

**Tác giả**  
**TS. ĐỖ VĂN CẦN**

SÁCH CHUYÊN KHẢO  
**MẠNG TRUYỀN THÔNG**  
**CÔNG NGHIỆP VÀ SCADA**

Nhà xuất bản Khoa học và Kỹ thuật

## MỤC LỤC

MỤC LỤC.....	i
DANH MỤC HÌNH VẼ.....	v
DANH MỤC CÁC BẢNG.....	ix
CÁC TỪ VIẾT TẮT .....	x
LỜI NÓI ĐẦU .....	xi
CHƯƠNG 1: CÁC KHÁI NIỆM CƠ BẢN VỀ MẠNG TRUYỀN THÔNG CÔNG NGHIỆP VÀ SCADA.....	1
1.1 Các khái niệm cơ bản .....	1
1.1.1 Kỹ thuật điều khiển .....	1
1.1.2 Hệ thống điều khiển phân tán (Distributed Control System - DCS)....	2
1.1.3 Điều khiển quá trình .....	2
1.1.4 Thông tin .....	3
1.1.5 Dữ liệu .....	4
1.1.6 Tín hiệu.....	4
1.1.7 Giao thức: .....	5
1.1.8 IEC.....	5
1.1.9 SCADA.....	6
1.2 Mô hình phân cấp chức năng.....	8
1.2.1 Phân loại mạng công nghiệp .....	9
1.2.2 Hệ thời gian thực .....	10
1.2.3 Nguyên tắc cơ bản của truyền thông .....	11
1.3 Câu hỏi ôn tập.....	12
CHƯƠNG 2: CƠ SỞ MẠNG CÔNG NGHIỆP .....	13
2.1 Kiến trúc giao tiếp .....	13
2.1.1 Kiến trúc Chủ/ tớ (Master/Slave) .....	13
2.1.2 Kiến trúc Client/Server.....	13
2.2 Cấu trúc mạng (network topology).....	14
2.2.1 Liên kết (link).....	14
2.2.2 Cấu trúc (Topology) .....	14
2.3 Kiểm soát truy nhập bus .....	14
2.3.1 Phương pháp kiểm soát tập trung chủ/tớ (Master/Slave).....	15
2.3.2 Phương pháp kiểm soát phân tán Token Passing .....	16
2.3.3 Kết hợp Token với Master/Slave (Multimaster) .....	17
2.3.4 Truy nhập nhận biết xung đột CSMA/CD .....	17
2.4 Bảo toàn dữ liệu.....	18
2.4.1 Lỗi dữ liệu .....	18
2.4.2 Bảo toàn dữ liệu kiểu bit chẵn/lẻ (parity bit) .....	19
2.4.3 Bảo toàn kiểu mã vòng (CRC) .....	20
2.4.4 Bảo toàn kiểu nhồi bit (Bit stuffing) .....	21
2.5 Mã hóa và giải mã bit .....	21
2.5.1 Phương pháp NRZ và RZ.....	21
2.5.2 Mã Manchester .....	22
2.5.3 Mã AFP (Alternate Flanked Pulse) .....	22
2.5.4 Mã FSK (Frequency Shift Keying) .....	23
2.6 Câu hỏi ôn tập chương.....	23
CHƯƠNG 3: KỸ THUẬT MẠNG CÔNG NGHIỆP .....	24

3.1	Kỹ thuật truyền dẫn .....	24
3.1.1	Phương thức truyền dẫn tín hiệu đơn cực .....	24
3.1.2	Phương thức truyền dẫn tín hiệu đối xứng .....	24
3.1.3	Phương thức truyền dẫn MBP (IEC 61158-2) .....	25
3.1.4	Chuẩn truyền thông RS-485 .....	25
3.2	Giao thức mạng .....	27
3.2.1	Định nghĩa giao thức mạng (network protocol) .....	27
3.2.2	Mô hình lớp .....	28
3.2.3	Mô hình qui chiếu ISO/OSI.....	28
3.2.4	Kiến trúc TCP/IP .....	31
3.3	Các thành phần trong mạng truyền thông.....	31
3.3.1	Dây dẫn.....	31
3.3.2	Vô tuyến: .....	33
3.3.3	NIC – Network Interface Card .....	33
3.3.4	Hộp .....	33
3.3.5	Các bộ kết nối mạng.....	34
3.3.6	Gateway .....	35
3.4	Phần cứng giao diện mạng.....	35
3.4.1	Ghép nối thiết bị điều khiển .....	35
3.5	Phần mềm trong hệ thống mạng .....	37
3.5.1	Phần mềm (xử lý) giao thức .....	37
3.5.2	Phần mềm thư viện:.....	37
3.5.3	Phần mềm giao diện lập trình (API).....	37
3.6	Câu hỏi ôn tập chương.....	38
<b>CHƯƠNG 4: CÁC MẠNG THÔNG DỤNG.....</b>		<b>39</b>
4.1	Mạng trường – AS Interface.....	39
4.1.1	Giới thiệu chung .....	39
4.1.2	Kiến trúc giao thức .....	40
4.1.3	Cấu trúc mạng & cáp truyền.....	40
4.1.4	Cơ chế giao tiếp.....	40
4.1.5	Cấu trúc bức điện.....	41
4.1.6	Mã hóa bit.....	41
4.1.7	Bảo toàn dữ liệu.....	41
4.1.8	Ứng dụng .....	42
4.2	Mạng Profibus .....	42
4.2.1	Giới thiệu chung .....	42
4.2.2	Kiến trúc giao thức .....	43
4.2.3	Kỹ thuật truyền dẫn (lớp 1) .....	43
4.2.4	Truy nhập bus (lớp 2) .....	45
4.2.5	Dịch vụ truyền dữ liệu (lớp 2).....	45
4.2.6	Cấu trúc bức điện (lớp 2).....	46
4.3	Interbus .....	47
4.3.1	Giới thiệu chung .....	47
4.3.2	Kiến trúc giao thức .....	47
4.3.3	Cấu trúc mạng .....	47
4.3.4	Kỹ thuật truyền dẫn .....	48
4.3.5	Cơ chế giao tiếp.....	48

4.3.6	Cấu trúc bức điện.....	49
4.4	Mạng CAN .....	49
4.4.1	Giới thiệu chung .....	49
4.4.2	Kiến trúc giao thức .....	49
4.4.3	Cấu trúc mạng & KT truyền dẫn.....	50
4.4.4	Cơ chế giao tiếp.....	50
4.4.5	Cấu trúc bức điện.....	50
4.4.6	Bảo toàn dữ liệu.....	51
4.5	Mạng Ethernet .....	51
4.5.1	Giới thiệu chung .....	51
4.5.2	Kiến trúc giao thức .....	53
4.5.3	Cấu trúc mạng và Kỹ thuật truyền dẫn.....	53
4.5.4	Cơ chế giao tiếp.....	54
4.5.5	Cấu trúc bức điện.....	54
4.5.6	Các tiến bộ công nghệ mới.....	55
4.6	Câu hỏi ôn tập chương.....	55
<b>CHƯƠNG 5: SCADA TRONG HỆ THỐNG ĐIỆN.....</b>		<b>56</b>
5.1	Tổng quan .....	56
5.2	Các loại hình SCADA trong hệ thống điện.....	57
5.2.1	SCADA điều độ cấp quốc gia .....	57
5.2.2	SCADA trạm .....	58
5.3	Nguyên tắc làm việc của hệ thống SCADA như sau: .....	59
5.3.1	Thu thập dữ liệu: .....	59
5.3.2	Điều khiển: .....	60
5.3.3	Giám sát:.....	60
5.4	Các thiết bị trong SCADA EVN .....	60
5.4.1	Các RTU.....	60
5.4.2	Gateway.....	63
5.4.3	Server ứng dụng AS .....	64
5.4.4	Server thu nhận dữ liệu.....	64
5.4.5	Giao tiếp người và máy (MMC).....	64
5.5	Các chức năng SCADA trong hệ thống điện.....	65
5.5.1	Thu nhận dữ liệu.....	65
5.5.2	Giao tiếp người máy .....	65
5.5.3	Quản lý giám sát.....	65
5.5.4	Điều khiển xa.....	65
5.5.5	Đo lường xa .....	66
5.6	Các bộ chuyển đổi trong hệ thống SCADA của hệ thống điện.....	67
5.6.1	Bộ chuyển đổi - Transducer .....	67
5.6.2	Bộ chuyển đổi tương tự - số (ADC- Analog Digital Converter).....	67
5.7	Ghép nối RTU với hệ thống điện .....	68
5.7.1	Ghép nối tín hiệu tương tự .....	68
5.7.2	Ghép nối tín hiệu số.....	69
5.7.3	Ghép nối tín hiệu đầu ra tương tự .....	70
5.7.4	Ghép nối tín hiệu đầu ra số (DOT).....	70
5.8	Các thiết bị phụ trợ cho SCADA hệ thống điện.....	71
5.8.1	Nguồn UPS.....	71



5.8.2	Hệ thống Máy phát điện - Diesel.....	72
5.8.3	Hệ thống thông tin liên lạc .....	72
5.8.4	Tổng đài điều độ (Lineseizer -LSZ).....	72
5.8.5	Thiết bị Ghi âm.....	73
5.9	Câu hỏi ôn tập chương.....	74
<b>CHƯƠNG 6: THIẾT KẾ MẠNG CÔNG NGHIỆP VÀ SCADA .....</b>		<b>75</b>
6.1	Các bước thiết kế mạng công nghiệp .....	75
6.1.1	Xác định yêu cầu hệ thống .....	75
6.1.2	Phương án thiết kế lựa chọn cấu hình mạng .....	75
6.1.3	Xây dựng vào/ra(I/O) .....	75
6.1.4	Lựa chọn thiết bị mạng.....	75
6.1.5	Xây dựng thuật toán .....	75
6.1.6	Viết chương trình.....	75
6.1.7	Kiểm tra đánh giá kết quả.....	76
6.2	Thiết kế mạng MPI .....	76
6.2.1	Phần mềm thiết kế mạng .....	76
6.2.2	Thiết lập cấu hình phần cứng cho các trạm.....	76
6.2.3	Thiết lập giao diện mạng .....	78
6.2.4	Lập trình cho hệ thống.....	79
6.3	Mạng Profibus .....	80
6.3.1	Tạo giao diện truyền thông (ví dụ mạng Profibus) .....	80
6.3.2	Cấu hình truyền thông cho từng trạm PLC .....	80
6.3.3	Lập trình .....	84
6.4	Thiết kế mạng truyền thông Ethernet qua Step 7 .....	85
6.4.1	Cấu hình phần cứng.....	85
6.4.2	Thiết lập cấu hình mạng .....	87
6.4.3	Chọn card theo cơ chế giao tiếp TCP/IP .....	89
6.5	Câu hỏi ôn tập chương.....	89
<b>CHƯƠNG 7: SCADA NHÀ MÁY CÔNG NGHIỆP .....</b>		<b>90</b>
7.1	Hướng dẫn sử dụng Win CC .....	90
7.1.1	Tổng quan WinCC.....	90
7.1.2	Thiết lập thuộc tính.....	90
7.1.3	Giao tiếp biến (Tag) nội .....	92
7.1.4	Xây dựng dự án tạo giao diện đơn .....	96
7.1.5	Mô phỏng biến (Tag) ngoại trong WinCC .....	99
7.2	Kết nối Win CC với S7-200 .....	99
7.3	Kết nối Win CC với S7-300 .....	104
7.3.1	Tạo liên kết S7-300 ảo với WinCC qua biến (Tag) ngoại.....	104
7.3.2	Tạo nút nhấn hai tác động trên WinCC.....	108
7.3.3	Nhập xuất số thực và số nguyên trong WinCC .....	112
7.3.4	Khai thác đối tượng thư viện trong WinCC .....	114
7.3.5	Tạo thanh trượt trong WinCC .....	115
7.3.6	Xử lý timer trong WinCC.....	116
7.3.7	Tạo nút ấn hai tác động .....	116
7.3.8	Tạo chuyển động thẳng trong WinCC.....	117
7.4	Câu hỏi ôn tập chương.....	118
Tài liệu tham khảo.....		119

## DANH MỤC HÌNH VẼ

Hình 1.1: Sơ đồ mạng PCS7 (Siemens) trong công nghiệp [1].....	1
Hình 1.2: Một số dạng tín hiệu thông dụng [1] .....	4
Hình 1.3: Mô tả một hệ thống SCADA điển hình.....	6
Hình 1.4: Sơ đồ phân cấp chức năng điều khiển [1] .....	9
Hình 1.5: Sơ đồ đấu nối vào/ra mạng công nghiệp [26] .....	10
Hình 1.6: Các dạng của thời gian thực [22] .....	11
Hình 1.7: Nguyên tắc truyền dẫn trong mạng công nghiệp.....	11
Hình 2.1: Kiến trúc Slave/Master .....	13
Hình 2.2: Vào ra phân tán thiết bị trường.....	14
Hình 2.3: Sơ cấu trúc bus liên kết mạng truyền thông công nghiệp .....	14
Hình 2.4: Truy nhập bus theo phương pháp Master/Slave.....	15
Hình 2.5: Giao tiếp theo cơ chế Master/Slave [31] .....	15
Hình 2.6: Truy nhập bus theo phương pháp kiểm soát phân tán Token Passing [26], [32].....	16
Hình 2.7: Truy nhập bus kết hợp 2 phương pháp Master/Slave với Token [33] .....	17
Hình 2.8: Sơ đồ giả định xảy ra xung đột đường truyền [1] .....	18
Hình 2.9: Mã hóa bit bằng phương pháp NRZ và RZ.....	21
Hình 2.10: Mã hóa bit bằng phương pháp Manchester .....	22
Hình 2.11: Mã hóa bit bằng phương pháp AFP .....	22
Hình 2.12: Mã hóa bit bằng phương pháp FSK .....	23
Hình 3.1: Phương thức truyền dẫn dữ liệu không đối xứng .....	24
Hình 3.2: Phương thức truyền dẫn dữ liệu đối xứng.....	24
Hình 3.3: Kỹ thuật truyền dẫn MBP.....	25
Hình 3.4: Mức tín hiệu quy định RS 485 .....	26
Hình 3.5: Sơ đồ ghép nối RS 485 .....	26
Hình 3.6: Tốc độ truyền dẫn RS 485 .....	27
Hình 3.7: Sơ đồ giao thức mạng .....	28
Hình 3.8: Sơ đồ mô hình lớp cơ bản.....	28
Hình 3.9: Sơ đồ mô hình quy chiếu.....	29
Hình 3.10: Sơ đồ mô hình OSI .....	29
Hình 3.11: Sơ đồ mô hình lớp của giao thức [1].....	30
Hình 3.12: Sơ đồ mô hình OSI .....	30
Hình 3.13: Sơ đồ mô hình OSI và TCP/IP .....	31
Hình 3.14: Mô hình cáp đồng trục.....	31
Hình 3.15: Mô hình cáp đôi dây xoắn .....	32
Hình 3.16: Mô hình cáp quang .....	32
Hình 3.17: Dải tần truyền dẫn vô tuyến .....	33
Hình 3.18: Hình ảnh một số thiết bị trong mạng.....	34
Hình 3.19: Ghép nối PLC [31] .....	35
Hình 3.20: Card PCMCIA .....	36
Hình 3.21: Sơ đồ phần mềm mạng công nghiệp .....	37
Hình 4.1: Mô hình mạng ASI International.....	39
Hình 4.2: Sơ đồ mạng AS-Interface .....	40
Hình 4.3: Cấu trúc bức điện trong mạng AS-Interface .....	41
Hình 4.4: Sơ đồ mã hóa bit mạng AS-Interface .....	41

Hình 4.5: Ứng dụng kết nối của AT/IO8 [32] .....	42
Hình 4.6: Kiến trúc của mạng Profibus [1] .....	43
Hình 4.7: Mô hình mạng Profibus FMS .....	44
Hình 4.8: Mô hình mạng Profibus DP .....	44
Hình 4.9: Mô hình mạng Profibus PA[43] .....	45
Hình 4.10: Mô hình truy nhập bus [43] .....	45
Hình 4.11: Sơ đồ dịch vụ truyền dữ liệu .....	46
Hình 4.12: Sơ đồ cấu trúc mạng sử dụng dây đôi xoắn .....	48
Hình 4.13: Giao tiếp theo cơ chế đồng bộ hóa dữ liệu .....	48
Hình 4.14: Sơ đồ kiến trúc liên kết của cấu trúc dữ liệu .....	50
Hình 4.15: Sơ đồ cấu trúc bức điện .....	51
Hình 4.16: Kiến trúc giao thức mạng Ethernet.....	53
Hình 4.17: Bộ kết nối mạng Ethernet.....	54
Hình 5.1: Sơ đồ phân cấp SCADA trong hệ thống điện Việt Nam cấp miền .....	58
Hình 5.2: Cấu hình đặc trưng của hệ thống SCADA/EMS.....	61
Hình 5.3: Hình ảnh một RTU sử dụng trong hệ thống điện.....	62
Hình 5.4: Thiết bị Gateway được sử dụng trong hệ thống mạng .....	63
Hình 5.5: Mô hình truyền dẫn đo lường xa dùng ADC.....	67
Hình 5.6: Sơ đồ nguyên lý ghép nối P, Q, U, I .....	68
Hình 5.7: Sơ đồ nguyên lý ghép nối tín hiệu tần số .....	68
Hình 5.8: Sơ đồ nguyên lý ghép nối tín hiệu chỉ thị chuyển nấc MBA .....	69
Hình 5.9: Sơ đồ nguyên lý ghép nối tín hiệu chỉ thị trạng thái máy cắt.....	70
Hình 5.10: Sơ đồ nguyên lý ghép nối tín hiệu điều khiển tương tự .....	70
Hình 5.11: Sơ đồ nguyên lý ghép nối tín hiệu điều khiển máy cắt .....	71
Hình 5.12: Sơ đồ ghép nối LSZ với các kênh liên lạc tại A0.....	73
Hình 6.1: Thiết lập giao diện cho mạng MPI .....	76
Hình 6.2: Cấu hình phần cứng cho trạm.....	77
Hình 6.3: Khai báo phần cứng và cấu hình địa chỉ .....	77
Hình 6.4: Cấu hình phần cứng cho trạm 2.....	78
Hình 6.5: Cấu hình mạng MPI .....	78
Hình 6.6: Cửa sổ truyền nhận dữ liệu giữa các CPU .....	78
Hình 6.7: Thiết lập dữ liệu truyền nhận cho mạng MPI.....	79
Hình 6.8: Giao diện lập trình cho CPU mạng MPI .....	79
Hình 6.9: Giao diện cho mạng truyền thông Profibus cho 3 trạm S7-300 .....	80
Hình 6.10: Thiết lập cấu hình phần cứng cho trạm Slave 2 .....	80
Hình 6.11: Cấu hình giao tiếp I/O của trạm Slave với Master .....	81
Hình 6.12: Kết quả thiết lập cấu hình trạm Slave 2.....	82
Hình 6.13: Kết quả thiết lập cấu hình trạm Slave 1.....	82
Hình 6.14: Cấu hình địa chỉ I/O cho Master .....	83
Hình 6.15: Kết quả thiết lập địa chỉ giao tiếp Master với Slave 1 .....	83
Hình 6.16: Kết quả thiết lập CPU giao tiếp và các thiết bị mạng .....	84
Hình 6.17: Chương trình lập trình cho các trạm trong mạng Profibus.....	85
Hình 6.18: Cấu hình địa chỉ IP cho trạm .....	86
Hình 6.19: Kết quả cấu hình phần cứng cho trạm Ethernet.....	86
Hình 6.20: Kết quả cấu hình trạm thứ 2 cho mạng Ethernet.....	87
Hình 6.21: Cấu hình mạng Profibus trên trạm số 2.....	87
Hình 6.22: Cấu hình I/O cho hệ thống Profibus của trạm số 2 .....	88

Hình 6.23: Kết quả cấu hình mạng Ethernet cho hai trạm S7-300.....	88
Hình 7.1: Giao diện hệ thống phần mềm SCADA WinCC.....	90
Hình 7.2: Thiết lập thuộc tính nút bấm.....	91
Hình 7.3: Cài đặt thuộc tính nút bấm .....	91
Hình 7.4: Giao diện tạo Tag nội .....	92
Hình 7.5: Giao diện thiết kế giao diện ON/OFF .....	93
Hình 7.6: Đặt thuộc tính cho biến nội Den.....	93
Hình 7.7: Kết quả thử nghiệm Tag nội cho hai tác động ON- OFF lên Tag “Den”.....	94
Hình 7.8: Thiết lập giao diện vùng hiển thị I/O số nguyên.....	94
Hình 7.9: Kết nối giữa Tag interger và giao diện vùng hiển thị I/O .....	95
Hình 7.10: Lập trình Tag interger.....	95
Hình 7.11: Giao diện và cài đặt cấu hình Tag nội real.....	96
Hình 7.12: Kết quả thực hiện ví dụ về Tag nội dạng số thực.....	96
Hình 7.13: Giao diện tạo biến nội cho WinCC giao tiếp S7-300 ảo .....	97
Hình 7.14: Đặt thuộc tính cho các biến .....	97
Hình 7.15: Đặt thuộc tính cho biến đầu ra/ đầu vào của đối tượng thiết kế giao diện..	98
Hình 7.16: Kết quả cài đặt tham số .....	98
Hình 7.17: Kết quả mô phỏng trên Win CC.....	99
Hình 7.18: Kết nối chương trình mô phỏng S7-200 Simulator với chương trình ứng dụng .....	101
Hình 7.19: Khai báo biến và kết nối mô phỏng với PLC .....	101
Hình 7.20: Giao diện tạo dự án trên WinCC .....	102
Hình 7.21: Chọn cấu hình OPC trên WinCC .....	102
Hình 7.22: Khai báo Tag (biến) cho OPC .....	103
Hình 7.23: Tạo giao diện thiết kế .....	103
Hình 7.24: Lựa chọn thuộc tính cho đối tượng trong hàm thư viện có sẵn.....	104
Hình 7.25: Kết nối chương trình ứng dụng PLC S7-200 với PC Access.....	104
Hình 7.26: Giao diện cấu hình phần S7 với WinCC .....	105
Hình 7.27: Thiết lập cấu hình kết nối máy tính và S7-300 .....	105
Hình 7.28: Kết nối biến nhớ vào WinCC .....	106
Hình 7.29: Cấu hình Hardware cho S7-300 .....	106
Hình 7.30: Chương trình trên PLC S7-300 với biến (Tag) trên WinCC.....	106
Hình 7.31: Giao diện mô phỏng cho S7-300 trên PLCSim.....	107
Hình 7.32: Đặt thuộc tính cho biến .....	107
Hình 7.33: Kết quả kết nối PLC S7-300 với WinCC [2], [57].....	108
Hình 7.34: Thiết lập dự án trên S7-300 cho nút_an và den.....	108
Hình 7.35: Thiết lập cấu hình giao tiếp MPI cho nút_an .....	109
Hình 7.36: Thiết lập biến ngoại.....	109
Hình 7.37: Thiết kế giao diện hệ thống nút ấn hai chế độ.....	109
Hình 7.38: Kết quả thực hiện giao tiếp WinCC với S7-300 ảo.....	110
Hình 7.39: Chương trình S7-300 với số nguyên (interger) .....	110
Hình 7.40: Tạo Tag interger cho phép cộng trên WinCC .....	111
Hình 7.41: Thiết lập thuộc tính của nút CONG và KETQUA .....	111
Hình 7.42: Kết quả xây dựng Tag số nguyên cho phép cộng 10 .....	111
Hình 7.43: Kết quả thiết kế giao tiếp PLC S7-300 với Tag real .....	112
Hình 7.44: Thiết kế giao diện nhập xuất giá trị số nguyên và số thực .....	112
Hình 7.45: Chương trình cho VD4.....	113

Hình 7.46: Cấu hình Tag cho WinCC .....	113
Hình 7.47: Kết quả thực hiện xuất nhập số nguyên và số thực trên WinCC .....	113
Hình 7.48: Khai thác thư viện có trong WinCC.....	114
Hình 7.49: Xây dựng thuộc tính cho đối tượng thư viện .....	114
Hình 7.50: Cài đặt thuộc tính màu sắc thanh Bar.....	115
Hình 7.51: Kết quả sử dụng thanh trượt.....	115
Hình 7.52: Đặt thuộc tính sử dụng đồng hồ trong WinCC.....	116
Hình 7.53: Kết quả xây dựng một nút hai tác động trên WinCC .....	117
Hình 7.54: Thiết kế giao diện và Tag cho hệ thống chuyển động lên xuống.....	118

**DANH MỤC CÁC BẢNG**

Bảng 4.1: Bảng so sánh giữa ba dạng của mạng profibus [46] .....	43
Bảng 4.2: Khoảng cách truyền và tốc độ truyền: .....	44
Bảng 7.1: Bảng symbol cho chương trình ví dụ .....	99

## CÁC TỪ VIẾT TẮT

Viết tắt	Diễn giải
ADC	Analog Digital Converter
CRC	Cyclic Redundancy Check
DCS	Distributed Control System
HMI	Human - Machine Interface
HTĐK	Hệ thống điều khiển
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
NRZ	Non-return to Zero
PLC	Programmable Logic Controller
RTU	Remote Terminal Units
RZ	Return to Zero
SCADA	Supervisory Control And Data Acquisition
TCP	Transmission Control Protocol

## LỜI NÓI ĐẦU

Với sự hướng công nghiệp hóa hiện đại hoá đất nước, thì ứng dụng công nghệ mới vào sản xuất và công tác quản lý được mở rộng và áp dụng ngày càng rộng rãi hơn. Lĩnh vực kỹ thuật điều khiển cũng thế, các hệ thống điều khiển, giám sát và thu thập dữ liệu – SCADA ngày nay được thực hiện bằng các phần mềm trên các màn hình giám sát hoặc máy tính.

Cuốn sách này trang bị người đọc kiến thức cơ bản về mạng truyền thông công nghiệp ở các chương 1, 2, 3. Chương 4 giới thiệu người đọc kiến thức tổng quan về các mạng công nghiệp ngày nay đang được ứng dụng; chương 5 mô tả khái quát hệ thống SCADA được ứng dụng từ những năm 90s ở Tập đoàn Điện lực Việt Nam. Các chương 6, 7 giúp cho người đọc thực thành các bước cụ thể khi xây dựng một mạng công nghiệp và hệ thống SCADA trên nền tảng WinCC.

Nội dung cuốn sách là sự kết hợp giữa ba lĩnh vực điều khiển, tự động hoá và một phần công nghệ thông tin. Từ đó, kỹ sư có thể thực hiện các thao tác của con người được thay thế bằng các hoạt động của máy móc, robot; sự tương tác giữa con người và máy móc hoặc giữa máy móc với nhau. Cuốn sách cung cấp cho người đọc kiến thức nền tảng về mạng truyền thông công nghiệp, các hệ thống điều khiển từ xa, các hệ thống tự động hoá xí nghiệp công nghiệp; cùng với sự hỗ trợ của công nghệ 4.0 những ý tưởng sáng tạo của quá trình công nghiệp hóa, hiện đại hóa trong tất cả các lĩnh vực sẽ được trở thành hiện thực. Cuốn sách có tính ứng dụng cao, đặc biệt người đọc được hướng dẫn tiếp cận cụ thể thực hành trên phần mềm WinCC.

Tác giả có tham khảo một số nội dung từ cuốn “Mạng truyền thông công nghiệp...” của tác giả Hoàng Minh Sơn trong các chương 1, 2, 3. Lần đầu xuất bản cuốn sách có những thiếu sót mong người đọc góp ý qua Email: [dovancan@qnu.edu.vn](mailto:dovancan@qnu.edu.vn) để tác giả hoàn chỉnh hơn.

Tác giả xin trân thành cảm ơn!

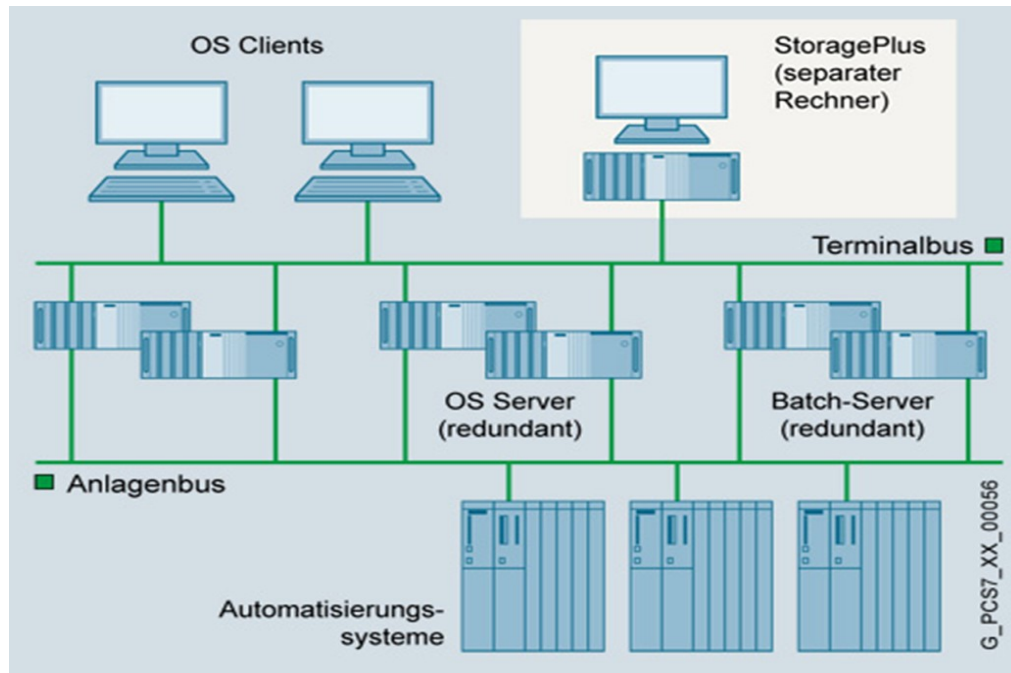
Đỗ Văn Cần



# CHƯƠNG 1: CÁC KHÁI NIỆM CƠ BẢN VỀ MẠNG TRUYỀN THÔNG CÔNG NGHIỆP VÀ SCADA

## 1.1 Các khái niệm cơ bản

Mạng truyền thông công nghiệp hay mạng công nghiệp là một khái niệm chung chỉ các hệ thống mạng truyền thông số, truyền bit nối tiếp, được sử dụng ghép nối các thiết bị công nghiệp. Giới thiệu về một hình ảnh mạng sử dụng trong công nghiệp.



Hình 1.1: Sơ đồ mạng PCS7 (Siemens) trong công nghiệp [1]

Có rất nhiều mạng công nghiệp của các tập đoàn trên thế giới như: Mạng PlantScap, DeltaV (Fisher-Rosermount), ProcessLogix (Allen-Bradley)...

### 1.1.1 Kỹ thuật điều khiển

Kỹ thuật điều khiển là chuyên ngành kỹ thuật mà áp dụng lý thuyết điều khiển để thiết kế hệ thống với các hành vi mong muốn. Việc sử dụng các bộ cảm biến để đo lường tín hiệu đầu ra của thiết bị được điều khiển và những đo đạc này có thể được sử dụng để cung cấp tín hiệu phản hồi cho các cơ cấu chấp hành đầu vào để điều chỉnh tới kết quả mong muốn. Khi một thiết bị được thiết kế để thực hiện mà không cần con người can thiệp để điều chỉnh thì nó được gọi là điều khiển tự động (chẳng hạn như hệ thống điều khiển hành trình để điều chỉnh tốc độ của xe hơi). Với tính chất đa chuyên ngành, các hoạt động của kỹ thuật hệ thống điều khiển tập trung vào thực hiện các hệ thống điều khiển, chủ yếu xuất phát từ mô hình toán học của các hệ thống đa dạng khác nhau.

### **1.1.2 Hệ thống điều khiển phân tán (Distributed Control System - DCS)**

DCS là một hệ thống kiểm soát thường của một hệ thống sản xuất, quá trình hoặc bất kỳ loại hệ thống năng động, trong đó các yếu tố điều khiển không phải là trung tâm trong vị trí (như não bộ), chúng được phân tán trên toàn hệ thống với mỗi thành phần tiểu hệ thống điều khiển bởi một hoặc nhiều bộ điều khiển. Toàn bộ hệ thống điều khiển được kết nối với mạng lưới giao tiếp và giám sát. DCS là một thuật ngữ được sử dụng rất rộng rãi trong nhiều ngành công nghiệp, để giám sát và kiểm soát thiết bị phân tán [2] và là xu hướng đang được nghiên cứu hiện nay [3], [4].

### **1.1.3 Điều khiển quá trình**

Điều khiển quá trình hoặc có thể sử dụng thông tin phản hồi hoặc nó có thể là vòng lặp hở. Điều khiển cũng có thể liên tục (điều khiển hành trình ô tô) hoặc gây ra một chuỗi các sự kiện rời rạc, chẳng hạn như một bộ định thời trên một máy tưới cỏ (on/off) hoặc điều khiển thang máy (logic tuần tự). Một bộ điều chỉnh nhiệt độ trên bộ gia nhiệt là một ví dụ về điều khiển on/off. Một cảm biến nhiệt độ bật nguồn nhiệt lên nếu nhiệt độ giảm xuống dưới điểm thiết lập và tắt nguồn nhiệt khi điểm thiết lập đã đạt được. Không có đo lường chênh lệch giữa điểm đặt và nhiệt độ đo được (ví dụ không có sai số đo lường) và không điều chỉnh được tốc độ mà tại đó nhiệt được gia tăng như thế nào. Một ví dụ quen thuộc của điều khiển phản hồi là điều khiển hành trình trên xe ô tô. Biến đo lường ở đây là tốc độ. Người lái (trình điều khiển) điều chỉnh đến điểm đặt tốc độ mong muốn (ví dụ như 100 km/giờ) và bộ điều khiển giám sát cảm biến tốc độ và so sánh tốc độ đo với điểm đặt. Bất kỳ sai lệch nào, chẳng hạn như thay đổi trong độ dốc, lực cản, tốc độ gió hoặc thậm chí sử dụng một lớp nhiên liệu khác (ví dụ ethanol pha trộn) được điều chỉnh bởi bộ điều khiển thực hiện một điều chỉnh bù tới vị trí mở của van nhiên liệu, ở đây là biến thao tác. Bộ điều khiển thực hiện điều chỉnh khi có thông tin chỉ khi có sai số (cường độ, tốc độ thay đổi hoặc sai số tích lũy) mặc dù các thiết lập được gọi là điều chỉnh được sử dụng để đạt được kiểm soát ổn định. Hoạt động của bộ điều khiển như vậy là đối tượng của lý thuyết điều khiển tự động.

Một thiết bị điều khiển thường được sử dụng được gọi là một bộ điều khiển logic khả lập trình, hoặc một bộ PLC, được sử dụng để đọc một tập hợp các đầu vào số và tương tự, áp dụng một tập các câu lệnh logic và tạo ra một tập hợp các kết quả đầu ra tương tự và số.

Ví dụ, nếu một van điều chỉnh được sử dụng để giữ cho mực nước trong bể ở một mức nào đó, các tập lệnh logic sẽ so sánh áp lực tương đương điểm đặt độ sâu với áp lực đọc được của một bộ cảm biến thấp dưới mức bình thường của chất lỏng và xác định xem cần mở van ra hoặc đóng lại để giữ cho mực chất lỏng không đổi. Một đầu ra PLC sau đó sẽ tính toán một độ mở cần thiết của van. Các hệ thống phức tạp lớn hơn có thể được điều khiển bởi một hệ thống điều khiển phân tán (DCS) hoặc hệ thống SCADA. Trong thực tế, các quá trình có thể được mô tả như là một hoặc nhiều các hình thức sau đây:

**Rời rạc:** Tìm thấy trong nhiều ứng dụng sản xuất, chuyển động và đóng gói. Lắp ráp robot, được tìm thấy trong sản xuất ô tô, có thể được mô tả là điều khiển quá trình rời rạc. Hầu hết sản xuất riêng rẽ liên quan đến việc sản xuất các mảnh rời rạc của sản phẩm, như dập kim loại.

**Hàng loạt:** Một số ứng dụng yêu cầu số lượng cụ thể của các nguyên liệu được kết hợp theo những cách cụ thể trong khoảng thời gian cụ thể để tạo ra một kết quả trung gian hay kết quả cuối cùng. Một ví dụ là việc sản xuất chất kết dính và keo dán, thường đòi hỏi sự pha trộn nguyên liệu trong một bình nước nóng trong một khoảng thời gian để tạo thành một lượng sản phẩm cuối cùng. Ví dụ quan trọng khác là sản xuất thực phẩm, đồ uống và thuốc men. Các quá trình hàng loạt thường được sử dụng để sản xuất một số lượng sản phẩm tương đối từ thấp đến trung bình mỗi năm (một vài đến hàng triệu kg).

**Liên tục:** Thông thường, một hệ thống vật lý được biểu diễn thông qua các biến được làm mịn và không bị gián đoạn trong thời gian. Việc điều khiển nhiệt độ nước trong một lò đốt là một ví dụ về điều khiển quá trình liên tục [4]. Một số quy trình liên tục quan trọng là sản xuất nhiên liệu, hóa chất và nhựa. Quá trình liên tục trong sản xuất được sử dụng để sản xuất với số lượng rất lớn các sản phẩm mỗi năm (hàng triệu đến hàng tỷ kg).

#### **1.1.4 Thông tin**

Thông tin là một trong những khái niệm cơ sở quan trọng nhất trong khoa học kỹ thuật, cũng giống như vật chất và năng lượng. Các đầu vào cũng như các đầu ra của một hệ thống kỹ thuật chỉ có thể là vật chất, năng lượng hoặc thông tin, như mô tả trên Hình 2.1. Một hệ thống xử lý thông tin hoặc một hệ thống truyền thông là một hệ thống kỹ thuật chỉ quan tâm tới các đầu vào và đầu ra là thông tin. Tuy nhiên, đa số

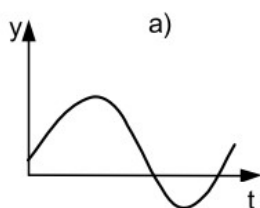
các hệ thống kỹ thuật khác thường có các đầu vào và đầu ra hỗn hợp (vật chất, năng lượng và thông tin), một số tài liệu [5], [6] có nghiên cứu kỹ hơn về thông tin.

### 1.1.5 Dữ liệu

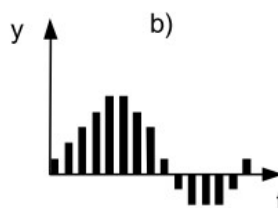
Nếu thông tin là một đại lượng khá trừu tượng, vì vậy cần được biểu diễn dưới một hình thức khác. Khả năng biểu diễn thông tin rất đa dạng, ví dụ qua chữ viết, hình ảnh, cử chỉ, v.v... Dạng biểu diễn thông tin phụ thuộc vào mục đích, tính chất của ứng dụng. Đặc biệt, thông tin có thể được mô tả, hay nói cách khác là được “số lượng hoá” bằng dữ liệu để có thể lưu trữ và xử lý trong máy tính [7], [8]. Trong trường hợp đó, ta cũng nói rằng thông tin được số hoá sử dụng hệ đếm nhị phân, hay mã hóa nhị phân. Nói trong ngữ cảnh cấu trúc một bức điện, dữ liệu chính là phần thông tin hữu ích được biểu diễn bằng dãy các bit  $\{1, 0\}$  [9].

### 1.1.6 Tín hiệu

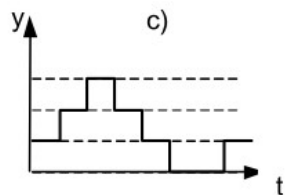
Việc trao đổi thông tin (giữa người và người, giữa người và máy) hay dữ liệu (giữa máy và máy) chỉ có thể thực hiện được nhờ tín hiệu. Có thể định nghĩa, tín hiệu là diễn biến của một đại lượng vật lý chứa đựng tham số thông tin/dữ liệu và có thể truyền dẫn được. Theo quan điểm toán học thì tín hiệu được coi là một hàm của thời gian [10], [11]. Trong các lĩnh vực kỹ thuật, các loại tín hiệu thường dùng là điện, quang, khí nén, thủy lực và âm thanh.



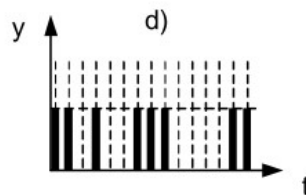
Dạng tín hiệu: tương tự, liên tục  
Tham số thông tin: Biên độ



Dạng tín hiệu: tương tự, gián đoạn  
Tham số thông tin: Biên độ xung



Dạng tín hiệu: rời rạc, liên tục  
Tham số thông tin: Biên độ



Dạng tín hiệu: rời rạc (số), gián đoạn  
Tham số thông tin: Tần số xung

Hình 1.2: Một số dạng tín hiệu thông dụng [1]

### **1.1.7 Giao thức:**

Giao thức giao tiếp hay còn gọi là giao thức truyền thông, giao thức liên mạng, giao thức tương tác, giao thức trao đổi thông tin (tiếng Anh là communication protocol) - trong công nghệ thông tin gọi tắt là giao thức (protocol). Có nhiều giao thức được sử dụng để giao tiếp hoặc truyền đạt thông tin trên Internet, dưới đây là một số các giao thức tiêu biểu:

TCP (Transmission Control Protocol): Thiết lập kết nối giữa các máy tính để truyền dữ liệu. Nó chia nhỏ dữ liệu ra thành những gói (packet) và đảm bảo việc truyền dữ liệu thành công.

IP (Internet Protocol): Định tuyến (route) các gói dữ liệu khi chúng được truyền qua Internet, đảm bảo dữ liệu sẽ đến đúng nơi cần nhận.

HTTP (HyperText Transfer Protocol): Cho phép trao đổi thông tin (chủ yếu ở dạng siêu văn bản) qua Internet.

FTP (File Transfer Protocol): Cho phép trao đổi tập tin qua Internet.

SMTP (Simple Mail Transfer Protocol): Cho phép gửi các thông điệp thư điện tử (e-mail) qua Internet.

POP3 (Post Office Protocol, phiên bản 3): Cho phép nhận các thông điệp thư điện tử qua Internet.

MIME (Multipurpose Internet Mail Extension): Cho phép một mở rộng của giao thức SMTP, cho phép gửi kèm các tập tin nhị phân, phim, nhạc,... theo thư điện tử.

WAP (Wireless Application Protocol): Cho phép trao đổi thông tin giữa các thiết bị không dây, như điện thoại di động. Chi tiết về giao thức được nghiên cứu trong các công trình [12], [13], [14], [15], [17].

### **1.1.8 IEC**

Ủy ban Kỹ thuật điện Quốc tế hay IEC (viết tắt của tiếng Anh: International Electrotechnical Commission) được thành lập năm 1906. Mục tiêu của IEC là thúc đẩy sự hợp tác quốc tế về tiêu chuẩn hoá trong lĩnh vực điện - điện tử và các vấn đề có liên quan như: chứng nhận sự phù hợp tiêu chuẩn điện và hỗ trợ cho thông hiểu quốc tế [1].

IEC có mối quan hệ hợp tác chặt chẽ với nhiều tổ chức tiêu chuẩn hoá và chuyên môn quốc tế như: ISO, Liên đoàn Viễn thông quốc tế - ITU; Ban Tiêu chuẩn hoá Kỹ thuật điện châu Âu - CENELEC. Đặc biệt, giữa IEC và ISO đã thiết lập một thoả thuận về phạm vi hoạt động của mỗi tổ chức. Theo thoả thuận này, phạm vi hoạt động

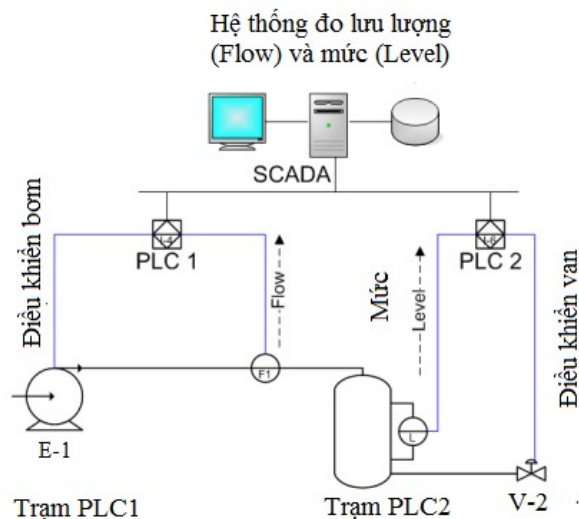
của IEC bao gồm tiêu chuẩn hoá trong lĩnh vực điện - điện tử. ISO và IEC đã phối hợp thành lập một ban kỹ thuật hỗn hợp về công nghệ thông tin được đặt trong cơ cấu các cơ quan kỹ thuật của ISO (ISO/IEC/JTC1). Trụ sở ban đầu của tổ chức này đóng ở Luân Đôn, nay chuyển trụ sở sang đóng tại Genève từ năm 1948.

Bộ tiêu chuẩn điện kỹ thuật (chuẩn hoá quốc tế IEC) bao gồm trên 6500 tiêu chuẩn về thiết kế, lắp đặt hệ thống điện.

Những tiêu chuẩn của IEC được sắp xếp theo dãy số từ 60000 đến 79999. Ví dụ IEC 60432. Bộ tiêu chuẩn cũ của IEC đưa ra trước năm 1997 được đánh số lại bằng cách cộng số cũ với 60000. Ví dụ tiêu chuẩn cũ số IEC 237 đặt lại là IEC 60237 và một số giao thức IEC khác [5], [17], [18], [19], [20].

### 1.1.9 SCADA

SCADA là viết tắt tiếng Anh: Supervisory Control And Data Acquisition hiểu theo nghĩa truyền thống là một hệ thống điều khiển giám sát và thu thập dữ liệu. Nhằm hỗ trợ con người trong quá trình giám sát và điều khiển từ xa [21]. Tuy nhiên, trong thực tế có một số hệ thống vẫn thường được gọi là SCADA, mặc dù những hệ thống này chỉ thực hiện duy nhất một chức năng là thu thập dữ liệu. Cấu trúc một hệ SCADA có các thành phần cơ bản sau (Hình 1.3) [21], [22],:



Hình 1.3: Mô tả một hệ thống SCADA điển hình

- Trạm điều khiển giám sát trung tâm: Là một hay nhiều máy chủ trung tâm (central host computer server).

