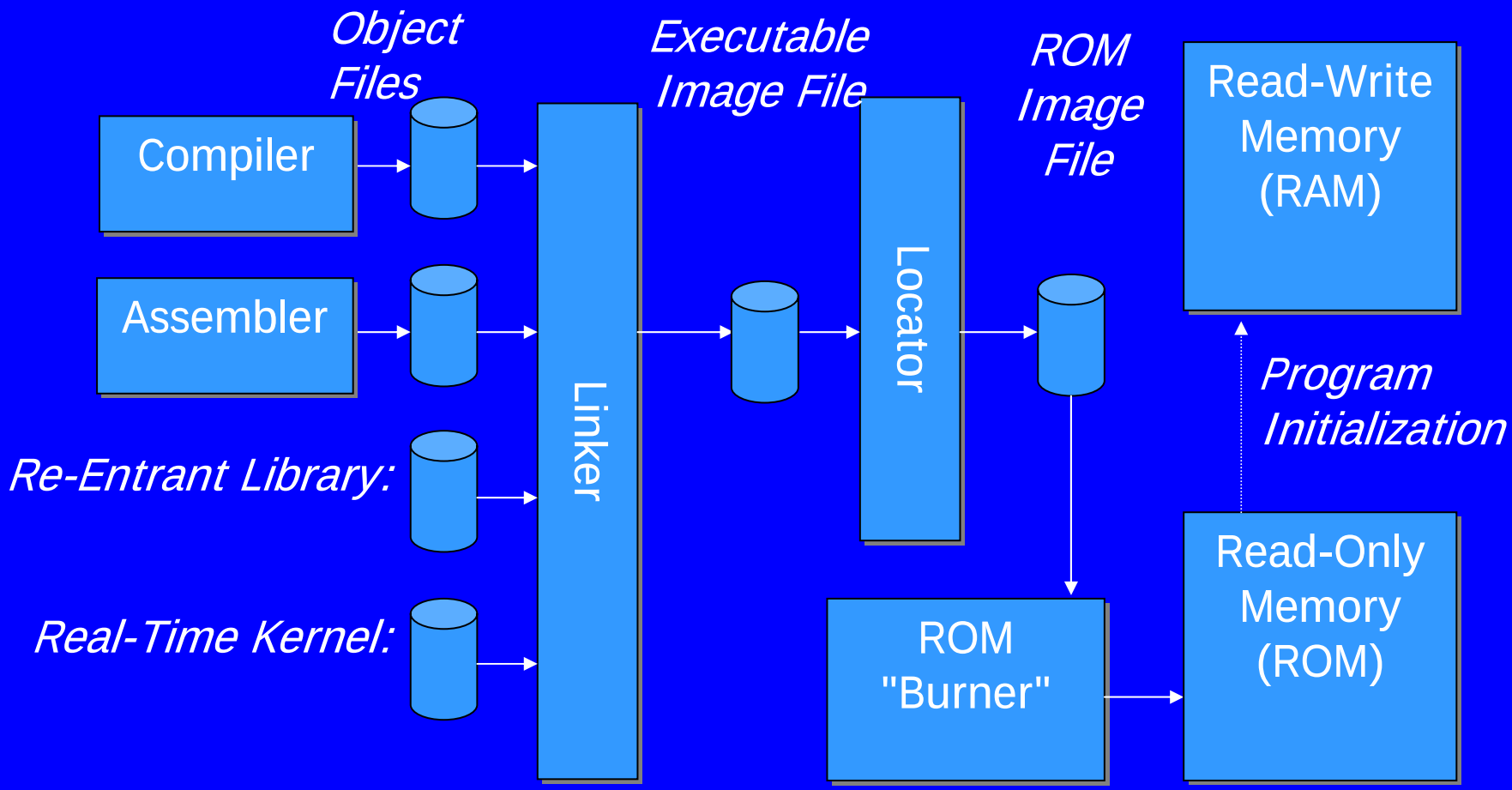
Programming Languages Used in New Embedded Designs



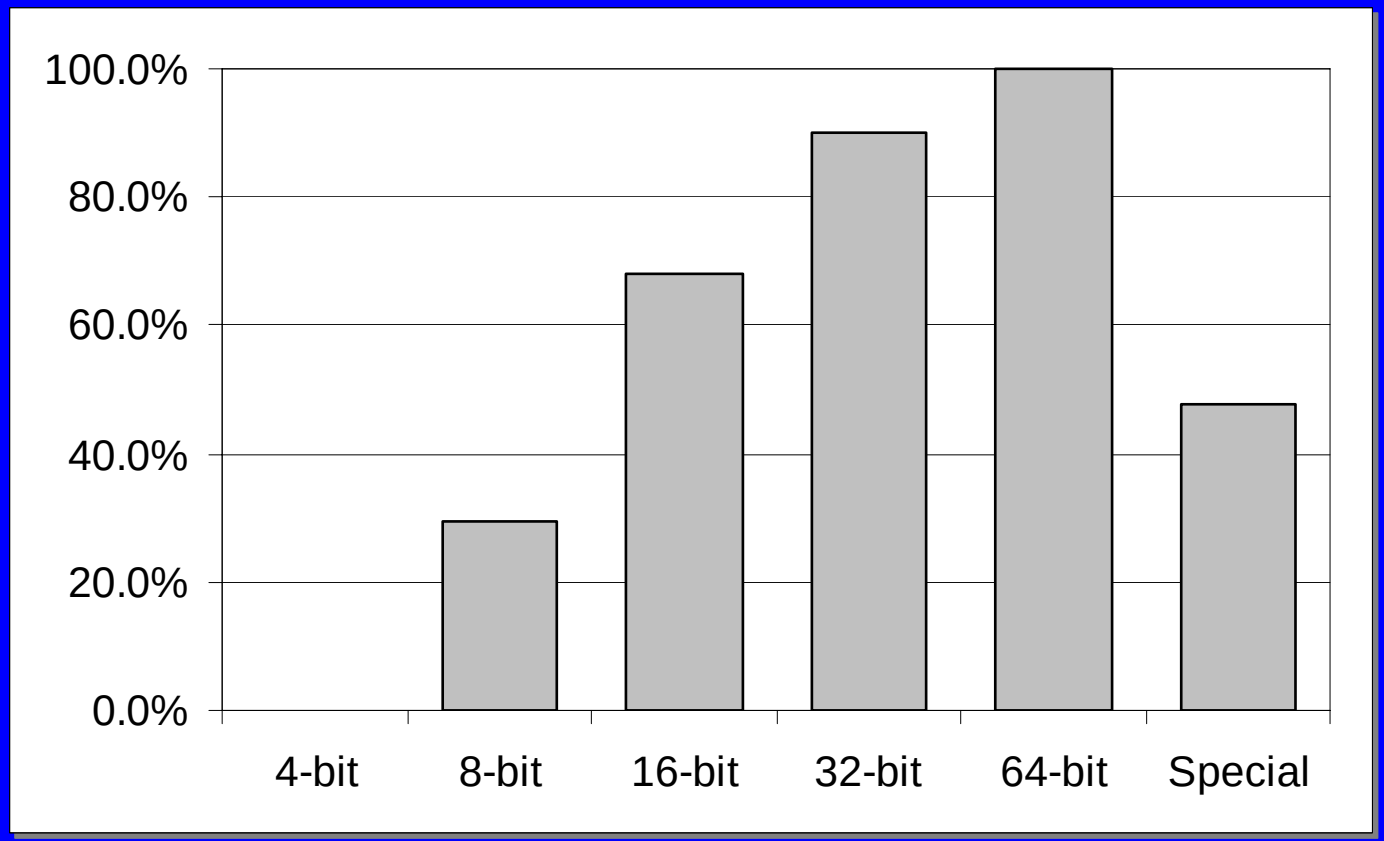
The build and load process for desktop application programs.



The build and load process for embedded application programs.



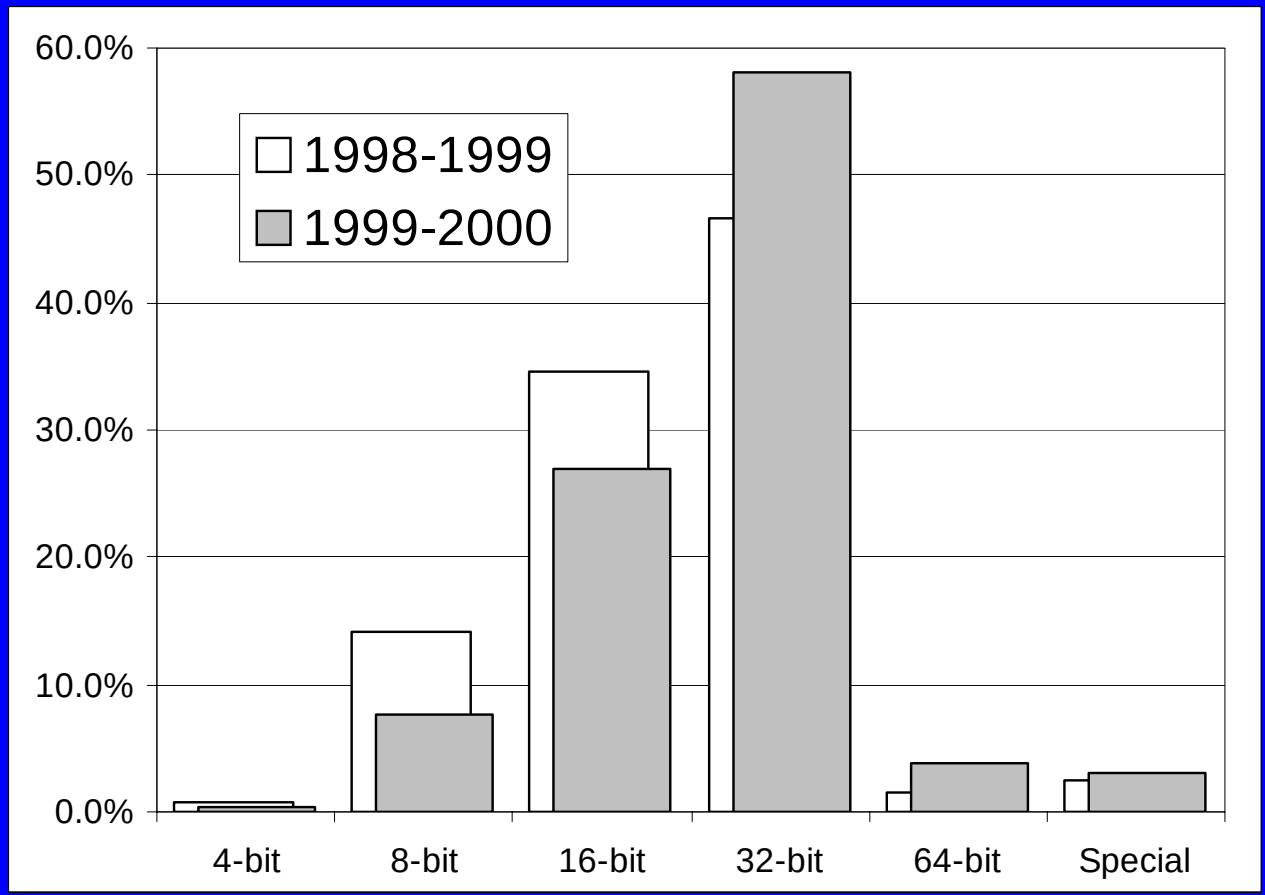
Use of Real-Time Kernels in New Embedded Designs.



Examples of Embedded Real-Time Software.