- Trạm thu thập dữ liệu trung gian: Là các khối thiết bị vào ra đầu cuối từ xa RTU (Remote Terminal Units) hoặc là các khối điều khiển logic khả trình PLC

(Programmable Logic Controllers) có chức năng giao tiếp với các thiết bị chấp hành cảm biến cấp trường, các hộp điều khiển đóng cắt và các van chấp hành [23]...

- Hệ thống truyền thông: Bao gồm các mạng truyền thông công nghiệp, các thiết bị viễn thông và các thiết bị chuyển đổi dồn kênh có chức năng truyền dữ liệu cấp trường đến các khối điều khiển và máy chủ.

- Giao diện người - máy HMI (Human - Machine Interface): Là các thiết bị hiển thị quá trình xử lý dữ liệu để người vận hành điều khiển các quá trình hoạt động của hệ thống.

#### 1.1.9.1. Công nghệ RTU tập trung

Thiết bị RTU được xây dựng trên cơ sở kỹ thuật vi xử lý. Các bộ vi xử lý ngày nay được sử dụng thuộc loại từ 16 bit trở lên [5].

Mỗi RTU có khả năng tiếp nhận hàng trăm lối vào đo lường và trạng thái;

Trên RTU có nhiều vi chức năng: CPU, bộ nhớ, ngoại vi cơ sở, lối vào tương tự (AI-Analog Input), lối vào trạng thái (DI\_digital Input).

Tùy theo dung lượng RTU mà các vi AI, DI được sử dụng với số lượng khác nhau.

Các thiết bị RTU được tổ chức thành 3 nhóm, mỗi nhóm gồm các thiết bị lắp đặt trong 1 tủ (có thể nhiều hơn).

Từ trạm và nhà máy, các tín hiệu được gom vào một tủ gọi là tủ trạm.

Từ tủ trạm các tín hiệu được dẫn sang tủ trung gian, tại đây lắp đặt các rơ le trung gian, các Transducer và các thiết bị lẻ khác.

Tủ RTU chứa các thiết bị điện tử (CPU, bộ nhớ, ngoại vi, vào ra tương tự, số,...)

Thông thường RTU có nhiều cửa vào ra nối tiếp (RS232) phục vụ giao tiếp với trung tâm điều khiển cấp trên (CC) và giao tiếp với máy tính Laptop khi thay đổi cấu hình RTU [22].

Phần mềm cơ sở dữ liệu cho phép thay đổi thông số trên RTU trong quá trình sử dụng bao gồm:

- Số lượng các tín hiệu vào ra;
- Các thông số của dữ liệu;
- Cách mã hoá trạng thái (1 hoặc 2 bit);
- Tốc độ truyền tin;
- Chọn giao thức truyền tin;
- ...

RTU thường được sử dụng độc lập với các hệ thống đo lường và giám sát các trạm và nhà máy điện. Đó là các trạm và nhà máy điện sử dụng công nghệ cũ.

Thông thường tồn tại độ vênh về giá trị (sai số) giữa 2 hệ thống đo lường nói trên.

#### *1.1.9.2 Công nghệ RTU phân tán:*

Công nghệ này không gom tín hiệu vào tủ trạm;

RTU chia nhỏ thành các phần nhỏ lắp đặt phân tán trong trạm và nhà máy;

Mỗi phần nhỏ của RTU đảm nhiệm chức năng như của một RTU nhỏ;

Các phần nhỏ nói trên được liên kết với nhau bằng cáp thông tin và cả hệ thống làm việc thống nhất như trên 1 RTU.

Công nghệ RTU phân tán cho phép:

- Đơn giản hoá thiết kế RTU;
- Đơn giản hoá thiết kế hệ thống, đặc biệt ở các trạm và nhà máy có các thiết bị lắp đặt quá xa nhau;
- Đơn giản hoá việc lắp đặt thiết bị;
- Giảm thiểu khối lượng cáp so với RTU tập trung;
- Phù hợp xu hướng phát triển công nghệ.

#### *1.1.9.3 Công nghệ GateWay:*

Các trạm và nhà máy mới hiện nay đều sử dụng các thiết bị công nghệ số. Cũng có thể sử dụng thêm các bộ thu thập dữ liệu, điều khiển giám sát vạn năng (PLC-Programmable Logic Control). Bằng công nghệ mạng, tất cả được tích hợp vào một hệ thống gọi là hệ thống tự động hoá trạm & nhà máy.

Như vậy các thiết bị điện và hệ thống thu thập dữ liệu, giám sát, điều khiển đã được thiết kế trong thể thống nhất.

Việc cung cấp thông tin cho các trung tâm điều khiển cấp trên (CC) chỉ là một phần nhỏ của hệ thống tự động hoá trạm & nhà máy.

Sai số của CC chính là sai số của hệ thống tự động hoá trạm & nhà máy.

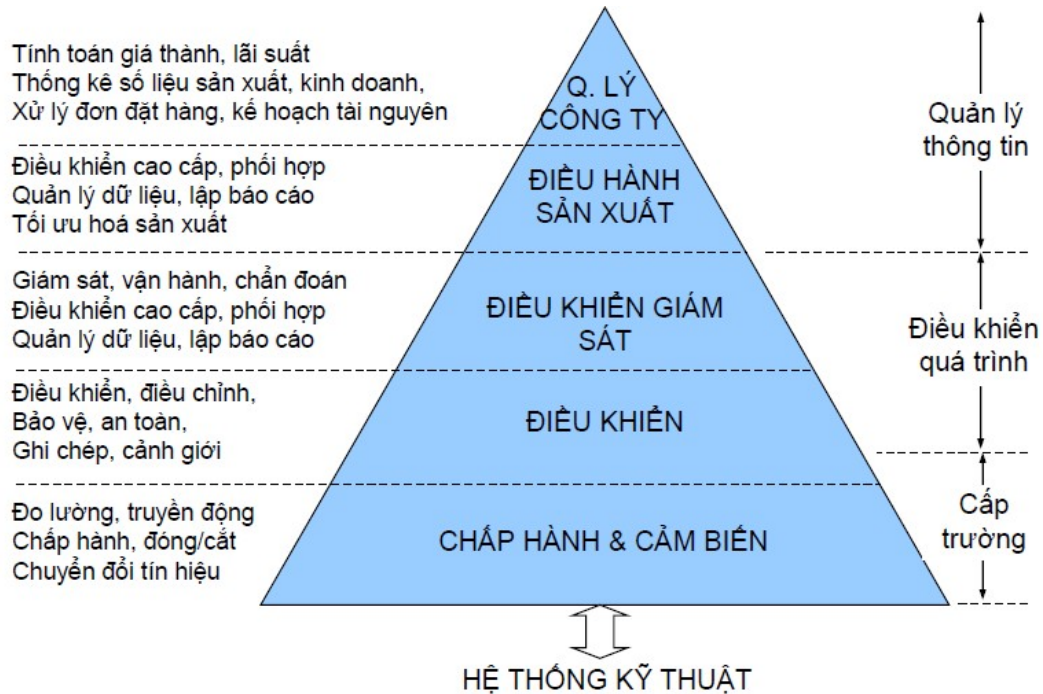
Để kết nối với CC chỉ cần kênh truyền, thiết bị ghép nối truyền tin phù hợp và thống nhất khai báo dữ liệu trao đổi thông tin.

## **1.2 Mô hình phân cấp chức năng**

Một hệ thống mạng được định nghĩa các cấp theo chức năng, không phụ thuộc lĩnh vực công nghiệp cụ thể. Mỗi cấp có chức năng và đặc thù khác nhau, với mỗi ngành công nghiệp, lĩnh vực ứng dụng có thể có các mô hình tương tự với số cấp nhiều hoặc



ít hơn. Ranh giới giữa các cấp không phải bao giờ cũng rõ ràng, càng ở những cấp dưới thì các chức năng càng mang tính chất cơ bản hơn và đòi hỏi yêu cầu cao hơn về độ nhanh nhạy, thời gian phản ứng, càng ở cấp trên quyết định càng quan trọng hơn, lượng thông tin cần trao đổi và xử lý càng lớn hơn. Trên Hình 1.4 là sơ đồ phân cấp trong hệ thống mạng công nghiệp chung [1], [2].



Hình 1.4: Sơ đồ phân cấp chức năng điều khiển [1]

### 1.2.1 Phân loại mạng công nghiệp

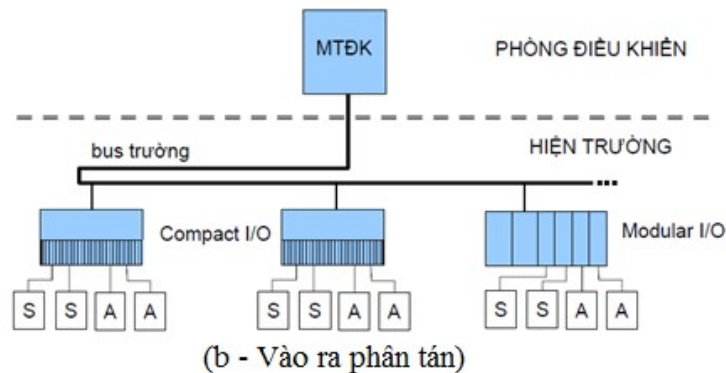
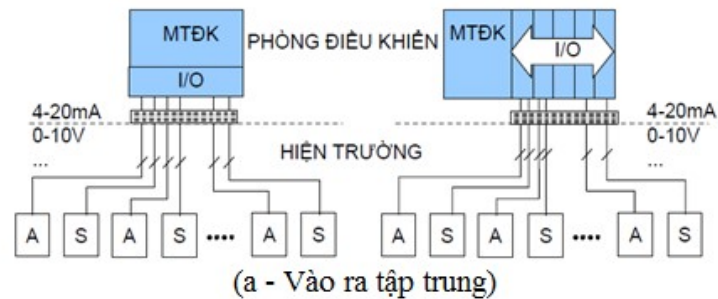
Tương ứng với năm cấp chức năng là bốn cấp của hệ thống truyền thông. Từ cấp điều khiển giám sát trở xuống thuật ngữ “bus” thường được dùng thay cho “mạng”, với lý do phần lớn các hệ thống mạng phía dưới đều có cấu trúc vật lý hoặc logic kiểu bus. Mạng công nghiệp chia làm hai loại vào/ra tập trung (central I/O) và vào/ra phân tán (distributed I/O).

Đặc điểm vào ra phân tán:

- Ưu điểm nhiều, song vẫn còn nổi dây truyền thống. Vào/ra phân tán với bus trường chuẩn;
- Tiết kiệm chi phí dây dẫn và công lắp đặt (Từ bộ điều khiển xuống tới các vào/ra phân tán chỉ cần một đường truyền duy nhất).
- Cấu trúc đơn giản nên thiết kế và bảo trì hệ thống dễ dàng hơn;
- Tăng độ tin cậy của hệ thống;
- Truyền kỹ thuật số vì vậy hạn chế lỗi;

- Nếu có lỗi truyền thông cũng dễ dàng phát hiện nhờ các biện pháp bảo toàn dữ liệu của hệ bus;

- Tăng độ linh hoạt của hệ thống;
- Tự do hơn trong lựa chọn các thiết bị vào/ra;
- Tự do hơn trong thiết kế cấu trúc hệ thống;
- Khả năng mở rộng dễ dàng hơn;
- Vào/ra phân tán không nhất thiết phải đặt gần tại hiện trường (chỉ lợi dụng ưu điểm cuối cùng).



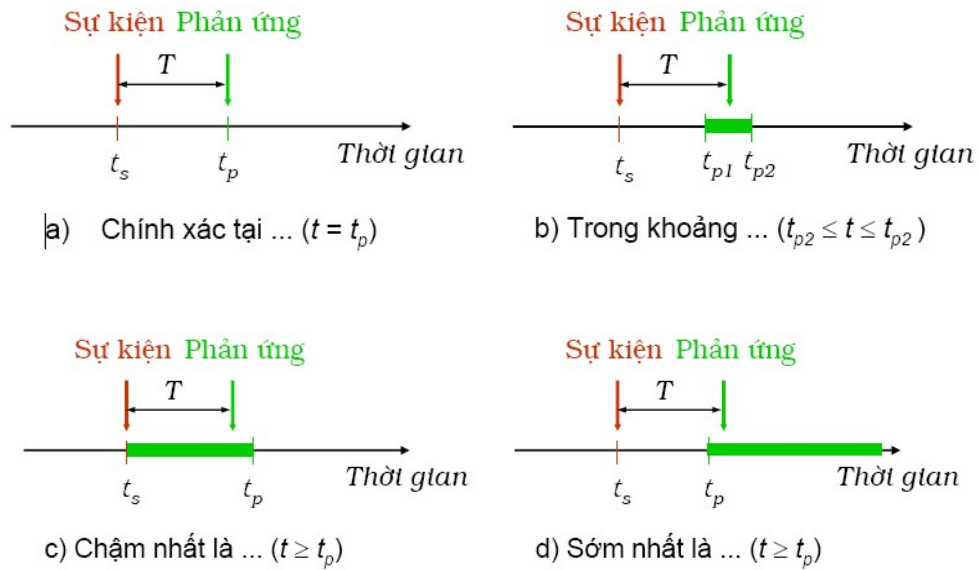
Hình 1.5: Sơ đồ đấu nối vào/ra mạng công nghiệp [26]

### 1.2.2 Hệ thời gian thực

Một hệ thời gian thực là một hệ thống mà sự hoạt động tin cậy của nó không chỉ phụ thuộc vào sự chính xác của kết quả, mà còn phụ thuộc vào thời điểm đưa ra kết quả để phản ứng với sự kiện bên ngoài.

Tính năng thời gian thực = tính chính xác + tính kịp thời

Các dạng của “tính thời gian thực”

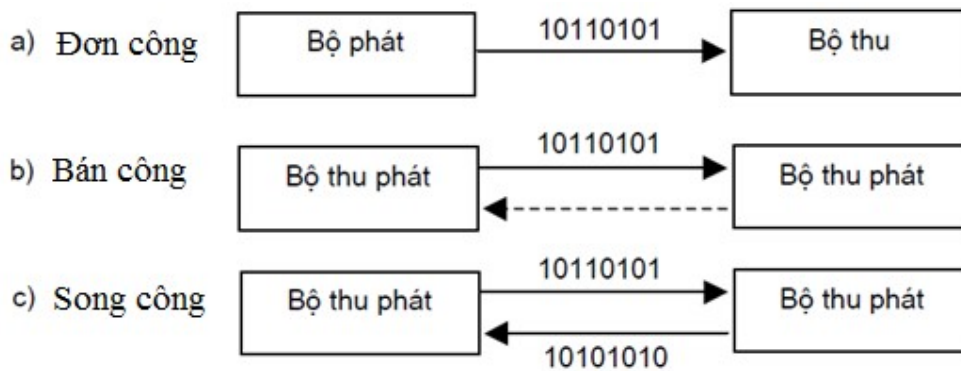


Hình 1.6: Các dạng của thời gian thực [22]

**1.2.3 Nguyên tắc cơ bản của truyền thông**

Chế độ truyền tải - điều chế tín hiệu là chế độ thông dụng nhất trong hệ thống truyền thông công nghiệp, với 3 dải truyền như sau:

- Truyền tải dải cơ sở: Tín hiệu mang một nguồn thông tin duy nhất trên dải tần cơ sở
- Truyền tải dải mang: Tín hiệu mang một nguồn thông tin duy nhất trên dải sóng mang.
- Truyền tải dải rộng: Tín hiệu mang nhiều nguồn thông tin cùng một lúc trên một dải tần rộng.



Hình 1.7: Nguyên tắc truyền dẫn trong mạng công nghiệp

Các thông số đặc trưng cho truyền dẫn

Tốc độ truyền và tốc độ bit

Thời gian bit/Chu kỳ bit  $T_B = 1/v$   $T_B = 1/f.n$ ,  $n$  là hệ số môi trường

Thời gian lan truyền tín hiệu  $T_S = l/(k*c)$   $l$  là chiều dài dây dẫn,

$c$  là tốc độ ánh sáng trong chân không (300.000.000m/s) và

$k$  là hệ số giảm tốc độ truyền

### **1.3 Câu hỏi ôn tập**

*Câu 1.1: Tại sao phải nhận biết các định nghĩa, các thuật ngữ sử dụng trong học phần này?*

*Câu 1.2: Có bao nhiêu khái niệm, định nghĩa trong chương này liên quan đến nội dung học phần và từ định nghĩa khái niệm, thuật ngữ nào là quan trọng?*

*Câu 1.3: Làm thế nào để đánh giá được một hệ thống điều khiển hiện đại, tiên tiến?*

## CHƯƠNG 2: CƠ SỞ MẠNG CÔNG NGHIỆP

Sử dụng mạng truyền thông công nghiệp, đặc biệt là bus trường để thay thế cách nối điểm - điểm cổ điển giữa các thiết bị công nghiệp mang lại hàng loạt những lợi ích.

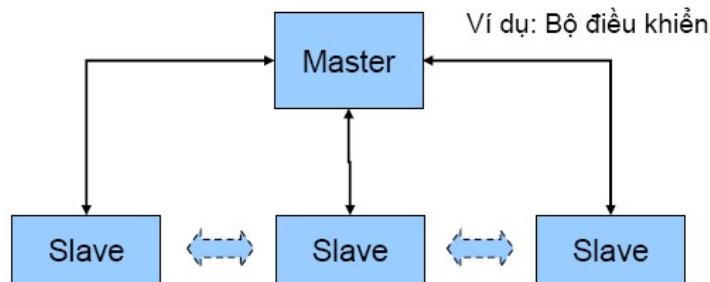
Bus trường (fieldbus) thực ra là một khái niệm chung được dùng trong các ngành công nghiệp chế biến để chỉ các hệ thống bus nối tiếp, sử dụng kỹ thuật truyền tin số để kết nối các thiết bị thuộc cấp điều khiển (PC, PLC) với nhau và với các thiết bị ở cấp chấp hành, hay các thiết bị trường [1].

Các chức năng chính của cấp chấp hành là đo lường, truyền động và chuyển đổi tín hiệu trong trường hợp cần thiết. Các thiết bị có khả năng nối mạng là các vào/ra phân tán (distributed I/O), các thiết bị đo lường (sensor, transducer, transmitter) hoặc cơ cấu chấp hành (actuator, valve) có tích hợp khả năng xử lý truyền thông. Một số kiểu bus trường chỉ thích hợp nối mạng các thiết bị cảm biến và cơ cấu chấp hành với các bộ điều khiển, cũng được gọi là bus chấp hành/cảm biến.

### 2.1 Kiến trúc giao tiếp

#### 2.1.1 Kiến trúc Chủ/tớ (Master/Slave)

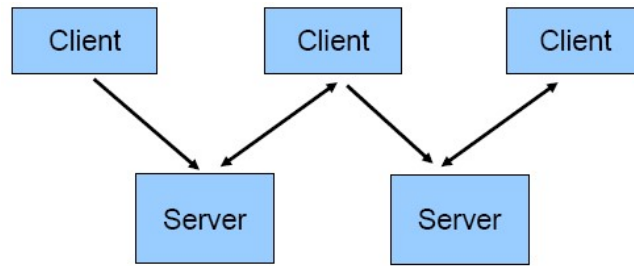
Một trạm chủ phối hợp hoạt động của nhiều trạm tớ, các trạm tớ có vai trò, nhiệm vụ tương tự như nhau, các trạm tớ có thể giao tiếp trực tiếp, hoặc không. Vai trò chủ động thuộc về Master [9], [17].



Hình 2.1: Kiến trúc Slave/Master

#### 2.1.2 Kiến trúc Client/Server

Kiến trúc Client/Server thực hiện các dịch vụ chung, phục vụ các Client. Giữa các Client không cần thiết có giao tiếp trực tiếp. Vai trò chủ động trong giao tiếp thuộc về client [27], [28].



Hình 2.2: Vào ra phân tán thiết bị trường

## 2.2 Cấu trúc mạng (network topology)

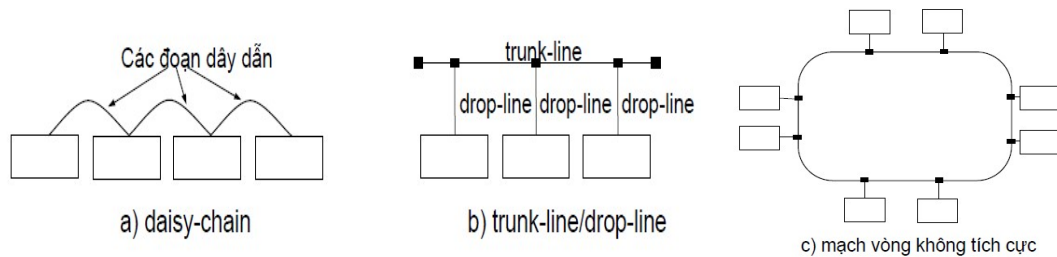
### 2.2.1 Liên kết (link)

Bao gồm các dạng liên kết trong mạng truyền thông công nghiệp sau [10], [29]:

Các kiểu liên kết: Liên kết điểm - điểm (point-to-point)

Liên kết điểm - nhiều điểm (multi-drop)

Liên kết nhiều điểm (multipoint)



Hình 2.3: Sơ cấu trúc bus liên kết mạng truyền thông công nghiệp

### 2.2.2 Cấu trúc (Topology)

Cấu trúc liên kết của một mạng, tổng hợp của các liên kết [16], [24].

- Cấu trúc bus
- Cấu trúc mạch vòng (tích cực)
- Cấu trúc hình sao

Cấu trúc bus liên quan tới tính năng [30]:

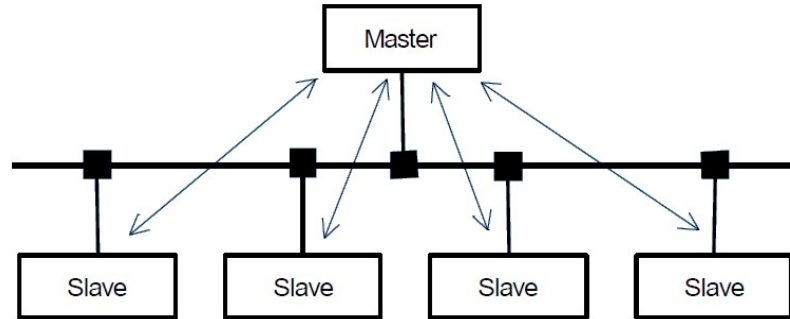
- + Tính thời gian thực
- + Độ tin cậy và tính sẵn sàng của hệ thống
- + Tính đơn giản
- + Khoảng cách truyền

## 2.3 Kiểm soát truy nhập bus

Kiểm soát truy nhập bus (*Bus access control, Medium Access Control*): Phân chia thời gian truy nhập đường truyền (gửi tín hiệu đi). Phương pháp kiểm soát truy nhập bus ảnh hưởng tới:

- Độ tin cậy
- Tính năng thời gian thực
- Hiệu suất sử dụng đường truyền

### 2.3.1 Phương pháp kiểm soát tập trung chủ/tớ (Master/Slave)

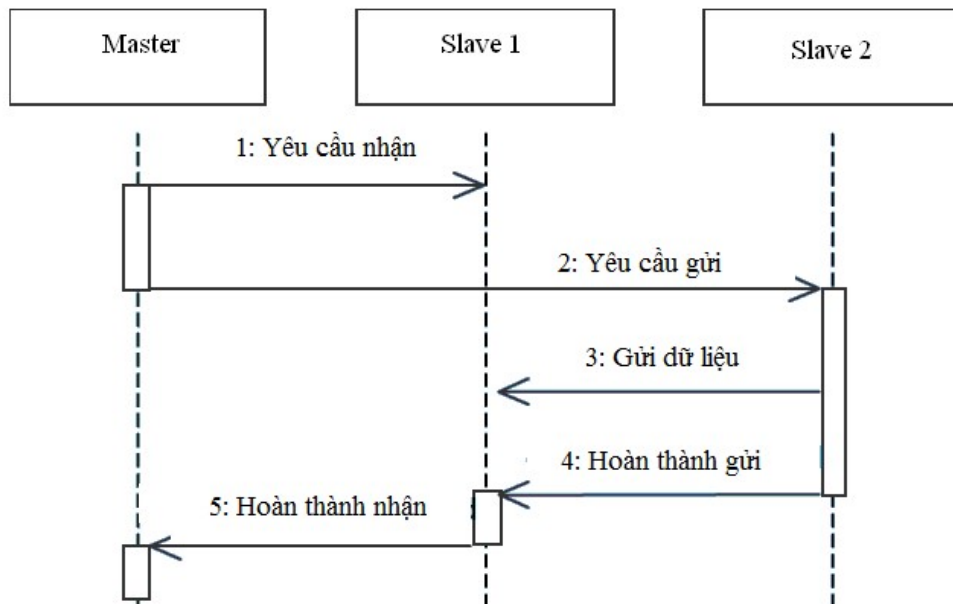


Hình 2.4: Truy nhập bus theo phương pháp Master/Slave

Vai trò của trạm chủ: Kiểm soát hoàn toàn giao tiếp trong hệ thống, hoặc chỉ đóng vai trò phân chia quyền truy nhập bus [17].

*Ưu điểm:*

- Tiên định
- Đơn giản, đỡ tốn kém
- Trí tuệ tập trung tại một trạm chủ



Hình 2.5: Giao tiếp theo cơ chế Master/Slave [31]

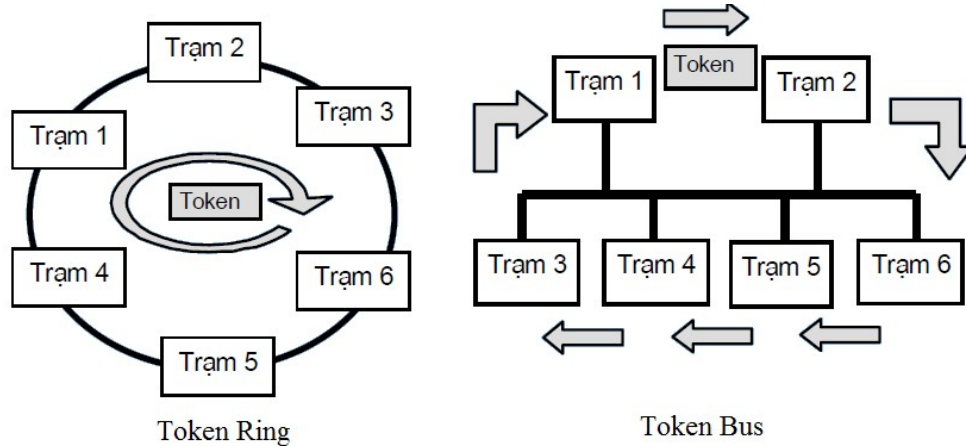
*Nhược điểm:*

- Độ tin cậy phụ thuộc vào một trạm duy nhất
- Hiệu suất trao đổi dữ liệu giữa hai trạm chủ/tớ thấp

Ứng dụng chủ yếu phổ biến trong các hệ thống bus cấp thấp (bus trường hay bus thiết bị) trao đổi thông tin hầu như chỉ diễn ra giữa trạm chủ là thiết bị điều khiển và các trạm tớ là thiết bị trường hoặc các module vào/ra phân tán.

Biểu đồ trình tự giao tiếp

### 2.3.2 Phương pháp kiểm soát phân tán Token Passing



Hình 2.6: Truy nhập bus theo phương pháp kiểm soát phân tán Token Passing [26], [32]

Vấn đề kiểm soát Token:

Giám sát token: Nếu do một lỗi nào đó mà token bị mất hoặc gia bội, cần phải thông báo xóa các token cũ và tạo một token mới.

Khởi tạo token: Sau khi khởi động một trạm được chỉ định có trách nhiệm tạo một token mới.

Tách trạm ra khỏi mạch vòng logic: Một trạm có sự cố phải được phát hiện và tách ra khỏi trình tự được nhận token.

Bổ sung trạm mới: Một trạm mới được kết nối mạng, một trạm cũ được thay thế hoặc đưa trở lại sử dụng phải được bổ sung vào mạch vòng logic để có quyền nhận token.

*Ưu điểm:*

- Tiên định
- Độ tin cậy cao hơn nhờ vai trò bình đẳng
- Phù hợp cho nhiều cơ chế giao tiếp khác nhau

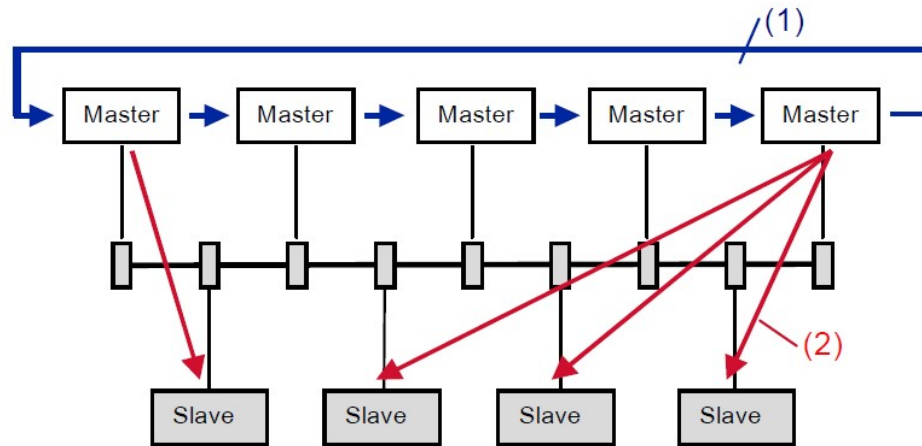
*Nhược điểm:*

- Phức tạp

Ứng dụng: chủ yếu ở cấp phía trên (bus điều khiển, bus hệ thống)



### 2.3.3 Kết hợp Token với Master/Slave (Multimaster)



(1) Token passing giữa các trạm tích cực

(2) Master/slave giữa một trạm tích cực và một số trạm không tích cực

Hình 2.7: Truy nhập bus kết hợp 2 phương pháp Master/Slave với Token [33]

*Ưu điểm:*

- Tiên định, phù hợp với trao đổi dữ liệu tuần hoàn
- Có thể đáp ứng yêu cầu rất ngặt nghèo về tính năng thời gian thực
- Không cần kiểm soát tập trung

*Nhược điểm:*

- Hiệu suất sử dụng đường truyền có thể không cao
- Đồng bộ hóa thời gian phức tạp

Ứng dụng: Thường là kết hợp với Master/Slave (ví dụ Profibus-DP V2.0, Interbus) hoặc Token Passing (Foundation Fieldbus H1). Chủ yếu ở cấp trường [33], [34].

### 2.3.4 Truy nhập nhận biết xung đột CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Đây một phương pháp truy nhập bus ngẫu nhiên, nổi tiếng cùng mạng Ethernet (IEEE 802.3) [35].

Carrier Sense: Cảm nhận, nghe ngóng đường truyền

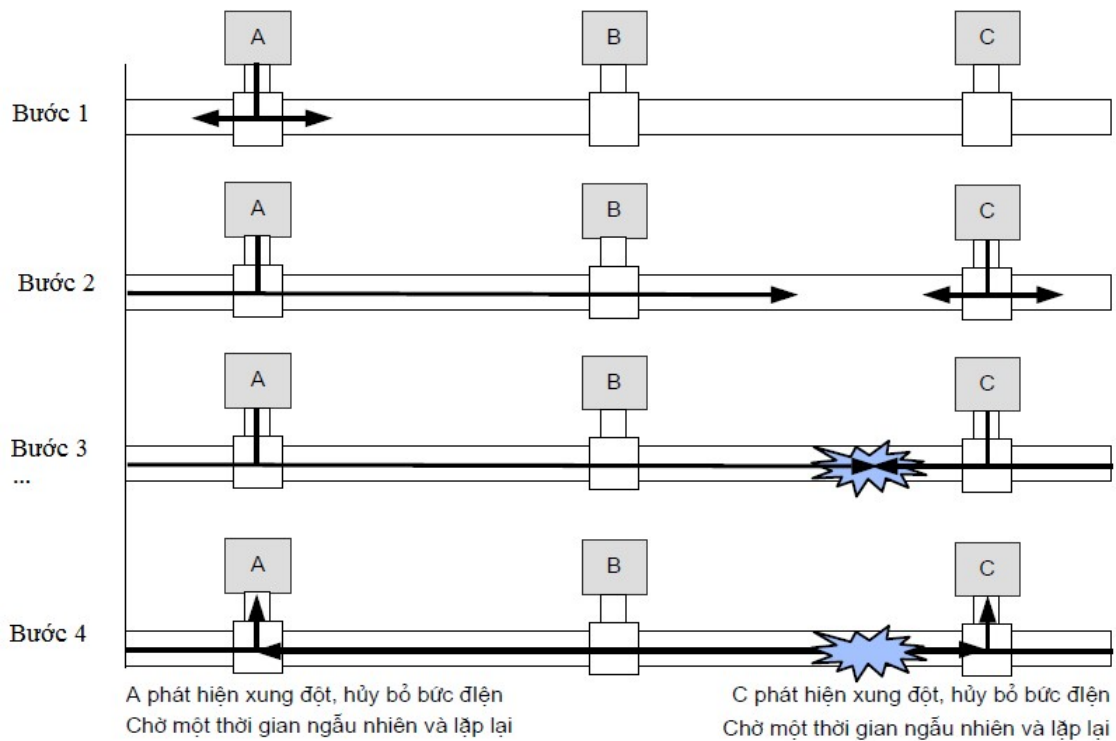
Multiple Access: Đa truy nhập (đương nhiên!)

Collision Detection: Nhận biết xung đột

Nguyên tắc làm việc

*Ưu điểm:*

- Rất linh hoạt, không cần đặt cấu hình mạng trước;
- Được sử dụng rộng rãi.



Hình 2.8: Sơ đồ giả định xảy ra xung đột đường truyền [1]

*Nhược điểm:*

- Thiếu tính tiên định;
- Thuật toán phức tạp;

Ứng dụng: Chủ yếu ở mạng cấp cao (Ethernet), gần đây được sử dụng ở cấp thấp:  
Sử dụng công nghệ chuyển mạch (switch) nhằm giảm xung đột tín hiệu.

## 2.4 Bảo toàn dữ liệu

### 2.4.1 Lỗi dữ liệu

- Phân loại lỗi
  - + Lỗi phát hiện được, không sửa được
  - + Lỗi phát hiện được nhưng sửa được
  - + Lỗi không phát hiện được.
- Giải pháp khắc phục lỗi
  - + Giải pháp phần cứng
  - + Giải pháp phần mềm (xử lý giao thức)
- Tỷ lệ bit lỗi  $p$  là thước đo đặc trưng cho độ nhiễu của kênh truyền dẫn, được tính bằng tỉ lệ giữa số bit bị lỗi trên tổng số bit được truyền đi.

- Tỷ lệ lỗi còn lại  $R$  là thông số đặc trưng cho độ tin cậy dữ liệu của một hệ thống truyền thông, sau khi đã thực hiện các biện pháp bảo toàn (kể cả truyền lại trong trường hợp phát hiện ra lỗi).

- Thời gian trung bình giữa hai lần lỗi  $T_{MTBF}$  ( $MTBF = \text{Mean Time Between Failures}$ ):  $T_{MTBF} = n/(v \cdot R)$

- Khoảng cách Hamming: thông số đặc trưng cho độ bền vững của một mã dữ liệu chính là khả năng phát hiện lỗi của một phương pháp bảo toàn dữ liệu.

#### 2.4.2 Bảo toàn dữ liệu kiểu bit chẵn/lẻ (parity bit)

Bit chẵn lẻ (parity bit) là một bit dùng để báo hiệu số lượng bit có giá trị bằng “1” trong một nhóm bit cho trước là một số chẵn hay là một số lẻ. Bit chẵn lẻ được sử dụng như là một mã dùng để phát hiện lỗi đơn giản nhất [7], [36].

Có hai loại mã chẵn lẻ: bit chẵn lẻ dùng quy luật số chẵn (even parity bit) và bit chẵn lẻ dùng quy luật số lẻ (odd parity bit). Bit chẵn lẻ dùng quy luật số chẵn có giá trị bằng “1” khi số lượng các bit “1”, trong một nhóm bit cho trước, là một số lẻ (và khi cộng thêm bit chẵn lẻ vào, tổng số lượng bit có giá trị bằng “1” là một số chẵn). Ngược lại, bit chẵn lẻ dùng quy luật số lẻ có giá trị bằng “1” nếu số lượng các bit “1”, trong một nhóm bit cho trước, là một số chẵn (và khi cộng thêm bit chẵn lẻ vào, tổng số bit có giá trị bằng “1” là một số lẻ). Bit chẵn lẻ dùng quy luật chẵn là một trường hợp đặc biệt của kỹ thuật kiểm tra độ dư tuần hoàn (cyclic redundancy check - CRC). Trong CRC, bit CRC được kiến tạo bằng cách dùng đa thức (polynomial)  $x+1$ .

Dãy bit nguyên bản: 1001101

Dãy bit gửi đi: 10011010

Giả sử nhận được 10111010 vì vậy lỗi phát hiện được

Giả sử nhận được 11111010 vì vậy lỗi không phát hiện được

Ví dụ: Khung UART

UART (*Universal Asynchronous Receiver/Transmitter*) được sử dụng khá rộng rãi

Start	0	1	2	3	4	5	6	7	P	Stop
0	LSB						MSB			1

Giải pháp bit chẵn lẻ hai chiều sẽ khắc phục được hạn chế trên, sau đây là mô tả bit chẵn lẻ hai chiều:

	1.	2.	3.	4.	5.	6.	7.	p		1.	2.	3.	4.	5.	6.	7.	p
1.	0	1	0	0	1	0	1	1	1.	0	1	0	0	1	0	1	1
2.	1	0	0	1	0	0	0	0	2.	1	0	0	1	0	0	0	0
3.	1	1	1	0	1	1	1	0	3.	1	1	1	1	1	1	1	0
4.	0	1	0	1	0	1	0	1	4.	0	1	0	1	0	1	0	1
5.	1	1	1	1	0	1	1	0	5.	1	1	1	1	0	1	1	0
6.	0	0	0	1	1	1	1	0	6.	0	0	0	1	1	1	1	0
7.	1	1	0	0	1	1	0	0	7.	1	1	0	0	1	1	0	0
p	0	1	0	0	0	1	0	0	p	0	1	0	0	0	1	0	0

### 2.4.3 Bảo toàn kiểu mã vòng (CRC)

- CRC (Cyclic Redundancy Check): thông tin kiểm lỗi (ở đây được gọi là *checksum*) phải được tính bằng một thuật toán thích hợp, trong đó giá trị mỗi bit của thông tin nguồn đều được tham gia nhiều lần vào quá trình tính toán. CRC được sử dụng rộng rãi trong đa số các hệ thống truyền thông công nghiệp. CRC còn được gọi là phương pháp đa thức, bởi nó sử dụng phép chia đa thức (nhị phân)[7], [36]:

- Đa thức được hình thành từ các hệ số là “0/1”, ví dụ:  $G = x^7 + x^6 + x^5 + x^2 + 1$

$G = x^7 + x^6 + x^5 + 0x^4 + 0x^3 + x^2 + 0x^1 + 1$  vậy mã  $G = \{11100101\}$

- Phép chia đa thức nhị phân được qui về các phép so sánh, sao chép và XOR

Nguyên tắc thực hiện

- Hai bên qui ước một “đa thức phát”  $G$  bậc  $n$ , ví dụ  $x^3+x+1$  tương ứng với dãy bit  $\{1011\}$ .

- Dãy bit mang thông tin nguồn  $I$  được thêm vào  $n$  bit 0 và coi như một đa thức nhị phân  $P$ .

- Ví dụ: thông tin nguồn là  $\{110101\}$  vì vậy  $P = \{110101000\}$

- Lấy  $P$  chia cho  $G$  ta được kết quả và phần dư  $R$

- Phần dư  $R$  của phép chia được thay thế vào chỗ của  $n$  chữ 0 bổ sung trong  $P$ , tức là ta có  $D = P$

+  $R$  được gọi là *checksum* và  $D$  chính là dãy bit được gửi đi thay cho  $I$ .

Giả sử dãy bit nhận được là  $D'$  không chia hết cho  $G$  vì vậy bức điện chắc chắn bị lỗi. Nếu  $D'$  chia hết cho  $G$ , thì xác suất rất cao là bức điện nhận được không có lỗi.

Ví dụ minh họa:

Thông tin cần truyền  $I = 110101$ , đa thức  $G = 1011$  (tức  $x^3 + x + 1$ )

Thêm 3 bit 0 vào thông tin nguồn  $I$ , ta có  $P = 110101000$

Chia đa thức  $P$ :  $G$

110101000: 1011 = 1111 dư 010

Dãy bit được chuyển đi:  $D = P + R = 110101010$

Giả sử dữ liệu nhận được là  $D' = 110101010$

Chia đa thức  $D'$ :  $G \ 110101111: 1011 = 111101$

Phần dư 0000 -> Xác suất rất cao là không có lỗi

#### 2.4.4 Bảo toàn kiểu nhồi bit (Bit stuffing)

Bên gửi: Nếu trong dữ liệu có  $n$  bit “1” đứng liền nhau thì thêm một bit “0” vào ngay sau đó. Như vậy trong dãy bit được chuyển đi không thể xuất hiện  $n+1$  bit “1” đi liền nhau [32].

Bên nhận: Nếu phát hiện thấy  $n$  bit “1” liền nhau mà bit tiếp theo là “0” thì được tách ra, còn nếu là bit “1” thì dữ liệu chắc chắn bị lỗi [1].

### 2.5 Mã hóa và giải mã bit

- Mã hóa đường truyền (Line encoding, signal encoding): Biểu diễn nguồn thông tin cần truyền bằng một tín hiệu thích hợp cho truyền dẫn, có thể bao gồm:

- + Mã hóa bit (biểu diễn một dãy bit thành một tín hiệu),
- + Các biện pháp dồn kênh.

- Mã hóa bit (Bit encoding): trường hợp đặc biệt của mã hóa đường truyền (không có dồn kênh, phân kênh) [11], [32]

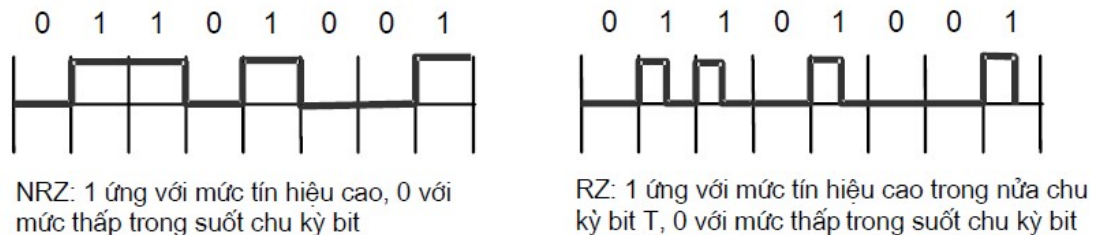
- + Trong truyền thông công nghiệp ta chỉ cần đề cập tới mã hóa bit
- + Mã hóa bit còn được gọi là điều chế tín hiệu (signal modulation)

- Giải mã bit: Khôi phục dãy bit từ một tín hiệu nhận được

Các yếu tố kỹ thuật chú ý khi mã hóa và giải mã

- Tần số, dải tần tín hiệu:
- Tính bền vững với nhiễu, khả năng phát hiện lỗi
- Triệt tiêu dòng một chiều/khả năng đồng tải nguồn
- Thông tin đồng bộ nhịp trong tín hiệu:

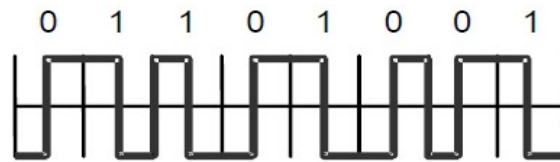
#### 2.5.1 Phương pháp NRZ và RZ



Hình 2.9: Mã hóa bit bằng phương pháp NRZ và RZ

- NRZ (Non-return to Zero), RZ (Return to Zero)
- Các tính chất [11], [32]:
  - + Tần số thấp, dải tần không hẹp
  - + Kém bền vững với nhiễu
  - + Tồn tại dòng một chiều
  - + Không mang thông tin đồng bộ nhịp
- Ứng dụng: Phổ biến nhất, Profibus-DP, Interbus

### 2.5.2 Mã Manchester

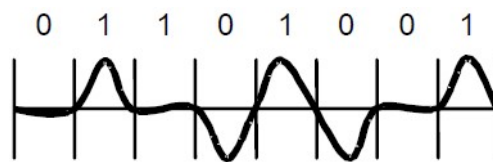


Manchester-II: 1 ứng với sườn xuống, 0 ứng với sườn lên của xung ở giữa chu kỳ bit

Hình 2.10: Mã hóa bit bằng phương pháp Manchester

- Các tính chất [10], [11]:
  - + Tần số cao hơn NRZ, dải tần không hẹp
  - + Khá bền vững với nhiễu, không có khả năng phối hợp nhận biết lỗi
  - + Triệt tiêu dòng một chiều, khả năng đồng bộ tải nguồn
  - + Mang thông tin đồng bộ nhịp
- Ứng dụng: Khá phổ biến, như: Ethernet, Profibus-PA, Foundation Fieldbus

### 2.5.3 Mã AFP (Alternate Flanked Pulse)

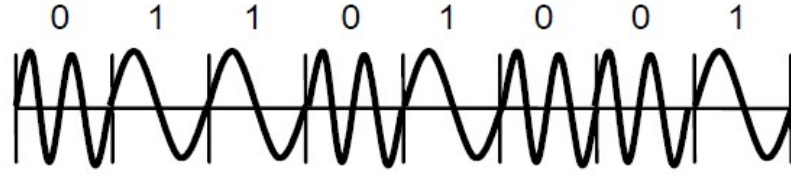


AFP: Thay đổi giữa 0 và 1 được đánh dấu bằng một xung xoay chiều

Hình 2.11: Mã hóa bit bằng phương pháp AFP

- Các tính chất [2], [20]:
  - + Tần số thấp nhất, dải tần hẹp nhất
  - + Khá bền vững với nhiễu, có khả năng phối hợp nhận biết lỗi
  - + Tồn tại dòng một chiều
  - + Không mang thông tin đồng bộ nhịp
- Ứng dụng: AS-Interface

#### 2.5.4 Mã FSK (*Frequency Shift Keying*)



FSK: 0 và 1 ứng với các tần số khác nhau

Hình 2.12: Mã hóa bit bằng phương pháp FSK

- Các tính chất [37], [38]:

- + Tần số cao (truyền tải dải mang), dải tần hẹp
- + Đặc biệt bền vững với nhiễu, có khả năng phối hợp nhận biết lỗi
- + Triệt tiêu dòng một chiều, có khả năng đồng tải nguồn
- + Mang thông tin đồng bộ nhịp
- Ứng dụng: HART, Powerline Communication

## 2.6 Câu hỏi ôn tập chương

Câu 2.1: Cơ sở kỹ thuật mạng (công nghiệp) là cái gì?