Property	*FAX Machine*	*CD Player*
Microprocessor:	16-bit	8-bit
Number of Threads:	6	9
Read-Write Memory (RAM):	2048 Bytes	512 Bytes
Total RAM Actually Used:	1346 Bytes (66%)	384 Bytes (75%)
Amount Used by Kernel:	250 Bytes (19%)	146 Bytes (38%)
Read-Only Memory (ROM):	32.0 KB	32.0 KB
Total ROM Actually Used:	28.8 KB (90%)	17.8 KB (56%)
Amount Used by Kernel:	2.5 KB (8.7%)	2.3 KB (13%)

Processor Types Used in New Embedded Designs



Product: Hunter Programmable Digital Thermostat.

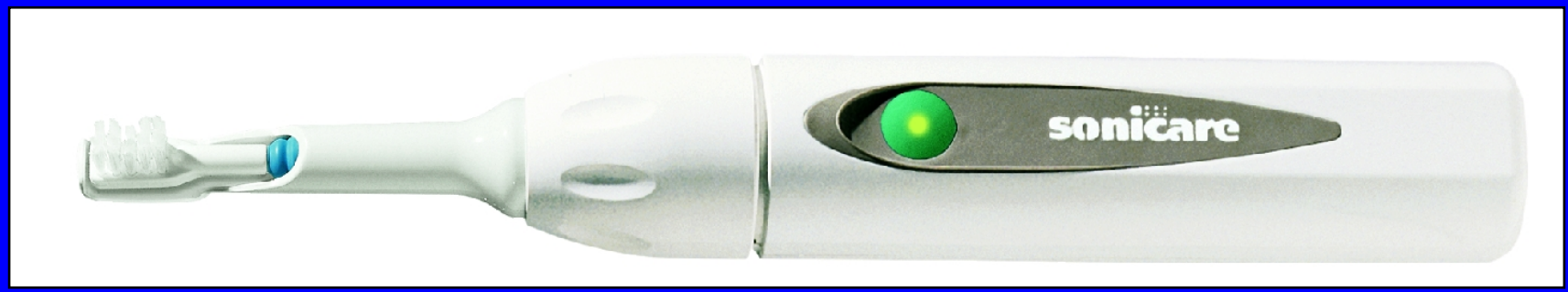
Microprocessor: 4-bit

Product:Vendo V-MAX 720 vending machine.

Microprocessor: 8-bit Motorola 68HC11.

Product: Sonicare Plus toothbrush.

Microprocessor: 8-bit Zilog Z8.



Product: Miele dishwashers.

Microprocessor: 8-bit Motorola 68HC05.

Product: NASA's Mars Sojourner Rover.

Microprocessor: 8-bit Intel 80C85.

Product: CoinCo USQ-712 coin changer.

Microprocessor: 8-bit Motorola 68HC912.

Product: Garmin StreetPilot GPS Receiver.

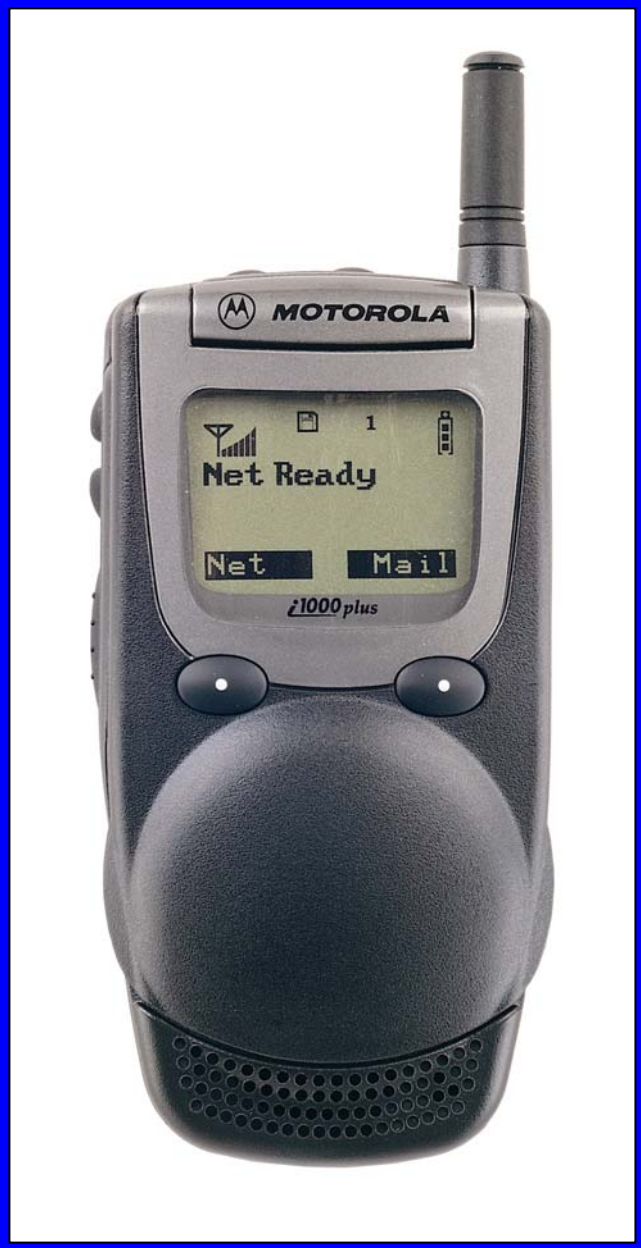
Microprocessor: 16-bit.

Product: TIQIT Computer's "Matchbox PC".

Microprocessor: 32-bit AMD Elan SC410.

Product: Palm Vx handheld.

Microprocessor: 32-bit Motorola Dragonball EZ.



Product: Motorola i1000plus iDEN Multi-Service Digital Phone.

Microprocessor: Motorola 32-bit MCORE.

Product: Rio 800 MP3 Player.

Microprocessor: 32-bit RISC.

Product: RCA RC5400P DVD player.

Microprocessor: 32-bit RISC.

Product: IBM Research's Linux wrist watch prototype.

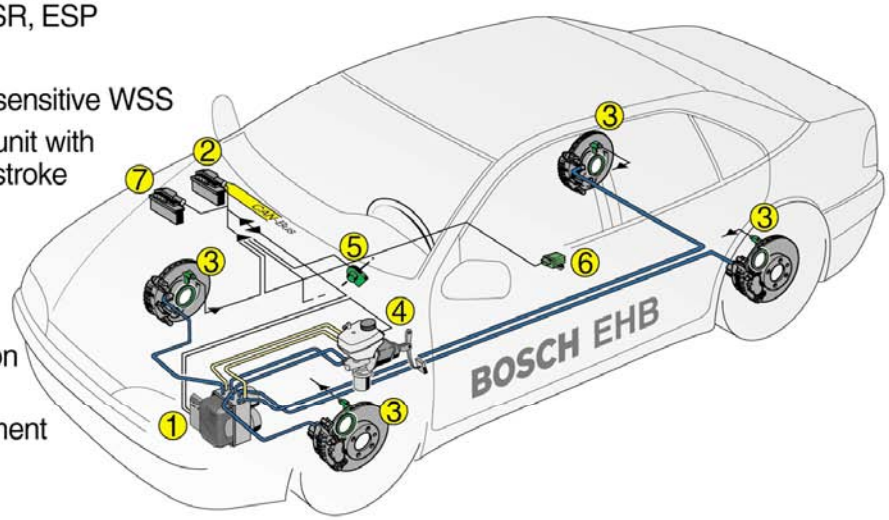
Microprocessor: 32-bit ARM RISC.

Product: Sony Aibo ERS-110 Robotic Dog.

Microprocessor: 64-bit MIPS RISC.

Bosch Electrohydraulic Brake EHB

① Electrohydraulic actuator for EHB, ABS, ASR, ESP
② EHB - ECU
③ Active, direction-sensitive WSS
④ Brake operation unit with integrated pedal stroke sensor
⑤ Steering wheel angle sensor
⑥ Yaw rate and lateral acceleration sensor
⑦ Engine management ECU



BOSCH

Press photo No. 1-K1-10583

Ch. 4 Programmable Controllers

- PLC/PC Overview
- Siemens SIMATIC S7-x00 seri PLCs
- STEP 7 – 300/400 Programming Language
- WinCC

4.1. Khái niệm PLCs

- Lịch sử:
  - 1960 – 1970s: Hard wire
  - 1980 – 1990: Programmable Logic Controller
  - 1990 – nay: Programmable Controller, Process Controller
- Các hãng sản xuất:
  - USA: Allen Bradley, GE-Fanuc
  - EC: Siemens, ABB, Schneider
  - As-Au: Omron, Hitachi, Misubishi…

- Cấu trúc: chia thành các modules:
  - CPU, Power supply Module có cổng nối bộ lập trình (PG)
  - [Expansion Memory Module (Flash, SRAM, DRAM, BBRAM)]
  - Digital Input Module (mức áp dc/ac, cách ly quang...)
  - Digital Output Module (relay, transistor, triac..., Relay/Opto Isolated)
  - Analog Input Module (u, i, cách ly...)

- Analog Output Module (u, i)
- Timer/ Counter Module (kHz, đếm xung, đo tốc độ, chiều dài)
- Communication Module: (RS232/485; Ethernet IEEE 802.x)
- 2/3 D Positioner Module (định vị 2/ 3 chiều)
- Interface Module - dùng để mở rộng thêm các Module khác
- Function Modules: các chức năng điều khiển PID, Servo/ Step Motors,...

❑ Hoạt động của PLC:

➢ Hoạt động theo chu kỳ các vòng quét:

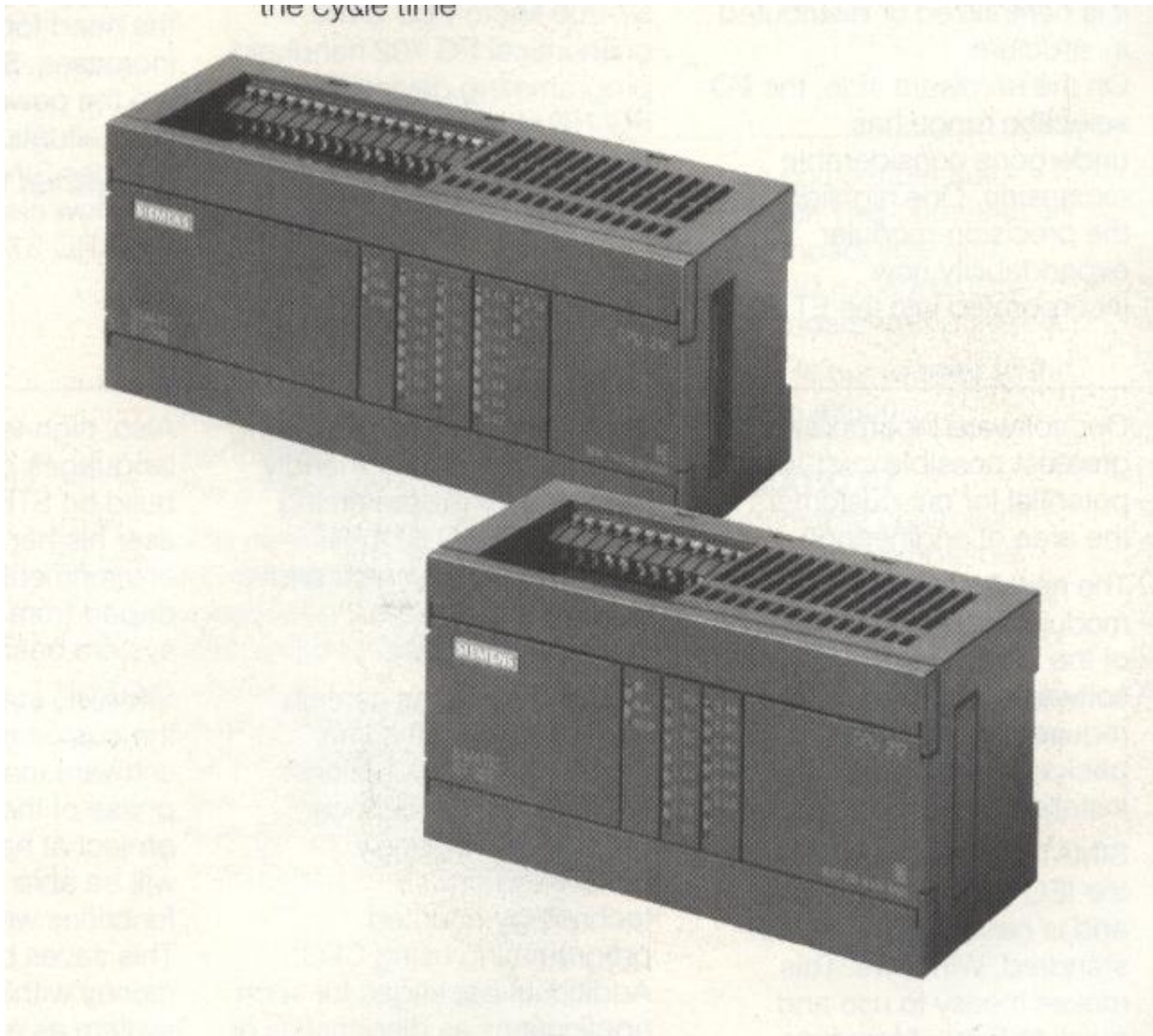
- Đọc các thông tin từ các lối vào: DI, AI, Counter, Communication…
- Xử lý, tính toán, Update data base, update các cờ trạng thái
- Gửi ra các port: DO, AO, Postioner, Communication…