Câu 2.2: Yếu tố nào là quan trọng nhất trong cơ sở kỹ thuật mạng?

Câu 2.3: Một mạng được đánh giá là tốt thì cần có những cơ sở kỹ thuật ra sao?

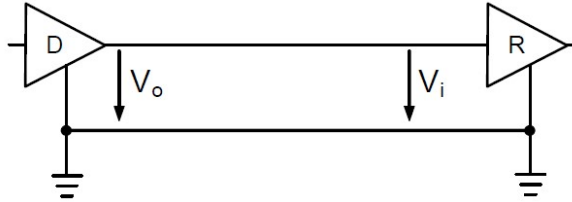
## CHƯƠNG 3: KỸ THUẬT MẠNG CÔNG NGHIỆP

### 3.1 Kỹ thuật truyền dẫn

#### 3.1.1 Phương thức truyền dẫn tín hiệu đơn cực

- Truyền dẫn không đối xứng hay đơn cực (*unbalanced mode, single-ended mode*):

Sử dụng điện áp chênh lệch giữa một dây dẫn và đất. Ví dụ: RS-232.



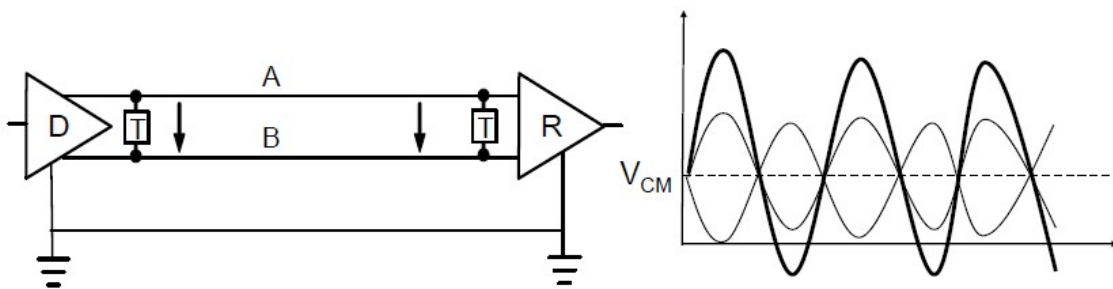
Hình 3.1: Phương thức truyền dẫn dữ liệu không đối xứng

Ưu nhược điểm của phương thức đơn cực

- Tiết kiệm dây dẫn
- Khả năng kháng nhiễu kém (nhiễu ngoại, nhiễu xuyên âm - *crosstalk*, chênh lệch điện áp đất [39])
- Phải sử dụng mức tín hiệu cao
- Tốc độ truyền kém
- Khoảng cách truyền ngắn

#### 3.1.2 Phương thức truyền dẫn tín hiệu đối xứng

- Phương thức truyền chênh lệch đối xứng [1] (*balanced differential mode*): sử dụng điện áp chênh lệch giữa hai dây dẫn A và B (hoặc - và +). Ví dụ: RS-422, RS-485, MBP (IEC-611582).



$V_{CM}$ : Điện áp chung

Hình 3.2: Phương thức truyền dẫn dữ liệu đối xứng

Ưu nhược điểm của phương thức chênh lệch đối xứng

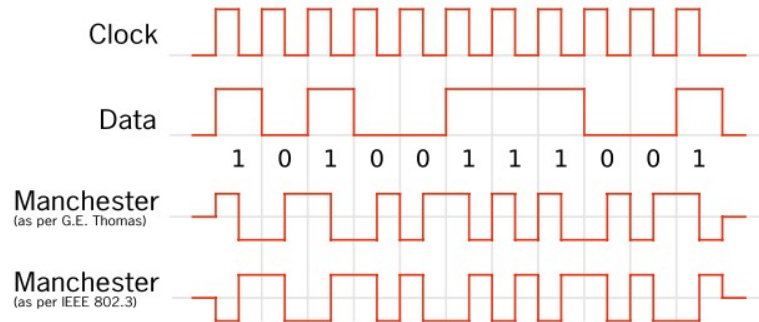
- Không tiết kiệm dây dẫn lắm
- Khả năng kháng nhiễu tốt



- Có thể sử dụng mức tín hiệu thấp
- Tốc độ truyền cao
- Khoảng cách truyền lớn

### 3.1.3 Phương thức truyền dẫn MBP (IEC 61158-2)

MBP (*Manchester Coded, Bus-Powered*): Áp dụng trong Foundation Fieldbus, Profibus-PA [19], [40]



Hình 3.3: Kỹ thuật truyền dẫn MBP

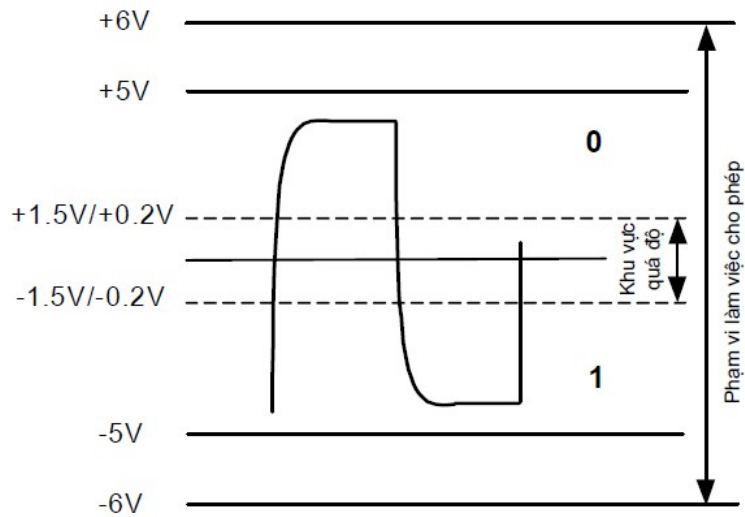
- Ứng dụng chủ yếu trong công nghiệp chế biến
- Khả năng dùng trong môi trường yêu cầu an toàn cháy nổ
- Mã Manchester, truyền đồng bộ
- Khả năng đồng bộ tải nguồn
- Truyền chệnh lệch đối xứng, mức tín hiệu chệnh lệch 0,75-1V
- Tốc độ truyền 31,25kbps (cố định)
- Số trạm tối đa 32/đoạn, 126/toàn mạng, tối đa 4 bộ lặp
- Khoảng cách truyền tối đa 1900m/đoạn vì vậy 9500m/toàn mạng
- Trở đầu cuối 100Ohm

### 3.1.4 Chuẩn truyền thông RS-485

Tên chính thức EIA/TIA-485, phiên bản mới nhất là EIA/TIA-485b. Truyền thông theo kiểu chệnh lệch đối xứng, vì vậy có nhiều ưu điểm đã nêu trên.

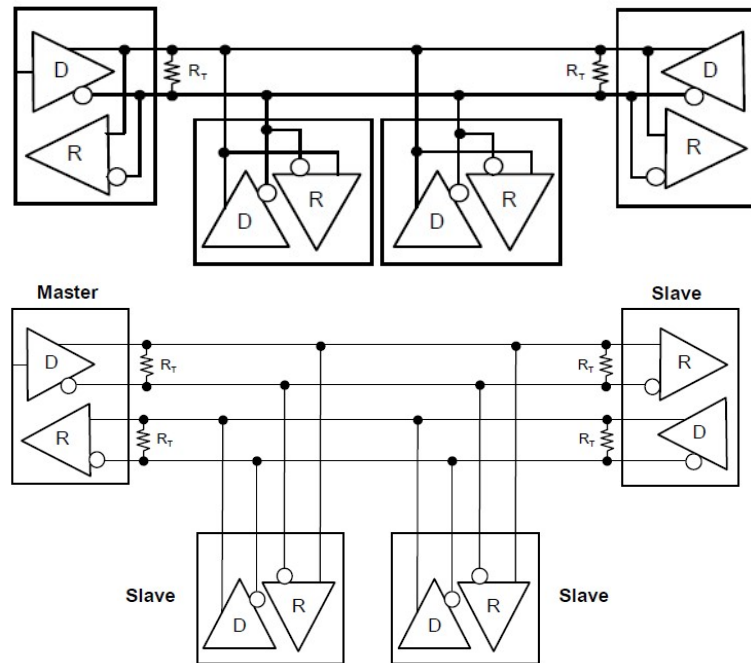
Là chuẩn được sử dụng thông dụng nhất trong các hệ thống truyền thông công nghiệp (Profibus FMS/DP, Interbus, AS-Interface và các giao thức riêng khác...)

Qui định mức tín hiệu [41], [42]



Hình 3.4: Mức tín hiệu quy định RS 485

Cấu hình ghép nối hai dây và 4 dây trong chuẩn truyền thông 485



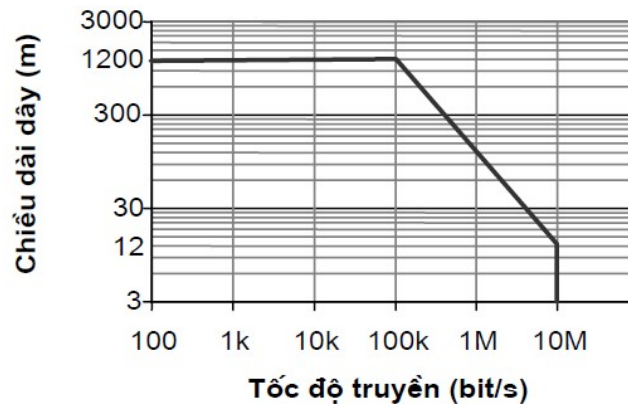
Hình 3.5: Sơ đồ ghép nối RS 485

Một số đặc điểm cơ bản

- Phương thức truyền dẫn chênh lệch đối xứng
- Chế độ truyền chủ yếu là hai chiều gián đoạn
- Ghép nối nhiều điểm, số trạm tối đa/đoạn mạng là 32
- Tốc độ truyền cao (có thể tới 10Mbps)
- Khoảng cách truyền lớn (có thể tới 1200m)
- Có thể dùng tới 3 bộ lặp (4 đoạn mạng), trong thực tế có thể hơn

- Trở đầu cuối: 100 hoặc 120 Ohm

Quan hệ giữa tốc độ truyền và khoảng cách truyền (sử dụng đôi dây xoắn AWG 24)



Hình 3.6: Tốc độ truyền dẫn RS 485

Theo qui định chuẩn, một bộ kích thích tín hiệu phải đảm bảo dòng tổng cộng 60mA vừa đủ để cung cấp cho:

- Hai trở đầu cuối mắc song song tương ứng tải 60Ω (120Ω tại mỗi đầu) với điện áp tối thiểu 1,5V vì vậy tổng mạng lên tới 25mA
- 32 tải đơn vị mắc song song với dòng 1mA qua mỗi đơn vị tải (trường hợp xấu nhất) vì vậy 32mA.

## 3.2 Giao thức mạng

Mục đích giao tiếp của hai đối tác (con người, thiết bị), trao đổi dịch vụ (cung cấp dịch vụ và sử dụng dịch vụ). Chức năng mà một thiết bị truyền thông hỗ trợ.

### 3.2.1 Định nghĩa giao thức mạng (network protocol)

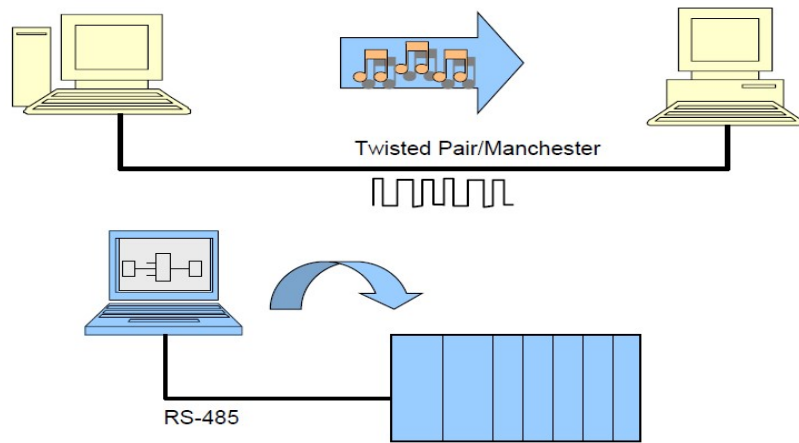
Giao thức mạng là qui tắc, thủ tục, hình thức giao tiếp giữa các thiết bị mạng: Chúng ta thực hiện một cuộc đàm thoại và “Ngôn ngữ” cho việc giao tiếp là:

- Cú pháp (syntax);
- Ngữ nghĩa (semantics);
- Định thời (timing).

Qui trình thực hiện và diễn giải giao thức vì vậy xử lý giao thức cần được thực hiện, thực tế tồn tại nhiều loại giao thức, nhiều cấp giao thức vì vậy yêu cầu phân loại và phân cấp giao thức

Ví dụ: Giao thức khung HDLC (High Level Data-link Control) [20]

01111110	8/16 BIT	8bit	N bit	16/32 bit	01111110
Flag	Address	Control	Data	FCS	Flag



Hình 3.7: Sơ đồ giao thức mạng

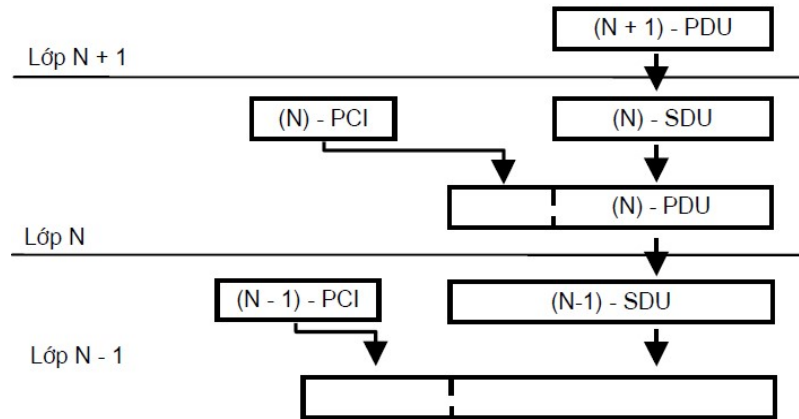
### 3.2.2 Mô hình lớp

Mô hình lớp: Phân loại dịch vụ và các giao thức của một hệ thống truyền thông thành các lớp [23], [30]:

Dịch vụ cấp cao và dịch vụ cấp thấp;

Giao thức cấp cao và giao thức cấp thấp;

Xử lý giao thức theo mô hình lớp.



Hình 3.8: Sơ đồ mô hình lớp cơ bản

SDUPDU: Protocol Data Unit –Khối dữ liệu giao thức

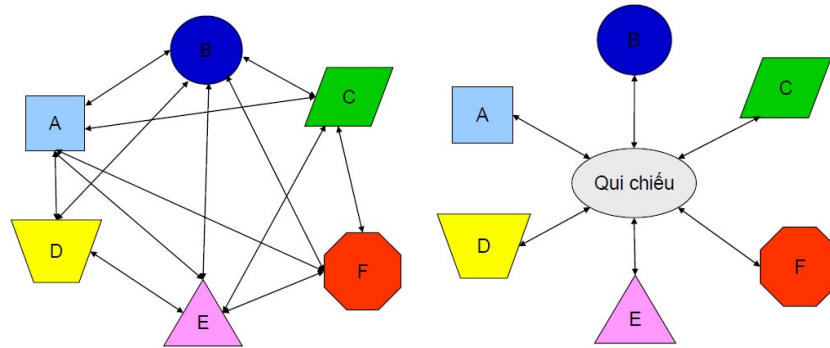
SDU: Service Data Unit – Khối dữ liệu dịch vụ

PCI: Protocol Control Information -Thông tin trong khối giao thức

### 3.2.3 Mô hình qui chiếu ISO/OSI

- Mô hình tham chiếu kết nối hệ thống mở
- Chuẩn hóa ISO 7498
- Một mô hình qui chiếu, cơ sở cho:
  - ✓ So sánh, đối chiếu các hệ thống truyền thông với nhau

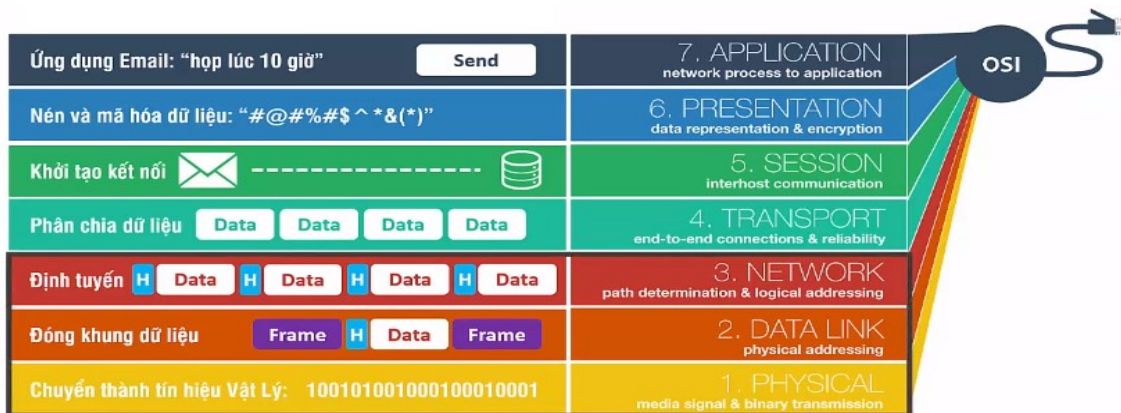
- ✓ Tìm hiểu một hệ thống truyền thông
  - ✓ Liên kết giữa các thiết bị/hệ thống với nhau
  - ✓ Phát triển một hệ thống truyền thông mới
- Không phải là một chuẩn giao thức, một chuẩn dịch vụ, chỉ là một mô hình!
  - Không đảm bảo, mà chỉ tạo điều kiện cho việc tương tác giữa các hệ thống
  - Vấn đề: N hệ thống truyền thông



Hình 3.9: Sơ đồ mô hình quy chiếu

Trả lời: N trường hợp so sánh, nếu ta có một hệ quy chiếu.

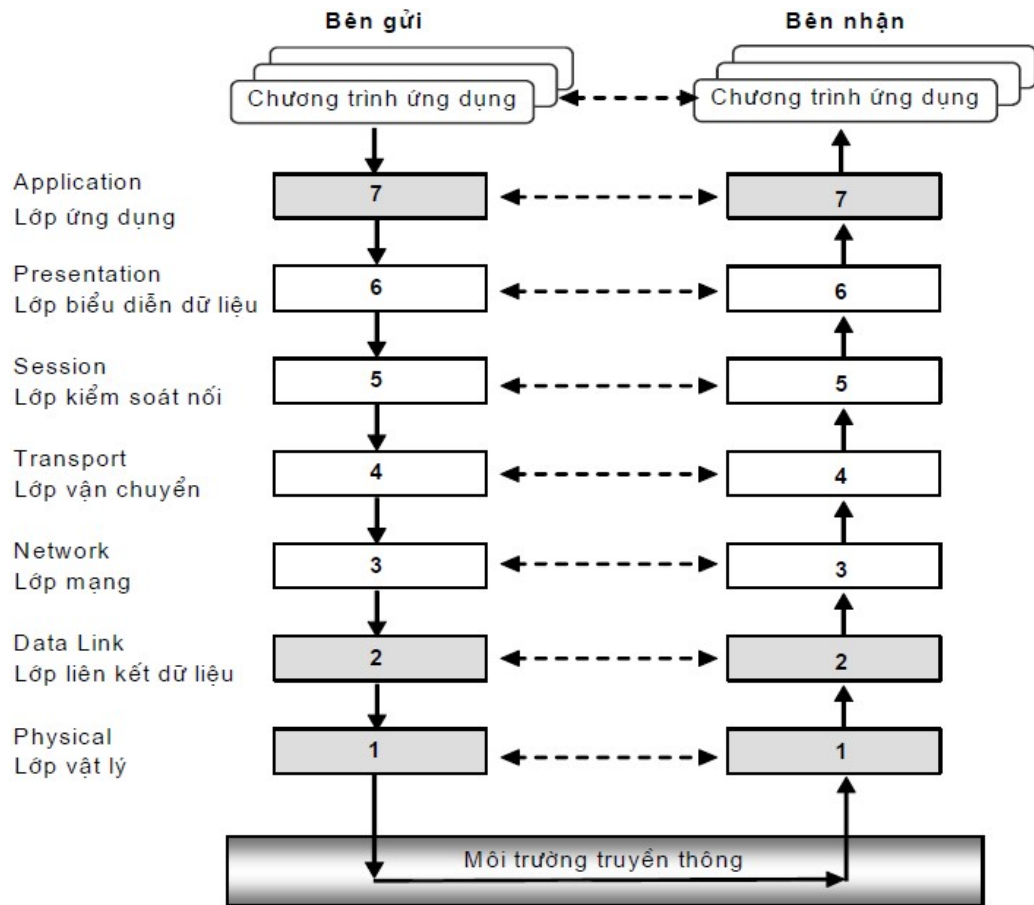
Ví dụ giao tiếp theo mô hình OSI [17]



Hình 3.10: Sơ đồ mô hình OSI

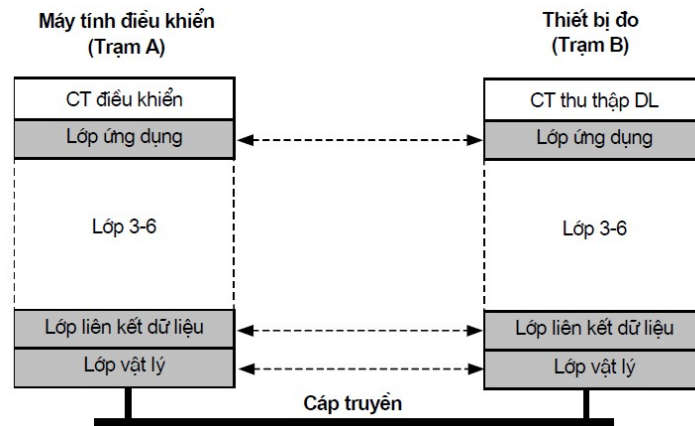
Mô hình OSI không phải là:

- Chuẩn dịch vụ (không qui định các dịch vụ phải thực hiện);
- Chuẩn giao thức (không qui định thực hiện các dịch vụ như thế nào);
- Chuẩn đảm bảo tương tác giữa các hệ thống;
- Mô hình về cấu trúc mạng.



Hình 3.11: Sơ đồ mô hình lớp của giao thức [1]

Ví dụ giao tiếp theo mô hình OSI



Hình 3.12: Sơ đồ mô hình OSI

Mô hình OSI không phải là:

- Chuẩn dịch vụ (không quy định các dịch vụ phải thực hiện)
- Chuẩn giao thức (không quy định thực hiện các dịch vụ như thế nào)
- Chuẩn đảm bảo tương tác giữa các hệ thống

- Mô hình về cấu trúc mạng

### 3.2.4 Kiến trúc TCP/IP

Kiến trúc TCP/IP được hiểu như sau [5], [16], [42]:

TCP: Transmission Control Protocol

IP: Internet Protocol

TCP/IP:

- Kiến trúc giao thức dựa trên nền tảng của TCP/IP
- Tập các giao thức (protocol stack) TCP, IP, FTP, TELNET,...

So sánh TCP/IP và OSI

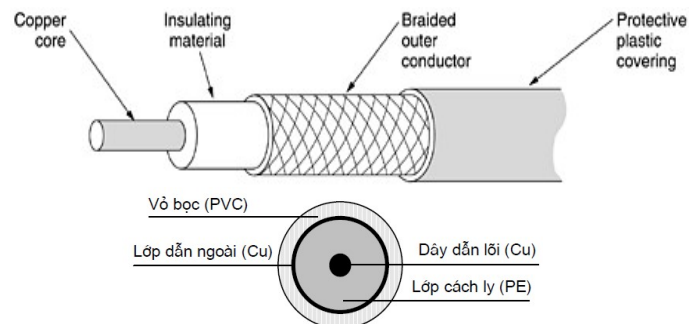
OSI	TCP/IP
Lớp ứng dụng	Lớp ứng dụng
Lớp biểu diễn dữ liệu	TELNET FTP SNMP SMTP DNS
Lớp kiểm soát nối	Lớp vận chuyển
Lớp vận chuyển	TCP UDP
Lớp mạng	Lớp Internet ICMP IP ARP RARP
Lớp liên kết dữ liệu	Lớp truy nhập mạng
Lớp vật lý	Lớp vật lý

Hình 3.13: Sơ đồ mô hình OSI và TCP/IP

## 3.3 Các thành phần trong mạng truyền thông

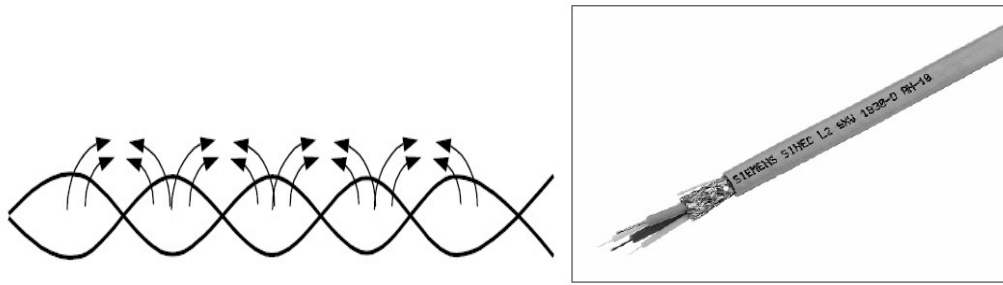
### 3.3.1 Dây dẫn

- Đơn gồm: Cáp đồng trục, đôi dây xoắn, cáp tron, cáp quang



Hình 3.14: Mô hình cáp đồng trục

- Đôi dây xoắn (Twisted Pair -TP) Phát minh của A. Gramh Bell,1881



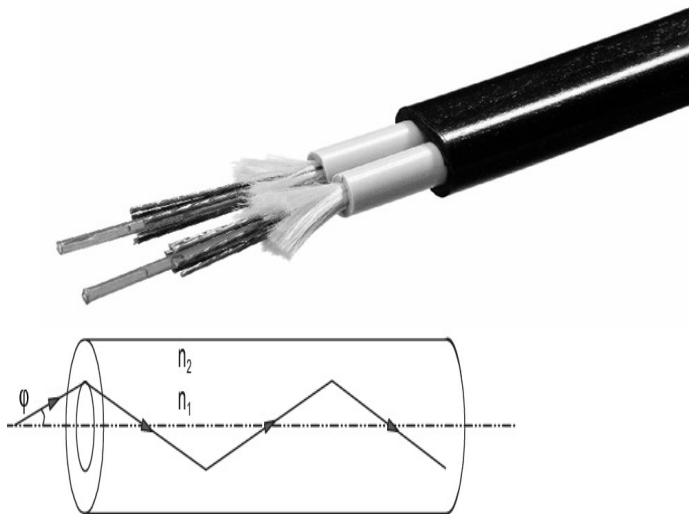
Hình 3.15: Mô hình cáp đôi dây xoắn

Hai loại: Shielded TP, Unshielded TP: Chất lượng phụ thuộc vào tiết diện và kiểu bọc lót, che chắn. Hạng chất lượng 1-5 hoặc D-A (IEC 61158-2), hạng 5 có thể cho tốc độ truyền 100Mbit/s (Fast Ethernet 100BASE-TX) [2], [32].

- Tốc độ truyền tối đa: 1-2 Gbit/s
- Chất lượng cao
- Lắp đặt phức tạp
- Sử dụng chủ yếu ở mạng cấp cao (Ethernet, ControlNet)

So sánh độ suy giảm trên đường truyền

Cáp quang



Hình 3.16: Mô hình cáp quang

- Các loại sợi quang

+ Sợi thủy tinh có hai loại:

*Sợi đa chế độ (Multimode Fiber, MMF)*: tín hiệu là các tia laser có tần số không thuần nhất. Khả năng truyền hạn chế trong phạm vi Gbit/s \* km.

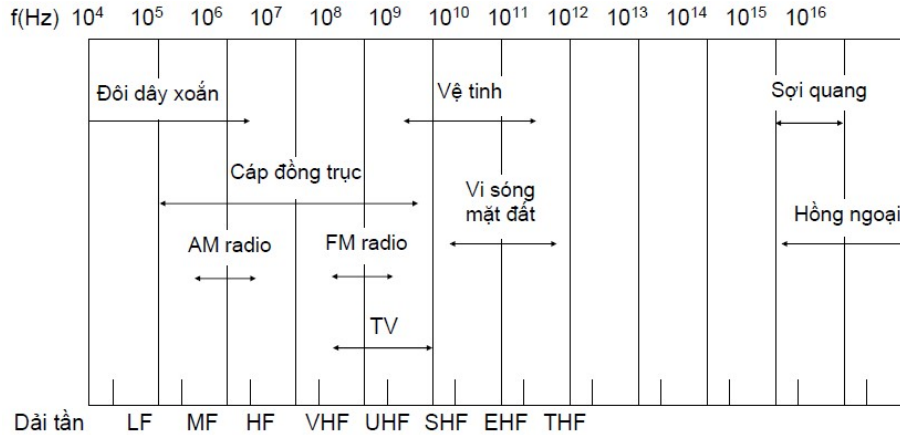
*Sợi đơn chế độ (Single-Mode Fiber, SMF)*: tín hiệu là các tia laser có tần số thuần nhất. Tốc độ truyền có thể đạt tới hàng trăm Gbit/s \* km.



- Sợi chất dẻo: Truyền với tốc độ thấp (khoảng vài chục tới vài trăm Mbit/s), khoảng cách truyền ngắn (tối đa 80m), giá thành thấp và lắp đặt dễ dàng hơn nhiều. Cáp quang được sử dụng ngày càng nhiều trong SCADA [32], [43].

### 3.3.2 Vô tuyến:

Sóng truyền hình (TV), sóng truyền thanh (radio AM, FM), tia hồng ngoại (UV), phương tiện truyền dẫn, dải tần Shannon là những sóng vô tuyến có tốc độ bit tối đa  $(\text{bits/s}) = H \log_2 (1+S/N)$



Hình 3.17: Dải tần truyền dẫn vô tuyến

### 3.3.3 NIC – Network Interface Card

- Nic là thiết bị phổ dụng nhất đối với máy tính. Trong NIC có bộ thu phát (Tranceiver) hoạt động như một Transmitter và một Receiver. Transmitter chuyển đổi các tín hiệu bên trong máy tính thành tín hiệu có thể truyền đi được qua đường mạng. Receiver làm ngược lại [5].

### 3.3.4 Hup

*HUB bị động (HUB – Passive):* Không chứa các linh kiện điện tử xử lý tín hiệu, chỉ có chức năng tổ hợp các tín hiệu từ một số các đoạn mạng. Khoảng cách lớn nhất giữa một máy tính với hub không thể lớn hơn một nửa khoảng cách cho phép giữa 2 máy tính.

*HUB chủ động (HUB – Active):* Có các linh kiện điện tử có thể khuếch đại và xử lý tín hiệu. Cho phép khoảng cách giữa các thiết bị tăng lên.

*HUB thông minh (Intelligent Hub):* Là hub chủ động nhưng có thêm các chức năng mới sau:

+ Quản trị Hub: Được bổ sung các giao thức quản trị mạng, cho phép Hub gửi các thông tin về trạm điều khiển mạng trung tâm, cho phép trạm trung tâm quản lý Hub.

+ Chuyển mạch: Chứa các vi mạch cho phép chọn đường nhanh cho các tín hiệu giữa các cổng trên Hub. Thay vì chuyển gói tin cho toàn bộ các cổng của Hub, chúng đang thay thế dần cho các Bridge và Router.

### 3.3.5 Các bộ kết nối mạng

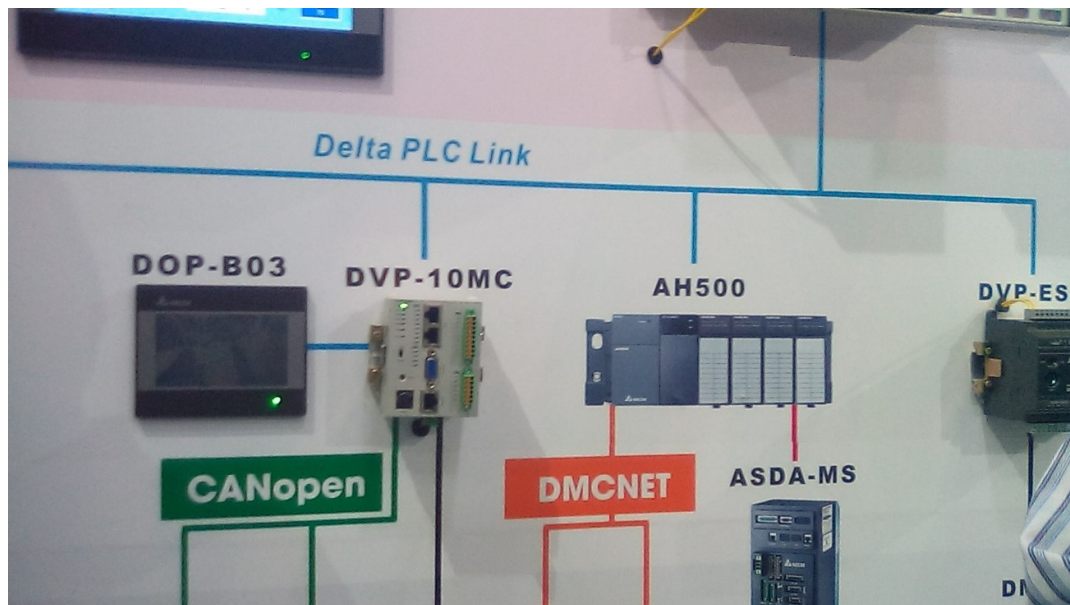
- *Repeater (Bộ chuyển tiếp)* Có chức năng tiếp nhận và chuyển tiếp các tín hiệu dữ liệu, thường được dùng nối hai đoạn cáp.

- *Bridge (Cầu)* Là một thiết bị mềm dẻo hơn Repeater. Một Repeater chuyển đi tất cả các tín hiệu mà nó nhận được. Nhưng Bridge có chọn lọc và chỉ chuyển đi các tín hiệu có đích ở phần mạng phía bên kia mạng Ethernet để mở rộng mạng. Có khả năng khuếch đại và tái sinh tín hiệu.

*Multiplexor (bộ dồn kênh)* Là thiết bị có chức năng tổ hợp một số tín hiệu để chúng có thể truyền được với nhau và sao cho khi nhận lại được tách ra trở lại các tín hiệu gốc.

*Modem (Modulation/Demodulation):* Là thiết bị có chức năng chuyển đổi tín hiệu thành tín hiệu tương tự và ngược lại, để kết nối các máy tính qua đường điện thoại. Cho phép trao đổi thư điện tử, truyền tệp, truyền fax và trao đổi dữ liệu theo yêu cầu.

*Router (Bộ chọn đường):* Là thiết bị thông minh hơn Bridge vì có còn thực hiện các giải thuật chọn đường đi tối ưu cho các gói tin. Bridge hoạt động ở hai tầng Physical và Datalink, trong khi Router có thể hoạt động lên tới tầng 3 (Network). Cho phép kết nối nhiều mạng với nhau tạo thành liên mạng.



Hình 3.18: Hình ảnh một số thiết bị trong mạng

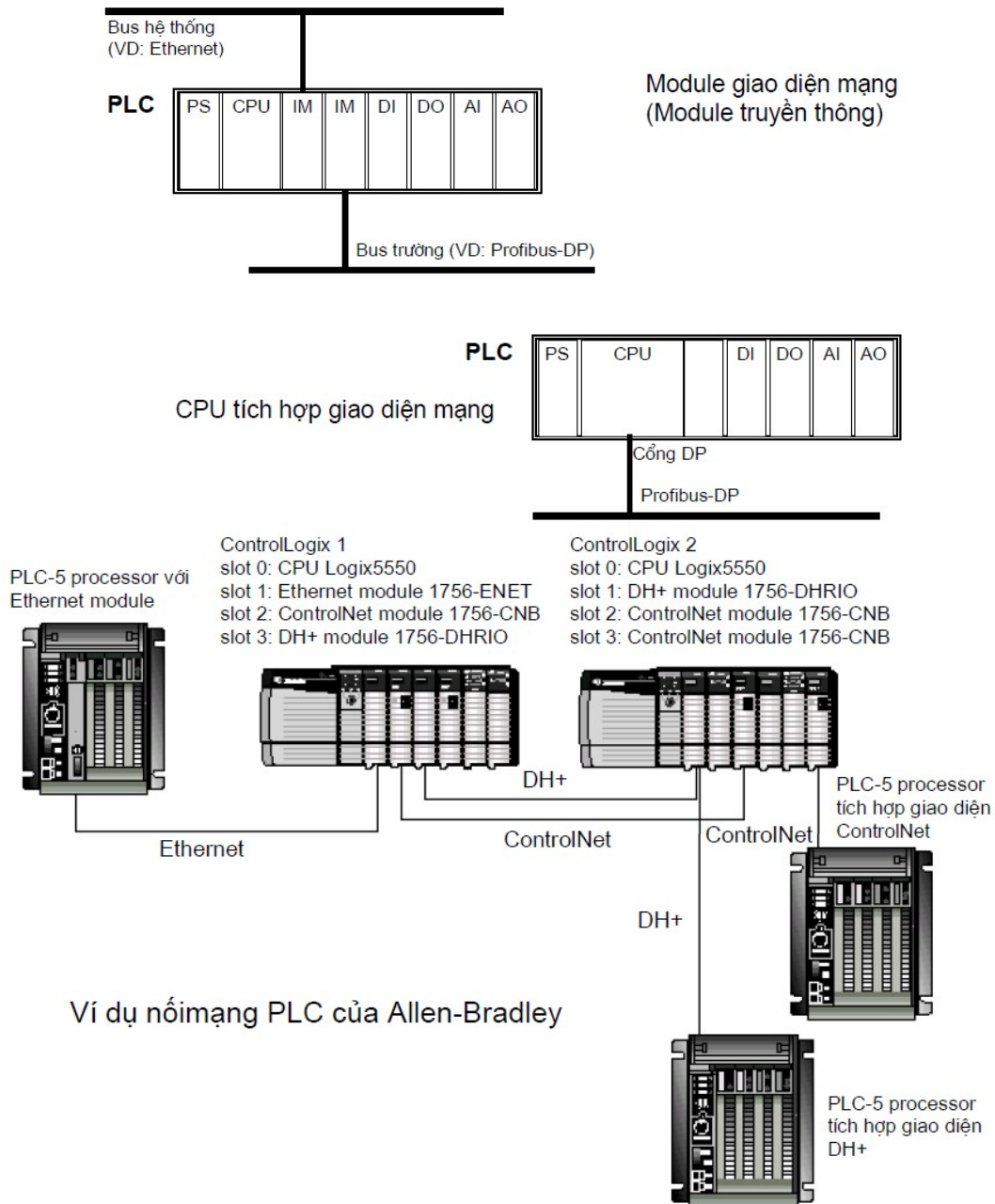
### 3.3.6 Gateway

Là thiết bị dùng nối ghép hai loại giao thức với nhau. Ví dụ: mạng của bạn sử dụng giao thức IP và mạng của ai đó sử dụng giao thức IPX, Novell, DECnet, SNA... hoặc một giao thức nào đó thì Gateway sẽ chuyển đổi từ loại giao thức này sang loại khác

## 3.4 Phần cứng giao diện mạng

### 3.4.1 Ghép nối thiết bị điều khiển

PLC (Programmable Logic Controller): Thiết bị điều khiển logic khả trình, cấu trúc module hoặc cấu trúc gọn [13], [22].



Hình 3.19: Ghép nối PLC [31]

DCS (Distributed Control System): Hệ thống điều khiển phân tán tích hợp dạng cấu trúc module;

Compact Digital Controller: Cấu trúc gọn, không lập trình được;

PC công nghiệp;

Ghép nối PLC (Programmable Logic Controller);

Ghép nối PC và PC công nghiệp;

PC công nghiệp cũng có thể có cấu trúc module (VD PC-104) vì vậy cách ghép nối tương tự như PLC;

Card giao diện mạng cho các khe cắm ISA, PCI, Compact-PCI;

Bo mạch chủ tích hợp giao diện mạng (ví dụ Ethernet, CAN);

Bộ thích ứng mạng qua các cổng nối tiếp (RS-232, USB);

Card PCMCIA.



Card Profibus (Siemens)  
CP 5412 (A2)

*Hình 3.20: Card PCMCIA*

#### 3.4.1.1 Ghép nối thiết bị trường

Thiết bị chấp hành:

- Biến tần (inverter)
- Bộ khởi động động cơ (motor starter)
- Van điều khiển (control valve)

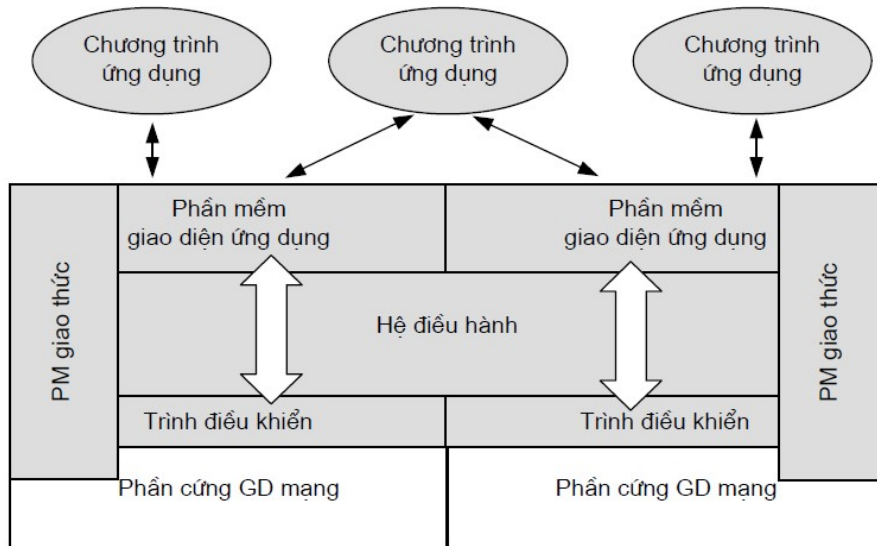
Thiết bị đo:

- Encoder
- Cân định lượng
- Thiết bị đo nhiệt độ (temperature transmitter)

- Thiết bị đo áp suất (pressure transmitter)

Thiết bị giao diện người - máy tại chỗ

### 3.5 Phần mềm trong hệ thống mạng



Hình 3.21: Sơ đồ phân mềm mạng công nghiệp

#### 3.5.1 Phần mềm (xử lý) giao thức

- Firmware:
  - Đổ cứng trong ROM hoặc “downloadable”
  - Nhanh hơn, hiệu suất cao
- Thành phần của hệ điều hành:
  - Tích hợp sẵn trong hệ điều hành (ví dụ cho PLC)
  - Có thể lựa chọn cài đặt (ví dụ các giao thức phổ thông như TCP/IP, NetBUI)

#### 3.5.2 Phần mềm thư viện:

- Thường dưới dạng mã nguồn hoặc mã đích C/C++
- Được liên kết với chương trình ứng dụng
- Tiện lợi cho xây dựng giải pháp nhúng

#### 3.5.3 Phần mềm giao diện lập trình (API)

Thư viện lập trình phổ thông (C, C++, VB)

- Sử dụng cho một loại card mạng nhất định
- Khác nhau lớn giữa nhiều thư viện
- Tiện lợi trên PC và các giải pháp nhúng

Thư viện hàm hoặc khối chức năng chuyên dụng:

- Giải pháp trong các hệ PLC hoặc DCS (ví dụ theo chuẩn IEC 61131-5)

- Không sử dụng được từ bên ngoài

Công nghệ đối tượng thành phần (component object technology), ví dụ COM, ActiveX, OPC

- Sử dụng khá thống nhất cho nhiều loại card mạng
- Hầu như chỉ hỗ trợ trên nền Windows

### **3.6 Câu hỏi ôn tập chương**

*Câu 3.1: Vai trò của truyền dẫn trong hệ thống mạng?*

*Câu 3.2: Trong giao thức mạng cái nào quan trọng nhất, vì sao?*

*Câu 3.3: Yêu cầu cơ bản cho một hệ thống mạng công nghiệp được ứng dụng (bao gồm các bài học trước)?*

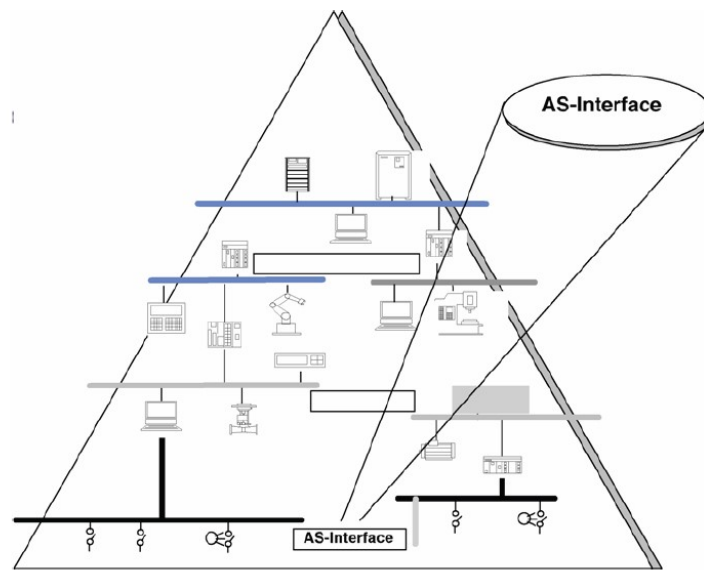
## CHƯƠNG 4: CÁC MẠNG THÔNG DỤNG

### 4.1 Mạng trường – AS Interface

#### 4.1.1 Giới thiệu chung

AS Interface là kết quả phát triển hợp tác của 11 hãng sản xuất các thiết bị cảm biến và cơ cấu chấp hành của châu Âu (Siemens, Schneider Electric, Moeller, Festo, Bürkert, Pepperl & Fuchs...). Chuyên dùng cho ghép nối bộ điều khiển trực tiếp với các thiết bị logic (rơ-le đóng cắt, van on/off, cảm biến chuyển mạch) bằng một đường cáp duy nhất [30], [41].

Chuẩn EN 50295, IEC 62026-2. Hiệp hội ASI - International Association hỗ trợ phát triển và ứng dụng



Hình 4.1: Mô hình mạng ASI International

Yêu cầu & đặc điểm chung:

- Yêu cầu lưu lượng dữ liệu thấp, tính thời gian thực ngặt nghèo
- Đơn giản, tiện dụng, giá cả hợp lý
- Khả năng đồng tải nguồn cho toàn bộ các cảm biến và một phần lớn các cơ cấu chấp hành.
- Bền vững trong môi trường công nghiệp nhưng không đòi hỏi cao về chất lượng đường truyền
- Cấu trúc mạng tương đối linh hoạt: đường thẳng, cây, hình sao
- Thực tế của phương pháp nối dây truyền thông: 36% mọi sự cố nhà máy, máy móc là do lỗi lắp đặt, đi dây (số liệu 1997, TU München) ASI giúp tiết kiệm tới 25% chi phí cáp truyền và 30% chi phí tổng thể

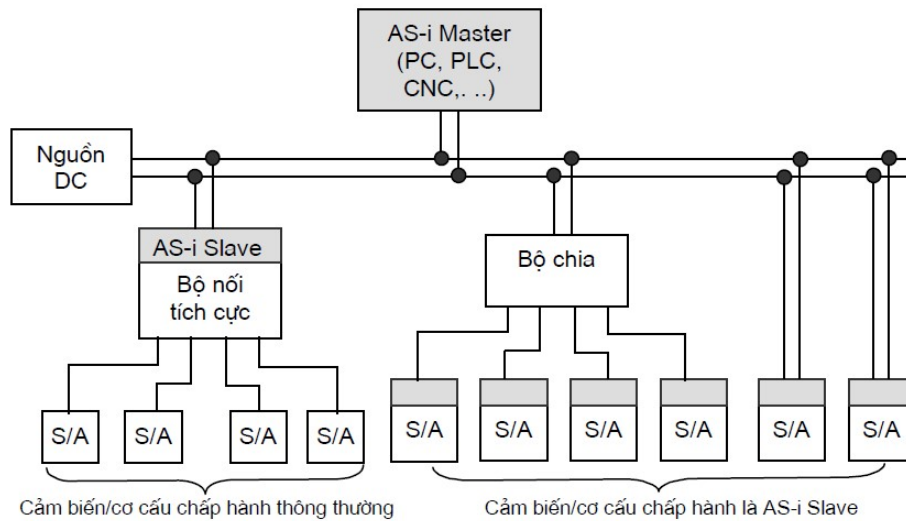


### 4.1.2 Kiến trúc giao thức

Đặc điểm hạn chế ở việc trao đổi dữ liệu thuần túy và lượng dữ liệu trao đổi rất nhỏ. Toàn bộ việc xử lý giao thức được gói gọn chỉ trong lớp 1 (lớp vật lý) theo mô hình OSI. Phương pháp mã hóa bit hoàn toàn mới để thích hợp với đường truyền 2 dây đồng tải nguồn và không dựa vào chuẩn truyền dẫn RS-485 thông dụng ở các hệ thống bus khác.

### 4.1.3 Cấu trúc mạng & cáp truyền

- Cấu trúc đường thẳng, cây, hình sao
- Không yêu cầu trở đầu cuối
- Chiều dài tổng cộng của cáp truyền cho phép tối đa là 100 mét.
- Số trạm tối đa trong một mạng là 31, tương ứng với tối đa 124 thiết bị (mỗi trạm có thể ghép nối được tối đa 4 thiết bị).
- Version 2: Tối đa 64 trạm/mạng [16]
- Tốc độ truyền 167 kbit/s, tương đương với thời gian bit là 6  $\mu$ s.



Hình 4.2: Sơ đồ mạng AS-Interface

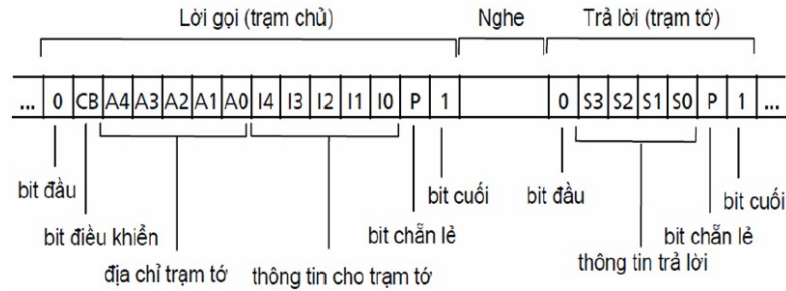
### 4.1.4 Cơ chế giao tiếp

Cơ chế giao tiếp của mạng AS-interface là chủ/tớ, phương pháp hỏi đáp tuần tự (polling), tuần hoàn. Chủ yếu là dữ liệu logic (tối đa 4 bit dữ liệu vào/ra trong một bức điện). Thời gian một chu kỳ bus tối đa được đảm bảo không lớn hơn 5 ms (với 31 trạm tớ), Version 2.0: Cho phép truyền dữ liệu tương tự (7 chu kỳ bus x 5 = 35 giây). Trạm chủ cũng có thể gửi kèm các thông báo khác mà không gây ảnh hưởng đáng kể tới thời gian chu kỳ bus [17], [45].



#### 4.1.5 Cấu trúc bức điện

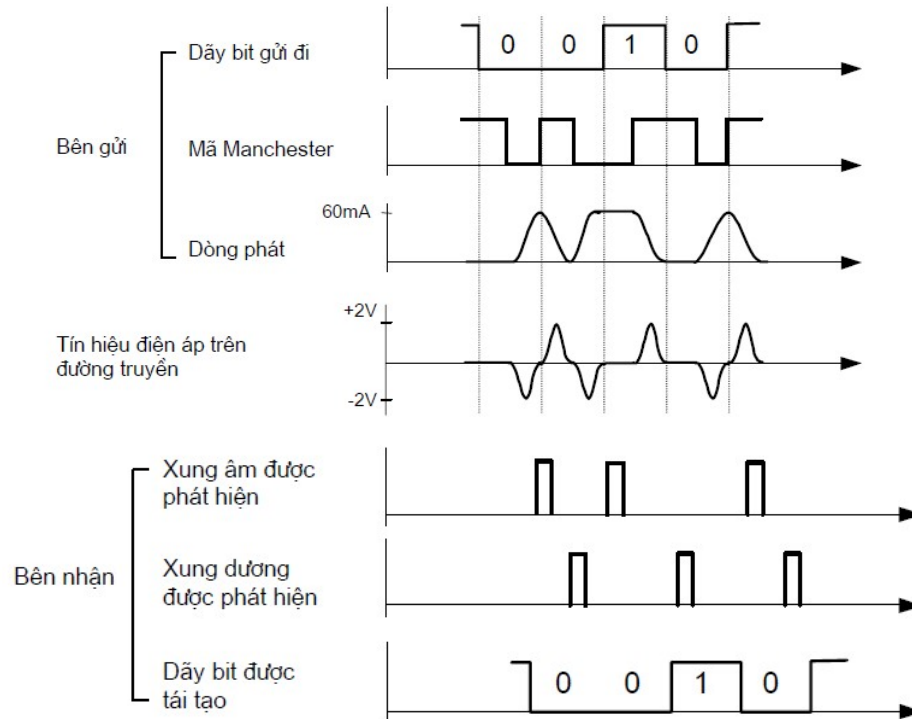
Các bước thực hiện: Đặt tham số, đặt địa chỉ, reset trạm tớ, xóa địa chỉ mặc định, đọc cấu hình vào ra, đọc mã căn cước, đọc trạng thái, xóa trạng thái [5].



Hình 4.3: Cấu trúc bức điện trong mạng AS-Interface

#### 4.1.6 Mã hóa bit

□ APM (*Alternate Pulse Modulation*): kết hợp giữa AFP và mã Manchester



Hình 4.4: Sơ đồ mã hóa bit mạng AS-Interface

#### 4.1.7 Bảo toàn dữ liệu

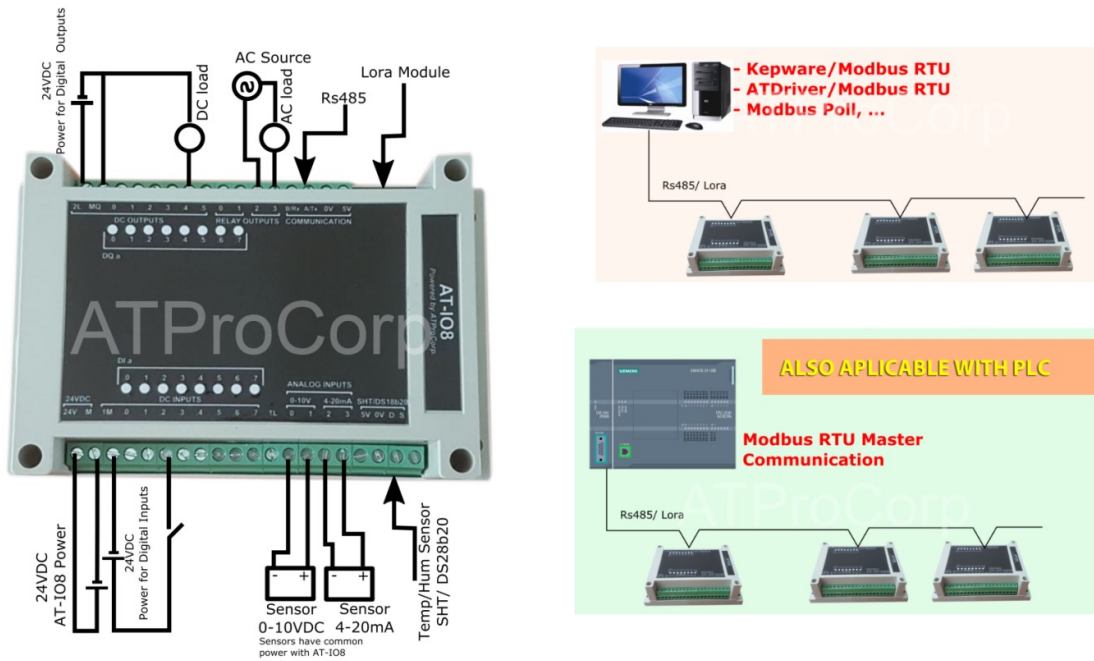
Lớp 1 chịu trách nhiệm hoàn toàn trong việc kiểm tra lỗi, dựa vào bit chẵn/lẻ kết hợp với phương pháp mã hóa bit hợp lý. Trong một chu kỳ bit (6  $\mu$ s) tín hiệu trên đường truyền được bộ thu lấy mẫu 16 lần vì vậy Nhận biết dạng tín hiệu theo mã APM.

Mỗi bức điện đều có chiều dài cố định, có bit đầu, bit cuối, ngăn cách bằng một thời gian nghỉ, kiểm tra bằng một bit chẵn lẻ.

### 4.1.8 Ứng dụng

AT-IO8 là một mô-đun IO mở rộng thoải mái. Nó phù hợp cho các ứng dụng SCADA. AT-IO8 được sử dụng để thu thập đầu vào số, đầu vào tương tự, tín hiệu nhiệt độ, độ ẩm hoặc để điều khiển đầu ra số mà không cần lập trình.

AT-IO8 kết nối trực tiếp với PC chạy phần mềm SCADA hoặc PLC bằng giao thức modbus RTU trên mạng RS485 hoặc mạng Lora không dây tầm xa (tùy chọn).



Hình 4.5: Ứng dụng kết nối của AT/IO8 [32]

## 4.2 Mạng Profibus

### 4.2.1 Giới thiệu chung

PROFIBUS (*Process Field Bus*) được phát triển tại Đức từ năm 1987, ban đầu là các chuẩn DIN 19245, EN 50 170 ngày nay là IEC 61158, IEC 61784. PROFIBUS không chỉ dừng lại là một hệ thống truyền thông, mà còn được coi là một công nghệ tự động hóa.

Một hệ thống bus trường hàng đầu hiện nay, cũng được sử dụng rất rộng rãi tại Việt Nam hỗ trợ bởi Profibus Nutzerorganisation (PNO), từ năm 1995 nằm trong Profibus International (PI) với hơn 1.100 thành viên trên toàn thế giới [22], [40].

Ba loại giao thức:

- Profibus -FMS (Fieldbus Message Specification)
- Profibus -DP (Decentral Peripheral)
- Profibus -PA

Bảng 4.1: Bảng so sánh giữa ba dạng của mạng profibus [46]

Đặc điểm	Profibus - FMS	Profibus - DP	Profibus - PA
Application	Cell level	Field level	Field level
Standard	EN 50 170	EN 50 170	IEC 1158-2
Connectable devices	PLC, PG/PC, field devices	PLC, PG/PC, binary and analog field devices, drives valves, OPs	Field devices for areas subject to explosion hazards
Resp. times	< 60ms	1 – 5 ms	<60ms
Network size	<= 100 km	<=100 km	Max 1.9km
Transmission rates	9.6 kbit/s – 12Mbit/s	9.6 kbit/s – 12Mbit/s	31.25 kbit/s

#### 4.2.2 Kiến trúc giao thức

Kiến trúc của profibus cũng như kiến trúc chung có 7 lớp. Các lớp dịch vụ và giao thức, lớp ứng dụng của FMS bao gồm hai lớp con, lớp liên kết dữ liệu FDL (*Fieldbus Data Link*), lớp vật lý. Cấu trúc các lớp xem trên hình 4.6

	PROFIBUS-FMS	PROFIBUS-DP	PROFIBUS-PA
Giao diện sử dụng	FMS-Profiles	DP-Profiles	PA-Profiles
		Các chức năng DP mở rộng	
		Các chức năng DP cơ sở	
Lớp 7	Fieldbus Message Specification (FMS)		
Lớp 3-6	K h ô n g t h ể h i ệ n		
Lớp 2	Fieldbus Data Link (FDL)		
Lớp 1	RS-485/RS-485IS/Cáp quang		MBP (IEC 1158-2)

Hình 4.6: Kiến trúc của mạng Profibus [1]

#### 4.2.3 Kỹ thuật truyền dẫn (lớp 1)

Sử dụng chuẩn truyền dẫn với RS-485, tốc độ truyền thông từ 9,6 kbit/s đến 12 MBit/s. Nếu sử dụng cấu trúc đường thẳng kiểu đường trục/đường nhánh (*trunk-line/drop-line*) hoặc *daisy-chain* thì tốc độ truyền từ 1,5 Mbit/s trở lên yêu cầu cấu trúc *daisy-chain*.

Cáp truyền được sử dụng là đôi dây xoắn có bảo vệ (STP). Hiệp hội PI khuyến cáo dùng cáp loại A. Trở kết thúc có dạng tin cậy (*fail-safe biasing*) với các điện trở lần lượt là  $390\Omega$ - $220\Omega$  -  $390\Omega$ . Chiều dài tối đa của một đoạn mạng từ 100 đến 1200m, phụ thuộc vào tốc độ truyền được lựa chọn. Quan hệ giữa tốc độ truyền và chiều dài tối đa của một đoạn mạng được tóm tắt trong bảng 4.2. Số lượng tối đa các trạm trong mỗi đoạn mạng là 32. Có thể dùng tối đa 9 bộ lặp tức 10 đoạn mạng. Tổng số trạm tối

đa trong một mạng là 126. Chế độ truyền tải không đồng bộ và hai chiều không đồng thời. Phương pháp mã hóa bit NRZ.

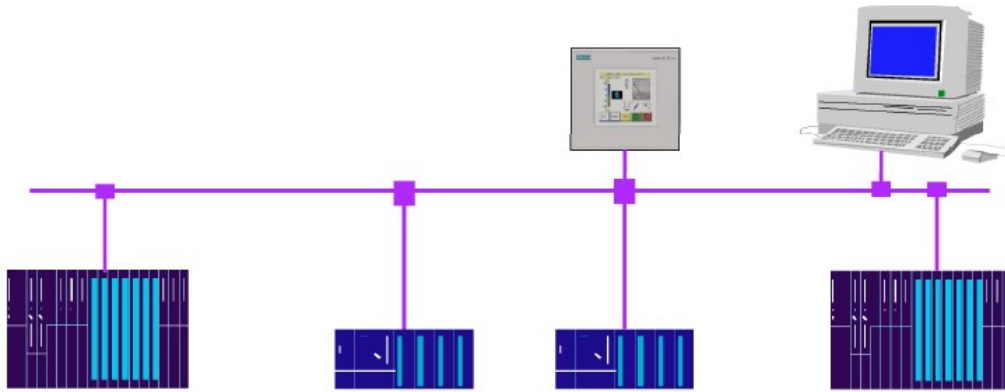
Bảng 4.2: Khoảng cách truyền và tốc độ truyền:

Tốc độ kbit/s	9.6/19.2/45.45/93.75	187.5	500	1500	3000/6000/12000
Chiều dài m	1200	1000	400	200	100

Ngoài ra mạng còn truyền dẫn với RS-485IS (*IS : Intrinsically Safe*) dùng phát triển để có thể phù hợp với môi trường đòi hỏi an toàn cháy nổ.

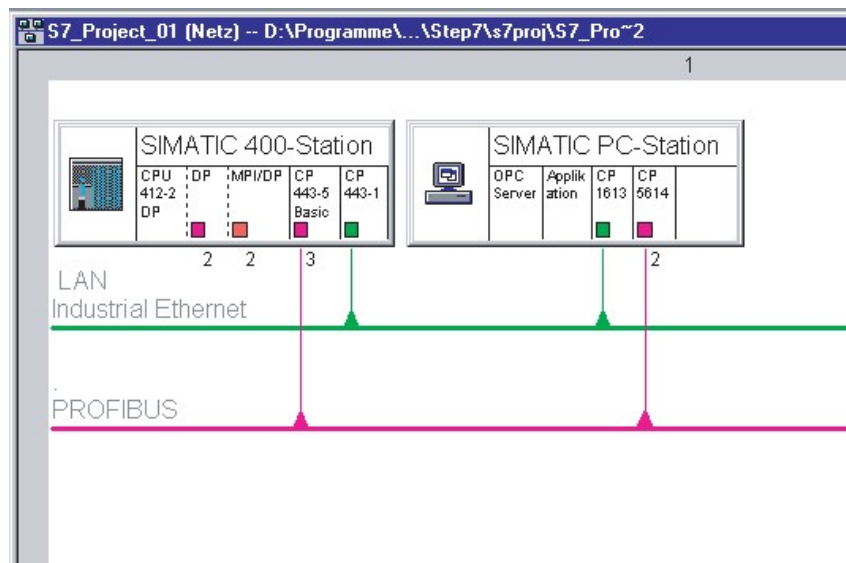
Truyền dẫn với cáp quang: thích hợp đặc biệt trong các lĩnh vực có môi trường làm việc nhiều mạnh hoặc đòi hỏi phạm vi phủ mạng lớn.

Cấu hình FMS tiêu biểu



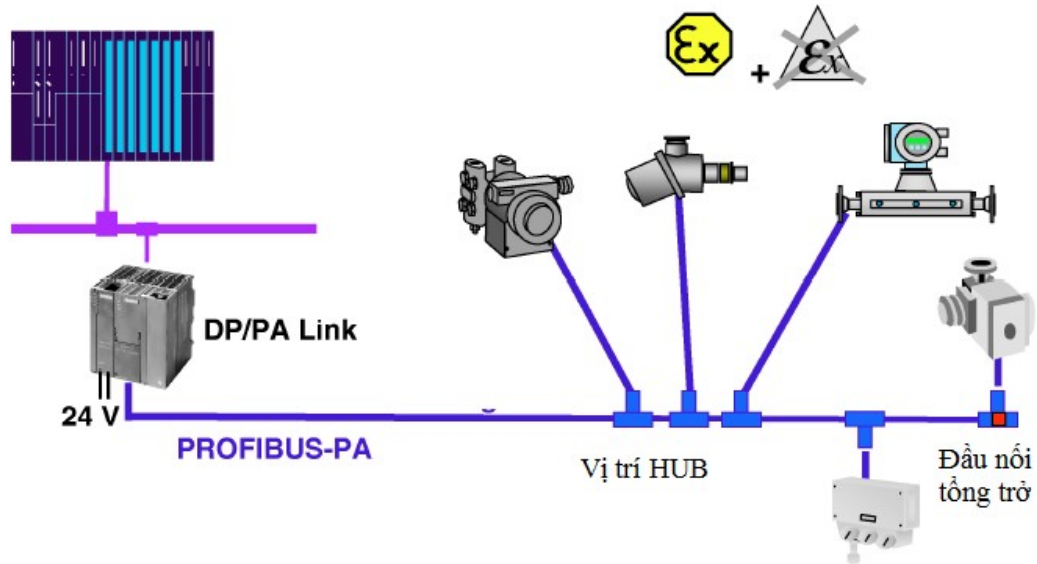
Hình 4.7: Mô hình mạng Profibus FMS

Cấu hình DP tiêu biểu



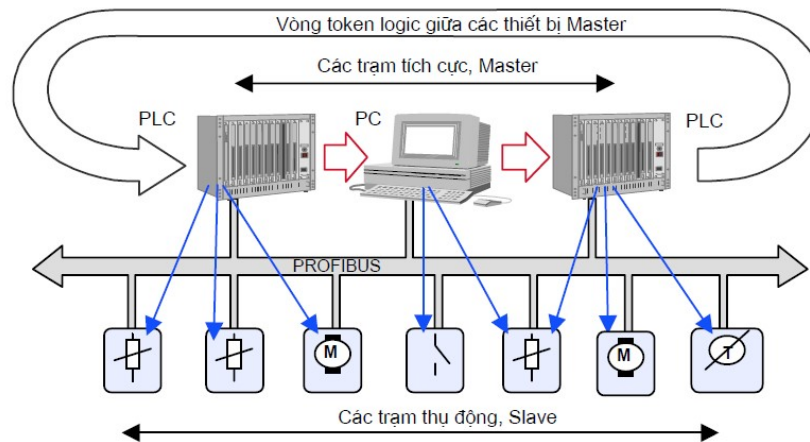
Hình 4.8: Mô hình mạng Profibus DP

### Cấu hình PA tiêu biểu



Hình 4.9: Mô hình mạng Profibus PA[43]

#### 4.2.4 Truy nhập bus (lớp 2)



Hình 4.10: Mô hình truy nhập bus [43]

#### 4.2.5 Dịch vụ truyền dữ liệu (lớp 2)

- Dịch vụ không tuần hoàn [40], [45]:

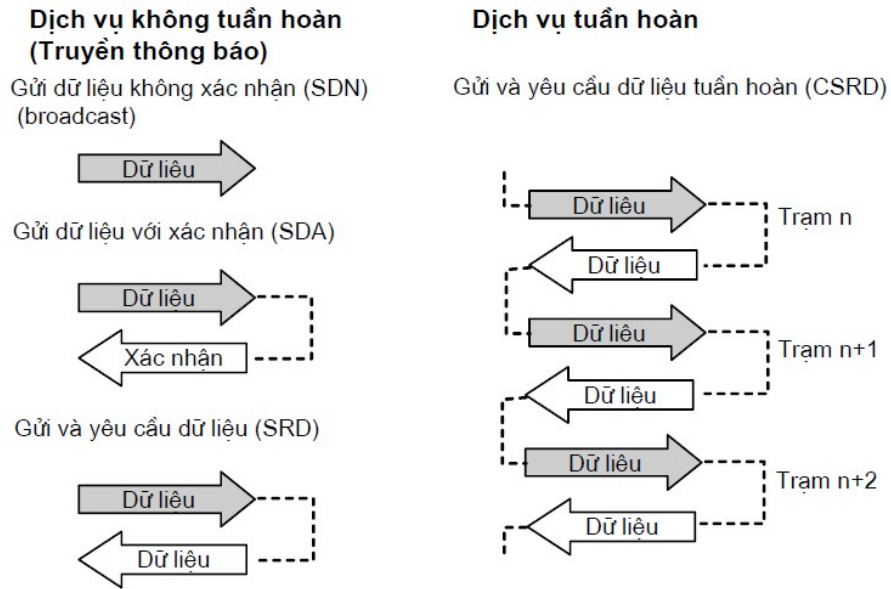
+ SDN (*Send Data with No Acknowledge*): Gửi dữ liệu không xác nhận

+ SDA (*Send Data with Acknowledge*): Gửi dữ liệu với xác nhận

+ SRD (*Send and Request Data with Reply*): Gửi và yêu cầu dữ liệu

- Dịch vụ tuần hoàn:

CSRD (*Cyclic Send and Request Data with Reply*): Gửi và yêu cầu dữ liệu tuần hoàn.



Hình 4.11: Sơ đồ dịch vụ truyền dữ liệu

#### 4.2.6 Cấu trúc bức điện (lớp 2)

Khung với chiều dài thông tin cố định, không mang dữ liệu:

SD1	DA	SA	FC	FCS	ED
-----	----	----	----	-----	----

Khung với chiều dài thông tin cố định, mang 8 byte dữ liệu:

SD3	DA	SA	FC	DU	FCS	ED
-----	----	----	----	----	-----	----

Khung với chiều dài thông tin khác nhau, 1-246 byte dữ liệu:

SD2	LE	LEr	SD2	DA	SA	FC	DU	FCS	ED
-----	----	-----	-----	----	----	----	----	-----	----

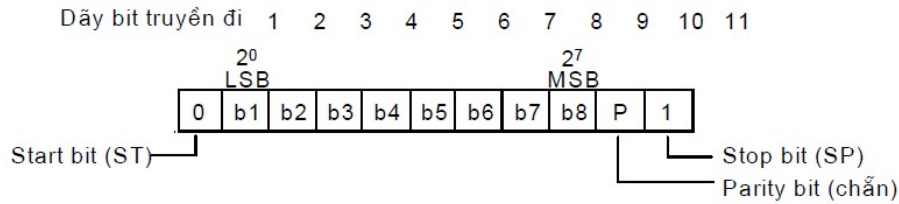
Token:

SD4	DA	SA
-----	----	----

Ký hiệu	Tên đầy đủ	Ý nghĩa
SD1... SD4	Start Delimiter	Byte khởi đầu, phân biệt giữa các loại khung SD1 = 10H, SD2=68H, SD3 = A2H, SD4=DCH
LE	Length	Chiều dài thông tin (4-249 byte)
LEr	Length repeated	Chiều dài thông tin nhắc lại vì lý do an toàn
DA	Destination Address	Địa chỉ đích (trạm nhận), từ 0-127
SA	Source Address	Địa chỉ nguồn (trạm gửi), từ 0-126
DU	Data Unit	Khối dữ liệu sử dụng
FC	Frame Control	Byte điều khiển khung
FCS	Frame Check Sequence	Byte kiểm soát lỗi, HD = 4
ED	End Delimiter	Byte kết thúc, ED = 16H



## Khung UART (FMS,DP)



### 4.3 Interbus

#### 4.3.1 Giới thiệu chung

Interbus là một phát triển riêng của hãng Phoenix Contact. Chuẩn hóa quốc tế IEC 61158-2, khả năng kết nối nhiều loại thiết bị khác nhau được sử dụng xuyên suốt trong hệ thống (bus trường, bus điều khiển, bus chấp hành-cảm biến) [45], [47]. Ứng dụng chủ yếu trong ngành công nghiệp chế tạo, lắp ráp và sản xuất vật liệu xây dựng. Số lượng thiết bị ghép nối: số 1 trên thế giới. Được sử dụng trong nhiều nhà máy gạch, sứ, thủy tinh ở Việt Nam.

#### 4.3.2 Kiến trúc giao thức

Ba lớp theo mô hình OSI:

- Lớp vật lý qui định phương pháp mã hóa bit, kỹ thuật truyền dẫn tín hiệu và giao diện giữa một thiết bị mạng với môi trường truyền,...
- Lớp liên kết dữ liệu có vai trò đảm bảo việc truyền dữ liệu tin cậy, chính xác, hỗ trợ cả dữ liệu quá trình (tuần hoàn) và các dữ liệu tham số (không tuần hoàn).
- Lớp ứng dụng: PMS (*Peripheral Message Specification*) là một tập con của MMS, về cơ bản tương thích với các dịch vụ của Profibus-FMS.

Hỗ trợ tối đa việc trao đổi dữ liệu giữa một bộ điều khiển trung tâm với các vào/ra phân tán, các thiết bị cảm biến và cơ cấu chấp hành.

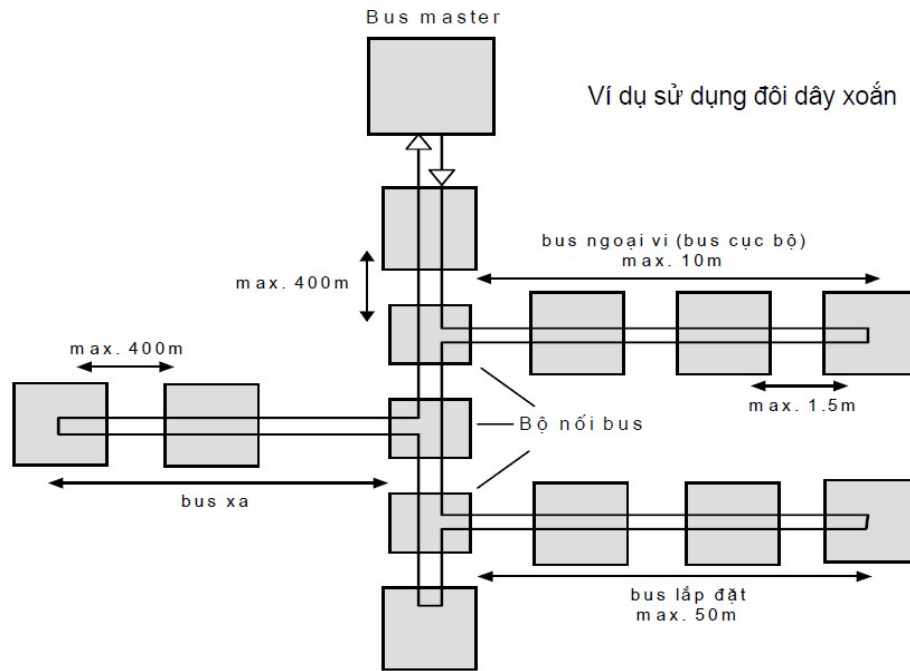
#### 4.3.3 Cấu trúc mạng

Nổi tiếng với cấu trúc mạch vòng tích cực

Có thể sử dụng mạch vòng phân cấp

Phương pháp truy nhập bus kết hợp giữa Master/Slave và TDMA

Ưu điểm: Phạm vi phủ mạng rất lớn, dễ dàng sử dụng cáp quang, được thiết kế để dễ lắp đặt, dễ chẩn đoán, truyền hai chiều đồng thời, định địa chỉ tự động dựa theo vị trí vật lý của một trạm trên mạch vòng. Việc bảo dưỡng, sửa chữa, mở rộng hệ thống đơn giản hơn.



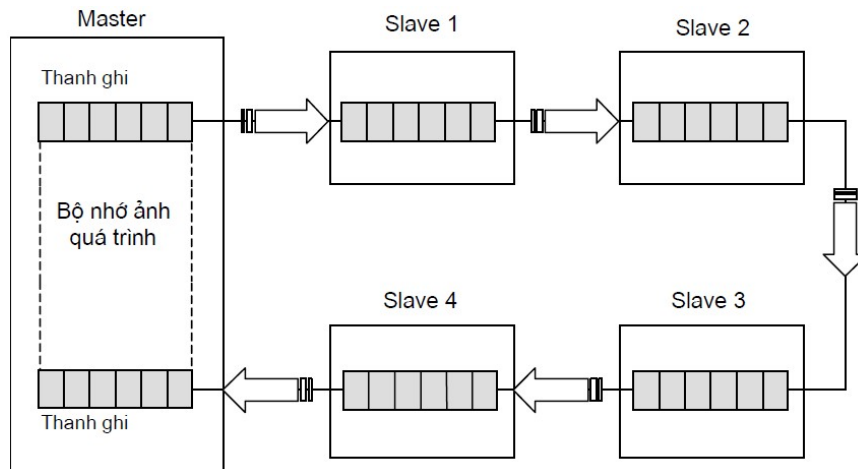
Hình 4.12: Sơ đồ cấu trúc mạng sử dụng dây đôi xoắn

#### 4.3.4 Kỹ thuật truyền dẫn

Cho phép sử dụng nhiều loại đường truyền khác nhau, ví dụ cáp đôi dây xoắn, cáp quang, hồng ngoại, v.v... Đôi dây xoắn + RS-485 được sử dụng rộng rãi nhất (5 dây giữa hai thiết bị). Tốc độ truyền là 500 kbit/s vì vậy khoảng cách tối đa giữa hai thiết bị là 400 m. Chiều dài tổng cộng max. 13 km. Tổng số trạm max. 256. Mã hóa bit NRZ, Interbus-Loop sử dụng mã Manchester cho môi trường dễ cháy nổ.

#### 4.3.5 Cơ chế giao tiếp

□ Truy nhập bus: Chủ/tớ kết hợp TDMA, theo kiểu xe đẩy xoay vòng (bức điện tổng) vì vậy rất hiệu quả. Tính năng thời gian thực rất tốt, chu kỳ bus: Đảm bảo vài ms, có cơ chế đồng bộ hóa dữ liệu.



Hình 4.13: Giao tiếp theo cơ chế đồng bộ hóa dữ liệu

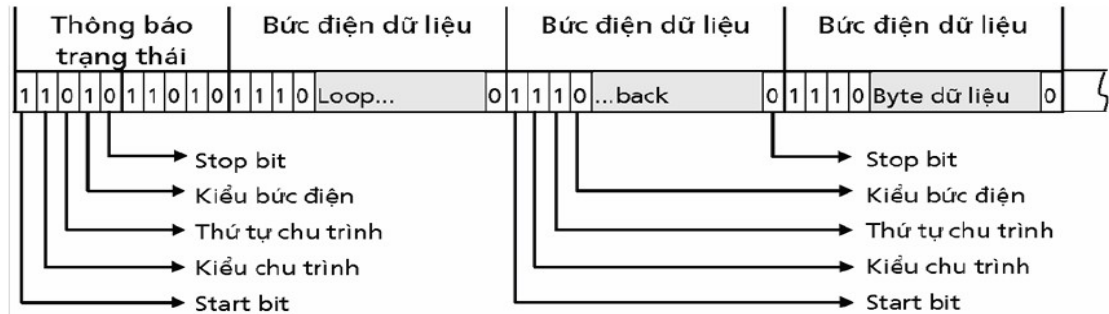


### 4.3.6 Cấu trúc bức điện

#### □ Lớp 2

Loopback	Dữ liệu sử dụng	CRC	CNTR
2 Byte	0-512 Byte	2 Byte	2 Byte

#### □ Lớp 1



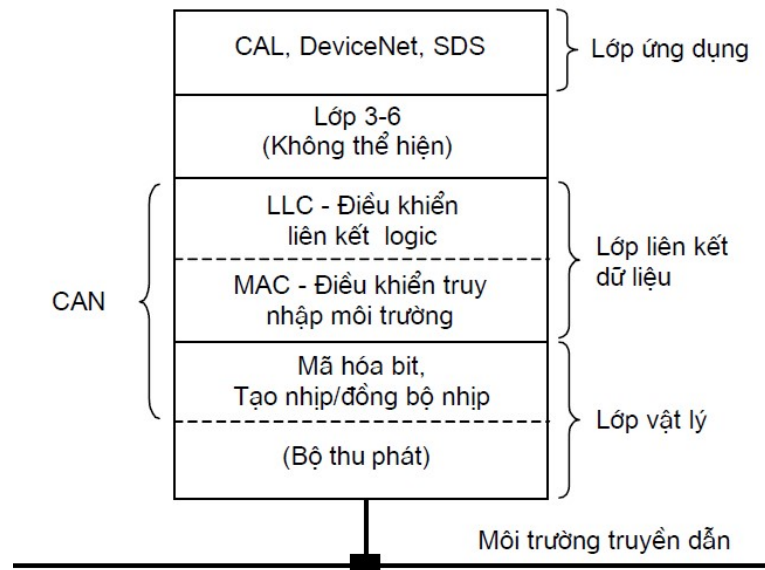
## 4.4 Mạng CAN

### 4.4.1 Giới thiệu chung

CAN (*Controller Area Network*) xuất phát là một phát triển chung của hai hãng Bosch và Intel. Lúc đầu được sử dụng trong công nghiệp ô tô, công nghệ này cũng đã thâm nhập được vào một số lĩnh vực tự động hóa quá trình công nghiệp. Chuẩn hóa quốc tế trong ISO 11898 [48].

### 4.4.2 Kiến trúc giao thức

- Phần chính của lớp vật lý:
  - + truyền tín hiệu, phương thức định thời, tạo nhịp bit (*bit timing*), phương pháp mã hóa bit và đồng bộ hóa.
  - + không qui định các đặc tính của các bộ thu phát, với mục đích cho phép lựa chọn môi trường truyền cũng như mức tín hiệu thích hợp cho từng lĩnh vực ứng dụng.
- Lớp liên kết dữ liệu:
  - + Lớp điều khiển truy nhập môi trường (MAC) là phần cốt lõi trong kiến trúc giao thức CAN. Lớp MAC có trách nhiệm tạo khung thông báo, điều khiển truy nhập môi trường, xác nhận thông báo và kiểm soát lỗi.
  - + Lớp điều khiển liên kết logic (LLC) đề cập tới các dịch vụ gửi dữ liệu và yêu cầu dữ liệu từ xa, thanh lọc thông báo, báo cáo tình trạng quá tải và hồi phục trạng thái



Hình 4.14: Sơ đồ kiến trúc liên kết của cấu trúc dữ liệu

#### 4.4.3 Cấu trúc mạng & KT truyền dẫn

CAN không qui định cụ thể về chuẩn truyền dẫn cũng như môi trường truyền thông. Cấp đôi dây xoắn kết hợp với chuẩn RS-485 được sử dụng rộng rãi nhất (cấu trúc mạng thích hợp nhất là đường trục/đường nhánh, chiều dài đường nhánh <0.3m). Phương pháp truy nhập bus CSMA/CA, tốc độ truyền tối đa là 1Mbit/s ở khoảng cách 40m và 50kbit/s ở khoảng cách 1000m.

Hai trạng thái logic của tín hiệu là mức trội (*dominant*) và mức lặn (*recessive*). Nhồi bit (bit 0 sau 5 bit 1) + NRZ

#### 4.4.4 Cơ chế giao tiếp

Truy nhập bus: CSMA/CA, đặc trưng của CAN là phương pháp định địa chỉ và giao tiếp hướng đối tượng. Tự do, linh hoạt theo kiểu yêu cầu - đáp ứng. Một trạm gửi dữ liệu bằng khung Remote Frame. Trạm có khả năng cung cấp nội dung thông tin đó sẽ gửi trả lại một khung dữ liệu Data Frame có cùng mã căn cước với khung yêu cầu.

#### 4.4.5 Cấu trúc bức điện

Mỗi thông báo được coi là một đối tượng, có một căn cước riêng biệt (Identifier, 11/29 bit)

Có 4 kiểu bức điện:

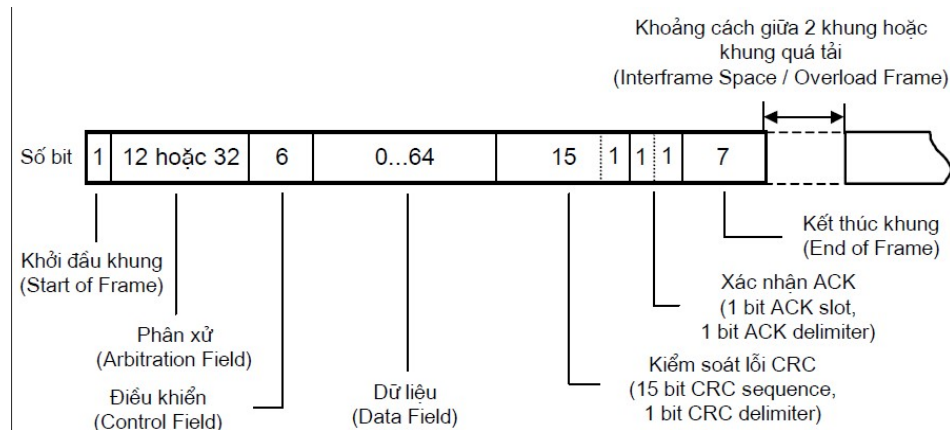
Khung dữ liệu (Data Frame) mang dữ liệu từ một trạm gửi tới các trạm nhận.

Khung yêu cầu dữ liệu (Remote Frame) được gửi từ một trạm yêu cầu truyền khung dữ liệu.

Khung lỗi (Error Frame) được gửi từ bất kỳ trạm nào phát hiện lỗi bus.

Khung quá tải (Overload Frame) tạo một khoảng cách thời gian bổ sung giữa hai khung dữ liệu hoặc yêu cầu dữ liệu trong trường hợp một trạm bị quá tải.

Giữa hai khung ít nhất 3 bit lặn (Interspace), khung dữ liệu/yêu cầu dữ liệu



Hình 4.15: Sơ đồ cấu trúc bức điện

#### 4.4.6 Bảo toàn dữ liệu

Theo dõi mức tín hiệu của mỗi bit truyền đi và so sánh với tín hiệu nhận được trên bus. Kiểm soát qua mã CRC, thực hiện nhồi bit (nhồi một bit nghịch đảo sau năm bit giống nhau). Kiểm soát khung thông báo.

- Khả năng phát hiện lỗi;
- Phát hiện được tất cả các lỗi toàn cục;
- Phát hiện được tất cả các lỗi cục bộ tại bộ phát;
- Phát hiện được tới 5 bit lỗi phân bố ngẫu nhiên trong một bức điện;
- Phát hiện được các lỗi đột ngột có chiều dài nhỏ hơn 15 bit trong một thông báo;
- Phát hiện được các lỗi có số bit lỗi là chẵn;
- Tỷ lệ lỗi còn lại (xác suất một thông báo còn bị lỗi không phát hiện) nhỏ hơn  $4.7 \cdot 10^{-11}$ .

## 4.5 Mạng Ethernet

### 4.5.1 Giới thiệu chung

Kỹ thuật cũ - Classful IP Addressing: Giá trị đầu tiên xác định phần địa chỉ mạng và phần địa chỉ trạm. Được sử dụng với những giao thức định tuyến theo lớp, ví dụ như RIPv1. Cấu trúc bảng định tuyến của Cisco cũng có cấu trúc theo kiểu phân lớp [5].

Kỹ thuật mới - Classless IP Addressing: Mật nạ mạng con xác định phần địa chỉ mạng và địa chỉ trạm. Giá trị đầu tiên không có ý nghĩa quyết định (như là trong

Classful IP addressing) Định tuyến liên vùng không phân lớp - Classless Inter-Domain Routing (CIDR). Địa chỉ IP không phân lớp được sử dụng trên Internet và trong phần lớn các mạng nội bộ. **CP/IP:** Transmission Control Protocol / Internet Protocol [12], [28], [47].

□ TCP (Transmission Control Protocol): Chuyên việc nối các hosts lại và bảo đảm việc giao hàng... nó vừa dùng sự xác nhận hàng đến (Acknowledgement) giống như thư bảo đảm, vừa kiểm xem kiện hàng có bị hư hại không.

Địa chỉ lớp A, B được mô tả trong bảng 4.3.

*Bảng 4.3: Bảng dưới đây tóm tắt sơ lược những cấp quản lý*

Address Class	First Octet Range	Number of Possible Networks	Number of Hosts per Network
Class A	0 to 127	128 (2 are reserved)	16,777,214
Class B	128 to 191	16,348	65,534
Class C	192 to 223	2,097,152	254

#### *Địa chỉ lớp D*

Một địa chỉ lớp D bắt đầu với các bits 1110 trong byte đầu tiên. Giá trị byte đầu tiên nằm trong khoảng từ 224 đến 239. Địa chỉ lớp D được sử dụng để đại diện cho một nhóm các trạm được gọi là một nhóm.

#### *Địa chỉ lớp E*

Byte đầu tiên của địa chỉ IP bắt đầu với các bits 1111. Các địa chỉ lớp E được dành riêng cho mục đích thí nghiệm và không nên dùng đánh địa chỉ cho các trạm hay các nhóm.

1. 192.168.1.3    Class C    Default Mask: 255.255.255.0

Network: 192.168.1.0    Broadcast: 192.168.1.255

Hosts: 192.168.1.1    through    192.168.1.254

2. 1.12.100.31    Class A    Default Mask: 255.0.0.0

Network: 1.0.0.0    Broadcast: 1.255.255.255

Hosts: 1.0.0.1    through    1.255.255.254

3. 172.30.77.5    Class B    Default Mask: 255.255.0.0

Network: 172.30.0.0    Broadcast: 172.30.255.255

Hosts: 172.30.0.1.    through    172.30.255.254

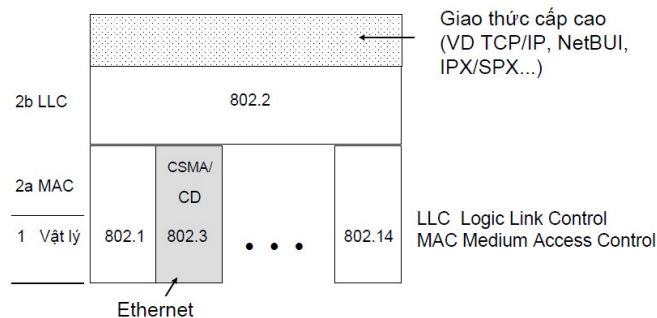
Chuyển các địa chỉ và mặt nạ mạng dưới đây về dạng nhị phân

192.168.1.0 → 11000000.10101000.00000001.00000000  
 255.255.255.0 → 11111111.11111111.11111111.00000000  
 192.168.1.255 → 11000000.10101000.00000001.11111111  
 192.168.0.0 → 11000000.10101000.00000000.00000000  
 255.255.0.0 → 11111111.11111111.00000000.00000000  
 192.168.255.255 → 11000000.10101000.11111111.11111111  
 192.168.0.0 → 11000000.10101000.00000000.00000000  
 255.255.255.0 → 11111111.11111111.11111111.00000000  
 192.168.0.255 → 11000000.10101000.00000000.11111111

Ethernet là kiểu mạng cục bộ (LAN) lần đầu tiên do hãng Xerox phát triển, được sử dụng rộng rãi nhất hiện nay. Ethernet chỉ là mạng cấp dưới (lớp vật lý và một phần lớp liên kết dữ liệu chuẩn hóa IEEE 802.3 [5].