➢ Ngôn ngữ lập trình:

- Ladder
- Statement List
- Flow control

4.2. Siemens SIMATIC S7-x00 PLC:

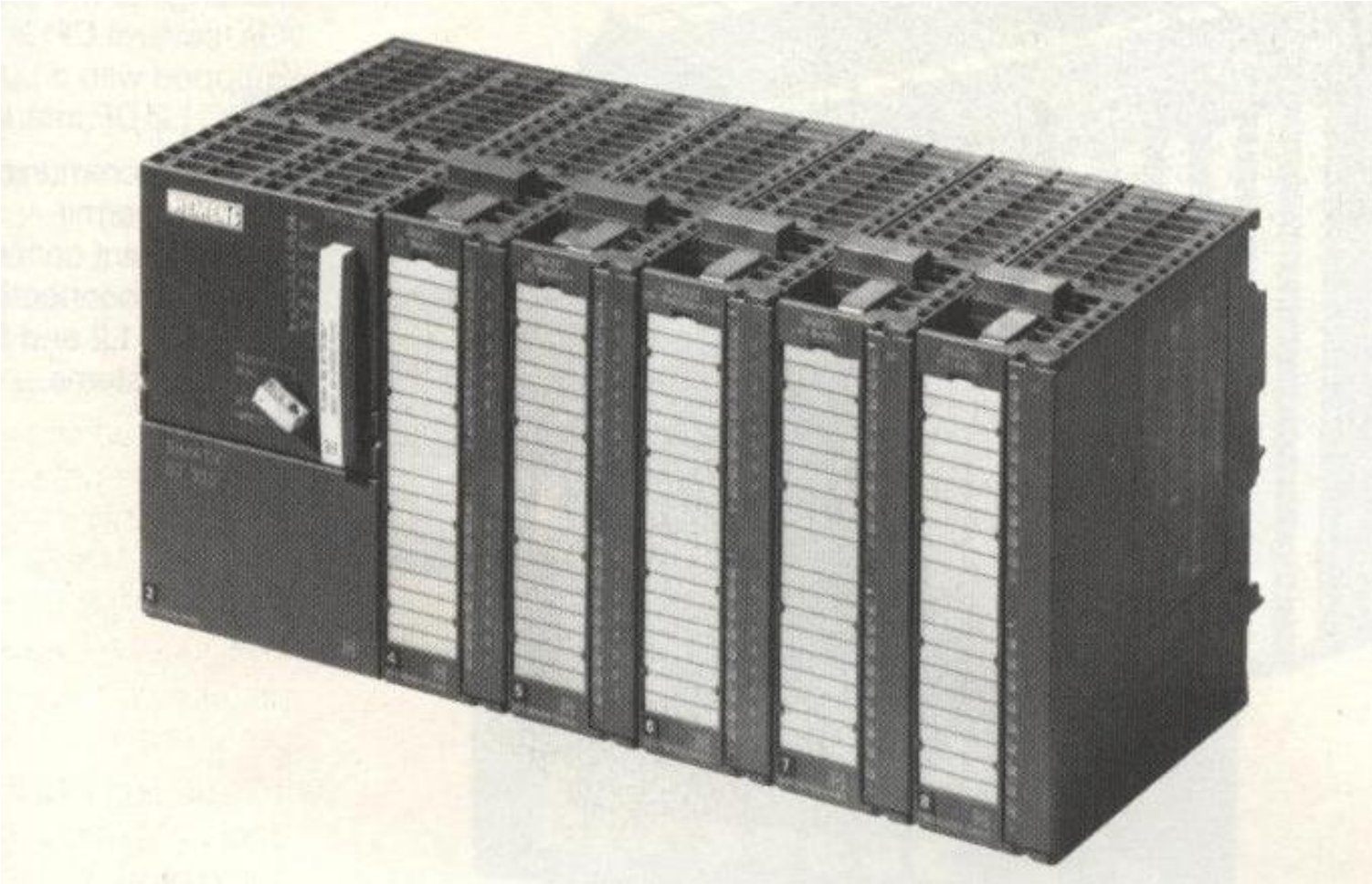
4.2.1. S7-200:



Hình 402.
PLC S7-200

- Micro type, high-speed, compact, low-cost solution for automation tasks within the low-end performance range.
- Có nhiều loại CPU: 212 (214…)
  - RAM for Program & data:
    - 212 CPU: 1Kbyte – 512 statement, 2048 word data
    - 214 CPU: 4Kbyte – 2048 statement, 2048 word data
  - Execution time of 1024Statements: 1,3ms (212CPU) và 0.8ms (214 CPU)
  - Bit memory: 128 (256)
  - Counters, Timer: 46 (128)
  - DI/DO max/onboard: 30/14 (64/24)
  - AI/AO max: 8 (16)
  - Communication: PPI
  - Real time clock: CPU 214.

4.2.2. S7-300



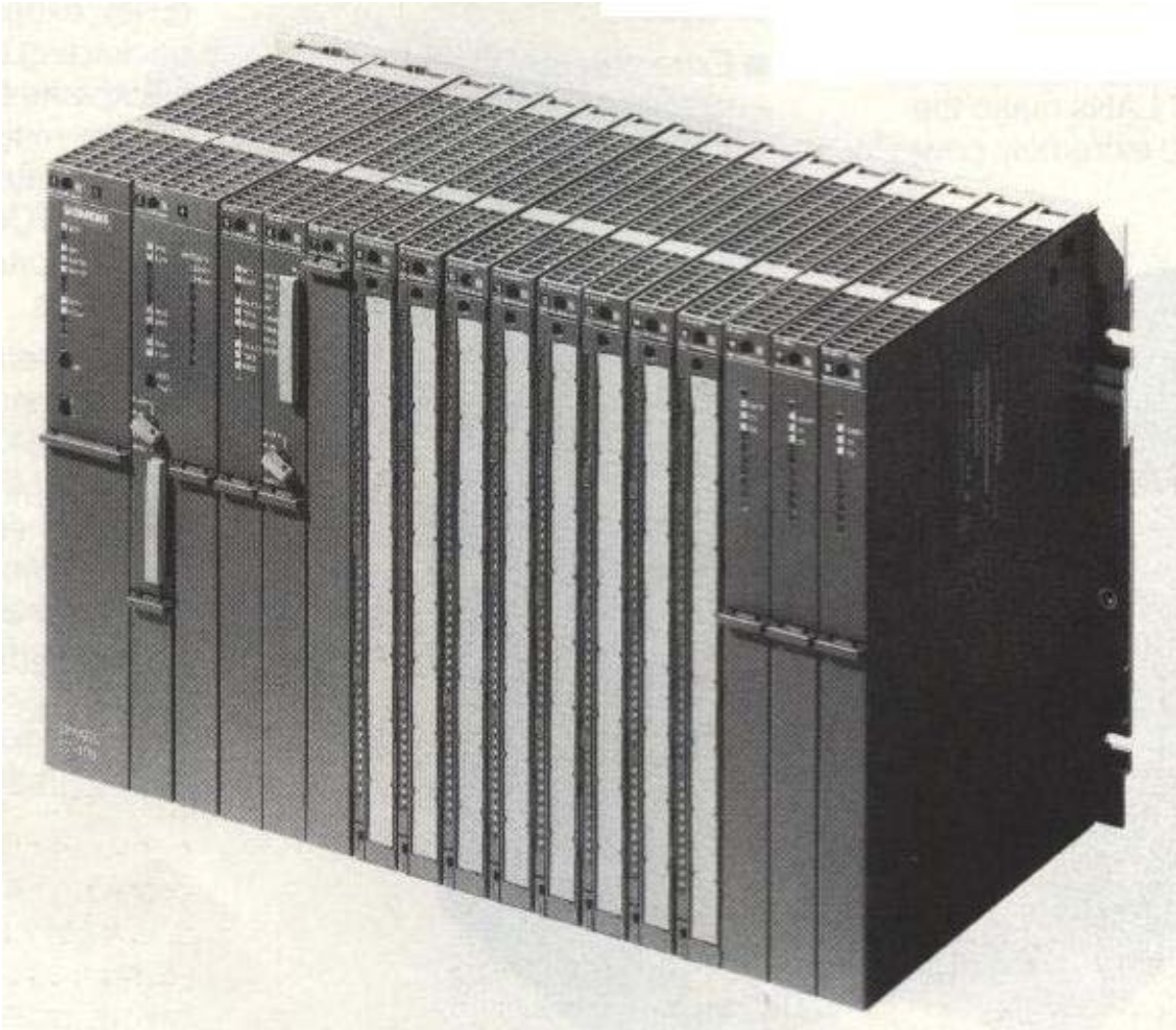
Hình 403a – PLC S7-300

- Mini PLC system, the custom solution for extremely fast processes/ automation tasks requiring additional data processing capabilities
- Spec.:
  - High computeing performance,
  - Complete instruction set,
  - Multi Point Interface – MPI
  - 5 CPUs for a wide varietyof requirement
  - Expandability: upto 3 Expansion Racks (ERs)

SIMATIC S7-300 with CPU 312 IFM	CPU 313	CPU 314	CPU 315	CPU 315-2 DP
6 Kbytes / typ. 2 K statements 1 statement = 3 bytes (typ.)	12 Kbytes / typ. 4 K statements 1 statement = 3 bytes (typ.)	24 Kbytes / typ. 8 K statements 1 statement = 3 bytes (typ.)	48 Kbytes / typ. 16 K statements 1 statement = 3 bytes (typ.)	48 Kbytes / typ. 16 K statements 1 statement = 3 bytes (typ.)
0.6 ms	0.6 ms	0.3 ms	0.3 ms	0.3 ms
1024	2048	2048	2048	2048
32	64	64	64	64
64	128	128	128	128
144/16	128/0	512/0	1024/0	1024/0 (freely addressable)
32	32	64	128	128 (freely addressable)
■	■	■	■	■
MPI interface	MPI interface	MPI interface	MPI interface	MPI interface
SINEC L2/L2-DP	SINEC L2/L2-DP	SINEC L2/L2-DP	SINEC L2/L2-DP	SINEC L2/L2-DP
—	—	built-in	built-in	built-in

4.2.3. S7-400:

Hình 404a. S7-400

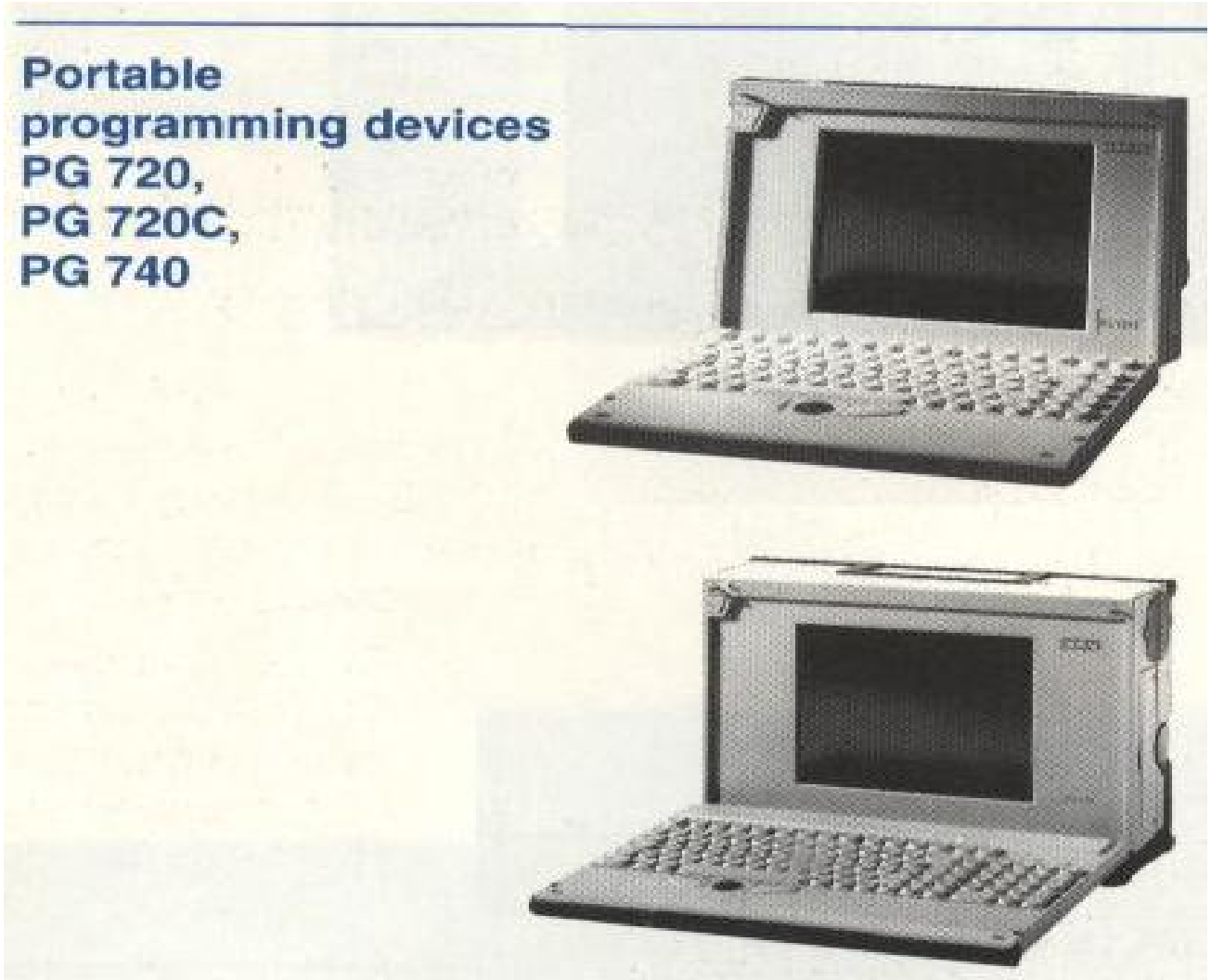


- Power PLC for automation tasks within mid & upper range:
  - High Speed, 1K statement – 200 us
  - Rugged: full enclosed, for industrial environment
  - Module can be hot pluggible
  - Communications power house:
    - Connection to SINEC L2 or SINEC H1 or Point-to-Point
    - Fast data exchange to the distributed I/Os

	SIMATIC S7-400 CPU 412-1	with CPU 413-1/413-2 DP	CPU 414-1/414-2 DP	CPU 416-1
RAM for program and data, built-in	48 Kbytes	72 Kbytes	128 Kbytes	512 Kbytes
Execution time per 1 K binary statements	0.2 ms	0.2 ms	0.1 ms	0.08 ms
Bit memories	4096	4096	8192	16384
Counters	256	256	256	512
Timers	256	256	256	512
Digital inputs and outputs, each	4 K	16 K	64 K	128 K
Analog inputs and outputs, each	256	1024	4096	8192
Operator interface systems	■	■	■	■
Communication port	MPI interface	MPI interface SINEC L2-DP[1)]	MPI interface SINEC L2-DP[1)]	MPI interface
Networking	SINEC L2/H1	SINEC L2/H1	SINEC L2/H1	SINEC L2/H1
Real-time clock	built-in	built-in	built-in	built-in

4.2.4. Programming Devices

Hình 405a.



Hình 405b.

4.2.5. Distributed IOs

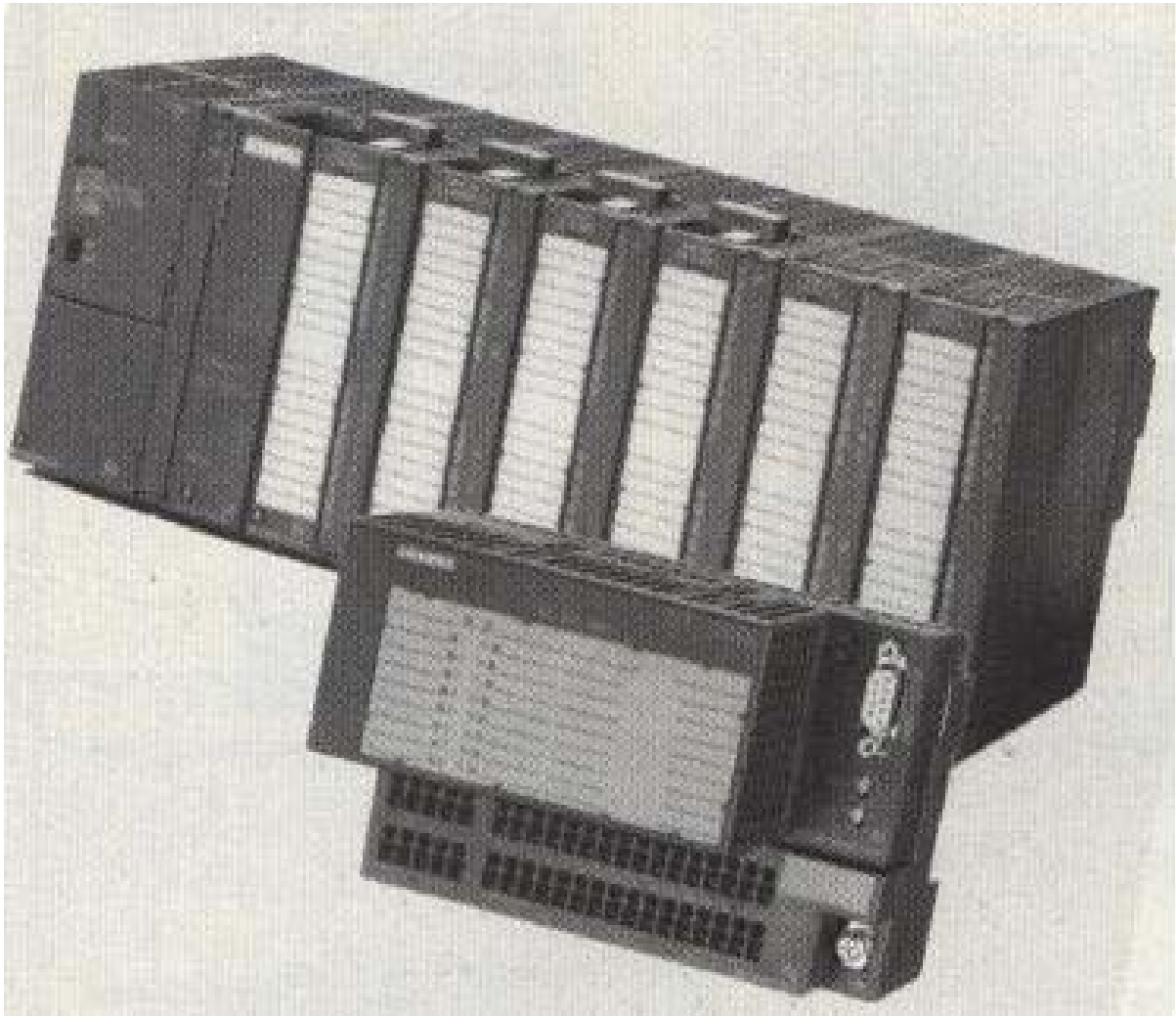


Fig. 406. Distributed IO Modules

- In conventionally automated Plants, IO are plugged directly into PLC. Frequently this leads to extensive wiring with
  - High cabling cost
  - Reduced flexibility in the case of modifications and expansions
- A distributed configuration means:
  - The PLCs, IO Modules and Field Devices are connected over a single cable known as a field bus,
  - The IO Modules can be installed in the immediate vicinity of sensors and actuators
  - The process signals can be converted and processed locally