Các phiên bản sau: Fast Ethernet (IEEE 802.3u), Wireless Ethernet (IEEE 802.11), Gigabit Ethernet,.. Các dạng mở rộng, sử dụng trong công nghiệp: High-Speed Ethernet, Ethernet/IP, Industrial Ethernet...

#### 4.5.2 Kiến trúc giao thức



Hình 4.16: Kiến trúc giao thức mạng Ethernet

#### 4.5.3 Cấu trúc mạng và Kỹ thuật truyền dẫn

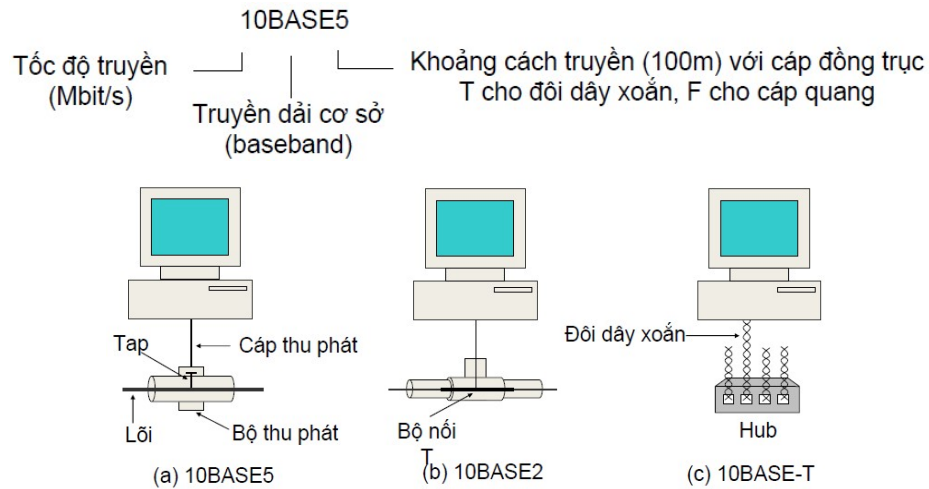
Logic: Cấu trúc bus

Vật lý: Đường thẳng hoặc hình sao

Mã hóa Manchester, truyền chênh lệch đối xứng ( $\pm 0,85V$ )

Phương tiện truyền dẫn:

- Cáp đồng trục: 10BASE2 (cáp mỏng), 10BASE5 (cáp dày)
- Đôi dây xoắn: 10BASE-T, 100BASE-T4, 100BASE-TX
- Cáp quang: 10BASE-F, 100BASE-FX,..



Hình 4.17: Bộ kết nối mạng Ethernet

Tên hiệu	Loại cáp	Chiều dài đoạn tối đa	Số trạm tối đa/đoạn
10BASE5	Cáp đồng trục dày	500 m	100
10BASE2	Cáp đồng trục mỏng	200 m	30
10BASE-T	Đôi dây xoắn	100 m	1024
10BASE-F	Cáp quang	2000 m	1024

#### 4.5.4 Cơ chế giao tiếp

Truy nhập bus: CSMA/CD

Cơ chế giao tiếp chủ yếu: Tay đôi (peer-to-peer), tự do, không cần đặt cấu hình trước (giao thức cấp trên có thể yêu cầu đặt cấu hình)

Hỗ trợ gửi đồng loạt (broadcast) và gửi theo nhóm (multicast):

- Bit đầu tiên của địa chỉ nhận = 1: gửi đồng loạt hoặc gửi theo nhóm
- Tất cả các bit = 1: gửi đồng loạt

Địa chỉ MAC: 48 bit, bit 46 phân biệt giữa địa chỉ toàn cục và địa chỉ cục bộ vì vậy bao nhiêu địa chỉ có thể dùng được?

#### 4.5.5 Cấu trúc bức điện

7 byte	1 byte	2/6 byte	2/6 byte	2 byte	46-1500 byte	4 byte	
Mở đầu (555..5H)	SFD (D5H)	Địa chỉ đích	Địa chỉ nguồn	Độ dài/ Kiểu gói	Dữ liệu	PAD	FCS

Đa thức phát cho mã

$$CRC: G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

#### **4.5.6 Các tiến bộ công nghệ mới**

Tốc độ truyền cao: 100Mbit/s, Gbit/s

Switching Ethernet

Bổ sung giao thức cấp trên phù hợp với ứng dụng công nghiệp

Linh kiện, thiết bị mạng phù hợp với yêu cầu trong công nghiệp.

#### **4.6 Câu hỏi ôn tập chương**

*Câu 4.1: Mỗi mạng công nghiệp cần quan tâm đặc điểm yếu tố nào?*

*Câu 4.2: So sánh ưu nhược điểm mạng công nghiệp?*

*Câu 4.3: Áp dụng thiết kế cơ sở nền tảng một mạng công nghiệp vào cơ quan hoặc trường học?*

## CHƯƠNG 5: SCADA TRONG HỆ THỐNG ĐIỆN

### 5.1 Tổng quan

Hệ thống SCADA của ngành điện Việt Nam hiện nay được chia thành ba cấp: cấp quốc gia, cấp vùng miền và cấp tỉnh. Khi hệ thống trở thành phức tạp hơn, có thể sẽ có cấp huyện [41]. Trung tâm điều độ quốc gia theo dõi và điều khiển các nhà máy phát điện lớn 30MW, các đường dây/trạm 500kV và các đường dây/trạm 220kV lớn. Ba trung tâm điều độ miền theo dõi và điều khiển các đường dây/trạm 220kV và các đường dây/trạm 110kV lớn trong khu vực mình (nay chuyển sang cấp tỉnh). Các trung tâm điều độ cấp tỉnh theo dõi và điều khiển hệ thống phân phối điện trong khu vực của mình. Các hệ thống SCADA dùng RTU ngày càng được thay thế bởi PLC, các hệ SCADA cho hệ thống điều độ điện cấp quốc gia hay vùng miền cũng đang ngày càng đi theo xu thế này. Việc xây dựng các hệ thống SCADA dùng PLC sẽ đem lại các lợi thế sau:

- Kinh phí sẽ thấp hơn nhiều.
- Các hệ điều khiển cũ có nhiều tủ, bảng, khoá, nút ấn... Do đó chúng rất cồng kềnh, chiếm nhiều diện tích. Ngoài ra còn rất khó khăn trong việc lắp đặt, kiểm định, vận hành, giám sát, bảo dưỡng. Tuy nhiên công việc này sẽ rất đơn giản nếu chúng ta sử dụng hệ SCADA dùng PLC.
- Các kỹ sư Việt Nam dễ tiếp cận với công nghệ PLC hơn và do đó khả năng thiết kế, nâng cấp và làm chủ công nghệ dễ dàng hơn.
- Mua thiết bị dễ dàng hơn.
- Dễ bảo dưỡng và thay thế các thiết bị.
- Đặc biệt với hệ SCADA thì việc thu thập, lưu trữ, báo cáo, thống kê, phân tích hệ thống rất dễ dàng.
- Các hệ thống SCADA sẽ trở nên đơn giản hơn và phổ biến hơn trong tương lai bởi lẽ các thiết bị trong lĩnh vực tự động hoá đang ngày càng phát triển mạnh.

Trong việc quản lý và điều hành hệ thống điện, hệ thống SCADA/EMS đóng vai trò rất quan trọng, giúp cho kỹ sư điều hành hệ thống điện (HTĐ) nắm bắt và xử lý chính xác, theo sát mọi diễn biến trong hệ thống điện.

Mục đích của việc SCADA cho các trạm điện trong hệ thống điện lực Việt Nam trước tiên nhằm đáp ứng nhu cầu về tự động hoá và số hoá hệ thống điện Việt Nam.



Nó phản ánh một bước đi tất yếu của việc hiện đại hoá hệ thống điện, đồng thời nó cũng phản ánh trình độ về kinh tế-kỹ thuật của lưới điện Việt Nam.

Bảng 5.1: Bảng dưới đây tóm tắt sơ lược những cấp quản lý

Cấp quản lý	Nội dung quản lý chính
Phát và truyền tải điện lực siêu cao áp 500kV xuyên quốc gia	- Phương án phân phát P, Q trên toàn lãnh thổ quốc gia. - Quản lý tần số, dự phòng ổn định tĩnh, động của hệ thống điện quốc gia. - Thu thập số liệu, thao tác, bảo vệ rơle, chẩn đoán, bảo dưỡng các thiết bị cao áp.
Phát và truyền tải điện đến các trạm trong mạng cao áp 220kV khu vực	- Phương án phân bố P, Q trên các khu vực cụ thể. - Phân bố điện áp 220kV ở các trọng tâm tải và dự phòng bảo vệ nguồn. - Thu thập số liệu, thao tác, bảo vệ rơle, chẩn đoán hỏng hóc và bảo dưỡng thiết bị.
Phân phối và truyền tải điện trong địa bàn các mạng 110kV	Phát bù công suất phản kháng Q, phân bố điện áp trên địa bàn. Thu thập các số liệu, thao tác, bảo vệ, chẩn đoán và bảo dưỡng thiết bị.
Phân phối điện xuống mạng 35kV trở xuống	Phát bù công suất phản kháng Q. Điều khiển điện áp trung áp và xa tải theo yêu cầu. Thu thập số liệu, bảo vệ và bảo dưỡng hệ thống.
Cung cấp điện lực hạ áp khu dân cư và xí nghiệp nhỏ.	Tiến hành các thao tác đóng cắt, bảo vệ và bảo dưỡng hệ

## 5.2 Các loại hình SCADA trong hệ thống điện

Dựa vào các phân tích bên trên ta đề ra hai loại hình SCADA sau:

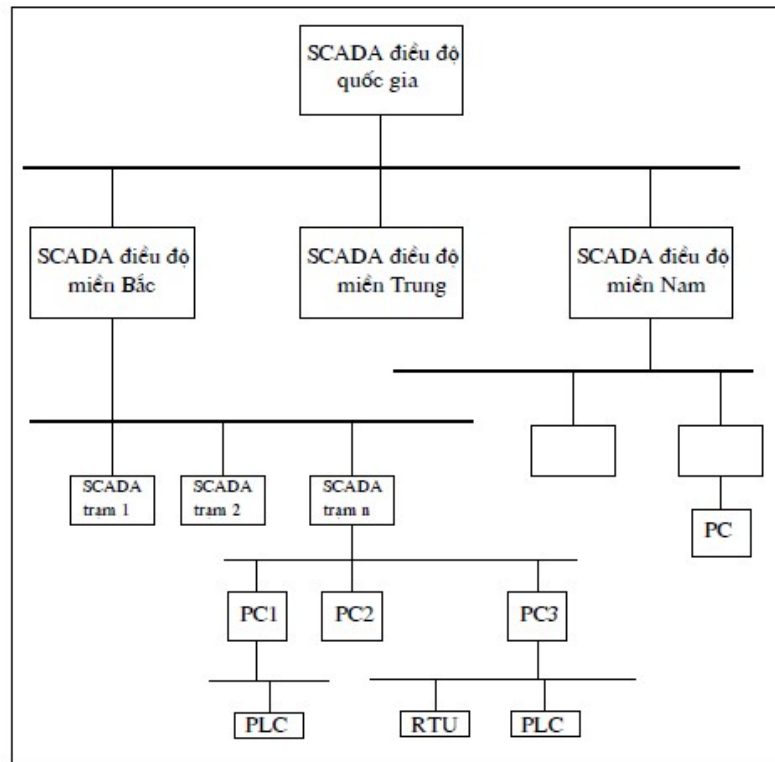
- SCADA điều độ
- SCADA trạm

### 5.2.1 SCADA điều độ cấp quốc gia

Đây là một trung tâm mang tính điều độ cấp cao, mang tính huyết mạch của hệ thống điện Việt Nam. Nó làm nhiệm vụ điều tiết toàn bộ điện năng trên lưới. SCADA điều độ quốc gia giúp cho việc phân bố điện năng thông suốt trên khắp ba miền. SCADA điều độ quốc gia đảm đương các nhiệm vụ sau:

- Thu thập các số đo, các trạng thái, tình hình phụ tải từ các trung tâm điều độ miền đưa lên.
- Trên cơ sở các số liệu thu được tiến hành phân tích, nhận dạng, đánh giá và đưa ra các điều khiển tối ưu cho hệ thống về phân bố công suất cũng như ổn định dự phòng trong lưới. Thực chất trung tâm SCADA điều độ quốc gia không trực tiếp làm nhiệm

vụ thu thập số liệu về hệ thống và cũng không điều khiển trực tiếp lên hệ thống mà chỉ thông qua các trạm phía dưới để thu thập dữ liệu và điều khiển hệ thống thông qua các lệnh dưới dạng các bản tin.



Hình 5.1: Sơ đồ phân cấp SCADA trong hệ thống điện Việt Nam cấp miền

Tại các trung tâm điều độ miền, các dữ liệu về hệ thống được các trạm gửi lên, với những phân tích và đánh giá của mình các trung tâm này đưa ra các quyết định điều khiển tác động lên lưới nhằm một mục tiêu nhất định là ổn định hệ thống. SCADA điều độ miền là cấp trung gian giữa SCADA điều độ quốc gia và SCADA trạm nên nó có một số nhiệm vụ đặc trưng sau:

- Thu thập số liệu từ các SCADA trạm.
- Phân tích biểu đồ phụ tải thu được, tiến hành đánh giá và đưa ra các phương án điều độ và phân chia phụ tải và ổn định lưới. Các trung tâm điều độ miền đóng vai trò quan trọng và định hướng cho các SCADA trạm trong việc điều tiết công suất tải và điều khiển hệ thống.

### 5.2.2 SCADA trạm

Đây là một trung tâm máy tính điều khiển mà tác động trực tiếp đến chất lượng trong lưới điện vì đây là một nơi mà các tác động điều khiển trực tiếp tác động vào hệ

thống điện. Lưới điện có thể ổn định và bền vững hay không phụ thuộc rất nhiều các trung tâm SCADA trạm này. Vậy nhiệm vụ của SCADA trạm là phải trực tiếp:

- Thao tác điều khiển lên các thiết bị của hệ thống, các máy biến áp...
- Thu thập và giám sát các thông số về hệ thống.
- Điều khiển đóng/cắt nhằm bảo vệ hệ thống trong trường hợp lưới gặp sự cố như quá tải, chạm chập...
- Đưa các dữ liệu về báo cáo với SCADA cấp trên phục vụ cho việc phân tích, đánh giá hệ thống khi cần khắc phục sự cố hay nâng cấp hệ thống. Mạch thu thập số liệu và điều khiển được thiết kế bằng:

- Một PLC và các module AI/AO, DI/DO.
- Một bộ RTU với các tín hiệu tương tự.
- Một bộ các tín hiệu số thông minh.

SCADA trạm được thiết kế còn có các bus truyền tin phục vụ cho các tác vụ truyền thông sau:

- Một bus truyền số liệu, truyền lệnh hiện trường kiểu RS-485 nối các PLC, các RTU và các transmitter số thông minh với trung tâm điều khiển là các máy tính PC.
- Một bus truyền tin theo kiểu RS-323 để giao tiếp truyền thông với SCADA điều độ cấp trên. Trung tâm điều khiển là các máy tính PC, tùy theo quy mô của trạm mà số lượng máy có thể là nhiều hay ít. Với mỗi trạm tùy vào mức độ đòi hỏi về độ tin cậy của việc điều khiển mà ta có thể lắp các máy dự phòng. Các trạm với quy mô nhỏ ta có thể chỉ cần dùng một máy tính PC tốc độ cao, khả năng xử lý nhanh và có dung lượng bộ nhớ lớn là có thể đảm nhận việc của một trung tâm điều khiển và giám sát. Còn đối với các trạm lớn và đòi hỏi tính an toàn cao thì ta nên dùng một máy chuyên làm nhiệm vụ điều khiển, một máy PC khác thì làm nhiệm vụ thu thập và giám sát nếu cần thiết có thể dùng thêm một máy chuyên thực hiện các tác vụ về truyền thông.

### **5.3 Nguyên tắc làm việc của hệ thống SCADA như sau:**

#### **5.3.1 Thu thập dữ liệu:**

Dữ liệu từ các trạm biến áp và các nhà máy điện được chia làm ba loại chính:

- Dữ liệu trạng thái: trạng thái các máy cắt, dao cách ly, dao tiếp địa, trạng thái vị trí các khoá điều khiển từ xa/ tại chỗ v.v... Cảnh báo của các bảo vệ.
- Dữ liệu tương tự: Công suất tác dụng MW, phản kháng MVAR, điện áp V dòng điện A, vị trí nấc biến áp, tần số v.v...

- Dữ liệu tích lũy theo thời gian: Điện năng kWh, kVArh v.v...

Các dữ liệu trạng thái (Digital) từ các rơ le trung gian được đưa vào các đầu vào số của RTU. Các dữ liệu tương tự (Analog) từ cuộn thứ cấp của máy biến dòng điện và điện áp được đưa vào các bộ biến đổi (Transducer). Đầu ra của bộ biến đổi được đưa vào các vi đầu vào tương tự của RTU. Tại RTU dữ liệu được số hoá và thông qua kênh truyền (giao thức) gửi về trung tâm điều độ.

### 5.3.2 Điều khiển:

Lệnh điều khiển từ hệ thống SCADA của trung tâm điều độ thông qua kênh truyền gửi đến RTU (hoặc SAS), các lệnh điều khiển có thể là:

- Lệnh đóng cắt máy cắt, dao cách ly, dao tiếp địa (open/close).
- Lệnh điều khiển tăng giảm (Raise/Lower)
- Lệnh điều khiển thay đổi giá trị đặt (Set point)

### 5.3.3 Giám sát:

Dữ liệu thu thập từ các trạm về trung tâm điều khiển sẽ được máy tính xử lý:

- Hiện thị trên các sơ đồ, bảng biểu và các dạng đồ thị xu hướng.
- Đối với dữ liệu trạng thái (máy cắt, dao cách ly, cảnh báo v.v...) khi phát hiện ra có sự thay đổi trạng thái hệ thống SCADA sẽ phát cảnh báo bằng âm thanh và dòng thông báo để lôi kéo sự chú ý của người vận hành.
- Đối với dữ liệu giá trị đo xa, dữ liệu nhận được sẽ được kiểm tra so sánh với các ngưỡng dưới và ngưỡng trên (đã được định trước), nếu giá trị đo được bị vi phạm thì hệ thống sẽ phát cảnh báo cho người vận hành.

Một vài ví dụ hệ thống SCADA được nghiên cứu và ứng dụng trong thực tiễn trên thế giới trong các tài liệu [18], [21], [51], [22], [24], [28], [40]–[42], [49], [50]...

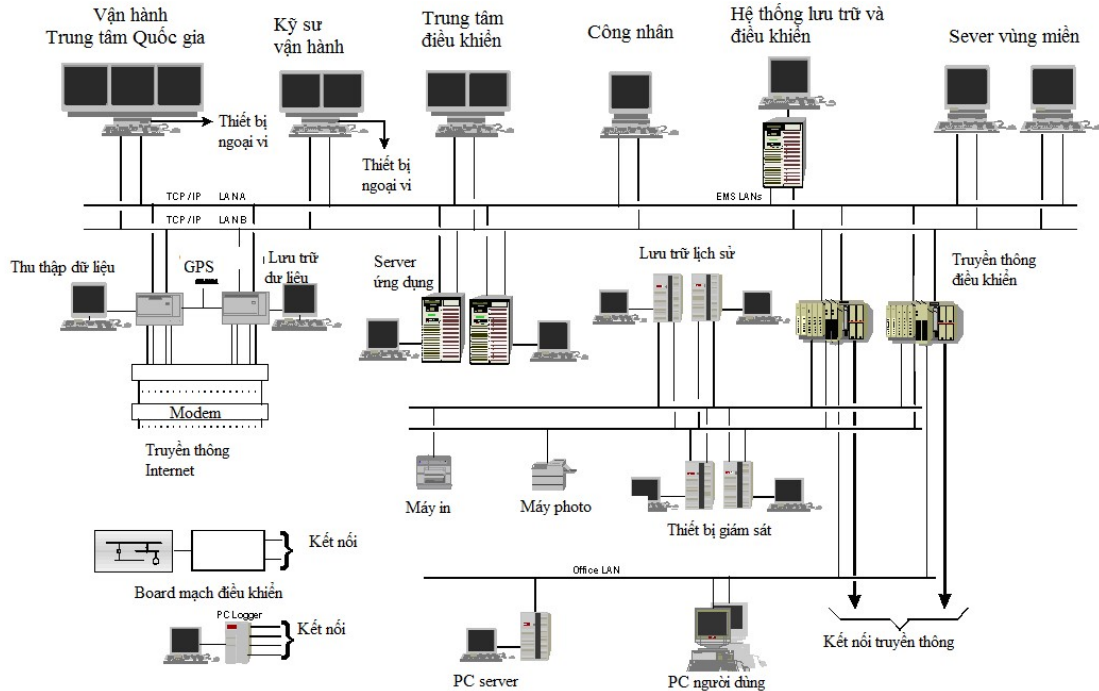
## 5.4 Các thiết bị trong SCADA EVN

Hệ thống bao gồm nhiều khối cho phép tùy biến trong hệ thống khi bảo trì các bộ phận hợp thành. Bất cứ phần tử nào của hệ thống cũng có thể đặt cấu hình được. Hình 5.2 là sơ đồ chung của toàn bộ cấu hình hệ thống.

### 5.4.1 Các RTU

Các thiết bị RTU có cấu trúc mô-đun khá linh hoạt, thuận lợi cho mở rộng trạm, tăng số lượng tín hiệu nối đến RTU, mỗi môđun có khối xử lý và các khối tín hiệu vào/ra, mỗi khối xử lý có hệ điều hành đa nhiệm thời gian thực cho phép có thể làm việc độc

lập, nên các modul có thể bố trí phân tán tại các tủ thiết bị trong trạm hoặc nhiều modul có thể được liên kết với nhau để tích hợp thành một RTU tập trung [45].



Hình 5.2: Cấu hình đặc trưng của hệ thống SCADA/EMS

Ở mỗi trạm, RTU chỉ là một thiết bị giao tiếp giữa hệ thống quản lý mạng và các thiết bị đóng cắt. RTU bao gồm nhiều đầu vào/ra, gần như nó không thực hiện các chức năng tại chỗ mà chỉ thông tin đến các trung tâm điều khiển ở xa. RTU và các trung tâm điều khiển tạo nên hệ thống SCADA, để giám sát, điều khiển và quản lý hệ thống điện từ xa bởi sự can thiệp của con người. Nó cung cấp thông tin theo thời gian thực (thông tin tín hiệu tương tự và tín hiệu số) cũng như các thông tin quá khứ cho người vận hành và hỗ trợ người vận hành quyết định việc điều khiển giám sát hiệu quả.

Một vài đặc điểm của RTU XCELL

- Scalable, Flexible, Architecture.
- Exceptionally High Reliability.
- SCADA Protocol Support (Serial & IP Protocol).
- IED Integration.
- IEC 61131 PLC programming.
- IEC 61850 Integration (Client & Server).
- DLMS Smart Meter Support.

- High Density Plant Interface.
- Redundant I/O Processors.
- Web server.



*Hình 5.3: Hình ảnh một RTU sử dụng trong hệ thống điện*

Việc cài đặt cấu hình của RTU có thể thực hiện bằng công cụ chạy trên môi trường Windows. RTU có chức năng kết nối với các dạng tín hiệu sau đây:

- Các tín hiệu trạng thái: Các tín hiệu của máy cắt, dao cách ly các lộ đường dây và máy biến áp, các tín hiệu của dao nối đất, các tín hiệu cảnh báo, các tín hiệu của role bảo vệ các lộ đường dây, máy biến áp, các tín hiệu tác động của hệ thống role bảo vệ các tổ máy phát. Tất cả đều được role trung gian chuyển về trạng thái số trước khi đến RTU.

- Tín hiệu đo lường:

*Đối với máy biến áp:* Công suất tác dụng (MW), công suất phản kháng (MVAR), điện áp (KV), cường độ dòng điện (A) ở các cấp điện áp khác nhau của máy biến áp, nấc của máy biến áp.

*Đối với lộ đường dây:* Công suất tác dụng (MW), công suất phản kháng (MVAR), điện áp (KV), cường độ dòng điện (A).

*Đối với tổ máy:* Công suất tác dụng (MW), công suất phản kháng (MVAR), điện áp đầu cực (KV), tổng công suất tác dụng của nhà máy (MW), tổng công suất phản kháng của nhà máy (MVAR).

*Đối với thanh cái:* điện áp (KV).

*Tín hiệu đo lường tần số*

*Giá trị lưu kế:* sản lượng trao đổi (MWH, MVARH)

- Tín hiệu của điều khiển:

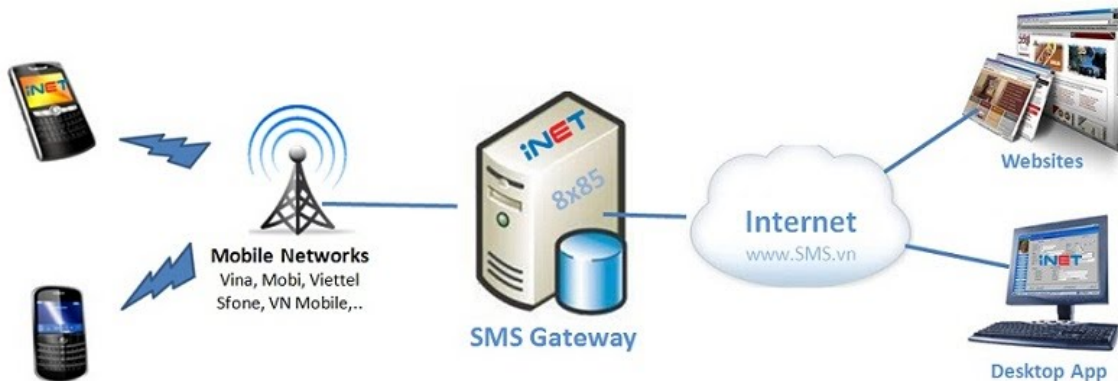
*Điều khiển tổ máy (AGC)*

- + Phương thức điều khiển Raise/Lower hay Setpoint.
- + Giới hạn điều chỉnh cao của tổ máy
- + Giới hạn điều chỉnh thấp của tổ máy
- + Điều khiển tự động (Auto control)
- + Chạy máy (Startup)
- + Dừng máy (Shutdown)

*Điều khiển nấc máy biến áp, máy cắt, dao cách ly*

#### 5.4.2 Gateway

Chức năng của Gateway trong hệ thống mạng IP [01/06/2015] Gateway là một phần tử không nhất thiết phải có trong một giao tiếp H.323. Nó đóng vai trò làm phần tử cầu nối và chỉ tham gia vào một cuộc gọi khi có sự chuyển tiếp từ mạng H.323 (ví dụ như mạng LAN hay mạng Internet) sang mạng phi H.323 (ví dụ mạng chuyển kênh hay PSTN). Một Gateway có thể kết nối vật lý với một hay nhiều mạng IP hay với một hay nhiều mạng chuyển mạch kênh [15].



Hình 5.4: Thiết bị Gateway được sử dụng trong hệ thống mạng

Một Gateway có thể bao gồm: Gateway báo hiệu, Gateway truyền tải kênh thoại, Gateway điều khiển truyền tải kênh thoại. Một hay nhiều chức năng này có thể thực

hiện trong một Gatekeeper hay một Gateway khác. Gateway báo hiệu SGW: cung cấp kênh báo hiệu giữa mạng IP và mạng chuyển mạch kênh. Gateway báo hiệu là phần tử trung gian chuyển đổi giữa báo hiệu trong mạng IP (ví dụ H.323) và báo hiệu trong mạng chuyển mạch kênh (ví dụ R2, CCS7). Gateway báo hiệu có các chức năng sau: Chức năng kết nối các giao thức điều khiển cuộc gọi. Chức năng kết nối báo hiệu từ mạng chuyển mạch kênh: phối hợp hoạt động với các chức năng báo hiệu của Gateway điều khiển truyền tải kênh thoại. Chức năng báo hiệu: chuyển đổi báo hiệu giữa mạng IP với báo hiệu mạng chuyển mạch kênh phi phối hợp hoạt động với Gateway điều khiển truyền tải kênh thoại. Chức năng giao diện mạng chuyển mạch gói: kết cuối mạng chuyển mạch gói. Chức năng bảo mật kênh báo hiệu: đảm bảo tính bảo mật của kênh báo hiệu nối với thiết bị đầu cuối. Chức năng quản lý: giao tiếp với hệ thống quản lý mạng. Chức năng ghi các bản tin sử dụng: xác định hoặc ghi lại các thông tin về sự kiện (truy nhập, cảnh báo) và tài nguyên. Chức năng báo cáo các bản tin sử dụng: báo cáo các bản tin đã được sử dụng ra thiết bị ngoại vi.

#### **5.4.3 Server ứng dụng AS**

Applications Server (AS) là trái tim của hệ thống. Nó hỗ trợ các ứng dụng mạng và các chức năng SCADA, quản lý các trung tâm xử lý phân tán và duy trì cơ sở dữ liệu quan hệ. AS có thể hoạt động trong cấu hình "failsafe" với cơ sở dữ liệu cấu hình kép đảm bảo không bị mất dữ liệu trong trường hợp sự cố. AS trao đổi với các thành phần khác của hệ thống qua TCP/IP.

#### **5.4.4 Server thu nhận dữ liệu**

Có nhiệm vụ như bộ tiền xử lý cung cấp giao diện vật lý, tập hợp và kiểm tra các dữ liệu nhận được từ đầu cuối rồi xử lý sơ bộ để AS sử dụng.

Ngoài ra còn truyền các lệnh giám sát và nhận các phản hồi, theo dõi và điều khiển đường truyền giữa EMS và các đầu cuối.

#### **5.4.5 Giao tiếp người và máy (MMC)**

MMC là trạm làm việc cùng với màn hình màu đồ họa. Mỗi MMC có thể có đến 3 màn hình hiển thị, mỗi MMC là một hệ thống máy tính đầy đủ với hệ điều hành, hệ thống nhớ, các cổng truyền tin, đĩa cứng và card giao tiếp mạng. Điều độ viên đưa ra các lệnh thông qua bàn phím, chuột, và dựa trên menu trên màn hình.



## 5.5 Các chức năng SCADA trong hệ thống điện

Các phần mềm được chia ra bốn nhóm: Thu nhận dữ liệu, Giao tiếp người máy, Quản lý SCADA và ứng dụng SCADA.

### 5.5.1 Thu nhận dữ liệu

Hệ thống thu nhận dữ liệu tập hợp dữ liệu gửi lệnh điều khiển và duy trì các đường kết nối tới RTU và các hệ SCADA khác.

- Thu nhận dữ liệu RTU - RTU Data Acquisition (RDA)
- Thu nhận dữ liệu từ hệ thống khác- Computer-to-Computer Remote (CCR)
- Giám sát điều khiển - Supervisory Control (SCS)
- Tính toán - Calculations (CAL)

### 5.5.2 Giao tiếp người máy

Hệ thống giao tiếp người máy cung cấp các thao tác hệ thống cùng với thể hiện dữ liệu và điều khiển các thiết bị. Các giao tiếp thực hiện qua màn hình, bàn phím và các thiết bị in. Hệ thống này cũng cung cấp “console” để cấu hình và bảo trì hệ thống [30].

- Giao tiếp điều khiển - Console Interface (CIS)
- Hiển thị - Display Retrieval and Update (DRU)
- Dữ liệu vào - Data Entry (DES)
- Ghi - Logging (LOG)
- Biểu đồ xu thế - Trending (TRN)
- Chuyển đổi Console - Console Switching (CCS)

### 5.5.3 Quản lý giám sát

Hệ thống quản lý SCADA bao gồm một số hệ thống con hỗn hợp dùng bởi các hệ thống khác. Đó là khởi động, khởi động lại, cảnh báo, kiểm soát lỗi và các chức năng quản lý khác.

- Khai báo ban đầu - Restart Initialization (INI)
- Cảnh báo - Alarms (ALL)
- Hệ thống tính toán lỗi - System Error Accounting (SEA)
- Quản lý - Executive (EXC)

### 5.5.4 Điều khiển xa

Điều khiển từ xa hiện nay được triển khai trên cơ sở công nghệ truyền số liệu. Dưới góc độ truyền số liệu bản chất điều khiển từ xa là truyền 2 loại dữ liệu:

- Dữ liệu về nội dung điều khiển (điều khiển cái gì)

- Dữ liệu về bản thân lệnh điều khiển (hành động điều khiển)

Nếu coi điều khiển gồm 2 bước: bước 1 là dự lệnh và bước 2 là lệnh, ta có thể hiểu "điều khiển cái gì" là bước 1 và "hành động điều khiển" là bước 2. Bản thân cơ cấu nhận lệnh điều khiển từ xa của thiết bị đã được thiết kế theo triết lý điều khiển nói trên.

Giao thức truyền tin đã cho phép các loại dữ liệu được truyền đi an toàn và chính xác giữa 2 thiết bị [20]. Giao diện người máy của các lệnh điều khiển được thiết kế thân thiện và đảm bảo an toàn về kỹ thuật và về trách nhiệm pháp lý của người điều khiển (mật khẩu, nội dung lệnh và lệnh,...)

- Điều khiển đóng/mở (on/off): Điều khiển đóng/mở áp dụng cho các thiết bị có 2 trạng thái như máy cắt và dao cách ly.

- Điều khiển tăng/ giảm: Điều khiển tăng/giảm áp dụng cho các thiết bị có nhiều trạng thái như thiết bị chuyển đổi nấc biến áp, tăng giảm công suất tổ máy... Để điều khiển tăng giảm giá trị nào đó của thiết bị thì bản thân thiết bị cũng đã được thiết kế để tăng giảm giá trị từng bước (step by step) mà phương pháp điều khiển số yêu cầu.

Hệ thống các ứng dụng SCADA bao gồm các hàm thực hiện trình bày dữ liệu ở mức cao [32]:

- Tính toán thời gian thực - RAS Real-Time Calculations (RTC)
- Định vị trí - Mapboard (MBD)
- Tải chương trình dự phòng - Load Shed Restore (LSR)
- Hiển thị lỗi đo lường - Meter Error Monitor (MEM)

### 5.5.5 Đo lường xa

Các giá trị đo lường trong hệ thống điện (HTĐ) bao gồm các đại lượng vật lý như điện áp, dòng điện, công suất hữu công, vô công, điện năng tiêu thụ, nấc máy biến áp [38], [45],...

Tín hiệu trạng thái trong HTĐ cho biết trạng thái đóng hoặc mở của các thiết bị như máy cắt, dao cách ly và các cảnh báo.

Đo lường xa các thông số HTĐ là tổ chức hệ thống thu thập dữ liệu HTĐ tại các thiết bị đầu cuối (RTU-Remote Terminal Unit) và gửi về trung tâm điều khiển (CC-Control Centre).

Các kênh viễn thông khác nhau đảm bảo liên kết giữa các RTU và CC.

Biến dòng và biến áp (CT và VT)

CT và VT được sử dụng rộng rãi trong hệ thống điện. Chúng cho phép biến đổi dòng điện và điện áp nhất thứ sang dòng điện và điện áp nhị thứ, phục vụ công tác đo lường. Hệ số biến đổi của CT và VT được thiết kế và chuẩn hoá theo cấp điện áp và dòng điện. CT và VT cho phép cách ly nhất thứ và nhị thứ bằng 2 cuộn dây độc lập.

## 5.6 Các bộ chuyển đổi trong hệ thống SCADA của hệ thống điện

### 5.6.1 Bộ chuyển đổi - Transducer

Transducer là các thiết bị chuyển đổi các đại lượng ở lõi ra CT và VT sang dòng điện có thang chuẩn hóa: 0 -10mA, -5mA - 5mA... tương ứng với đại lượng cần đo [37], [52]. Tồn tại các Transducer dòng, áp, công suất vô công, hữu công...

Các dòng điện ở lõi ra các Transducer được dẫn tới lõi vào đo lường của RTU với tổng trở dây dẫn từ 0-vài k $\Omega$  tùy theo nhà chế tạo [53], [52].

Việc sử dụng nguồn dòng cho phép nối lõi ra Transducer với lõi vào đo lường RTU với độ dài cáp khác nhau mà vẫn không ảnh hưởng tới độ chính xác [53].

Việc sử dụng nguồn dòng cũng làm tăng khả năng chống nhiễu.

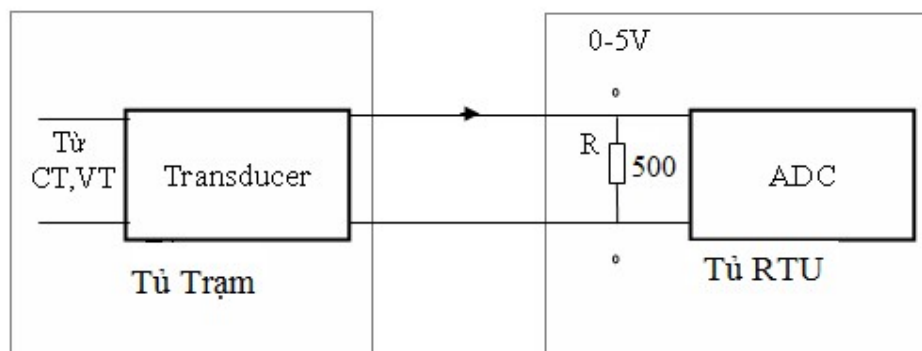
### 5.6.2 Bộ chuyển đổi tương tự - số (ADC- Analog Digital Converter)

ADC cho phép số hoá các điện áp vào thành các giá trị nhị phân

Việc tạo ra điện áp ở lõi vào ADC từ lõi ra dòng điện của Transducer được thực hiện bằng cách mắc nối tiếp với một điện trở,

Giá trị của điện trở này được tính trên thang dòng của lõi ra Transducer và thanh áp vào của ADC. Xem hình vẽ.

Ví dụ: Dòng ra của Transducer biến thiên từ 0-10mA, ứng với điện áp vào của ADC biến thiên từ 0-5V. Ta có:

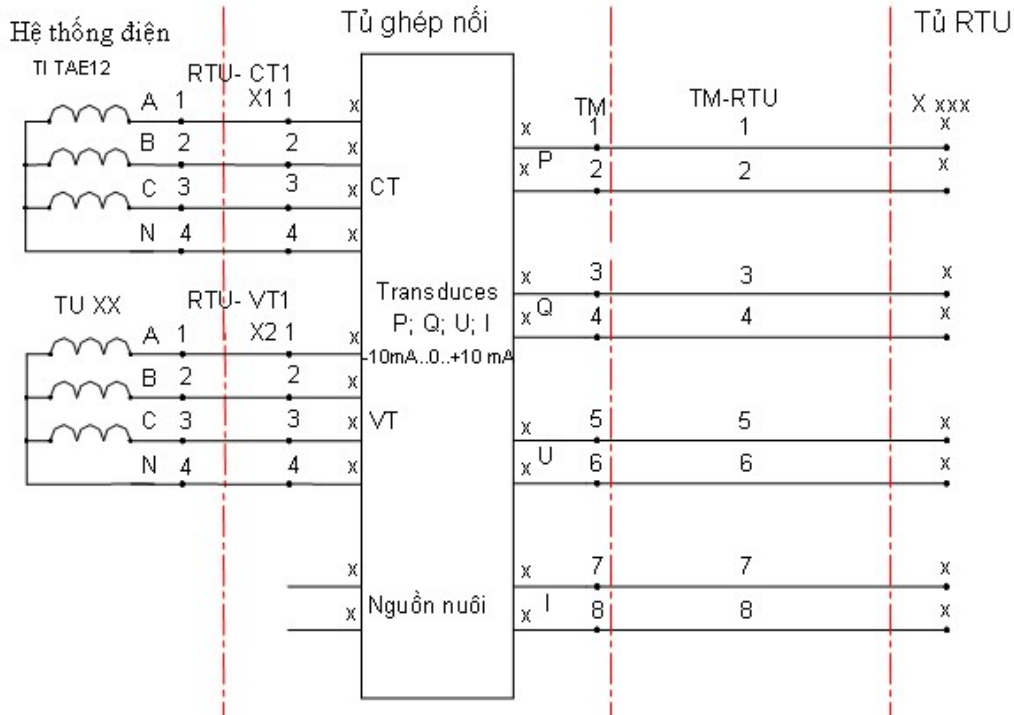


Hình 5.5: Mô hình truyền dẫn đo lường xa dùng ADC

## 5.7 Ghép nối RTU với hệ thống điện

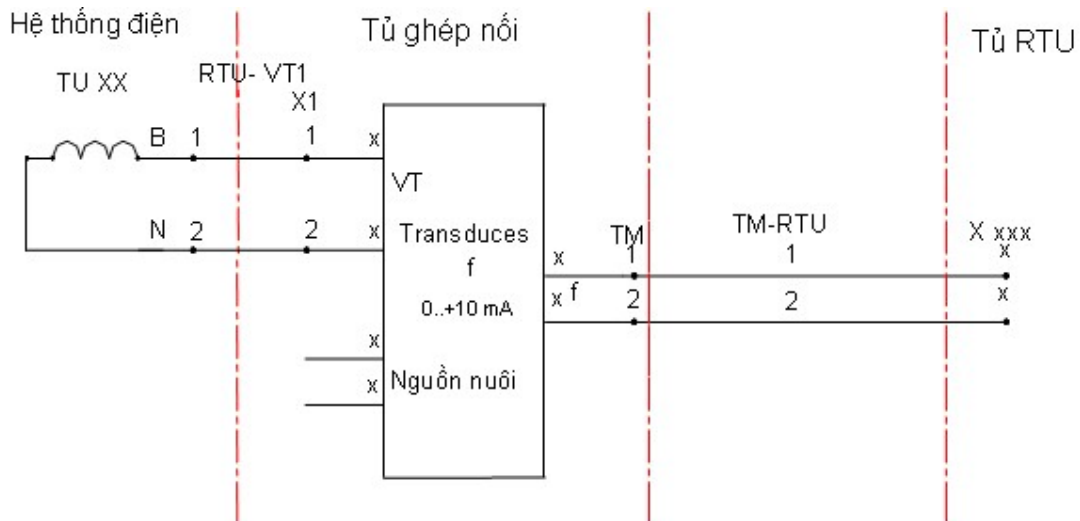
### 5.7.1 Ghép nối tín hiệu tương tự

Đối với tín hiệu P, Q, U, I, sử dụng BBD để biến các tín hiệu dòng điện, điện áp,  $\cos(\varphi)$  thành tín hiệu dòng điện tỷ lệ tương ứng. Sơ đồ nguyên lý như hình vẽ.



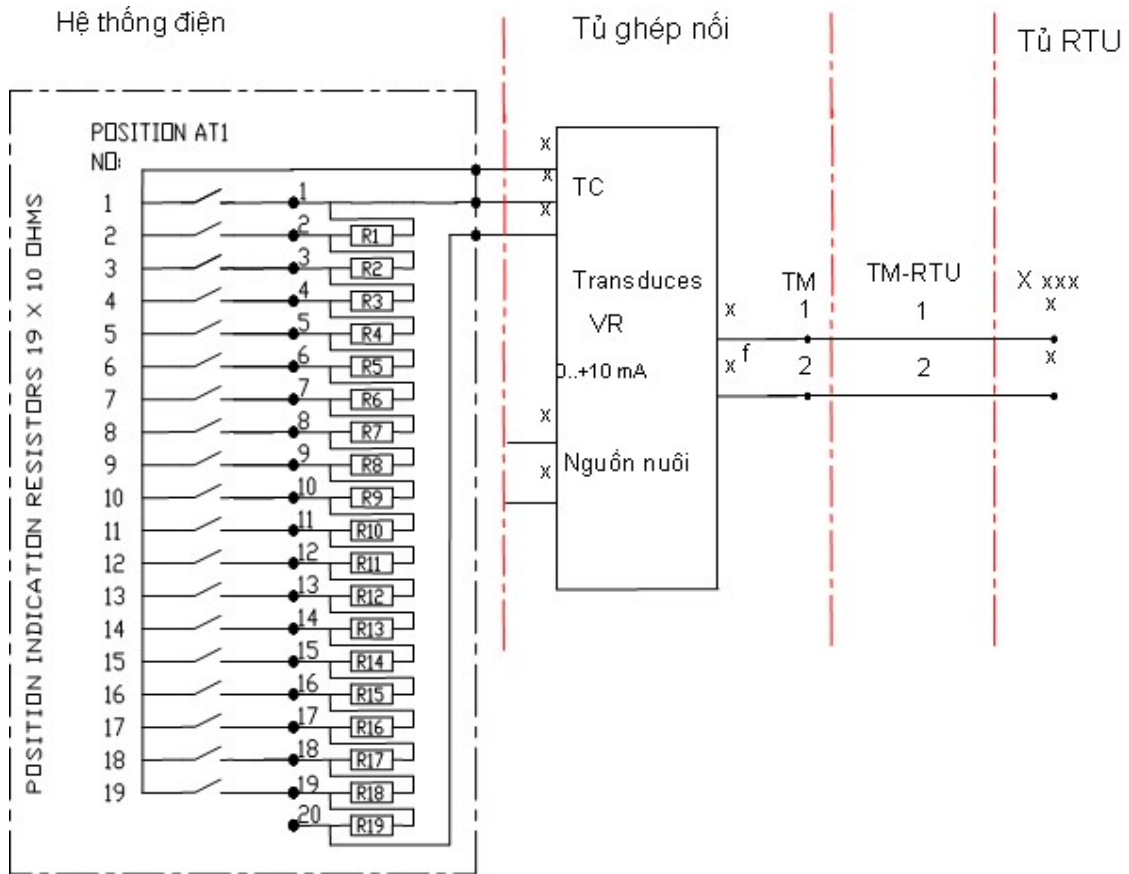
Hình 5.6: Sơ đồ nguyên lý ghép nối P, Q, U, I

Đối với tín hiệu tần số, sử dụng bộ biến đổi để biến f (Hz) thành tín hiệu dòng điện tỷ lệ tương ứng. Sơ đồ nguyên lý như hình vẽ.