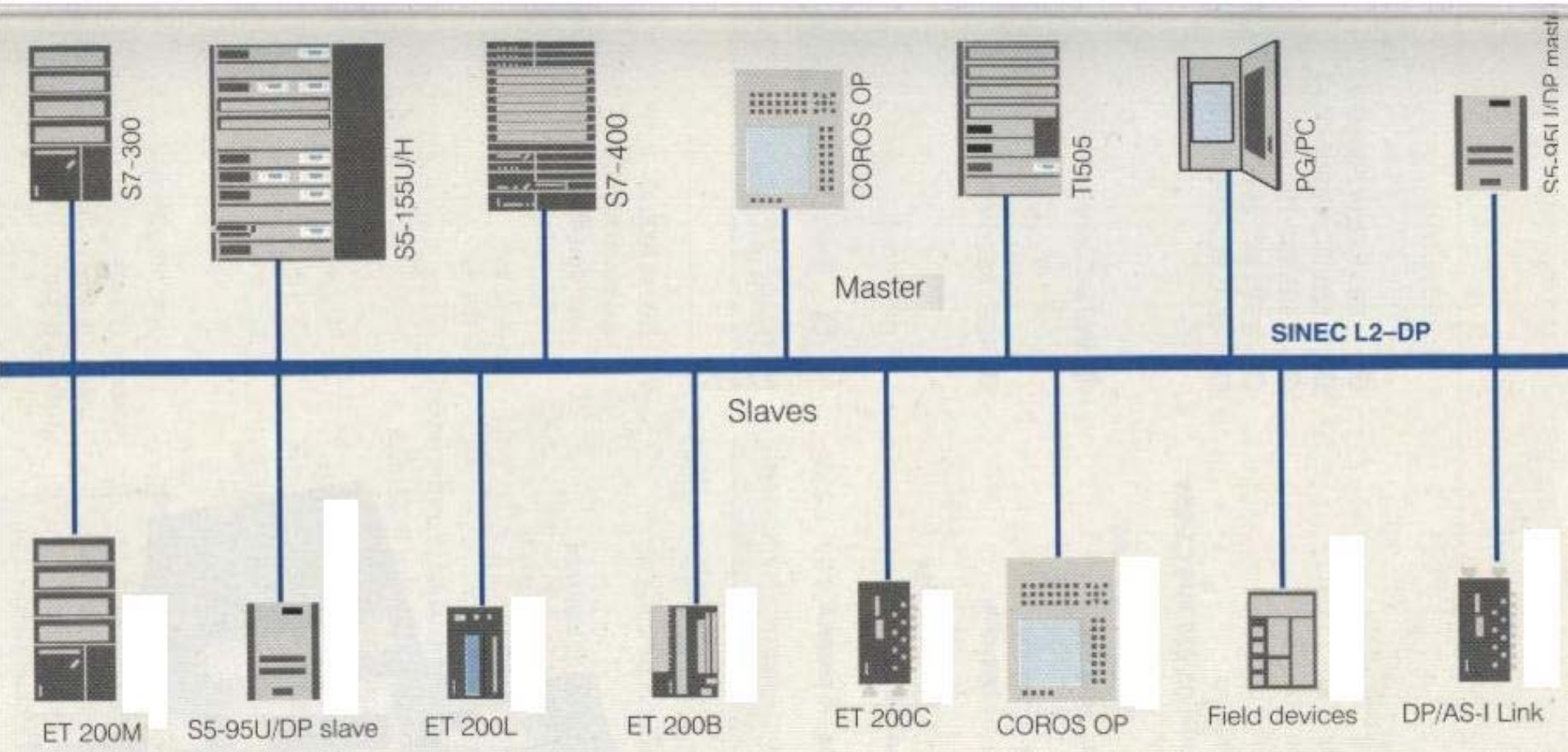


Fig. 406a. SINEC L2-DP with Distributed IO Modules

- The following can be connected to the ProFiBus-DP:
  - Active Stations:
    - S/M7 300 – 400 automation systems …as well as from other manufacturers
    - Programming devices and AT compatible PCs
    - COROS Operator Panels
  - Passive Stations:
    - ET200M/L/B/C/U distributed IO Stations, S5 Seri PLCs, DP/AS-I link transceiver
    - MMI
    - Additional field Devices as well as third party devices with slave interface Modules…

4.3. SIMATIC SOFTWARE

- STEP 7 Mini programming software
- STEP 7 Micro/DOS/Win programming software

4.3.1. Introdution

- Application:
  - SIMATIC software are array of tools based on standard for PLCs S7
  - It provides all software functions required for:
    - Configuring
    - Programming
    - Testing
    - Starting up and
    - Servicing PLCs

- Design:
  - Feature:
    - Comprehensive:
      - Shared data management; All data of a project are filed in a single central database.
      - Comprehensive series of tools; for every phase of an automation project there are user-friendly functions: configuration, parameterization of the hardware, creation and documentation of programs, as well as testing, startup and servicing.
      - Openness: Imp/Exp interface ensure connection with the PC world

- User-friendly:
  - Individual programming languages, Help and doc. Functions
  - Extensive set of command and detailed information functions (Err that may occur and their causes…)
- Standard: based on Windows OS, satisfy the standard DIN EN 6.1131-3

- Package:
  - STEP7 Micro/DOS/WIN: for programming S7-200
  - STEP7 Mini: for programming stand-alone S7-300
  - STEP7: the universal software for S7-300, -400
  - High level programming languages S7-SCL: similar to PASCAL

Technology-Oriented Software Package (w/o knowledge of PLC, computer or programming):

- S7 Graph: describing event driven processes w sequential Operation.
- S7 HiGraph: describing event driven processes w non-sequential Operation.

Software for special applications:

- COROS for parameterization of the MMI
- SIMATIC S7 standard control system
- Fuzzy control

….

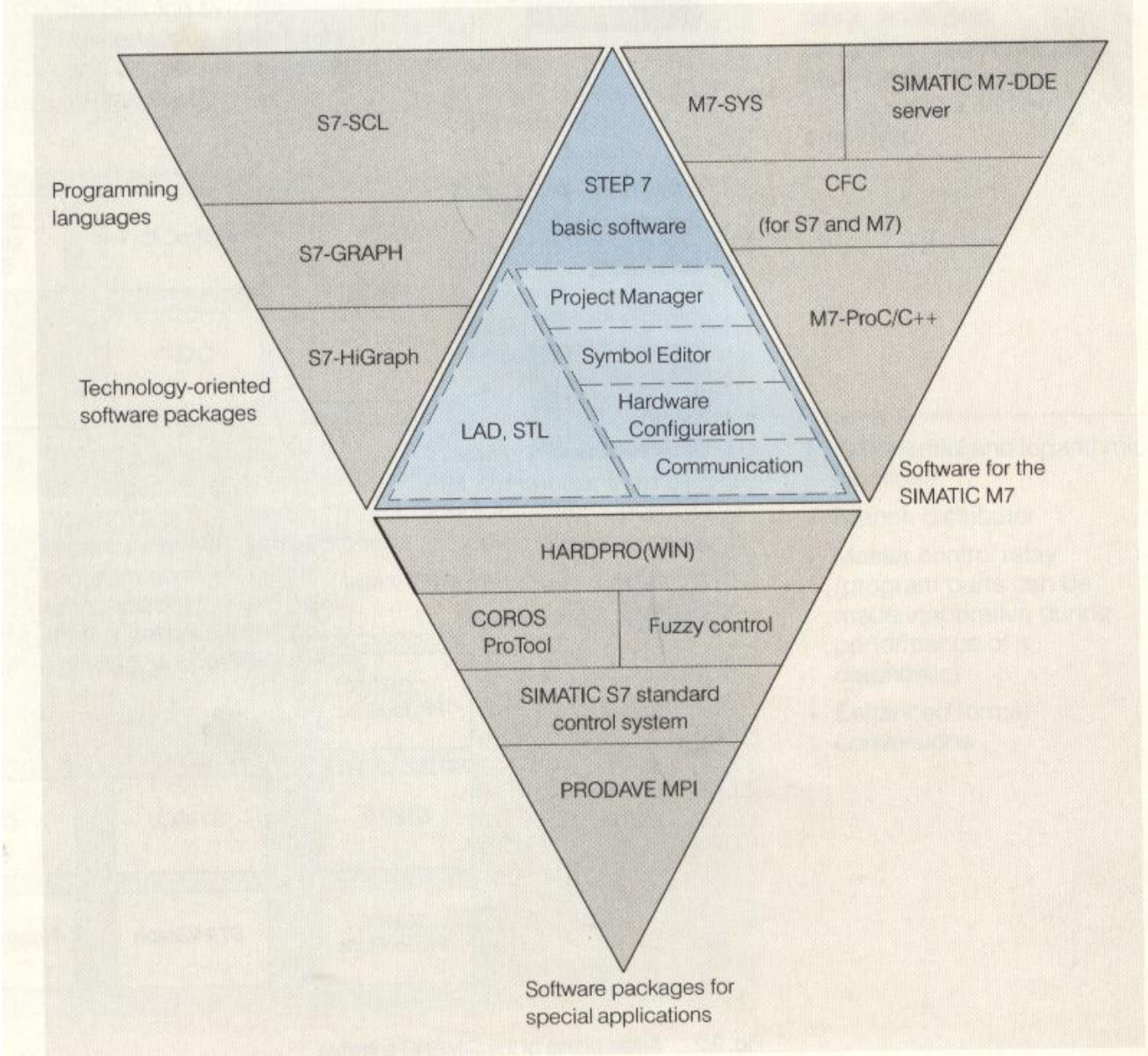


Fig 407a. STEP7 software package

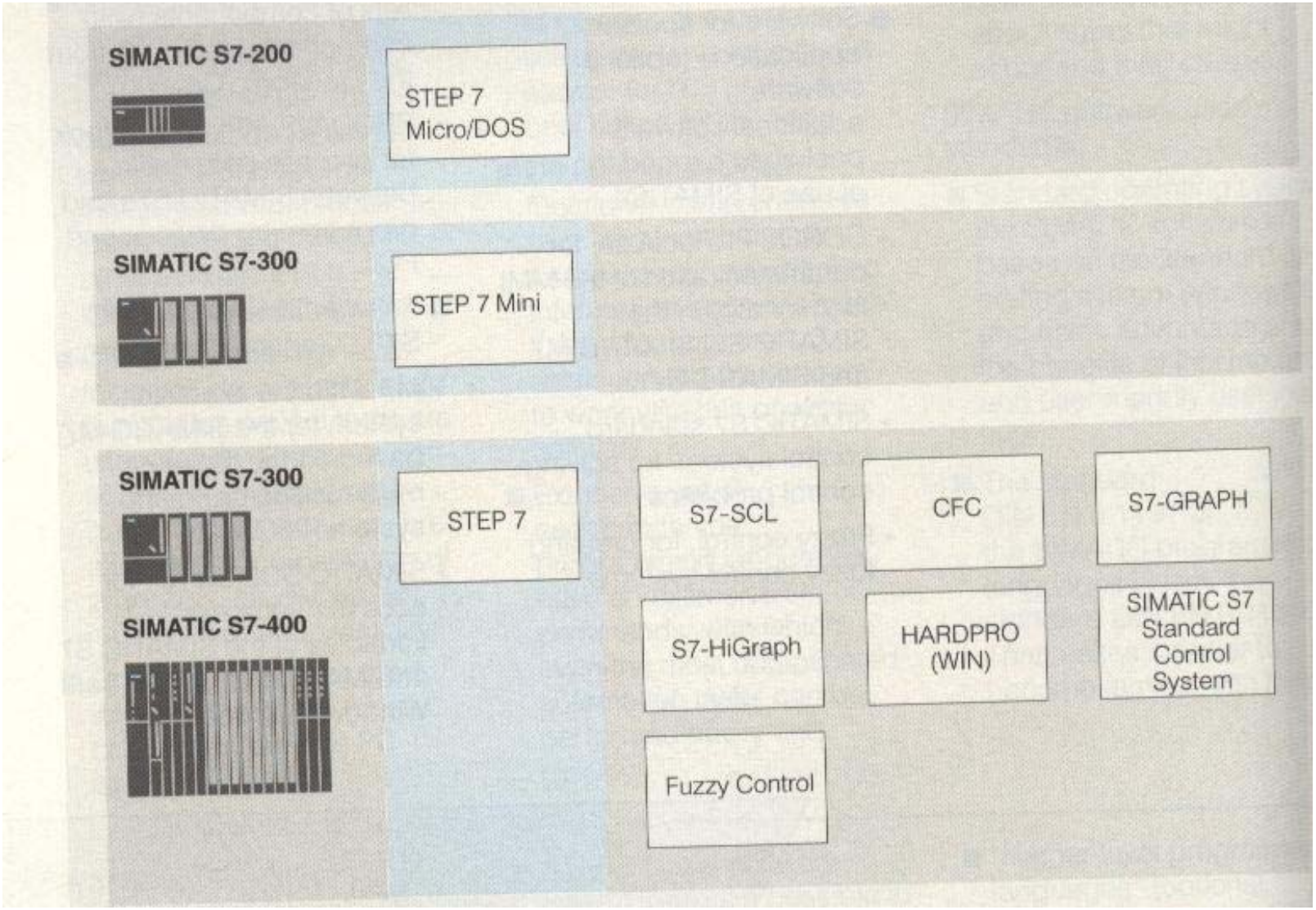


Fig 407c. PLC S7 seri software tools

4.3.2. Micro/DOS/Win for s7-200

- Configuring
- Programming
- Debugging
- Testing

4.3.3. S7-300/400

- Configuring
- Instruction Set

4.3.3.1. The modules of S7-300

- CPU Modules:
  - CPU, Mem/OS, Timer, Comm 485, onboard I/O ports (Option)
  - CPU Module: CPU 312, 314, 315, CPU31x IMF (Integrated Function Module - Onboard I/O & OS)
  - 2 Comm ports CPU - CPU 31x - DP

    (Ditributed Port): the second for networking.

- Expanded Modules:
  - PS - Power Supply: 2, 5, 10 Amp
  - SM - Signal Module: In/Out signal modules:
    - DI: Digital Input, 8, 16, 32
    - DO: Digital Output, 8, 16, 32
    - DI/DO 8/8 or 16/16
    - AI: 12 bit ADC, 2/4/8 channel
    - AO: 8/12 bit DAC, 2/4 channel
  - IM: Interface Modules: For expanding more rack. Each rack for 8 modules max (Not including CPU & PS). 1 CPU S7-300 can connect to 4 racks max via IMs.

- FM: Function modules: PID controller, Step motor, servo... modules.
- CP: Communication Modules: to communicate between PLCs and Computers

4.3.3.2. DATA & MEMORY MAPPING:

- **Data types:**
  - **Elementary data types:**

Format	Size in Bits	Number Notation
Hexadecimal	8, 16, and 32	B#16#, W#16#, and DW#16#
Binary	8, 16, and 32	2#
IEC date	16	D#
IEC time	32	T#
Time of day	32	TOD#
Character	8	'A'

- Bool
- Byte: 8 bit or ASCII character: *L B#16#14 // load byte 14h into Accu1*
- word: *L W#16#32A*
- Int: -32768 .. +32767:
- DInt: 4 byte *L DW#16#234F*
- Real: Floating Point 4 byte
- S5T (S5TIME): interval (hh/mm/ss/ms) *L S5T#2h_1m_7s_13ms.*
- TOD - Time of day: hh/mm/ss *L TOD#12:34:40.*
- DATE: *L DATE#2004-12-31.*
- CHAR: max 4 char *L 'HE_6'*

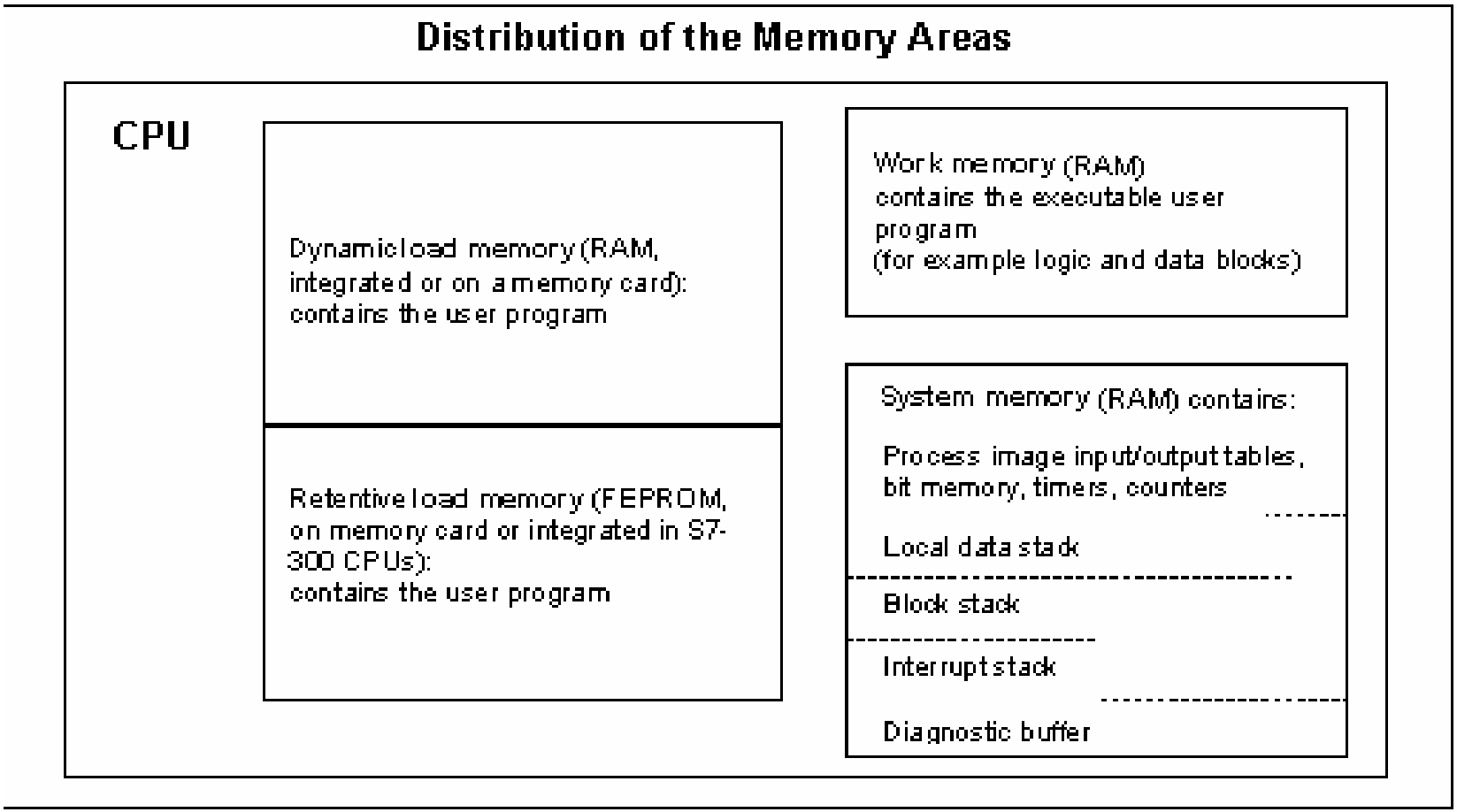
➢Complex data types

Data Type	Description
DATE_AND_TIME DT	Defines an area with 64 bits (8 bytes). This data type saves in binary coded decimal format:
STRING	Defines a group with a maximum of 254 characters (data type CHAR). The standard area reserved for a character string is 256 bytes long. This is the space required to save 254 characters and a header of 2 bytes. You can reduce the memory required for a string by defining the number of characters that will be stored in the character string (for example: string[9] 'Siemens').
ARRAY	Defines a multidimensional grouping of one data type (either elementary or complex). For example: "ARRAY [1..2,1..3] OF INT" defines an array in the format 2 x 3 consisting of integers. You access the data stored in an array using the Index ("[2,2]"). You can define up to a maximum of 6 dimensions in one array. The index can be any integer (-32768 to 32767).
STRUCT	Defines a grouping of any combination of data types. You can, for example, define an array of structures or a structure of structures and arrays.
UDT	Simplifies the structuring of large quantities of data and entering data types when creating data blocks or declaring variables in the variable declaration. In STEP 7, you can combine complex and elementary data types to create your own "userdefined" data type. UDTs have their own name and can therefore be used more than once.
FB, SFB	You determine the structure of the assigned instance data block and allow the transfer of instance data for several FB calls in one instance DB.

➢ Parameter data types

Parameter	Capacity	Description
TIMER	2. bytes	Indicates a timer to be used by the program in the called logic block. Format: T1
COUNTER	2 bytes	Indicates a counter to be used by the program in the called logic block. Format: C10
BLOCK_FB BLOCK_FC BLOCK_DB BLOCK_SDB	2 bytes	Indicates a block to be used by the program in the called logic block. Format: FC101 DB42
POINTER	6 bytes	Identifies the address. Format: P#M50.0
ANY	10 bytes	Is used when the data type of the current parameter is unknown. Format: P#M50.0 BYTE 10 P#M100.0 WORD 5

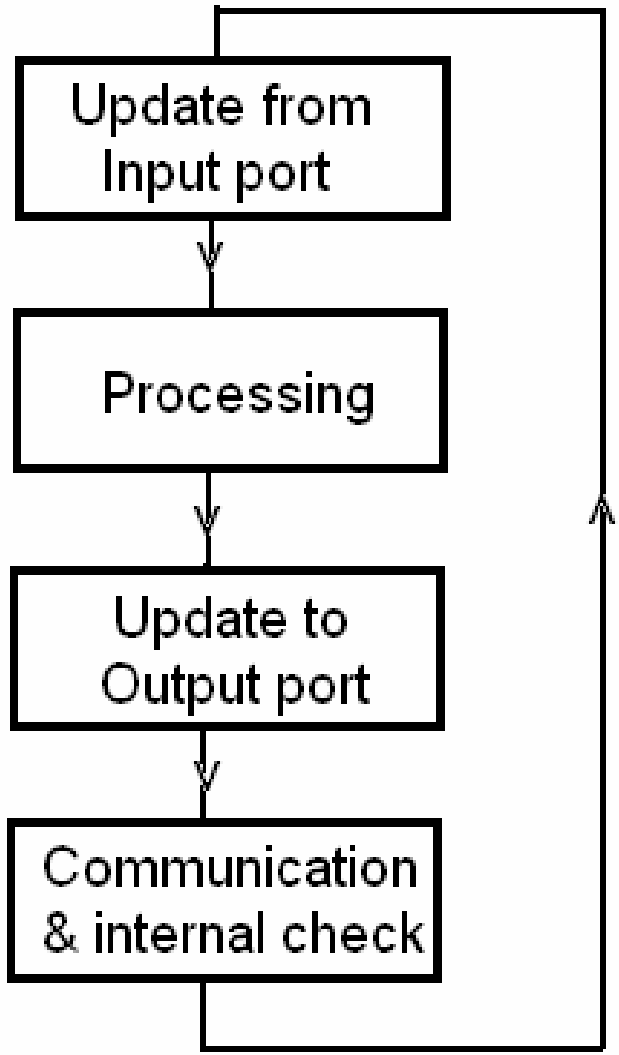
❑ Memory: 3 parts



- **Application Program memory Part - 3 sections:**
  - OB: Organisation Block
  - FC: Function - Sub module with dummy parameters of main program
  - FB: Function Block: Sub module with data exchange to/from other modules. The data must be DB (data block)
- **Data Area of OS and Appliacation - 7 sub areas:**
  - I (Process Image Input): data input buffer for DI ports. CPU just read this buffer, not ports
  - Q (Process Image Output): data output buffer for DO ports. CPU just writes this buffer, not ports
  - M: Status/Conditional: bit (M), byte (MB), word (MW), double word (MD)
  - T: Time buffer: preset/current time value and logic output.
  - C: Counter: preset/current counter value and logic output.
  - PI: I/O External Input Address for analog inputs: PIB, PIW, PID
  - PQ: I/O External Output Address for analog outputs: PQB, PQW, PQD
- **Data Blocks - 2 blocks:**
  - DB: data block, accessible by: DBX (bit), DBB, DBW, DBD
  - L (Local data blocks) local data memory of OB, FC, FB. Accessible: L (bit), LB, LW, LD.

4.3.3.3. SCAN LOOP:

- 4 phases
- Scan time not fix - tùy nhiều hay ít lệnh
- Interrupt Service block: OB40, OB80... được thực hiện tại bất kỳ thời điểm nào - không cần trật tự.