Hình 5.7: Sơ đồ nguyên lý ghép nối tín hiệu tần số

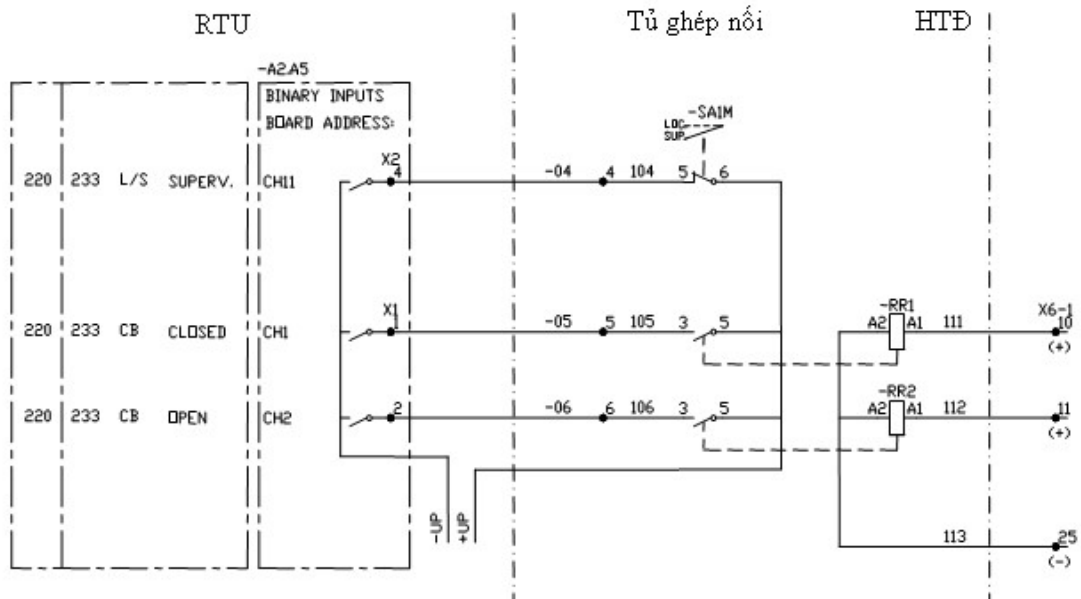
Đối với tín hiệu chỉ thị nấc MBA, sử dụng BBD để biến  $R(\Omega)$  thành tín hiệu dòng điện tỷ lệ tương ứng. Sơ đồ nguyên lý như hình vẽ sau.



Hình 5.8: Sơ đồ nguyên lý ghép nối tín hiệu chỉ thị chuyển nấc MBA

### 5.7.2 Ghép nối tín hiệu số

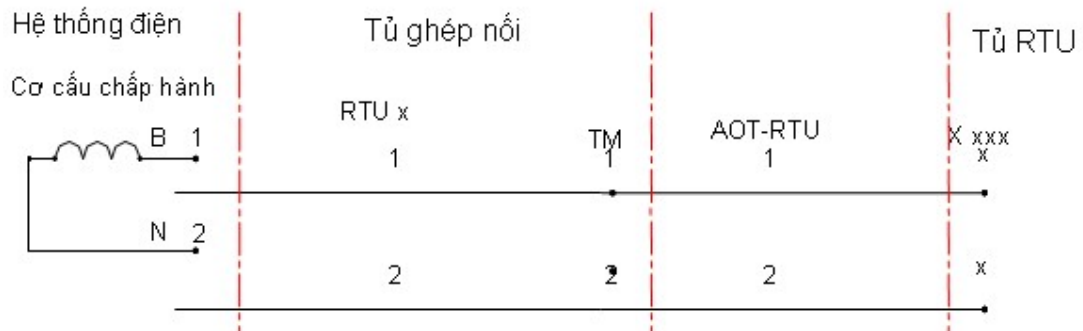
Đối với tín hiệu số, sử dụng role trung gian để ghép nối HTĐ với RTU. Sơ đồ nguyên lý như hình vẽ .



Hình 5.9: Sơ đồ nguyên lý ghép nối tín hiệu chỉ thị trạng thái máy cắt

### 5.7.3 Ghép nối tín hiệu đầu ra tương tự

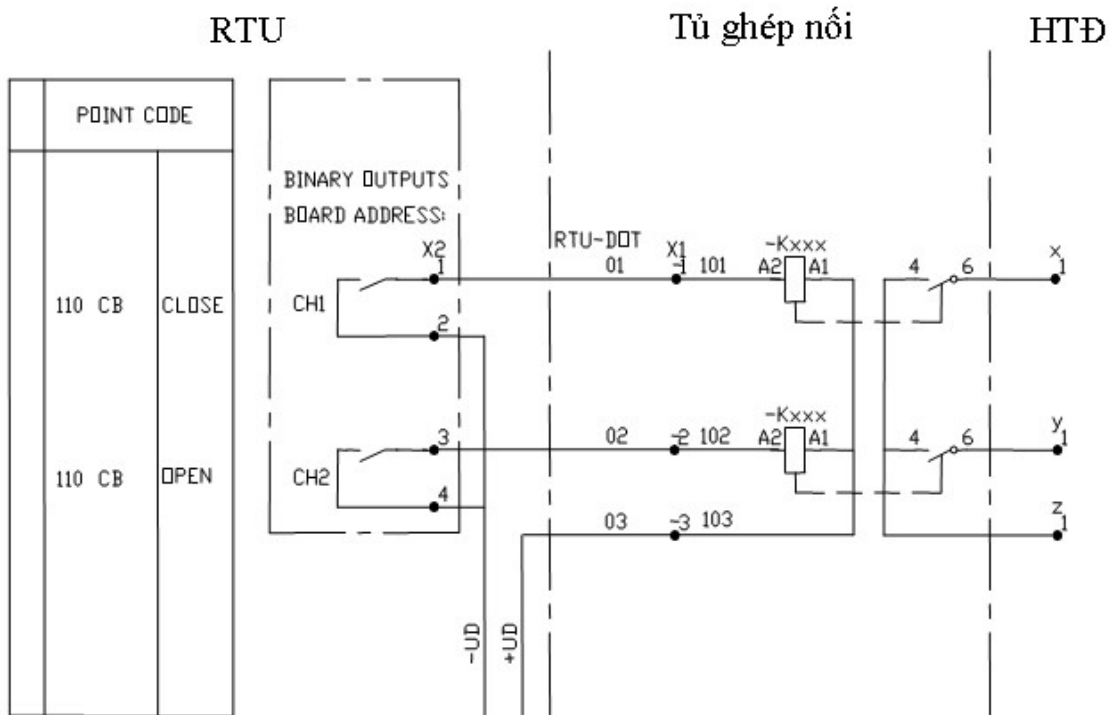
Đối với tín hiệu ra tương tự (Analog), tín hiệu ra được nối trực tiếp vào cơ cấu chấp hành của hệ thống điều khiển [45].



Hình 5.10: Sơ đồ nguyên lý ghép nối tín hiệu điều khiển tương tự

### 5.7.4 Ghép nối tín hiệu đầu ra số (DOT)

Đối với tín hiệu số, sử dụng role trung gian để ghép nối HTĐ với RTU. Sơ đồ nguyên lý như hình vẽ.



Hình 5.11: Sơ đồ nguyên lý ghép nối tín hiệu điều khiển máy cắt

## 5.8 Các thiết bị phụ trợ cho SCADA hệ thống điện

### 5.8.1 Nguồn UPS.

Hệ thống UPS là hệ thống đảm bảo cấp nguồn liên tục cho hệ thống SCADA tại Trung tâm. Hệ thống bao gồm 2 bộ UPS 911 được đấu song song. Mỗi bộ UPS được nối với 2 tổ ắc quy 220VDC.

Khi mất điện lưới, nguồn được cấp từ các tổ ắc quy sẽ qua bộ biến đổi (Inverter) sẽ chuyển từ điện áp 1 chiều thành điện áp 220VAC. Hoạt động trong chế độ vận hành bình thường. Hệ thống UPS trong chế độ vận hành bình thường liên tục cấp nguồn ổn định và liên tục cho hệ thống máy tính chủ tại Trung tâm Điều độ HTĐ Quốc gia.

Hoạt động trong chế độ vận hành bằng nguồn Ắc quy khi xảy ra 1 trong các trường hợp sau:

- + Mất điện lưới.
- + Có điện lưới nhưng thông số kỹ thuật (điện áp, tần số) vượt giới hạn cho phép.

Cấp nguồn cho tải bằng điện lưới khi xảy ra 1 trong các trường hợp sau:

- + Điện áp ắc quy thấp.
- + Chuyển sang chế độ bảo dưỡng.
- + Hỏng bộ chỉnh lưu (RECTIFIER); bộ biến đổi (INVERTER).
- + Khi hệ thống UPS bị quá tải.

### 5.8.2 Hệ thống Máy phát điện - Diesel

Máy phát Diesel, cũng được sử dụng làm hệ thống nguồn dự phòng tại A0, sử dụng khi mất nguồn lưới.

Công suất động cơ Diesel: 30 KVA.

Có Máy phát và Ấc quy để khởi động Diesel.

Khi mất điện lưới, hệ thống Diesel sẽ tự khởi động để cấp điện cho phụ tải.

### 5.8.3 Hệ thống thông tin liên lạc

Hệ thống thông tin liên lạc tại trung tâm bao gồm các thiết bị và kênh truyền đảm bảo thông thoại giữa kỹ sư điều hành HTĐ và các nhân viên trực tại các trạm và các nhà máy điện trong công tác điều hành hệ thống điện.

#### 5.8.3.1 Kênh trực thông

Kết nối trực thông (hotline) là kết nối thoại trực tiếp giữa 2 trạm; Người gọi chỉ cần nhắc tổ hợp điện thoại, cuộc gọi sẽ tự động kết nối với đầu xa (địa chỉ đầu xa đã được định trước);

Hiện tại có trên 60 kênh trực thông kết nối giữa A0 với các trạm, nhà máy điện, các Trung tâm Điều độ và các Trung tâm Truyền tải.

#### 5.8.3.2 Kênh quay số

Kênh quay số để kết nối thuê bao với tổng đài (ngành điện hoặc bưu điện). Việc liên lạc với một thuê bao khác thực hiện bằng quay số điện thoại yêu cầu. Hiện tại tổng đài điều độ cũng có kết nối với một số thuê bao quay số ngành điện và Bưu điện.

#### 5.8.3.3 Kênh bộ đàm

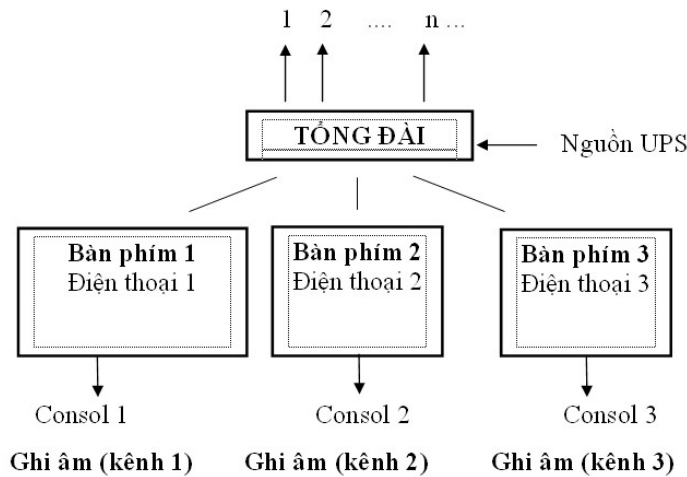
Ngoài cách liên lạc qua điện thoại quay số và điện thoại trực thông như đã nêu ở trên, còn sử dụng phương thức liên lạc qua máy bộ đàm (đang sử dụng tại Trung tâm Điều độ HTĐ miền Nam). Đặc điểm của phương thức liên lạc này:

- + Là hình thức liên lạc vô tuyến, bị hạn chế về cự ly và địa hình;
- + Là hình thức liên lạc đơn công (tại 1 thời điểm chỉ có thể hoặc nghe hoặc nói);
- + Hình thức này chỉ áp dụng trong 1 số hoàn cảnh đặc biệt;

### 5.8.4 Tổng đài điều độ (Lineseizer -LSZ)

Thay vì đặt nhiều máy điện thoại trên bàn làm việc, LSZ là thiết bị cho phép gom tất cả các kênh liên lạc (không kể kênh bộ đàm) để làm việc trên 03 bàn điều khiển điện thoại (Consol) với 03 điện thoại số và 03 bàn phím. Các tính năng chính của LSZ:





Hình 5.12: Sơ đồ ghép nối LSZ với các kênh liên lạc tại A0

- + Có thể đảm bảo kết nối trực thông tới nhiều nơi,
- + Dễ dàng nhận biết chính xác cuộc gọi đến (đặc biệt khi có sự cố xảy ra khi có nhiều cuộc gọi đến).

- + Dễ dàng thao tác khi thực hiện cuộc gọi đi theo từng địa chỉ.

Hiện tại tổng đài có khả năng kết nối với 64 kênh (trực thông và quay số), Tổng đài có khả năng mở rộng kết nối khi có yêu cầu. Các thuê bao nhắc thẳng hoặc quay số từ các hệ thống khác

### 5.8.5 Thiết bị Ghi âm

Ghi âm các cuộc đàm thoại của KS điều hành với trực ca của nhà máy và trạm điện, nhằm phục vụ cho phân tích các tình huống sự cố trong điều hành HTĐ.

Hiện tại Trung tâm đang có 2 thiết bị ghi âm:

Thiết bị ghi âm công nghiệp Marathon (thiết bị chính).

Thiết bị ghi âm dự phòng là sử dụng card ghép nối kênh và máy tính PC, được vận hành khi thiết bị chính có sự cố.

#### 5.8.5.1 Thiết bị ghi âm công nghiệp

Thiết bị ghi âm số MARATHON PRO do hãng ASC Telecom chế tạo là một thiết bị ghi âm hiện đại có 128 đầu vào có thể nối với đường thoại, máy TELEFAX hoặc thiết bị thông tin vô tuyến .. Việc vận hành thiết bị thông qua bàn phím; bóng di động vị trí “mouse” ở mặt trước của thiết bị. Màn hình LCD ở phía trước của thiết bị sẽ hiển thị toàn bộ các thông tin cần thiết cho việc giám sát và vận hành thiết bị.

*Đặc tính kỹ thuật:*

- Có khả năng vận hành liên tục 24/24.

Có khả năng ghi âm và giám sát đồng thời 128 cuộc gọi trên các kênh.

- Có khả năng mở rộng ghép nối (bằng cách thêm card ghép kênh).
- Có khả năng lưu trữ cao (100.000h).
- Vừa lưu trữ dữ liệu trên ổ cứng vừa lưu trữ trên băng từ.
- Có thể giám sát tình trạng của các kênh thông qua màn hình giám sát kênh.
- Có khả năng tìm kiếm các cuộc gọi đã được ghi âm theo các tiêu chuẩn khác nhau (theo thời gian cuộc gọi, theo số hiệu kênh...).
- Có khả năng lưu dữ cuộc gọi quan trọng để tiện tra cứu trong những địa chỉ lưu trữ riêng.

#### 5.8.5.2 Thiết bị ghi âm dự phòng (Máy tính + Card Ghi âm + Phần mềm ghi âm)

Hệ thống ghi âm dự phòng sử dụng card ghép kênh cắm trên máy tính PC. Dữ liệu được ghi trực tiếp trên ổ cứng của máy tính. Máy có khả năng ghép nối trực tiếp với kênh truyền hoặc ghép nối với nguồn tín hiệu âm tần. Hệ thống có giao diện tiện lợi cho người sử dụng và cho khả năng khởi động ghi âm theo nhiều cách, ngoài ra còn có nhiều tiện ích khác trong việc lưu trữ và tìm kiếm cuộc gọi.

### 5.9 Câu hỏi ôn tập chương

*Câu 5.1: Mục đích việc phân cấp trong hệ thống SCADA của EVN?*

*Câu 5.2: Nhiệm vụ chức năng của từng cấp SCADA trong EVN?*

*Câu 5.3: Sơ đồ đấu nối đo lường tín hiệu RTU?*

## **CHƯƠNG 6: THIẾT KẾ MẠNG CÔNG NGHIỆP VÀ SCADA**

### **6.1 Các bước thiết kế mạng công nghiệp**

Nhiều tài liệu ứng dụng mạng công nghiệp được nghiên cứu và triển khai [9], [28], [30], [54], trong cuốn sách này tác giả muốn cung cấp cho bạn đọc các bước cơ bản để xây dựng mạng công nghiệp bằng phần mềm WinCC, từ đó có thể đưa vào ứng dụng cụ thể trong công việc.

#### **6.1.1 Xác định yêu cầu hệ thống**

Từ yêu cầu hệ thống đặt ra, tác giả nắm rõ nguyên lý vận hành của hệ thống, phân tích từng chức năng thành phần mà chủ đầu tư yêu cầu. Khảo sát các điều kiện thực tế về hệ thống cần thiết kế như thực địa, không gian, cơ sở hạ tầng và nhu cầu sử dụng.

#### **6.1.2 Phương án thiết kế lựa chọn cấu hình mạng**

Đề xuất 2 phương án trở lên, phân tích từng phương án về mặt kinh tế và kỹ thuật. Tính toán giá thành các phương án và giải trình cho chủ đầu tư dự án. Lựa chọn và chốt phương án cho phù hợp với tình hình thực tế và theo yêu cầu của chủ đầu tư.

#### **6.1.3 Xây dựng vào/ra(I/O)**

Xem xét hệ thống mạng là một tổng thể khối thống nhất có các đầu vào và đầu ra, xác định từng đầu vào và từng đầu ra một cách cụ thể về số lượng, loại tín hiệu số, tương tự, rời rạc, liên tục cho đối tượng mức điện áp, dòng điện, phương pháp hiển thị...

#### **6.1.4 Lựa chọn thiết bị mạng**

Từ sơ đồ cấu trúc, ta xác định các thiết bị, thành phần có trong hệ thống mạng bảo đảm rằng các thiết bị là đồng bộ và có trên thị trường thương mại. Liệt kê danh mục thiết bị theo dạng bảng hoặc theo thứ tự cấp mạng. Căn cứ trên I/O để xác định loại đầu vào và loại đầu ra, thiết bị, giảm cấp TU, TI, chuyển đổi Transducer...

#### **6.1.5 Xây dựng thuật toán**

Thuật toán được xây dựng dựa trên nguyên lý và I/O, việc xây dựng thuật toán dựa trên nguyên tắc chung của “tin học” bao gồm khối bắt đầu, kết thúc, khối điều kiện, khối chấp hành, khối đầu vào, khối nhập liệu, khối đọc...

#### **6.1.6 Viết chương trình**

Căn cứ trên thiết bị lựa chọn, nhà thiết kế viết chương trình dựa trên các tiêu chuẩn IEC1183 ở các dạng LAD, STL, FBD, IL, C

### 6.1.7 Kiểm tra đánh giá kết quả

Tiến hành mô phỏng, đánh giá từng kịch bản có thể xảy ra cho chương trình, phân tích từng kịch bản và nhận xét về tính kỹ thuật của hệ thống.

## 6.2 Thiết kế mạng MPI

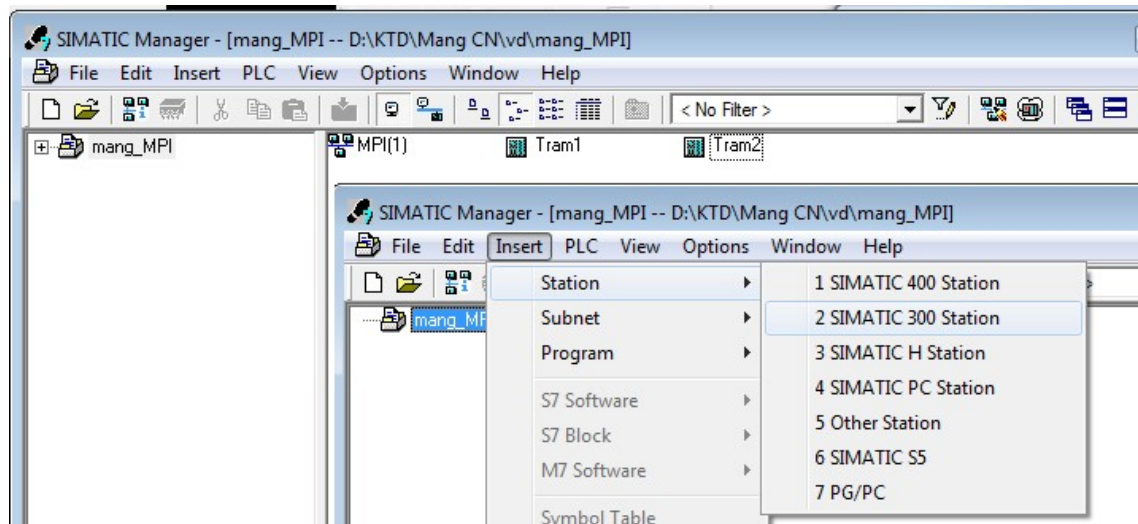
### 6.2.1 Phần mềm thiết kế mạng

Một thiết bị phần cứng kết nối với PC cũng có thể xem là một lớp mạng, giao thức truyền thông giữa chúng được gọi là MPI. Các bước khởi tạo một mạng MPI như sau [28]:

Khởi tạo Dự án và thiết lập giao diện

- Chọn mục file/ new/ đặt tên cho dự án (project) ví dụ đặt tên mang\_MPI, mặc định tất cả các thiết bị S7-300 trở lên đều có hỗ trợ mạng MPI nên chúng ta không cần chèn vào dự án.

- Chèn trạm S7-300 vào mạng MPI theo số trạm cần sử dụng (Hình 6.1), cụ thể ở đây chèn 2 trạm S7-300.



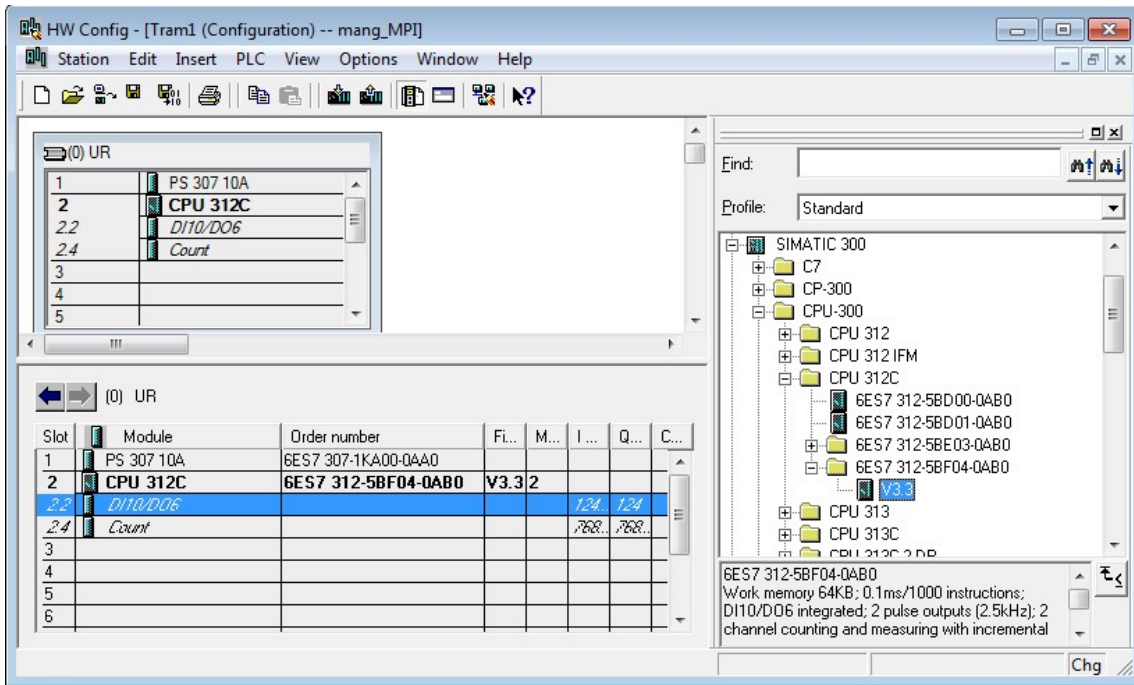
Hình 6.1: Thiết lập giao diện cho mạng MPI

### 6.2.2 Thiết lập cấu hình phần cứng cho các trạm

- Nhấp đúp vào từng trạm, đúp hardware để mở cửa sổ cấu hình “HW Config”. Từ cửa sổ cấu hình này chọn thư mục Simatic 300 thư viện bên phải lần lượt Simatic 300/ Rack 300/ Rail để thiết lập Rail cho các thiết bị cần gắn lên Rail trở thành một trạm. Mặc định các Rail là slot 1..11, trong đó slot 1 dành cho nguồn PS-300, slot 2 dành cho CPU -300, slot 3 trở đi là các modul mở rộng hoặc I/O.

- Tương tự, như đặt Slot ta tiến hành đặt toàn nguồn, CPU, I/O cần thiết, kết quả thiết lập cấu hình trên. Trường hợp này chọn CPU 312C v3.3, có tích hợp sẵn

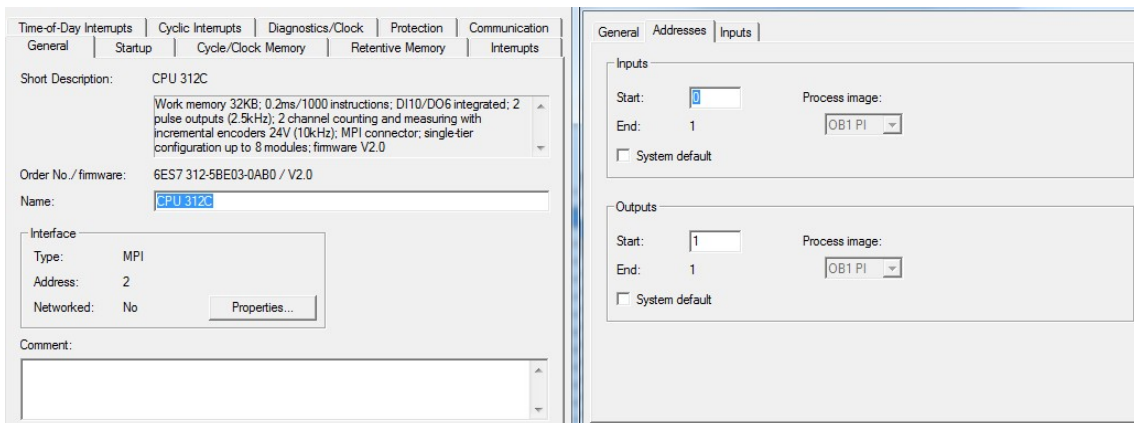
DI10/DO6, địa chỉ mặc định 124 và Counter có địa chỉ 768. Một hệ thống phân cứng PLC S7-300 trở lên cần phải có cấu hình phần cứng giống hoàn toàn so với thực tế thì hệ thống nó mới chạy được [55].



Hình 6.2: Cấu hình phần cứng cho trạm

- Đối với CPU trạm loại giao tiếp mặc định MPI, địa chỉ mạng là 2 (có thể chọn tùy ý từ 2 trở đi, địa chỉ 0 dành cho Host PC, 1 dành cho HMI).

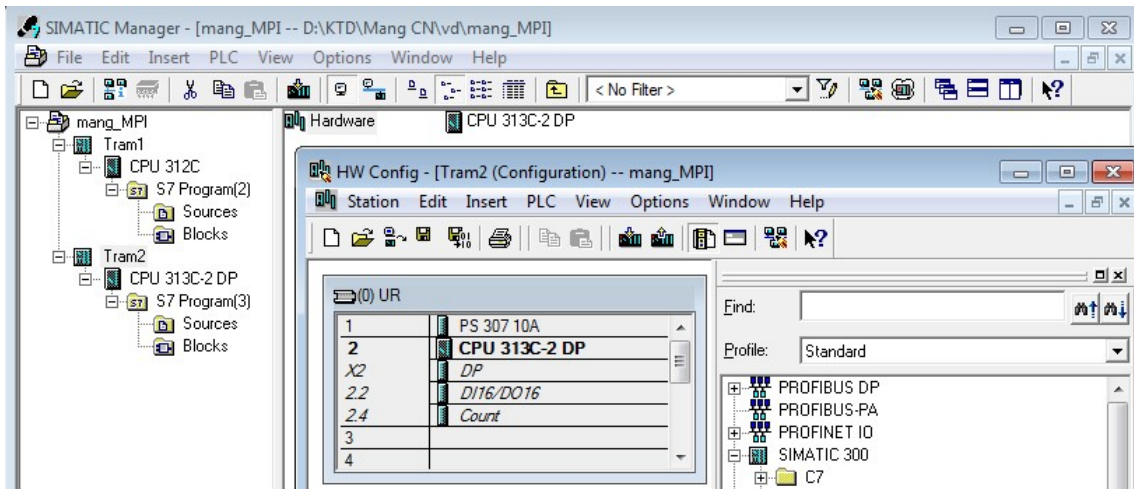
- Nhấp đúp vào CPU thay đổi networked từ No → MPI tốc độ 187.5kbps và thay đổi địa chỉ I/O mặc định từ 124/125 sang 0/1.



Hình 6.3: Khai báo phần cứng và cấu hình địa chỉ

- Tương tự, ta thực hiện cho trạm số 2 với địa chỉ mạng 3, thay đổi cấu hình mặc định bằng mạng MPI, tốc độ 187.5kbps, địa chỉ I/O 0/1. Trong đó, CPU của trạm 2 lựa

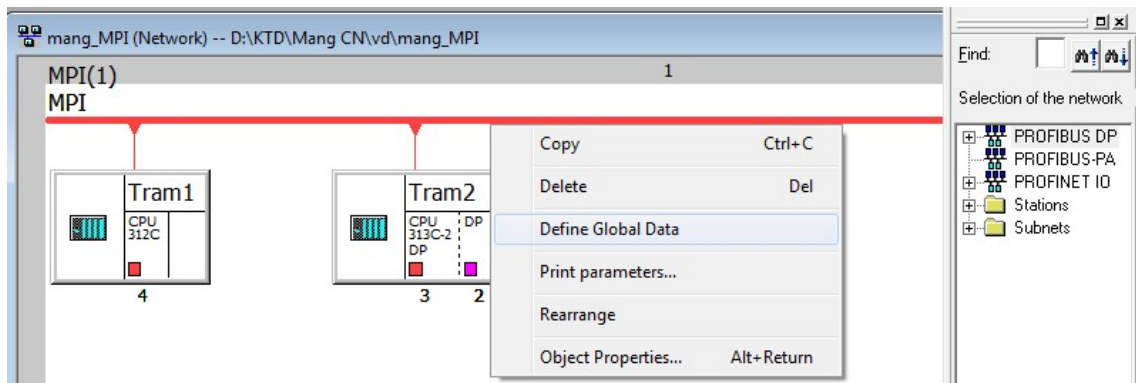
chọn 313C-2DP có hỗ trợ mạng Profibus nhưng trong trường hợp này không sử dụng mạng này. Như vậy, ta hoàn thành cài đặt cấu hình phần cứng cho các trạm con.



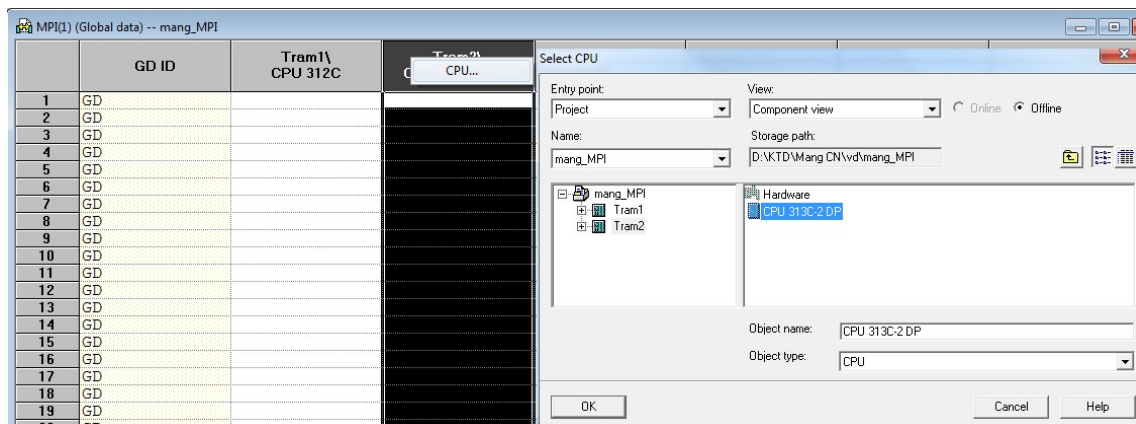
Hình 6.4: Cấu hình phần cứng cho trạm 2

### 6.2.3 Thiết lập giao diện mạng

- Mở giao diện mạng bằng cách nhấp đúp vào biểu tượng mạng MPI trên cửa của dự án, nhấp chuột phải chọn mục Define global data.



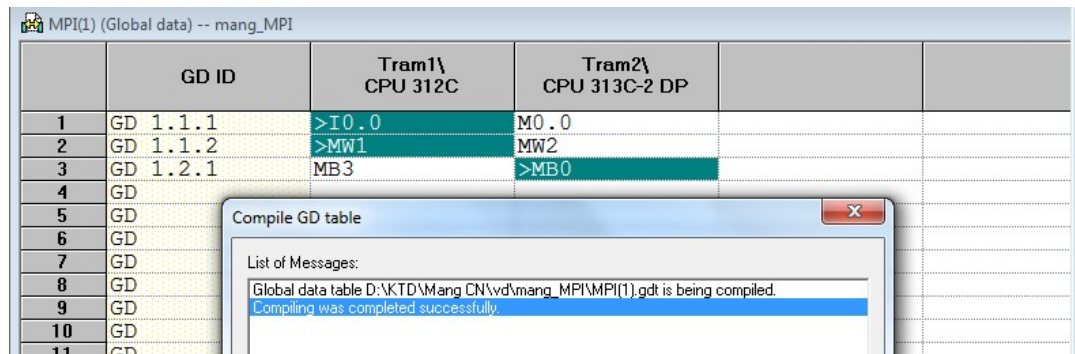
Hình 6.5: Cấu hình mạng MPI



Hình 6.6: Cửa sổ truyền nhận dữ liệu giữa các CPU

Sau khi xuất hiện giao diện Global data, nhấp chuột phải vào Menu thanh ngang trên cho CPU... hiện ra cửa sổ lựa chọn CPU tương ứng mỗi cột là một CPU ở đây có 2 CPU chọn cho 2 cột như Hình 6.6:

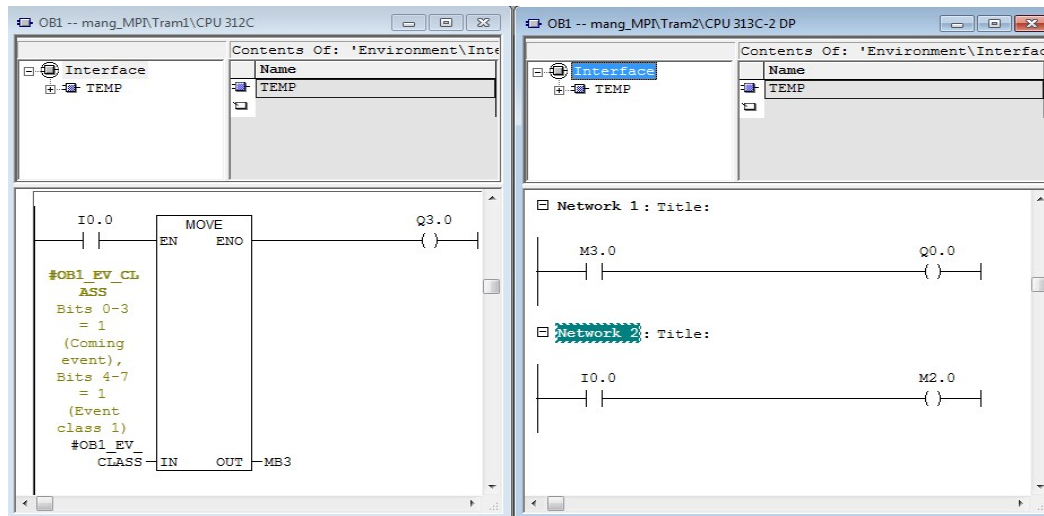
Bảng Data mặc định là nhận, vì vậy ta chọn chế độ truyền bằng cách nhấp chuột phải chọn Sender (gửi). Các dữ liệu truyền thông có thể Bit, Byte, Word, Dword, các dữ liệu khai báo trong bảng không được trung địa chỉ, không được đang xen vùng nhớ. Sử dụng biến trung gian M để làm biến vùng nhận. Tiến hành biên dịch không lỗi, các địa chỉ phải đặt giống với ban đầu thiết lập địa chỉ I/O phần cứng của CPU từng trạm.



Hình 6.7: Thiết lập dữ liệu truyền nhận cho mạng MPI

#### 6.2.4 Lập trình cho hệ thống

Lựa chọn khối lập trình chính OB1 để thực hiện chương trình giống như các chương trình logic S7-300.



Hình 6.8: Giao diện lập trình cho CPU mạng MPI

Sau khi lập trình lưu toàn bộ hệ thống biên dịch “compiler” và nạp cấu hình xuống PLC thực tế đầu nối dây qua RS485 của các CPU được hỗ trợ có sẵn trong tất cả các PLC S7 -300 trở lên (không cần modul mở rộng).



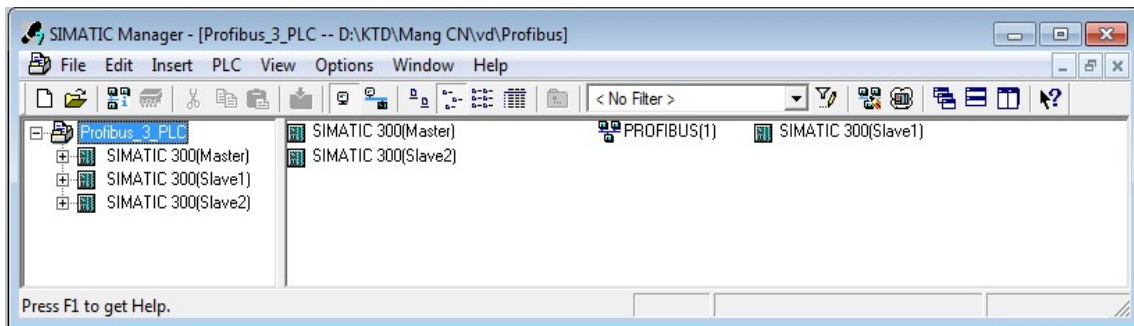
### 6.3 Mạng Profibus

Tương tự như mạng MPI, mạng Profibus được xây dựng dựa trên rất nhiều phần mềm khác nhau của các hãng như Siemens, ABB, Albenroll... Sau đây các bước cơ bản để thiết kế mạng Profibus dựa trên nền Step 7 của Siemens [40].

#### 6.3.1 Tạo giao diện truyền thông (ví dụ mạng Profibus)

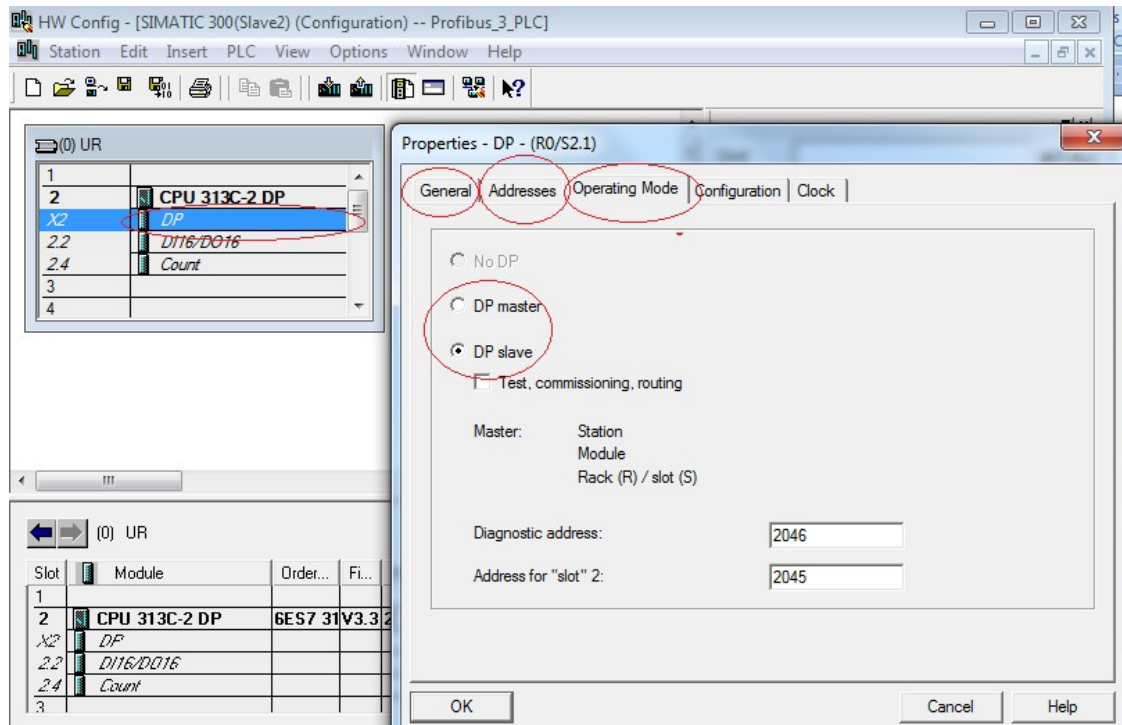
- Tạo một dự án (Project) đặt tên dự án, chèn số trạm mong muốn bằng cách Insert/ Station/ Simatic S7-300 hoặc 400. Ở phần này chọn số trạm tùy thích và chọn trạm cho phù hợp yêu cầu bài toán cũng như phần cứng.

- Tương tự chèn mạng gồm MPI, Profibus, Ethernet... bằng cách Insert/ subnet/ Profibus.



Hình 6.9: Giao diện cho mạng truyền thông Profibus cho 3 trạm S7-300

#### 6.3.2 Cấu hình truyền thông cho từng trạm PLC

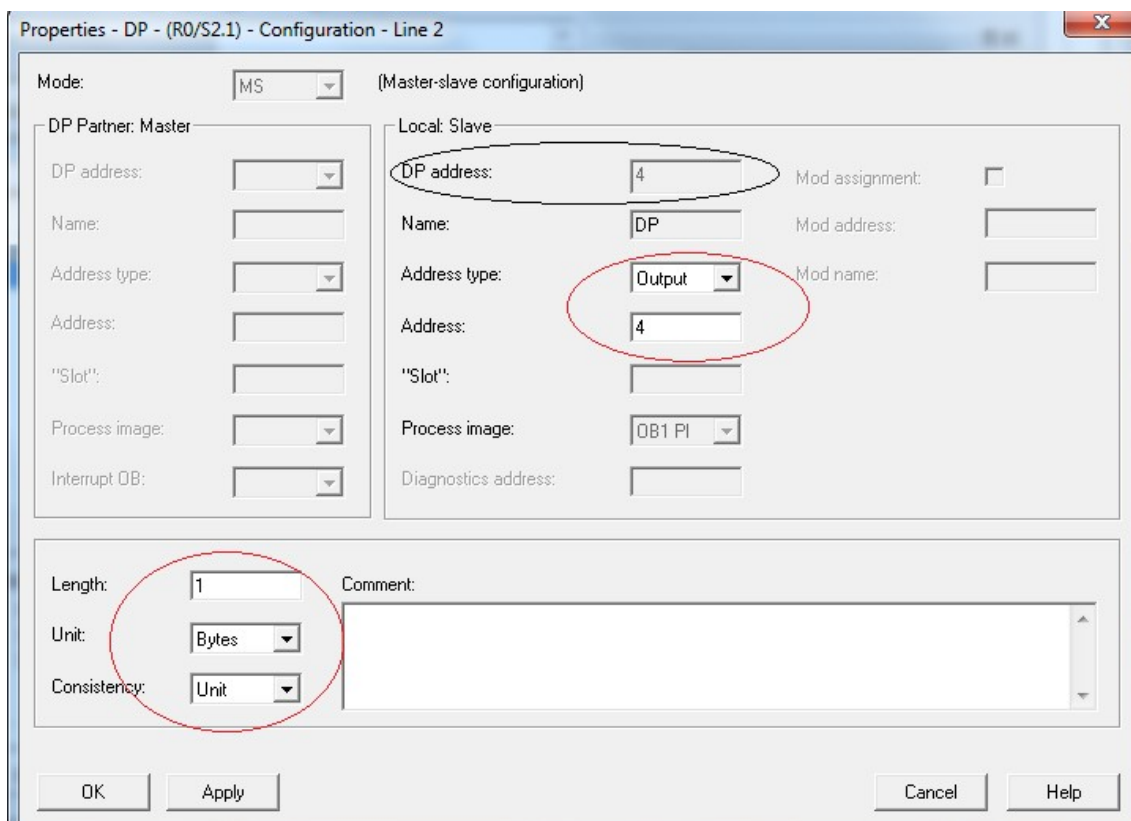


Hình 6.10: Thiết lập cấu hình phần cứng cho trạm Slave 2



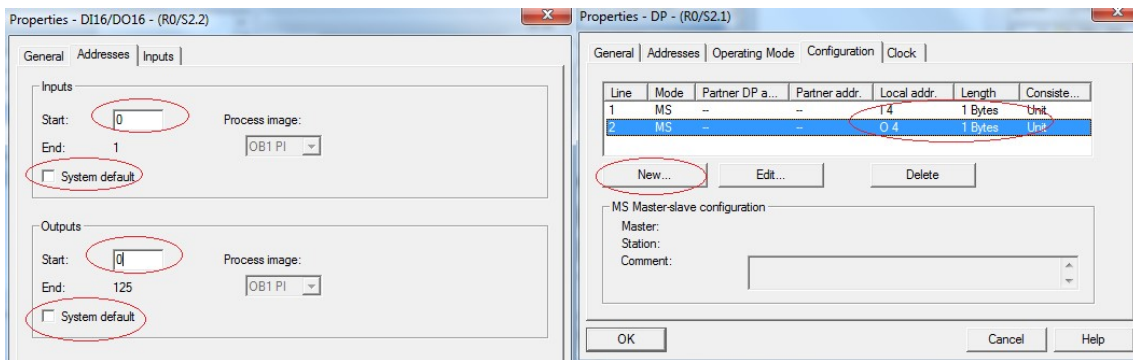
Đầu tiên thiết lập trạm tớ (slave) trước: nhấp đúp vào Hardware của trạm tớ trước, khai báo Rack S7-300; lựa chọn CPU phù hợp, nếu mạng Profibus DP thì chọn CPU có DP như CPU 313C-2DP cho trạm tớ Slave2; chọn Subnet Profibus 1.5Mbps, Address 4. Nhấp vào Rack X2 DP để thiết lập mạng DP cho Slave 2 như Hình 6.10 đặt tên DP Slave 2, chọn thuộc tính DP slave (mặc định DP master).

Vào Tab Configuration để thiết lập địa chỉ I/O giữa Master và Slave, bằng cách vào New... (mặc định address 0) là tùy ý theo số lượng I/O của từng trạm, trường hợp này chọn Address Input 4 trùng với địa chỉ mạng DP (tức là cấu hình 4.4.x) . Tương tự thiết lập cho địa chỉ Output cũng 4; cũng như thay đổi dữ liệu truyền thông có chiều dài Length 1 byte.



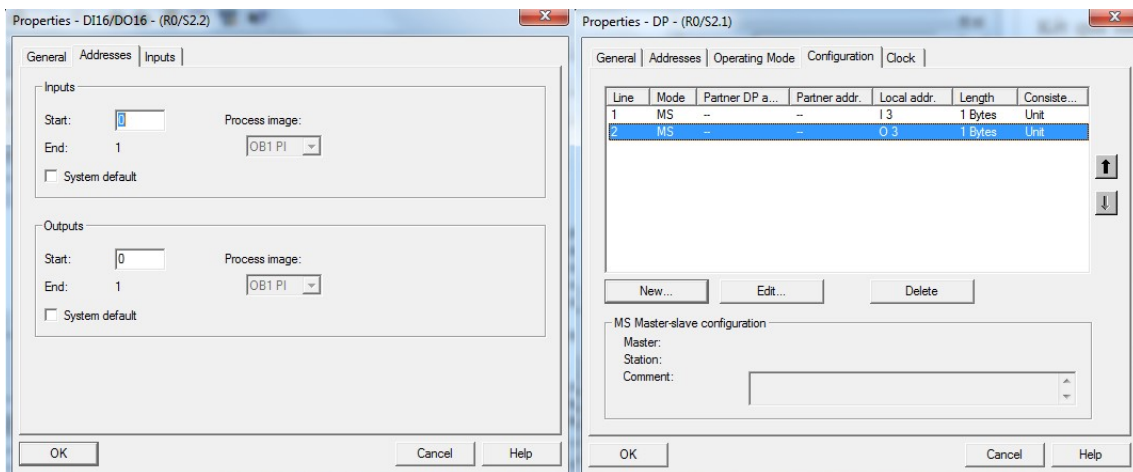
Hình 6.11: Cấu hình giao tiếp I/O của trạm Slave với Master

Kết quả sau khi thiết lập cấu hình cho địa chỉ cấp mạng DP 4 và địa chỉ I/O cho trạm Slave 2 như Hình 6.12.



Hình 6.12: Kết quả thiết lập cấu hình trạm Slave 2

Thông thường người ta bỏ mặc định của địa chỉ I/O trên CPU và thay bằng địa chỉ phù hợp với phần cứng trên CPU thường địa chỉ 0 và lưu & compiler. Tương tự, ta thiết lập cho trạm Slave 1 với địa chỉ mạng 3, địa chỉ I/O cũng 3 và kết quả thể hiện trên Hình 6.13



Hình 6.13: Kết quả thiết lập cấu hình trạm Slave 1

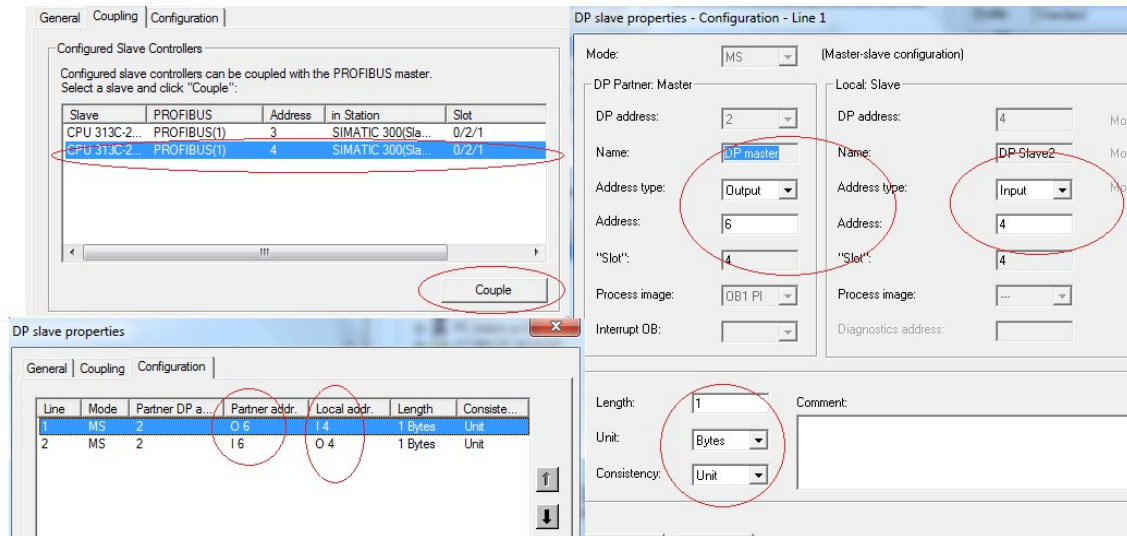
- Và cuối cùng làm cho trạm chủ (Master), sử dụng CPU 314 DP v3.3; tên DP Master, địa chỉ mạng DP 2. Vì đây là trạm chủ nên ta không thiết lập địa chỉ I/O cho nó từ New... thay vào đó ta thiết lập CPU trên mạng Profibus Matster ở bước 3.

### Bước 3: Thiết lập CPU giao tiếp mạng Profibus

- Sau khi thiết lập CPU và các địa chỉ cấp mạng, ta tiến hành thiết lập CPU mạng, bằng cách vào mục Profibus DP/ configured Station/ CPU 31x, kéo và thả vào đường mạng khi xuất hiện dấu +/- chọn CPU của trạm Slave 2/ couple.

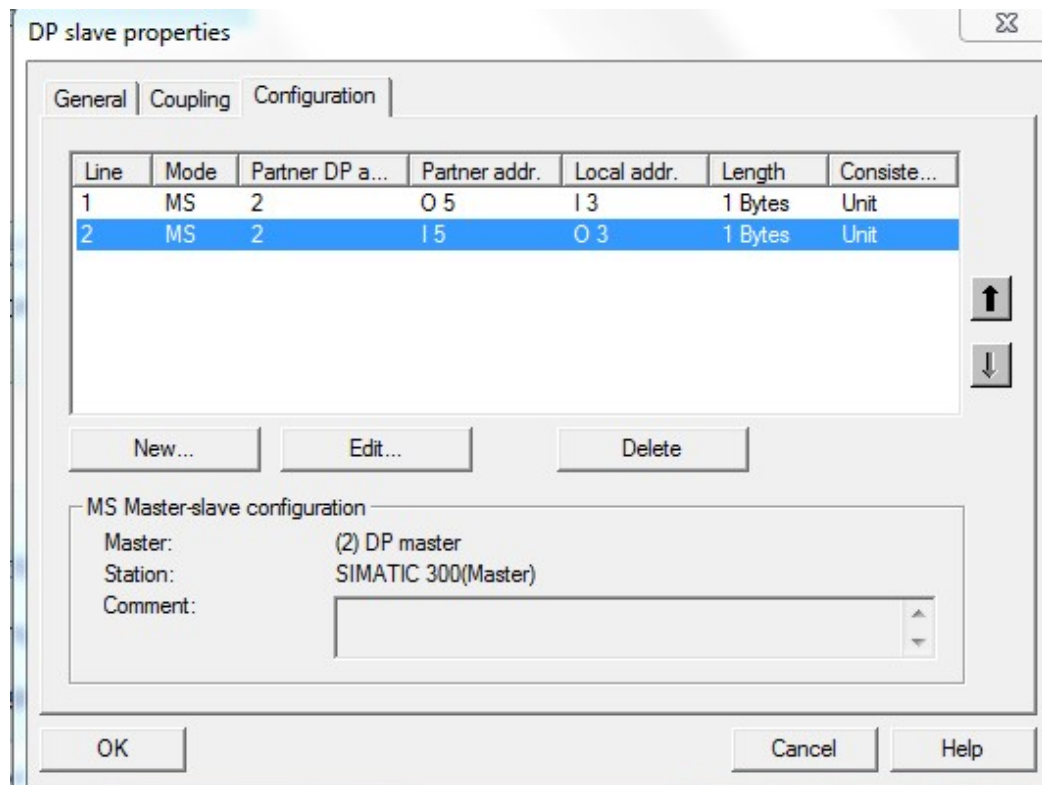
- Sang Tab configuration lần lượt chọn địa chỉ giao tiếp giữa Slave 2 với Master ở lần lượt line 1 và line 2 ứng với input và output. Nếu DP slave 2 là input thì Master là output địa chỉ có thể chọn tùy ý ở Master nhưng khác với các Slave ban đầu. Vì các

CPU nhiều I/O nên ta chọn địa chỉ 6 cho không trùng lặp các địa chỉ I/O khác. Địa chỉ I/O master là 6.x địa chỉ slave 2 là 4.x kể cả input và output.



Hình 6.14: Cấu hình địa chỉ I/O cho Master

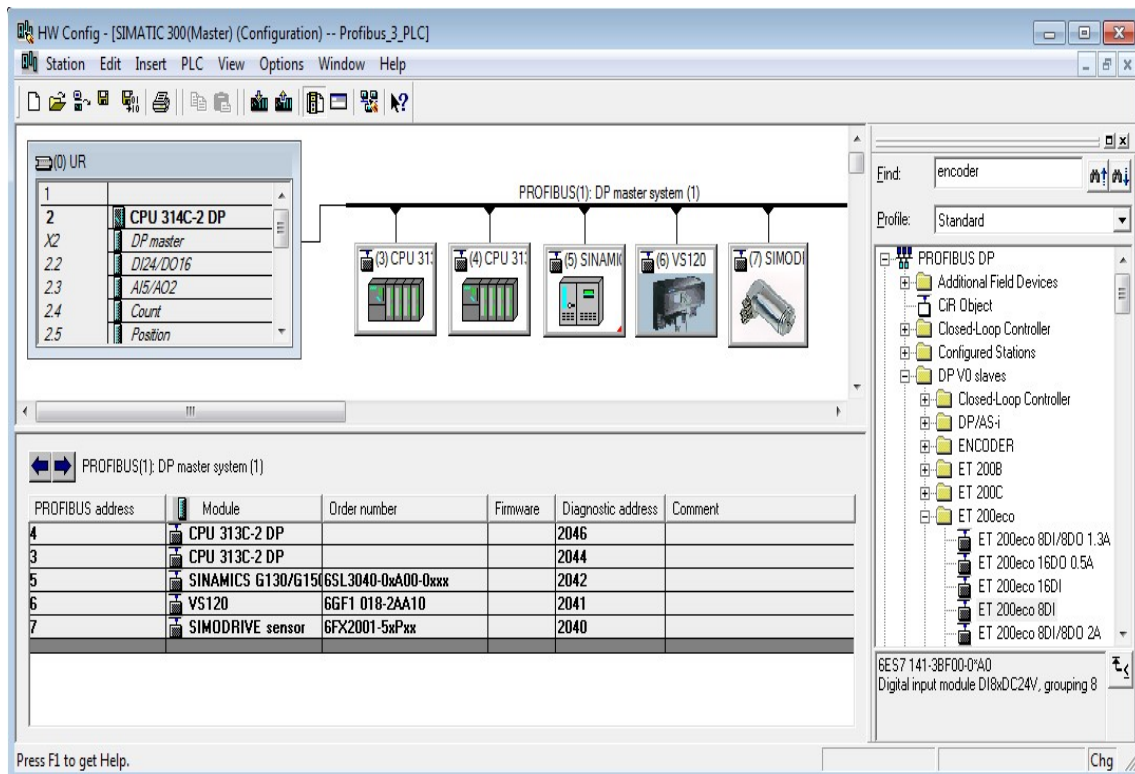
- Tương tự, ta tiến hành thiết lập giao tiếp CPU thứ 2 cho Slave 1 (và có bao nhiêu Slave bấy nhiêu CPU được thiết lập giao tiếp địa chỉ I/O cho mạng Profibus. Địa chỉ I/O của Master là 5.x khi giao tiếp với Slave 1. Kết quả như Hình 6.15



Hình 6.15: Kết quả thiết lập địa chỉ giao tiếp Master với Slave 1

- Thông thường người dùng chèn một số khối OB vào có chức năng lập trình mạng; lưu và compiler các kết quả thể hiện Hình 6.16.

- Chèn một số thiết bị có thể kết nối trực tiếp với mạng profibus như biến tần công suất lớn cho các động cơ >100kW. Cụ thể, vào thư mục Profibus DP/ Sinamics/ Sinamic G130, kéo thả vào đường dây mạng, chọn mạng, chọn địa chỉ phù hợp khi có thông báo. Thông thường địa chỉ 0 dành cho Host PC, 1 là mạng MPI vì thế các địa chỉ từ 2 trở đi ta có thể chọn tùy ý nhưng không trùng nhau. Các địa chỉ I/O có thể trùng với địa chỉ mạng. Tương tự, ta có thể kết nối Encoder, Sensor và nhiều thiết bị khác.

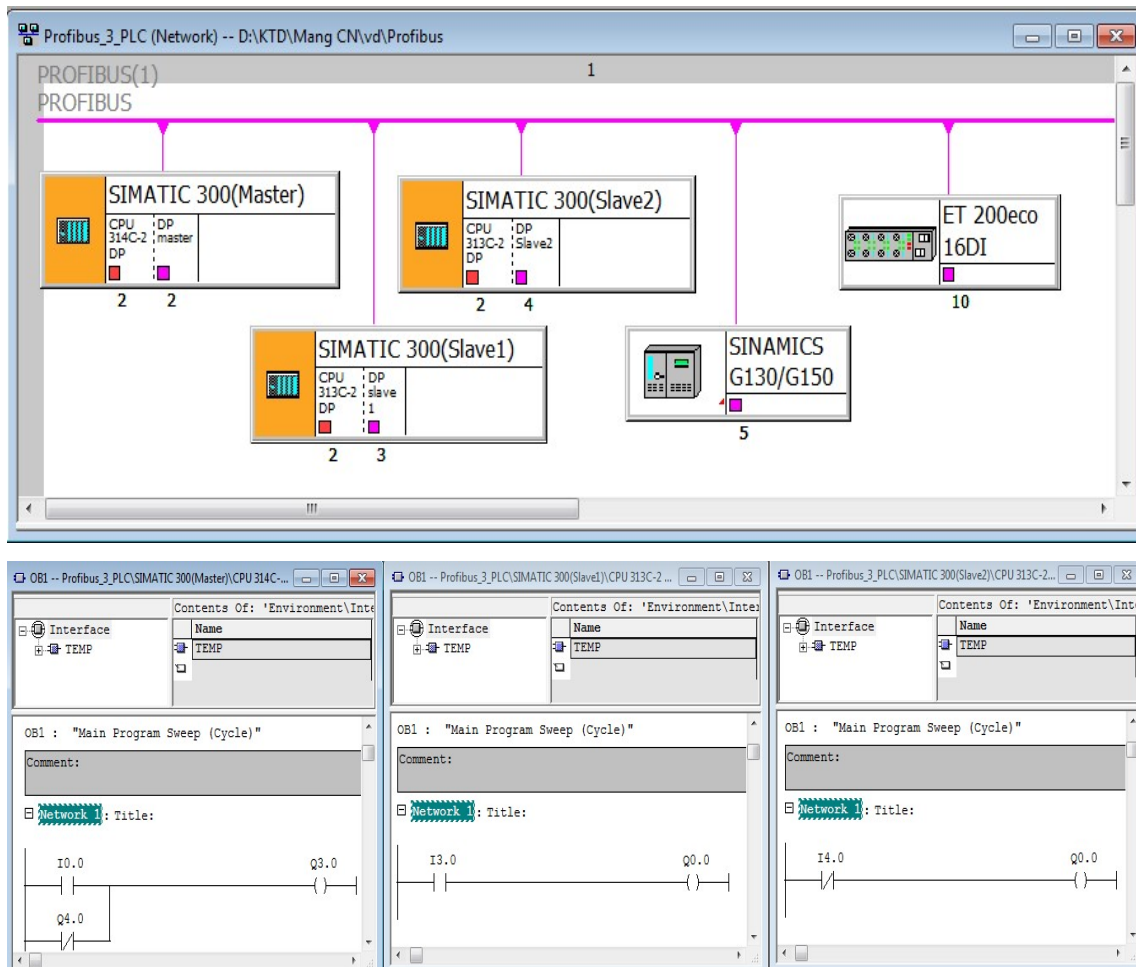


Hình 6.16: Kết quả thiết lập CPU giao tiếp và các thiết bị mạng

### 6.3.3 Lập trình

- Sau khi chèn một số khối cần thiết ngoài OB1 ta tiến hành lập trình như các chương trình ứng dụng S7-300, tuy nhiên cần chú ý các địa chỉ đã định dạng trong mạng Profibus.

Địa chỉ vào bên này (địa chỉ 5) là ra bên kia, địa chỉ bắt tay giữa các CPU với nhau, khi đó muốn truy xuất ra giá trị vật lý cần xác định địa chỉ của CPU thực trên thiết bị.



Hình 6.17: Chương trình lập trình cho các trạm trong mạng Profibus

## 6.4 Thiết kế mạng truyền thông Ethernet qua Step 7

Mạng Ethernet trong công nghiệp có cấu hình giống với mạng Internet mà chúng ta hay dùng chuẩn truyền thông Rj45 [18], [22].

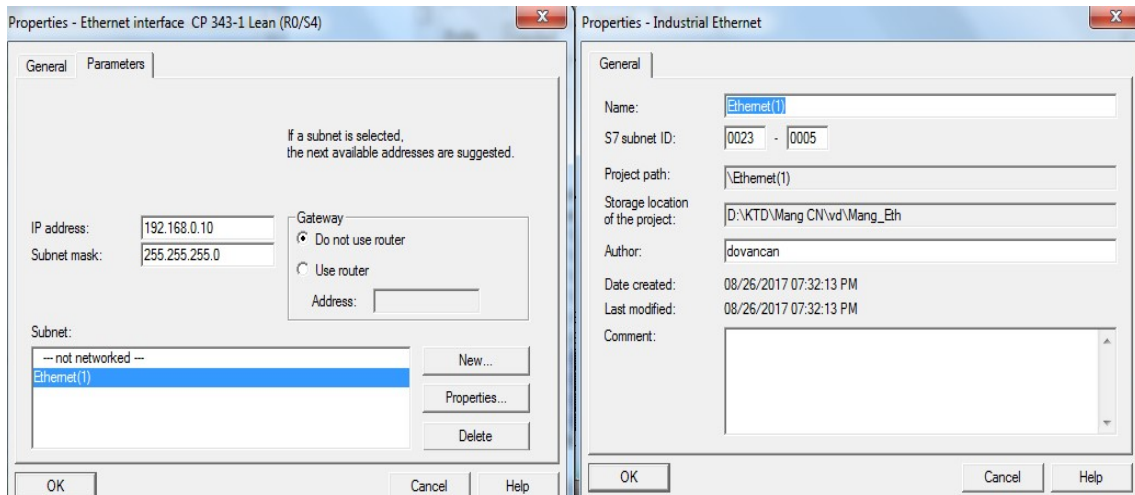
### 6.4.1 Cấu hình phần cứng

Tương tự như mạng Profibus ta tiến hành chèn trạm S7-300 vào dự án có tên Mang\_Ethernet S7, trong cấu hình phần cứng S7-300 cần có modul mở rộng có thể truyền thông được mạng Ethernet tại Slot4.

Để chọn modul mở rộng kết nối Ethernet, ta vào Simatic 300/ CP-300/ Industrial Ethernet/ CP343-1 Lean chọn version phù hợp.

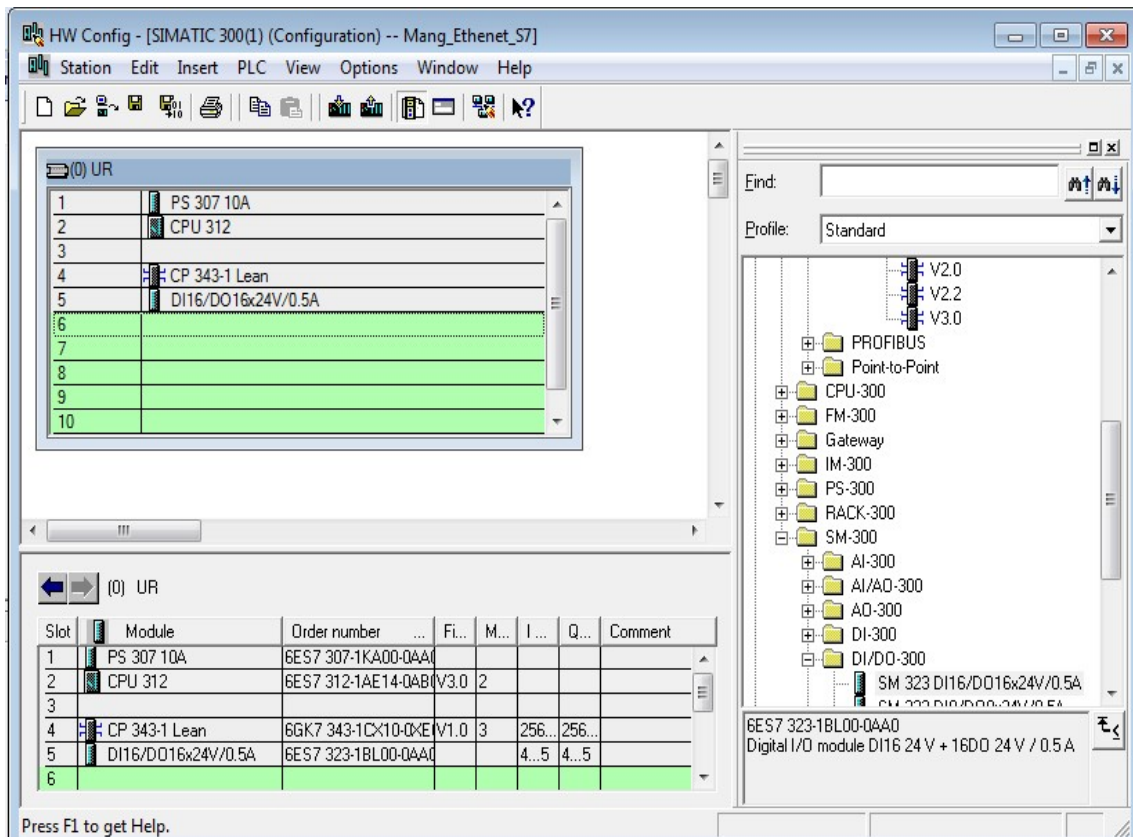
- Thiết lập địa chỉ IP cho trạm tương ứng từ cửa sổ Properties - Ethernet interface, chọn New, đặt tên mạng OK, quay lại cửa sổ ban đầu đặt địa chỉ IP (đặt 192.169.0.10) mỗi một trạm có một địa chỉ IP riêng, địa chỉ Subnet mask mặc định 255.255.255.0.





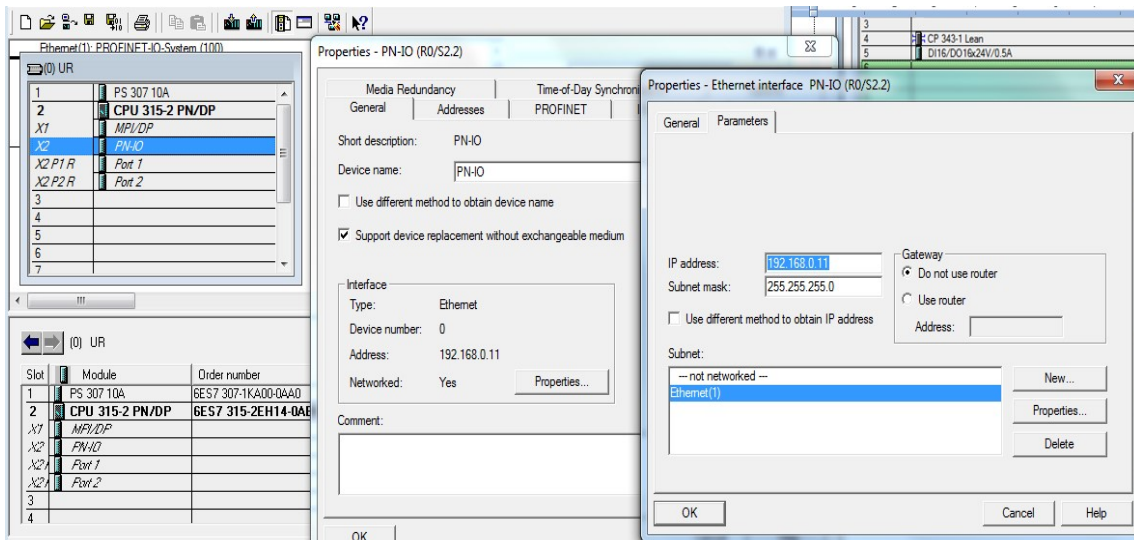
Hình 6.18: Cấu hình địa chỉ IP cho trạm

Thiết lập địa chỉ I/O cho CPU (vì CPU này không có I/O tích hợp sẵn) bắt đầu từ slot5 là DI16/DO16x24V/0.5A trong thư mục SM-300.



Hình 6.19: Kết quả cấu hình phần cứng cho trạm Ethenet

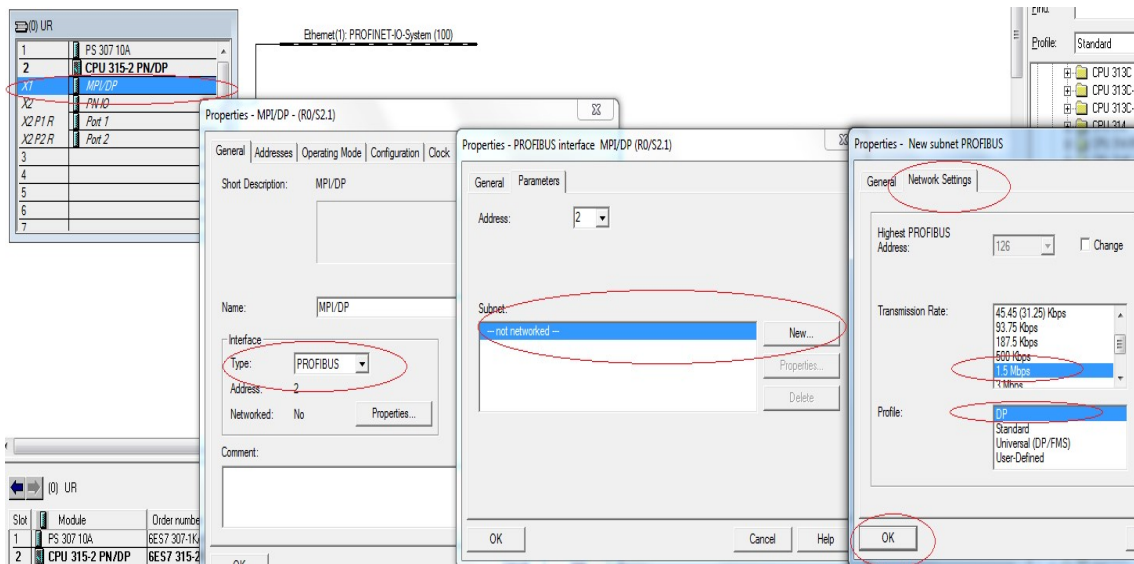
- Tương tự, ta tiến hành cho trạm thứ 2, chọn CPU 315-2PN/DP v3.2 hỗ trợ Finet và Profibus. Chọn địa chỉ IP 192.168.0.11, OK



Hình 6.20: Kết quả cấu hình trạm thứ 2 cho mạng Ethernet

#### 6.4.2 Thiết lập cấu hình mạng

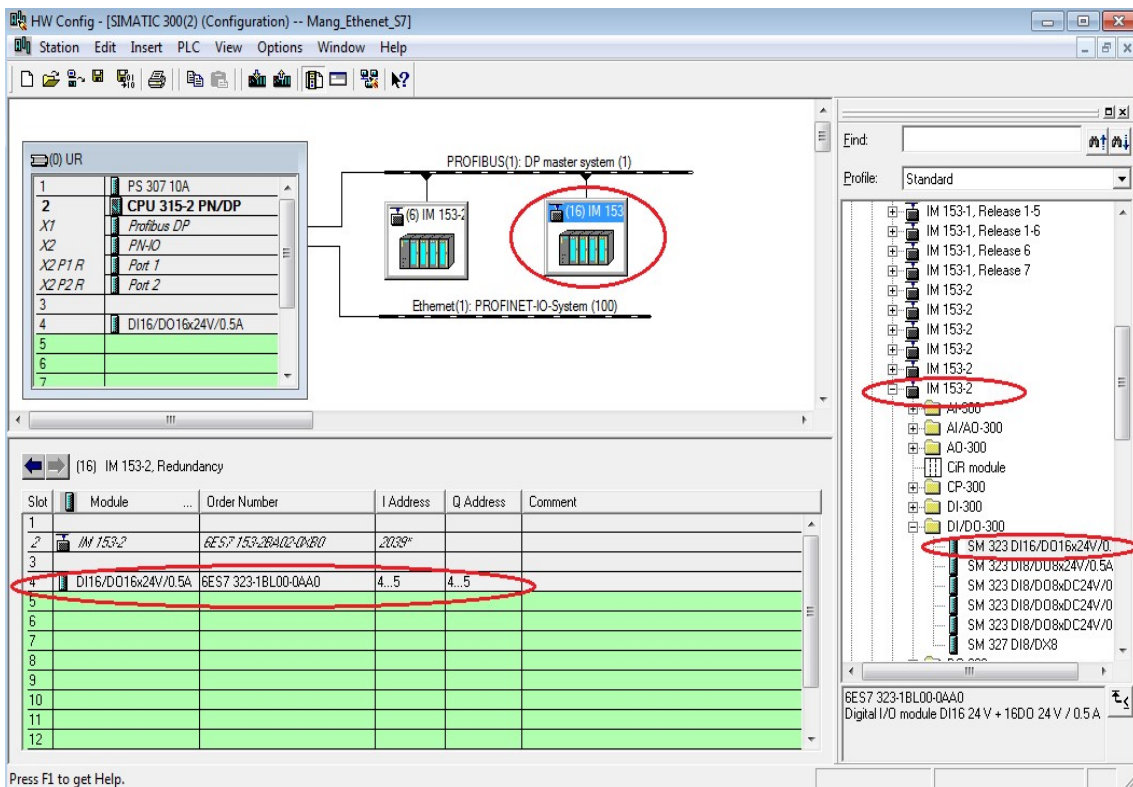
- Cấu hình đoạn mạng Profibus, bằng cách đúp vào Slot X1 MPI/DP (mặc định mạng MPI) tại ô Type ta chọn mạng Profibus/ chọn new/ tab Network settings/ chọn tốc độ truyền 1.5Mbps và Profile là loại DP



Hình 6.21: Cấu hình mạng Profibus trên trạm số 2

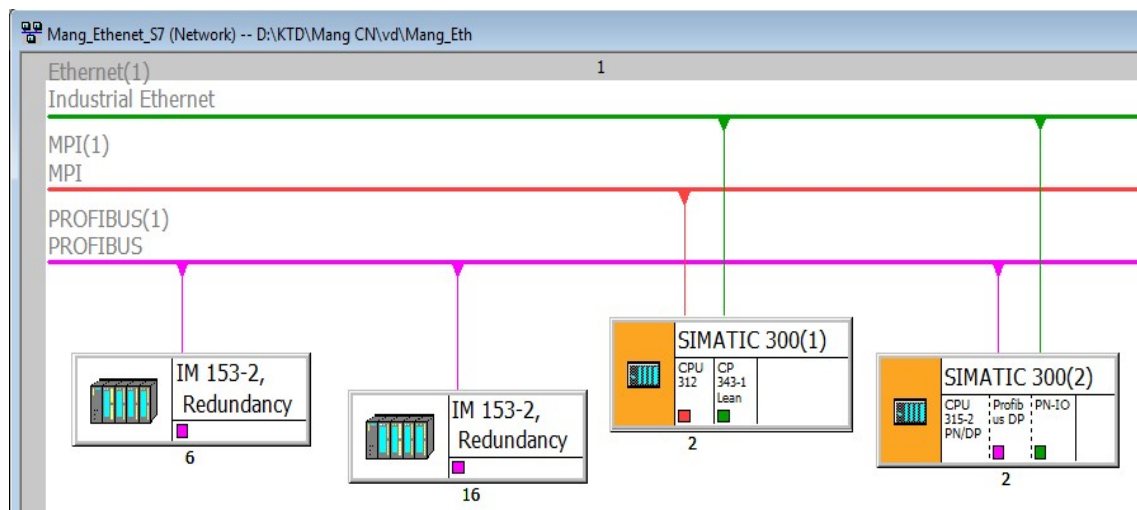
- Vào thư mục Profibus DP/ ET 200M/ IM 153-2 kéo thả vào đường mạng Profibus, chọn địa chỉ trong trường hợp này chọn địa chỉ là 9, OK.

- Tại Slot 4 chèn I/O cho thiết bị IM 153-2/ DI/DO-300/ SM 323 DI16/DO16x24V chúng ta có thể đặt nhiều modul IM 153-2 trong mạng profibus địa chỉ cái thứ 2 là 16. Mỗi một modul IM 153-2 tương ứng chèn vào các I/O của chính nó.



Hình 6.22: Cấu hình I/O cho hệ thống Profibus của trạm số 2

Kết quả của hệ thống gồm 2 CPU (trạm) liên kết nhau qua mạng Ethernet với IP 192.168.0.10. và 192.168.0.11, đối với CPU1 kết nối mạng tự có MPI địa chỉ 2 còn CPU thứ 2 được kết nối với mạng Profibus ở địa chỉ 2 với các I/O thông qua thiết bị I/O IM 153-2 có địa chỉ mạng lần lượt là 6, 16. Và ta cấu hình mạng MPI cho trạm 1 (CPU1) đã tích hợp sẵn bằng cách đúp vào CPU 312 chọn Properties chọn mạng MPI, chọn tốc độ 187.5kbps địa chỉ 2 kết quả thiết kế cấu hình phần cứng mạng Hình 6.23



Hình 6.23: Kết quả cấu hình mạng Ethernet cho hai trạm S7-300



### **6.4.3 Chọn card theo cơ chế giao tiếp TCP/IP**

- Vì download chương trình xuống PLC thông qua giao thức TCP/IP nên chúng ta phải thiết lập card giao tiếp LAN. Vào mục Option/ Set PG/PC interface, thiết lập địa chỉ IP và download chương trình cho từng CPU.

## **6.5 Câu hỏi ôn tập chương**

*Câu 6.1: Khai báo gì quan trọng trong việc xây dựng mạng công nghiệp?*

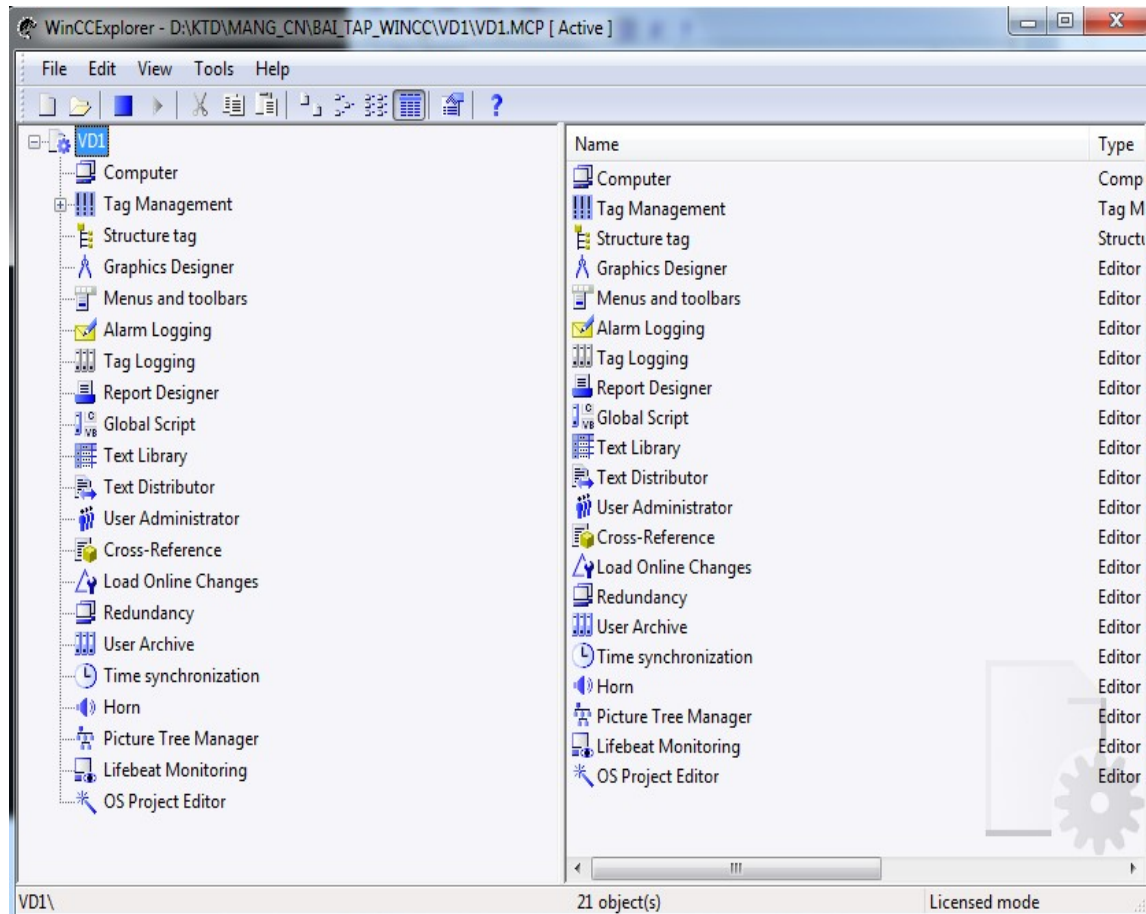
*Câu 6.2: Thiết kế một hệ thống mạng công nghiệp Profibus?*

*Câu 6.3: Thiết kế một hệ thống mạng công nghiệp chuẩn Ethernet?*

## CHƯƠNG 7: SCADA NHÀ MÁY CÔNG NGHIỆP

### 7.1 Hướng dẫn sử dụng Win CC

#### 7.1.1 Tổng quan WinCC



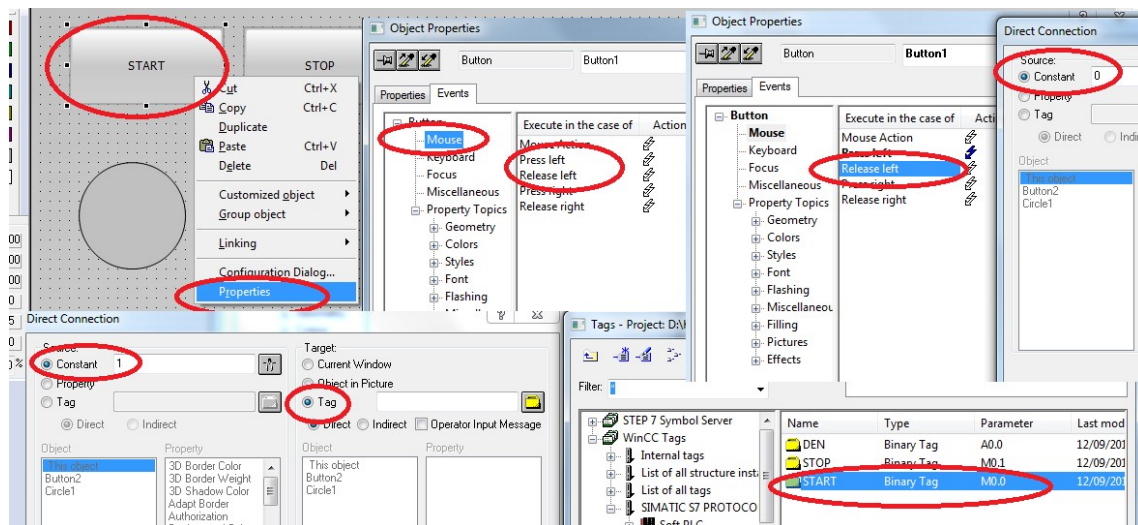
Hình 7.1: Giao diện hệ thống phần mềm SCADA WinCC

- Thiết kế giao diện giám sát trong Graphics Designer
- Quản lý biến Tag Management
- Cảnh báo Tag Logging
- Quản lý người dung User Administrator

#### 7.1.2 Thiết lập thuộc tính

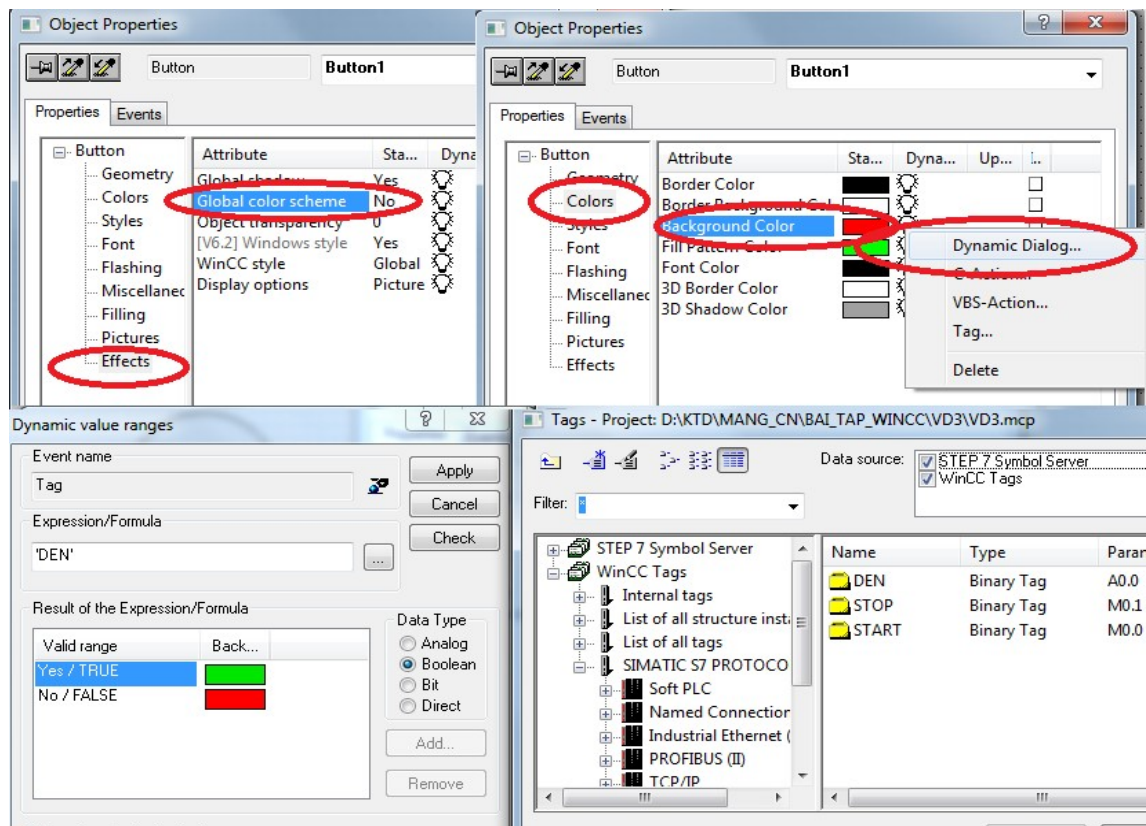
Nút nhấn Button:

Click chuột phải Properties/ Events/ Mouse chọn chế độ bán chuột (Press left) và nhả chuột (Release left). Click đúp vào chế độ chuột để vào thuộc tính constant nhập “1” đối với Press left và “0” Release left, chi tiết trong tài liệu [28].



Hình 7.2: Thiết lập thuộc tính nút bấm

Đổi màu của nút nhấn bằng cách Click chuột phải vào Properties/ Effects/ Global/ No bỏ thuộc tính mặc định, chuyển sang mục Colors/ Background Color/ chọn màu. Nếu muốn màu nền thay đổi theo chuyển động thuộc tính lập trình thì Click chuột phải cạnh Background Color/ chọn Dynamic/ ... chèn Tag vào Expression (Tag muốn thay đổi theo), tại mục Data Type chọn Boolean, chọn màu, xanh cho Yes -"1" và đỏ -"0" và thời gian tác động 250ms.



Hình 7.3: Cài đặt thuộc tính nút bấm

### 7.1.3 Giao tiếp biến (Tag) nội

#### a) Kiểu dữ liệu trong WinCC

Có nhiều kiểu dữ liệu trong WinCC, ở đây giới thiệu 3 kiểu cơ bản: Bit, Integer, Real [42], [55].

+ Bit biểu diễn trạng thái số 0/1, như cảm biến On/Off, trạng thái đóng/mở của các thiết bị điện, nút ấn, cảm biến, sw, công tắc tơ ví dụ M0.0, M0.1...

Đối với bit có các vùng nhớ:

+ Integer: số nguyên 2 byte, 16 bit thường tính thời gian, đếm sản phẩm, đếm số lượng ở dạng số nguyên từ 0-65.535 ví dụ MW0, MW2, MW4...

+ Real: dạng số thực có dấu phẩy, biểu diễn số thực như tương tự, dòng điện, điện áp, áp suất, nhiệt độ ví dụ MD0, MD4, MD8...