4.3.3.4. PROGRAM STRUCTURES:

- Linear Programming
- Structructured Programming: OB (Organization Blocks), FC (Program Blocks), FB (Function Blocks), DB (Data Blocks)
- Số các module gọi lồng nhau: CPU 314: là 8, nếu quá thì STOP

4.3.3.5. SPECIAL BLOCKS:

- OB10: Time of day Interrupt - single, multiple @ fix time from SFC28 (sys function block),
- OB20: Time delay Interrupt, SFC32,
- OB35: Cyclic Interrupt: default 100ms,
- OB40: Hardware Interrupt, báo ngắt thông qua một số module đặc biệt: SM, CP, FM, onboard IO.
- OB80: Cycle time Over, default of cycle scan time 150ms,
- OB81: Power Supply Fault,
- OB82: Diagnostic Interrupt: from IO Module
- OB85: Not Load Fault - No interrupt service block
- OB87: Communication Fault - parity, time out error
- OB100: Start Up Information - from STOP to START
- ...

4.4 Programming Languages

- 3 types of Prog Language
  - STL - Statement List,
  - LAD - Ladder and
  - FBD - Function Block Diagram.

  Trong đó LAD và FBD đơn giản hơn, vậy không chuyển được qua STL, nhưng ngược lại thì được.

4.4.1. Cấu trúc lệnh STL:

- **Label:** OpcodeOperand [// Comment]
- **Data Operand:** bit (logic), binary, hex, INT, DINT, REAL, S5T, TOD, DATE, C(ounter down), P - địa chỉ ô nhớ, CHAR...
- **Toán hạng là địa chỉ:**
  - M (bit-mem), MB (byte-mem), MW (word-mem), MD (DW-mem),
  - I (bit-Inp), IB (byte-Inp), IW (word-Inp), ID (DW-Inp),
  - Q, QB, QW, QD,
  - T(imer), C(ounter),
  - PIB (analog inp - byte), PIW, PID,
  - PQB, PQW, PQD,
  - DBX (bit), DBB, DBW, DBD, ...

- **Addresses and Data Types Permitted in the Symbol Table**
- Only one set of mnemonics can be used throughout a symbol table. Switching between SIMATIC (German) and IEC (English) mnemonics must be done in the SIMATIC Manager using the menu command **Options > Customize** in the "Language" tab.
- **IEC SIMATIC Description Data Type Value Range**

IEC	SIMATIC	Description	Data Type	Value Range
I	E	Input bit	BOOL	0.0 to 65535.7
IB	EB	Input byte	BYTE, CHAR	0 to 65535
IW	EW	Input word	WORD, INT, S5TIME	0 to 65534
ID	ED	Input double word	DWORD, DINT, REAL, TOD, TIME	0 to 65532
Q	A	Output bit	BOOL	0.0 to 65535.7
QB	AB	Output byte	BYTE, CHAR	0 to 65535
QW	AW	Output word	WORD, INT, S5TIME	0 to 65534
QD	AD	Output double word	DWORD, DINT, REAL, TOD, TIME	0 to 65532
M	M	Memory bit	BOOL	0.0 to 65535.7
MB	MB	Memory byte	BYTE, CHAR	0 to 65535
MW	MW	Memory word	WORD, INT, S5TIME	0 to 65534
MD	MD	Memory double word	DWORD, DINT, REAL, TOD, TIME	0 to 65532
PIB	PEB	Peripheral input byte	BYTE, CHAR	0 to 65535
PQB	PAB	Peripheral output byte	BYTE, CHAR	0 to 65535
PIW	PEW	Peripheral input word	WORD, INT, S5TIME	0 to 65534
PQW	PAW	Peripheral output word	WORD, INT, S5TIME	0 to 65534
PID	PED	Peripheral input double	DWORD, DINT, REAL, TOD,	0 to 65532

		word	TIME	
PQD	PAD	Peripheral output double word	DWORD, DINT, REAL, TOD, TIME	0..65532
T	T	Timer	TIMER	0 to 65535
C	Z	Counter	COUNTER	0 to 65535
FB	FB	Function block	FB	0 to 65535
OB	OB	Organization block	OB	1. to 65535
DB	DB	Data block	DB, FB, SFB, UDT	1. to 65535
FC	FC	Function	FC	0 to 65535
SFB	SFB	System function block	SFB	0 to 65535
SFC	SFC	System function	SFC	0 to 65535
VAT	VAT	Variable table		0 to 65535
UDT	UDT	User defined data type	UDT	0 to 65535

- Ví dụ:
  - I 1.3 // bit 3, byte 1 from Input port PII
  - M 101.5 // Bit 5, byte thứ 101 trong miền M
  - Q 4.5 // bit 5, byte 4 của PIQ
  - DIB 15 // Ô nhớ 1 byte, byte thứ 15 trong DB
  - DBW 18 // ô nhớ 1 word, byte 18 và 19 @ DB
  - DB2.DBW 15// byte 15 và 16 trong khối số liệu DB2
  - MD 105 // 4 byte 105..108 trong DB

Status Word: 9 bit (2 byte)

- Bit 0 - FC - First Check: khi = 1 báo thực hiện 1 dãy các lệnh logic, thực hiện xong FC = 0
- RLO Result of Logic Operation - kết quả của phép thực hiện logic. Ví dụ: *A I 0.3* Nếu trước đó, FC=0 thì chuyển bit I 0.3 vào RLO
- Nếu FC=1 thì (I 0.3 AND RLO) => RLO
- STA - Status bit, tương ứng với mức logic của port.
  Ví dụ *A* *I 0.3* *//* hoặc
  AN *I 0.3* *//* đều gán cho STA logic của port I 0.
- OR - giá trị logic của phép $\wedge$ để các phép $\vee$ sau đó.
- OS - Store Overflow bit - lưu lại cờ tràn ra mem cùng kết quả xử lý
- OV - Overflow: báo phép tính số học tràn
- CCO & CC I - condition code: cho 5 trường hợp tính toán khác nhau, ví dụ như tính toán số nguyên - không tràn

0	0	kết quả = 0
0	1	kết quả <0
1	0	kết quả >0

- BR - binary result bit: kết hợp 2 loại lập trình LAD và STL

4.4.2. Instruction Groups:

❑ Bit logic Instruction (1st):

➢ *Lệnh gán:*

- Cú pháp = <toán hạng - I/Q/M/L/D>
- *Ví dụ: gán giá trị từ cổng vào I 0.2 sang Q 2.1*

  Network 1

  A I0.2 = Q2.1

➢ *Lệnh AND (∧) :*

- Cú pháp: **A** <toán hạng - số liệu kiểu Bool hoặc địa chỉ I/Q/M/L/D>
- *Ví dụ: t/hphép AND và cất kết quả*

  Network 1

  A I0.2

  A I2.1 = Q4.6

➢ *Lệnh AND-NOT:*

- Cú pháp: **AN** <I/Q/M/L/D>
- *Ví dụ: t/hphép AND-NOT và cất kết quả*

Network 1
A I0.2
AN I2.1 = Q4.6

➢ *Lệnh OR:*

- Cú pháp **O** <I/Q/M/L/D>
- *Ví dụ: t/hphép OR và cất kết quả*

Network 1
A I0.2 //đọc nội dung I0.2, đưa vào RLO
O I2.1= Q4.6

- ***Lệnh OR-NOT:***
  - Cú pháp **ON** <I/Q/M/L/D>
  - *Ví dụ: t/hphép OR-NOT và cất kết quả*

```
Network 1
A       I0.2
ON      I2.1    =       Q4.6
```

- ***Lệnh AND với 1 biểu thức:***
  - Cú pháp **A(** - lệnh không toán hạng. Nếu FC=0, kết quả logic của biểuthức sẽ cất trong RLO. Nếu FC=1, sẽ AND kết quả logic biểu thức với RLO
- *Ví dụ: t/hphép AND và cất kết quả*

```
Network 1
A(
O       I0.2
O       I2.1    )               // chuyển k/quả vào RLO
A(
ON      I1.2
O       I2.3    )
=       Q4.6
```

❑ Tương tự như **AN(, O(, ON(**

- ***Lệnh XOR:***
  - Cú pháp **X** <I/Q/M/L/D>
  - *Ví dụ: t/hphép XOR và cất kết quả*

  Network 1

  AN I0.2

  A I0.5

  X I0.6 = Q4.6
- **Tương tự như XN, X(, XN(**
- ***Lệnh SET RLO:***
- ***Lệnh CLR RLO:***
- ***Lệnh NOT RLO:***

- ***Lệnh set bit mem có điều kiện:*** *Lệnh sẽ gán 1 vào địa chỉ ô nhớ khi RLO = 1* Cú pháp **S <toán hạng>**
- ***Lệnh clear bit mem có điều kiện:*** *Lệnh sẽ gán 1 vào địa chỉ ô nhớ khi RLO = 1* Cú pháp **R <toán hạng>**
- ***Lệnh nhận sườn lên :*** theo chu kỳ các vòng quét. Nếu trước đó, RLO =0, lưu vào M10.0 - bít nhớ cờ), chu kỳ sau RLO = 1
  - Cú pháp: **FP** **<Toán hạng>**
  - Ví dụ:

  A I1.0

  FP M10.0 = Q4.5
- ***Lệnh nhận sườn xuống***
  - **FN** **<Toán hạng>**
  - ***Copy RLO sang BR -*** *binary result*

Comparison Instructions (2nd Group)

- **Description:** ACCU1 and ACCU2 are compared according to the type of comparison you choose:
  - == ACCU1 is equal to ACCU2
  - <> ACCU1 is not equal to ACCU2
  - > ACCU1 is greater than ACCU2
  - < ACCU1 is less than ACCU2
  - >= ACCU1 is greater than or equal to ACCU2
  - <= ACCU1 is less than or equal to ACCU2
- If the comparison is true, the RLO of the function is "1". The status word bits CC 1 and CC 0 indicate the relations ‘’less,” ‘’equal,” or ‘’greater.”
- There are comparison instructions to perform the following functions:
- ? I Compare Integer (16-bit)
- ? D Compare Double Integer (32-bit)
- ? R Compare Floating-point Number (32-bit)

Conversion Instructions (3rd)

- **Description** You can use the following instructions to convert binary coded decimal numbers and integers to other types of numbers:
  - BTI BCD to Integer (16-bit)
  - ITB Integer (16-bit) to BCD
  - BTD BCD to Integer (32-bit)
  - ITD Integer (16-bit) to Double Integer (32-bit)
  - DTB Double Integer (32-bit) to BCD
  - DTR Double Integer (32-bit) to Floating-point (32-bit IEEE-FP)
- You can use one of the following instructions to form the complement of an integer or to invert the sign of a floating-point number:
  - INVI Ones Complement Integer (16-bit)
  - INVD Ones Complement Double Integer (32-bit)
  - NEGI Twos Complement Integer (16-bit)
  - NEGD Twos Complement Double Integer (32-bit)
  - NEGR Negate Floating-point Number (32-bit, IEEE-FP)

- You can use the following Change Bit Sequence in Accumulator 1 instructions to reverse the order of bytes in the low word of accumulator 1 or in the entire accumulator:
  - CAW Change Byte Sequence in ACCU 1-L (16-bit)
  - CAD Change Byte Sequence in ACCU 1 (32-bit)
- You can use any of the following instructions to convert a 32-bit IEEE floating-point number in accumulator 1 to a 32-bit integer (double integer). The individual instructions differ in their method of rounding:
  - RND Round
  - TRUNC Truncate
  - RND+ Round to Upper Double Integer
  - RND- Round to Lower Double Integer

❑ Counter Instructions (4th)

- **Description:** A counter is a function element of the STEP 7 programming language that acounts. Counters have an area reserved for them in the memory of your CPU. This memory area reserves one 16-bit word for each counter. The statement list instruction set supports 256 counters. To find out how many counters are available in your CPU, please refer to the CPU technical data.
- Counter instructions are the only functions with access to the memory area.
- You can vary the count value within this range by using the following Counter instructions:
  - FR Enable Counter (Free)
  - L Load Current Counter Value into ACCU 1
  - LC Load Current Counter Value into ACCU 1, BCD
  - R Reset Counter
  - S Set Counter Preset Value
  - CU Counter Up
  - CD Counter Down

Data Block Instructions (5th)

- **Description:** You can use the Open a Data Block (OPN) instruction to open a data block as a shared data block or as an instance data block. The program itself can accomodate one open shared data block and one open instance data block at the same time.
- The following Data Block instructions are available:

• OPN	Open a Data Block
• CDB	Exchange Shared DB and Instance DB
• L DBLG	Load Length of Shared DB in ACCU 1
• L DBNO	Load Number of Shared DB in ACCU 1
• L DILG	Load Length of Instance DB in ACCU1
• L DINO	Load Number of Instance DB in ACCU1

❑ Logic Control Instructions (6th)

- **Description:** You can use the Jump instructions to control the flow of logic, enabling your program to interrupt its linear flow to resume scanning at a different point. You can use the LOOP instruction to call a program segment multiple times. The address of a Jump or Loop instruction is a label. A jump label may be as many as four characters, and the first character must be a letter. Jumps labels are followed with a mandatory colon "**:**" and must precede the program statement in a line.
- **Note:** Please note for S7-300 CPU programs that the jump destination always (not for 318-2) forms the **beginning** of a Boolean logic string in the case of jump instructions. The jump destination must not be included in the logic string.

- You can use the following jump instructions to interrupt the normal flow of your program unconditionally:
  - JU Jump Unconditional
  - JL Jump to Labels
- The following jump instructions interrupt the flow of logic in your program based on the result of logic operation (RLO) produced by the previous instruction statement:
  - JC Jump if RLO = 1
  - JCN Jump if RLO = 0
  - JCB Jump if RLO = 1 with BR
  - JNB Jump if RLO = 0 with BR

- *Logic Control Instructions:* The following jump instructions interrupt the flow of logic in your program based on the signal state of a bit in the status word:
  - JBI Jump if BR = 1
  - JNBI Jump if BR = 0
  - JO Jump if OV = 1
  - JOS Jump if OS = 1
- The following jump instructions interrupt the flow of logic in your program based on the result of a calculation:
  - JZ Jump if Zero
  - JN Jump if Not Zero
  - JP Jump if Plus
  - JM Jump if Minus
  - JPZ Jump if Plus or Zero
  - JMZ Jump if Minus or Zero
  - JUO Jump if Unordered

❑ Integer Math Instructions (7th)

- **Description:** The math operations combine the contents of accumulators 1 and 2. The result is stored in accumulator 1. The old contents of accumulator 1 is shifted to accumulator 2. The contents of accumulator 2 remains unchanged.
- In the case of CPUs with four accumulators, the contents of accumulator 3 is hen copied into accumulator 2 and the contents of accumulator 4 into accumulator 3.
- The old contents of accumulator 4 remains unchanged.
- Using integer math, you can carry out the following operations with **two integer numbers** (16 and 32 bits):
  - +I Add ACCU 1 and ACCU 2 as Integer (16-bit)
  - -I Subtract ACCU 1 from ACCU 2 as Integer (16-bit)
  - *I Multiply ACCU 1 and ACCU 2 as Integer (16-bit)
  - /I Divide ACCU 2 by ACCU 1 as Integer (16-bit)

- + Add Integer Constant (16, 32 Bit)
- +D Add ACCU 1 and ACCU 2 as Double Integer (32-bit)
- -D Subtract ACCU 1 from ACCU 2 as Double Integer (32-bit)
- *D Multiply ACCU 1 and ACCU 2 as Double Integer (32-bit)
- /D Divide ACCU 2 by ACCU 1 as Double Integer (32-bit)
- MOD Division Remainder Double Integer (32-bit)

➢ See also Evaluating the Bits of the Status Word with Integer Math Instructions.

❑ Floating-point Math Instructions (8th)

- **Description:** The math instructions combine the contents of accumulators 1 and 2. The result is stored in accumulator 1. The old contents of accumulator 1 is shifted to accumulator 2. The contents of accumulator 2 remains unchanged.
- In the case of CPUs with four accumulators, the contents of accumulator 3 is copied into accumulator 2 and the contents of accumulator 4 into accumulator 3.
- The old contents of accumulator 4 remains unchanged.
- The IEEE 32-bit floating-point numbers belong to the data type called REAL.
- You can use the floating-point math instructions to perform the following math
- instructions using **two 32-bit IEEE floating-point numbers**:

- +R Add ACCU 1 and ACCU
- -R Subtract ACCU 1 from ACCU 2
- *R Multiply ACCU 1 and ACCU 2
- /R Divide ACCU 2 by ACCU 1

➢ Using floating-point math, you can carry out the following operations with **one 32-bit IEEE floating-point number**:

- ABS Absolute Value
- SQR Generate the Square
- SQRT Generate the Square Root
- EXP Generate the Exponential Value
- LN Generate the Natural Logarithm
- SIN Generate the Sine of Angles
- COS Generate the Cosine of Angles
- TAN Generate the Tangent of Angles
- ASIN Generate the Arc Sine
- ACOS Generate the Arc Cosine
- ATAN Generate the Arc Tangent

➢ See also Evaluating the Bits of the Status Word.

❑ Load and Transfer Instructions (9th)

- **Description:** The Load (L) and Transfer (T) instructions enable you to program an interchange of information between input or output modules and memory areas, or between memory areas. The CPU executes these instructions in each scan cycle as unconditional instructions, that is, they are not affected by the result of logic operation of a statement. The following Load and Transfer instructions are available:
  - L Load
  - L STW Load Status Word into ACCU 1
  - LAR1 AR2 Load Address Register 1 from Address Register 2
  - LAR1 <D> Load Address Register 1 with Double Integer (32-bit Pointer)

`

• LAR1	Load Address Register 1 from ACCU 1
• LAR2 <D>	Load Address Register 2 with Double Integer (32-bit Pointer)
• LAR2	Load Address Register 2 from ACCU 1
• T	Transfer
• T STW	Transfer ACCU 1 into Status Word
• TAR1 AR2	Transfer Address Register 1 to Address Register 2
• TAR1 <D>	Transfer Address Register 1 to Destination (32-bit Pointer)
• TAR2 <D>	Transfer Address Register 2 to Destination (32-bit Pointer)
• TAR1	Transfer Address Register 1 to ACCU 1
• TAR2	Transfer Address Register 2 to ACCU 1
• CAR	Exchange Address Register 1 with Address Register 2

❑ Program Control Instructions (10th)

- **Description:** The following instructions are available for performing program control instructions:
  - BE Block End
  - BEC Block End Conditional
  - BEU Block End Unconditional
  - CALL Block Call
  - CC Conditional Call
  - UC Unconditional Call
  - Call FB
  - Call FC
  - Call SFB
  - Call SFC
  - Call Multiple Instance
  - Call Block from a Library
  - MCR (Master Control Relay). Important Notes on Using MCR Functions
  - MCR(Save RLO in MCR Stack, Begin MCR
  -)MCR End MCR
  - MCRA Activate MCR Area
  - MCRD Deactivate MCR Area

❑ Shift and Rotate Instructions (11th)

➢ 11.1 Shift Instructions

- **Description:** You can use the Shift instructions to move the contents of the low word of accumulator 1 or the contents of the whole accumulator bit by bit to the left or the right (see also CPU Registers). Shifting by n bits to the left multiplies the contents of the accumulator by “2 n ”; shifting by n bits to the right divides the contents of the accumulator by “2 n ”. For example, if you shift the binary equivalent of the decimal value 3 to the left by 3 bits, you end up with the binary equivalent of the decimal value 24 in the accumulator. If you shift the binary equivalent of the decimal value 16 to the right by 2 bits, you end up with the binary equivalent of the decimal value 4 in the accumulator.

The number that follows the shift instruction or a value in the low byte of the low word of accumulator 2 indicates the number of bits by which to shift. The bit places that are vacated by the shift instruction are either filled with zeros or with the signal state of the sign bit (a 0 stands for positive and a 1 stands for negative). The bit that is shifted last is loaded into the CC 1 bit of the status word. The CC 0 and OV bits of the status word are reset to 0. You can use jump instructions to evaluate the CC 1 bit. The shift operations are unconditional, that is, their execution does not depend on any special conditions. They do not affect the result of logic operation.

- **The following Shift instructions are available:**
  - SSI Shift Sign Integer (16-bit)
  - SSD Shift Sign Double Integer (32-bit)
  - SLW Shift Left Word (16-bit)
  - SRW Shift Right Word (16-bit)
  - SLD Shift Left Double Word (32-bit)
  - SRD Shift Right Double Word (32-bit)

❑ 11.2 Rotate Instructions

- **Description:** You can use the Rotate instructions to rotate the entire contents of accumulator 1 bit by bit to the left or to the right (see also CPU Registers). The Rotate instructions trigger functions that are similar to the shift functions described in Section 14.1. However, the vacated bit places are filled with the signal states of the bits that are shifted out of the accumulator. The number that follows the rotate instruction or a value in the low byte of the low word of accumulator 2 indicates the number of bits by which to rotate. Depending on the instruction, rotation takes place via the CC 1 bit of the status word. The CC 0 bit of the status word is reset to 0.
- The following Rotate instructions are available:
  - RLD Rotate Left Double Word (32-bit)
  - RRD Rotate Right Double Word (32-bit)
  - RLDA Rotate ACCU 1 Left via CC 1 (32-bit)
  - RRDA Rotate ACCU 1 Right via CC 1 (32-bit)

❑ Timer Instructions (12th)

- **Description:** You can find information for setting and selecting the correct time under Location of a Timer in Memory and components of a Timer. The following timer instructions are available:
  - FR Enable Timer (Free)
  - L Load Current Timer Value into ACCU 1 as Integer
  - LC Load Current Timer Value into ACCU 1 as BCD
  - R Reset Timer
  - SD On-Delay Timer
  - SE Extended Pulse Timer
  - SF Off-Delay Timer
  - SP Pulse Timer
  - SS Retentive On-Delay Timer

❑ Word Logic Instructions (13th)

- **Description:** Word logic instructions compare pairs of words (16 bits) and double words (32 bits) bit by bit, according to Boolean logic. Each word or double word must be in one of the two accumulators. For words, the contents of the low word of accumulator 2 is combined with the contents of the low word of accumulator 1. The result of the combination is stored in the low word of accumulator 1, overwriting the old contents. For double words, the contents of accumulator 2 is combined with the contents of accumulator 1. The result of the combination is stored in accumulator 1, overwriting the old contents.
- If the result does not equal 0, bit CC 1 of the status word is set to "1". If the result does equal 0, bit CC 1 of the status word is set to "0".
- The following instructions are available for performing Word Logic operations:
  - AW AND Word (16-bit)
  - OW OR Word (16-bit)
  - XOW Exclusive OR Word (16-bit)
  - AD AND Double Word (32-bit)
  - OD OR Double Word (32-bit)
  - XOD Exclusive OR Double Word (32-bit)

❑ Accumulator and Address Register Instructions (14th)

- **Description:** The following instructions are available to you for handling the contents of one or both accumulators:
  - TAK Toggle ACCU 1 with ACCU 2
  - PUSH CPU with Two ACCUs
  - PUSH CPU with Four ACCUs
  - POP CPU with Two ACCUs
  - POP CPU with Four ACCUs
  - ENT Enter ACCU Stack
  - LEAVE Leave ACCU Stack
  - INC Increment ACCU 1-L-L
  - DEC Decrement ACCU 1-L-L
  - +AR1 Add ACCU 1 to Address Register 1
  - +AR2 Add ACCU 1 to Address Register 2
  - BLD Program Display Instruction (Null)
  - NOP 0 Null Instruction
  - NOP 1 Null Instruction