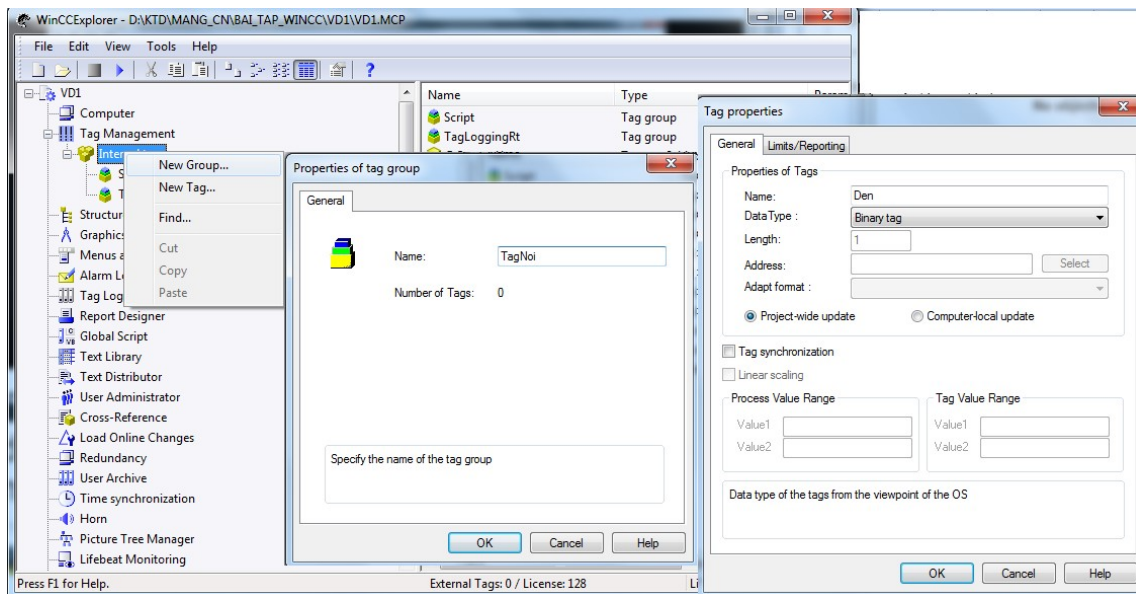
#### b) Tag (biến) trong WinCC

Tag là biến dùng kết nối WinCC với giao diện hoặc với thiết bị thực PLC hay HMI... có 2 loại Tag nội và Tag ngoại. Tag nội dùng để tính toán trong nội bộ WinCC mà không cần kết nối với thiết bị ngoại vi.

Tag ngoại dùng để giao tiếp WinCC với thiết bị ngoại vi

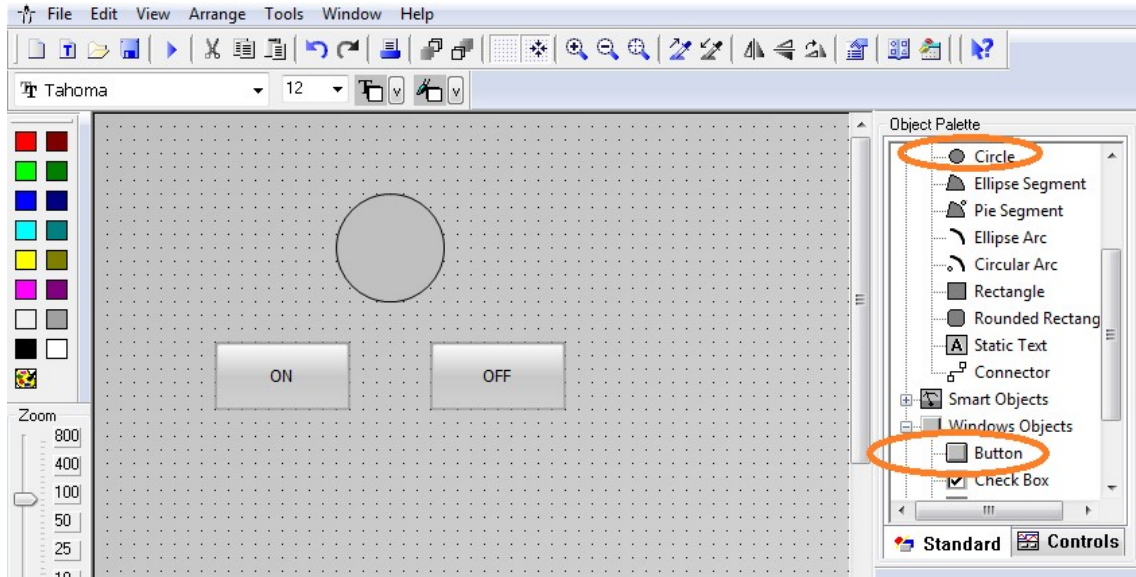
#### c) Ví dụ 1: Tạo 02 nút ấn On/Off cho Tag nội và kiểu dữ liệu trạng thái

Khởi động WinCC, đặt tên cho dự án (Project VD1), tạo một nhóm Tag mới bằng cách click chuột phải/ New group, đặt tên TagNoi để cho dễ quản lý Tag. Trong nhóm Tag chọn Tag đầu tiên là Den, kiểu dữ liệu Binary, chiều dài 1 bit



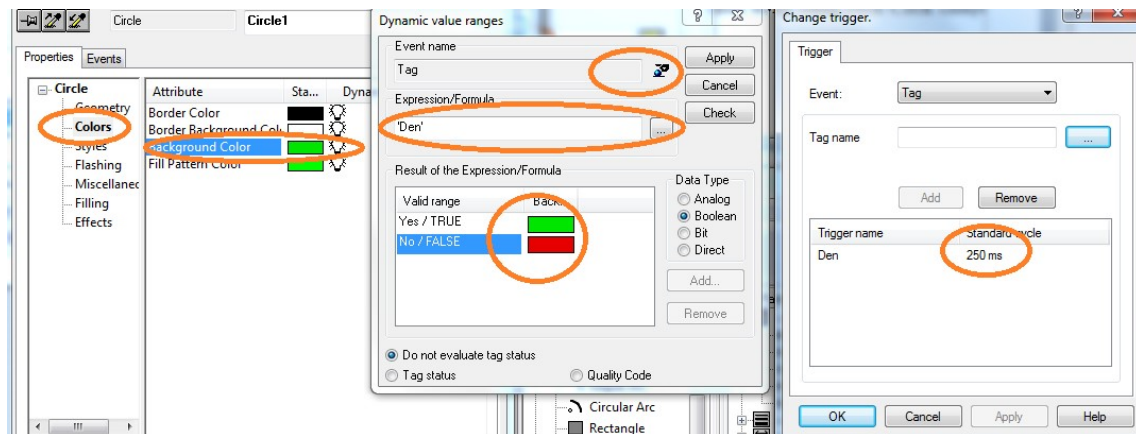
Hình 7.4: Giao diện tạo Tag nội

Thiết kế giao diện trong mục Graphics Designer/ click chuột phải chọn New Picture đặt tên TagNoi, mở giao thiết kế lên và chọn menu bên phải (Object Palette) vẽ vòng tròn (biểu tượng đèn) Circle. Tương tự, ta thực hiện vẽ 2 nút ON, OFF từ thư mục Windows Object/ Button.



Hình 7.5: Giao diện thiết kế giao diện ON/OFF

Đặt thuộc tính cho đèn, bằng cách click chuột phải, Properties/ Effects/ Global color schenme/ No, chuyển lên mục Clolor/ Background Color chọn màu tương ứng lúc OFF- No/ Click chuột phải/ Dynamic... chọn Tag Den chèn vào Dynamic của Background, chọn thời gian tác động 250ms, chọn Data Type là Boolean



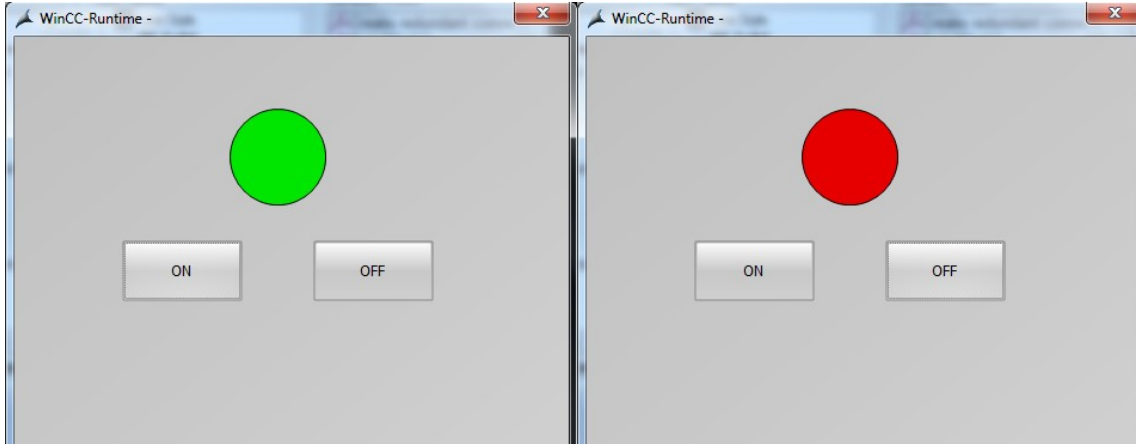
Hình 7.6: Đặt thuộc tính cho biến nội Den

Chuyển sang đặt thuộc tính cho nút ấn (ON, OFF). Tương tự như thuộc tính Den, ta click chuột phải/ chuyển sang sheet Events/ mouse (chọn hành động bằng cách Click chuột trái) đúp vào Press left/ tại mục Constant/ chọn “1-Yes” tức khi Click chuột biến Tag bằng “1”, tại ô Tag của Tab Target chọn biến chèn Tag Den vào, tức khi có bấm



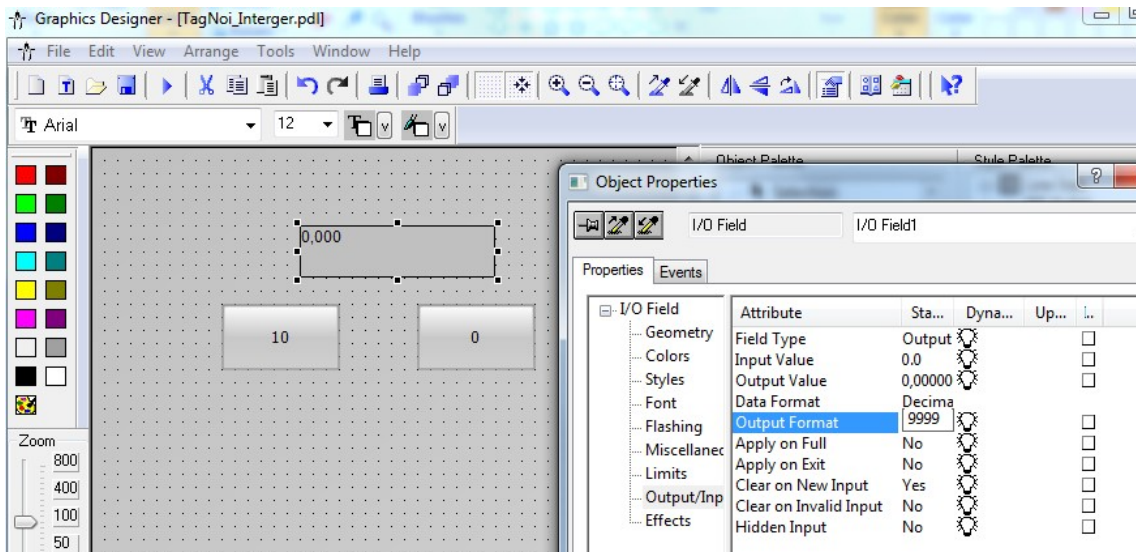
chuột lên nút ON thì thiết lập biến “1” và tác động đến biến Den. Tương tự nút OFF thiết lập lên tại mục Constant/ chọn “0- No” và cũng tác động đến Den khi No.

Như vậy với thuộc tính của Tag nội DEN có 2 màu mặc định nền là đỏ và có tác động là Xanh, trong Dynamics của properties/ color và kết quả như Hình 7.7



Hình 7.7: Kết quả thử nghiệm Tag nội cho hai tác động ON- OFF lên Tag “Den”

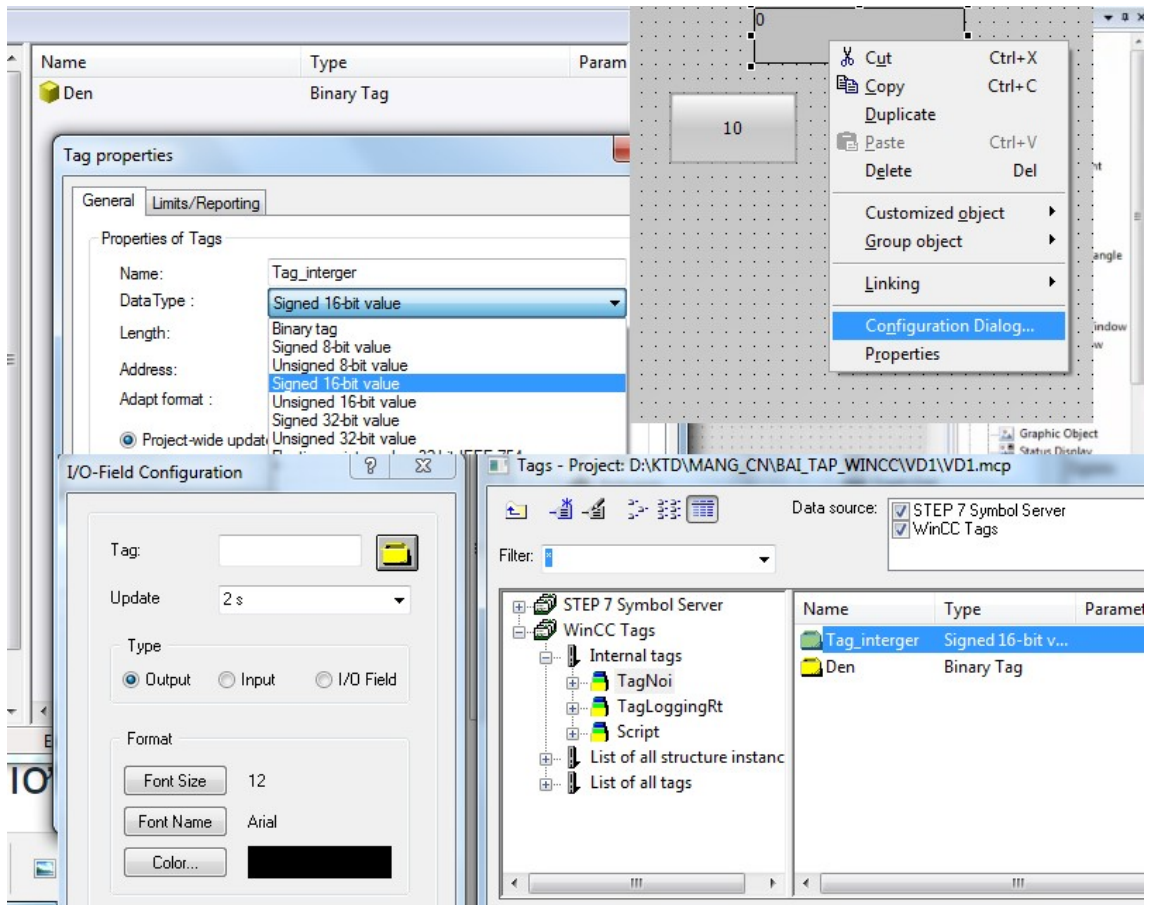
VD2: Tạo Tag số nguyên khi nhấn nút 10, hiển thị số 10 và nhấn số 0, hiển thị số 0. Tương tự như ví dụ 1 trong chương này ta thực hiện ví dụ 2 các bước ban đầu giống nhau với tên project. Giao diện thiết kế 2 nút nhấn 10 và 0, phần hiển thị số nguyên được lấy từ thanh bên phải Smart Objects/ I/O Field (vùng xuất nhập), để tạo thuộc tính số nguyên hiển thị ta click chuột phải vào vùng hiển thị thiết kế chọn properties/ Output/Input/ Output Format, nhập số nguyên cần hiển thị.



Hình 7.8: Thiết lập giao diện vùng hiển thị I/O số nguyên

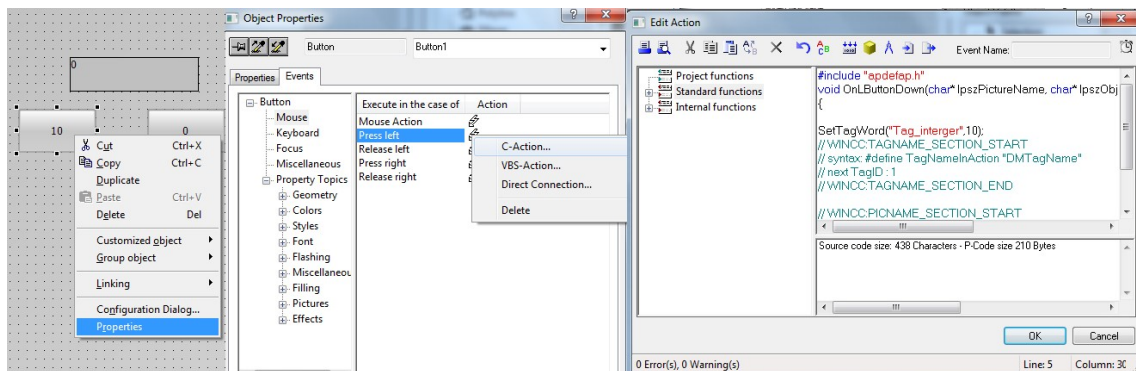
Tạo các biến Tag số nguyên, trong vùng TagNoi bài ví dụ 1 ta tiến hành thêm Tag\_Integer kiểu Unsigned 16 bit, như vậy Tag số nguyên đã được thiết lập, vì thế, ta

vào Graphics để cài đặt chèn Tag vào vùng hiển thị I/O, click chuột phải Configuration Dialog/ chèn Tag trong ô Tag, đặt thời gian tác động 250ms, Output...



Hình 7.9: Kết nối giữa Tag interger và giao diện vùng hiển thị I/O

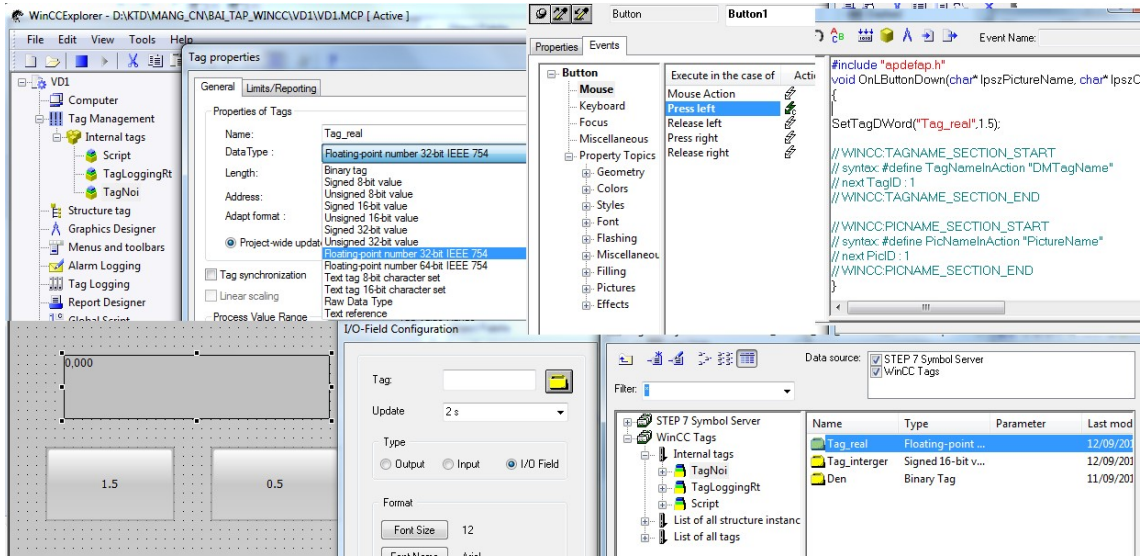
Tạo thuộc tính cho nút nhấn, click chuột phải Properties/ Events/ Mouse (thiết lập trạng thái khi có bấm chuột trái), chọn Press left C-Action vào viết chương trình C. trong chương trình chính, ta viết mã lệnh SetTagWord("Tag\_interger",10) tức là thiết lập một Tag\_interger có giá trị 10 khi có bấm chuột trái, sau đó biên dịch. Tương tự, áp dụng cho nút nhấn "0" cũng vậy thay giá trị "10" bằng giá trị "0".



Hình 7.10: Lập trình Tag interger

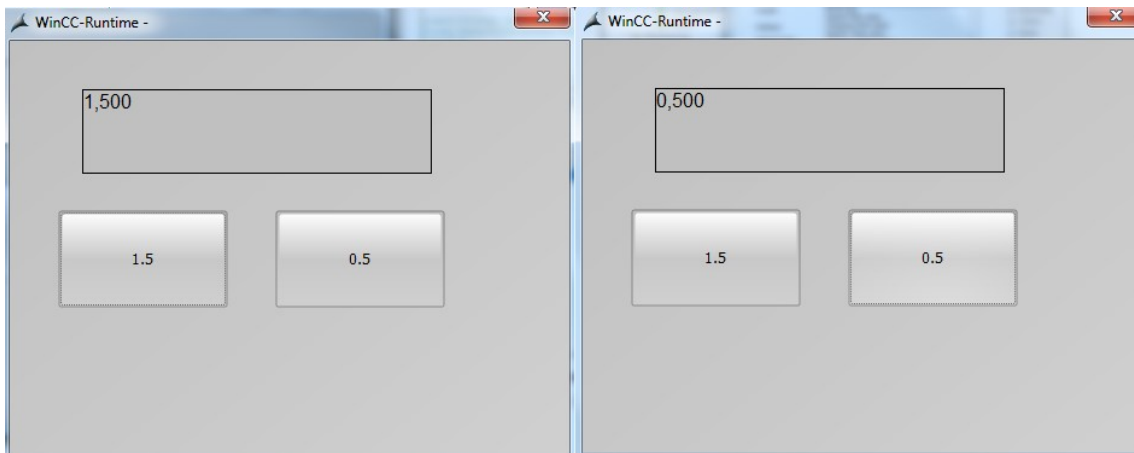
d) Ví dụ 3: Tạo tag nội với 2 nút thay bằng số thực như ví dụ 2.

Tương tự như ví dụ 2, ta tạo một Tag\_real trong intertag, với kiểu dữ liệu Floating point number 32 bit. Bên cửa sổ Graphics Designer tạo một giao diện TagNoi\_real.pdl, thiết kế 2 nút và một vùng hiển thị như trong ví dụ 2. Tuy nhiên, trong vùng I/O hiển thị cần thay đổi bằng cách chèn Tag\_real. Về viết code C cho nút nhấn thay SetTagWord("Tag\_interger",10) bằng SetTagFloat("Tag\_real",1.5). Tương tự, cho nút 0.5.



Hình 7.11: Giao diện và cài đặt cấu hình Tag nội real

Kết quả thực hiện điều khiển nút nhấn qua Tag nội và ô text hiển thị



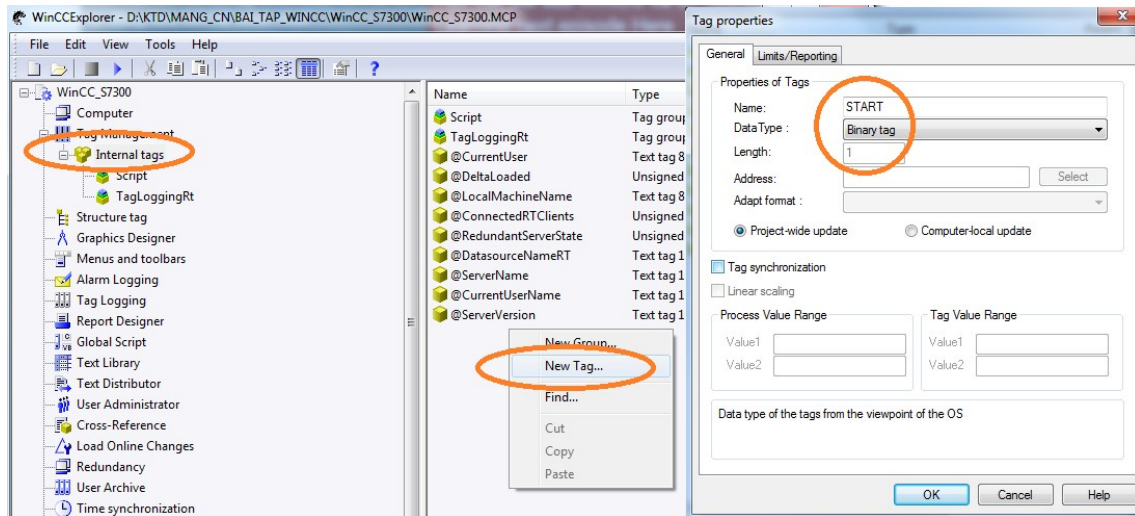
Hình 7.12: Kết quả thực hiện ví dụ về Tag nội dạng số thực

#### 7.1.4 Xây dựng dự án tạo giao diện đơn

Bước 1: Tạo biến nội



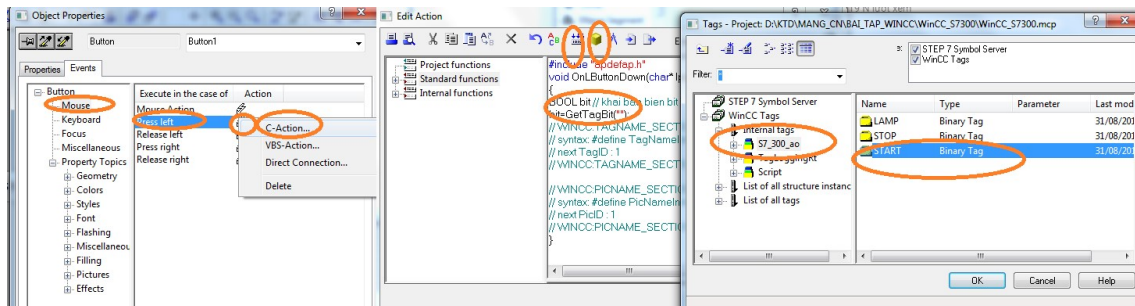
Khởi động WinCC và tạo một dự án (project), sau khi hoàn thành dự án, ta tạo các biến nội (Internal Tag) START, STOP, LAMP có giá trị 1 bit, các biến nội này không cần kết nối với các thiết bị thực S7-300.



Hình 7.13: Giao diện tạo biến nội cho WinCC giao tiếp S7-300 ảo

Bước 2: Thiết kế giao diện

Mở cửa sổ Graphics Designer, đặt tên S7\_300\_ao, đặt thuộc tính cho các đối tượng theo click chuột Events/ Mouse/ press left. Tại cột Action, bấm chuột phải chọn ngôn ngữ C để viết chương trình cho đối tượng START, STOP, LAMP...



Hình 7.14: Đặt thuộc tính cho các biến

Bước 3: Viết ngôn ngữ C ví dụ đoạn lệnh:

```
#include "apdefap.h"
```

```
void OnLButtonDown(char* lpszPictureName, char* lpszObjectName, char* lpszPropertyName, UINT nFlags, int x, int y)
```

```
{
```

```
    BOOL bit ; // khai bao bien bit
```

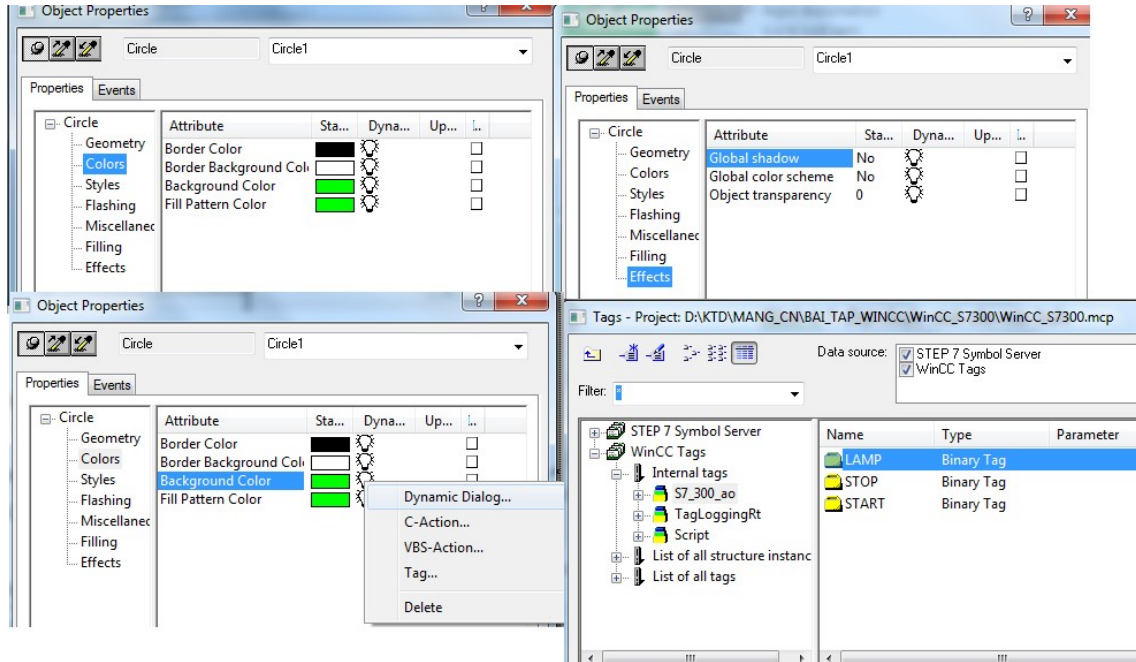
```
    bit=GetTagBit("START"); // đọc giá trị từ biến START
```

```
    if (bit ==1) // Nếu biến ==1
```

```
SetTagBit("LAMP",1); // thiết lập biến LAMP =1
}
```

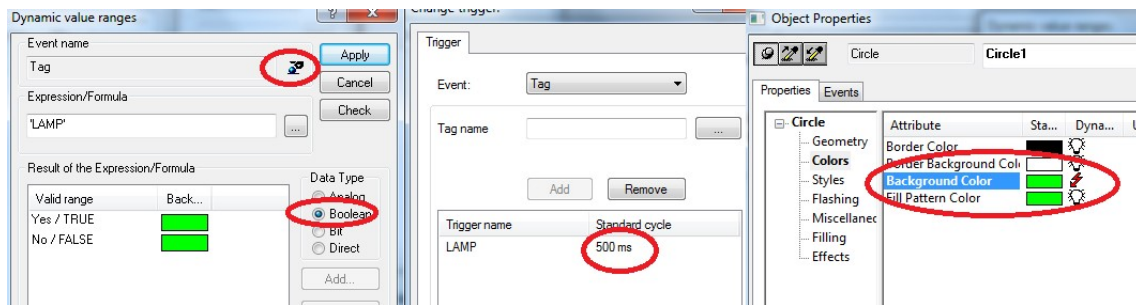
Tương tự viết cho các biến cần thiết có trong giao diện đã thiết kế.

Trường hợp biến đầu ra chúng ta cần thiết lập màu sắc và chèn biến như sau: chọn Effects đặt hiệu ứng Yes/No sau đó chọn Colors để chọn màu phù hợp với hiệu ứng đó. Tiếp theo vào Background Color/ chọn Dynamic Dialog/ chọn ...



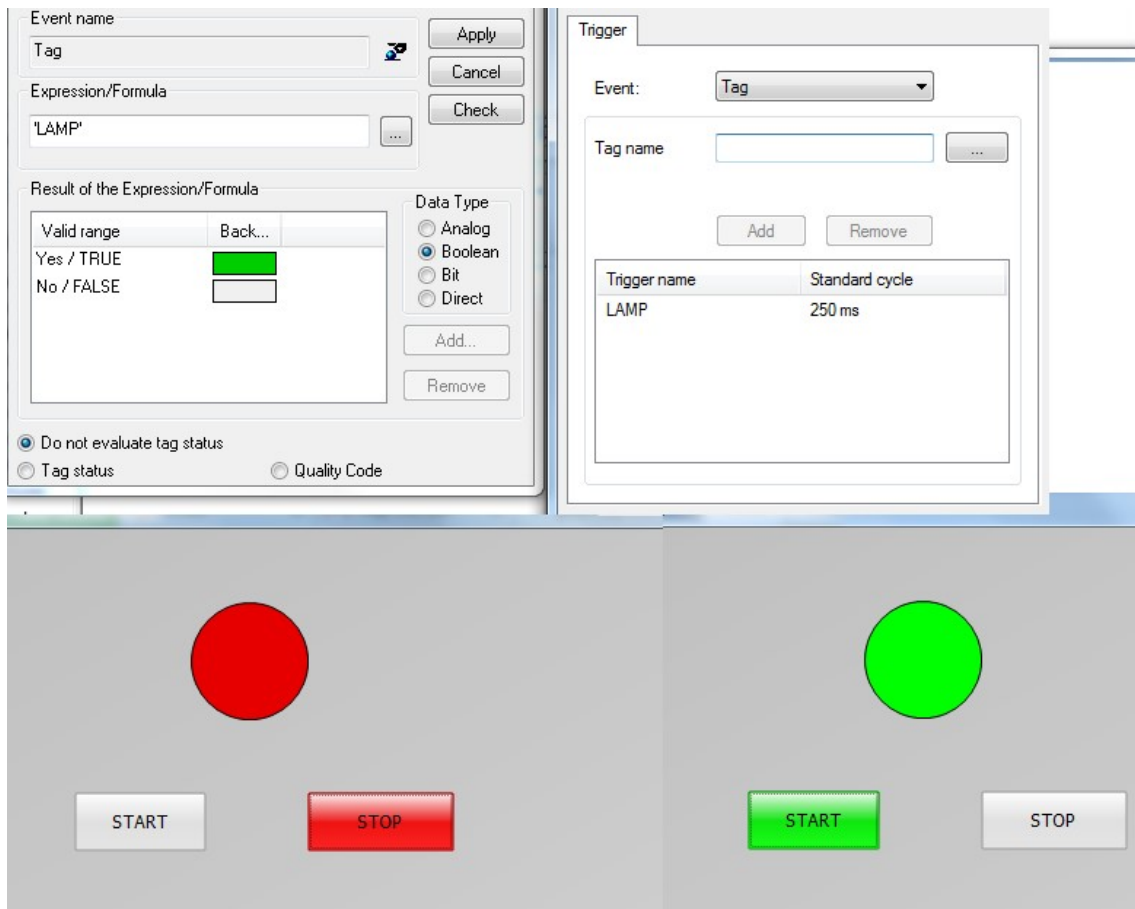
Hình 7.15: Đặt thuộc tính cho biến đầu ra/ đầu vào của đối tượng thiết kế giao diện

Tag/ chọn biến ra LAMP/ tích ô thuộc tính Boolean để đặt biến LAMP Yes/True và No/False, chọn lại màu sắc cho phù hợp và chọn thời gian trễ trong hộp Tag.



Hình 7.16: Kết quả cài đặt tham số

Thiết lập thuộc tính cho chính đối tượng, click chuột phải Properties/ effects chọn No, No trong mục Global shadow và Global color scheme, chuyển sang thư mục Colors tại Background Color/ Dynamic Dialog vẫn chọn biến LAMP (thực hiện đổi màu START theo LAMP), thay đổi thời gian và thuộc tính Boolean như trên.



Hình 7.17: Kết quả mô phỏng trên Win CC

Bước 4: Xây dựng chương trình S7-300

### 7.1.5 Mô phỏng biến (Tag) ngoại trong WinCC

## 7.2 Kết nối Win CC với S7-200

Chuẩn bị phần mềm WinCC, Step 7 Microwin 4.0, PC access và PLC Simulator

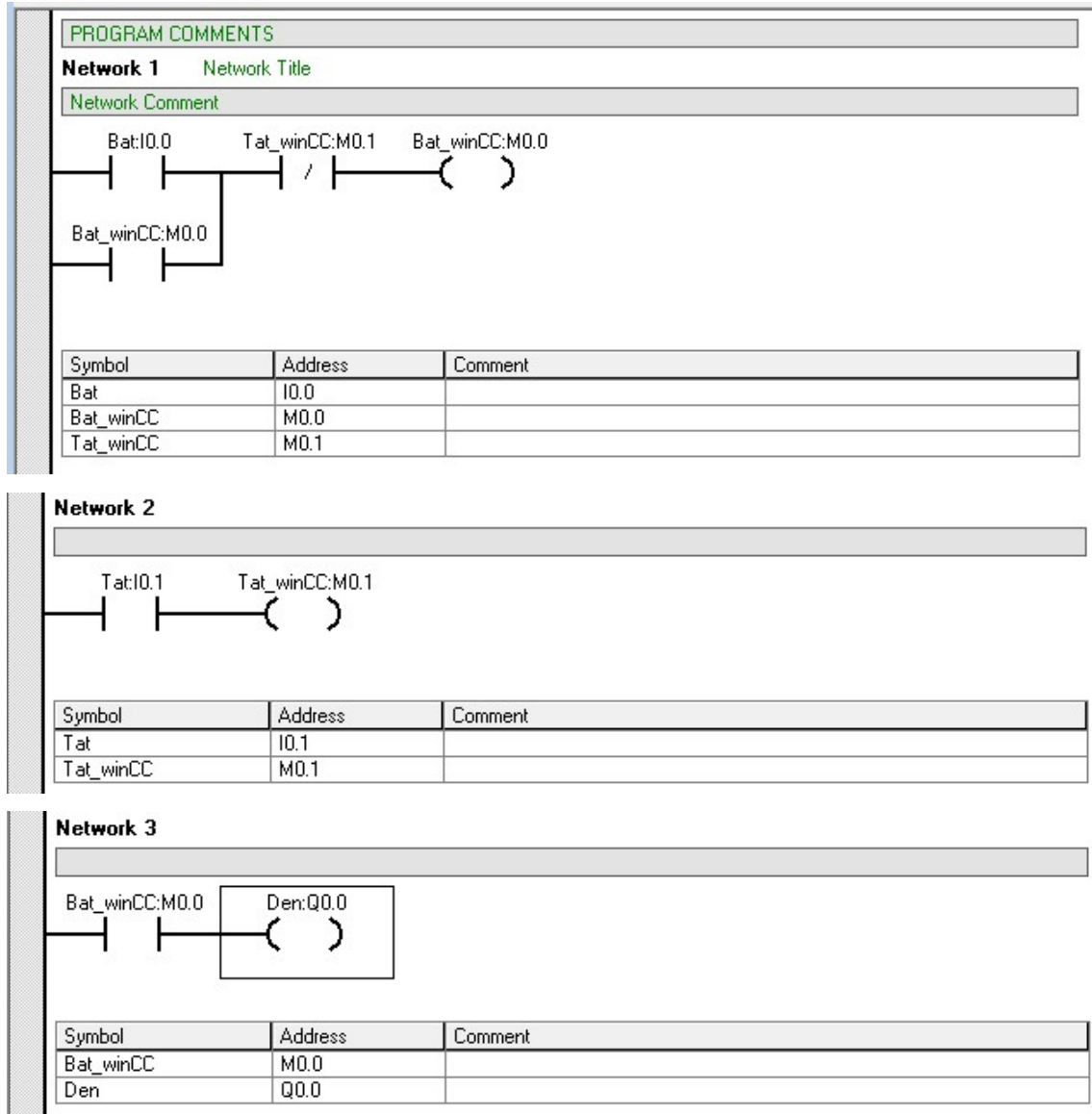
Bước 1: Xây dựng chương trình S7-200

Sử dụng phần mềm S7-200 Microwin để soạn thảo chương trình ví dụ On/off cho s7-200. Để kết nối được win CC cần bảng sysbol và sử dụng vùng nhớ trung gian M hoặc V để làm liên kết với WinCC.

Bảng 7.1: Bảng sysbol cho chương trình ví dụ

Symbol Table				
		Symbol	Address	Comment
1		Bat	I0.0	
2		Tat	I0.1	
3		Den	Q0.0	
4		Bat_winCC	M0.0	
5		Tat_winCC	M0.1	
6				

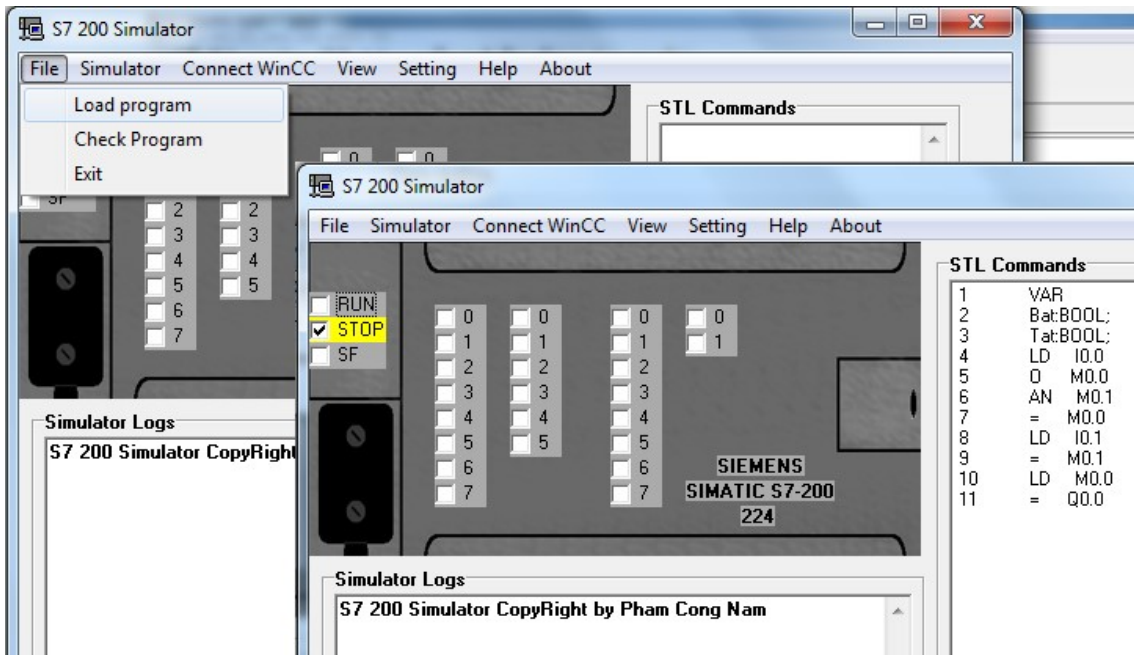
Chương trình xây dựng trên LAD VD\_S7\_200 như sau:



Bước 2: Mô phỏng PLC S7-200 ảo

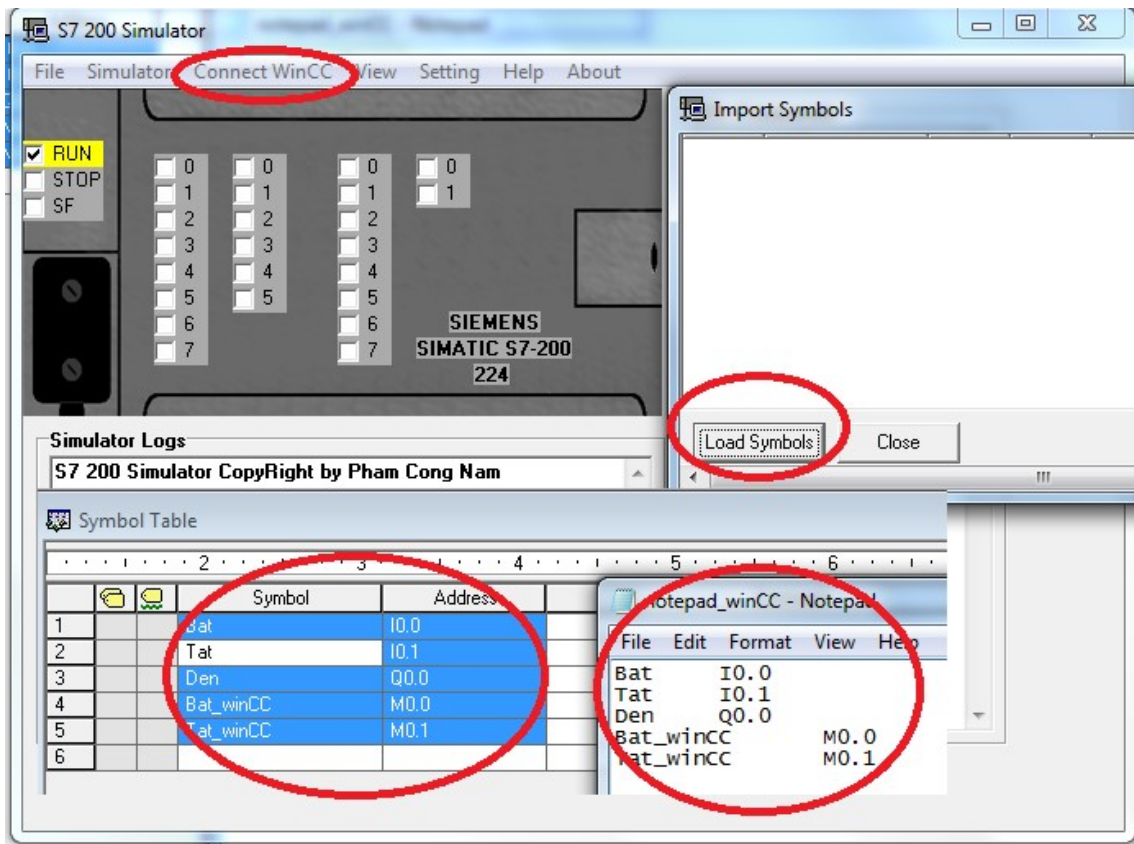
Khởi động phần mềm PLC Simulator repack, xuất file PLC đã lập trình VD\_S7\_200 chuyển sang định dạng .awl bằng cách từ chương trình step 7 Micro/Win chọn Export, lưu cùng tên, cùng thư mục với chương trình lập trình có đuôi .awl để mô phỏng.

Từ phần mềm mô phỏng chọn Load program, chọn file .awl vừa xuất từ chương trình ứng dụng.



Hình 7.18: Kết nối chương trình mô phỏng S7-200 Simulator với chương trình ứng dụng

Tạo một file notepad cho bảng sysbol, copy bảng sysbol bao gồm sysbol và address vào file notepad vừa tạo có tên notepad\_winCC lưu lại. Vào mục Connect WinCC/ Load Sysbol chọn file notepad\_winCC vừa tạo.



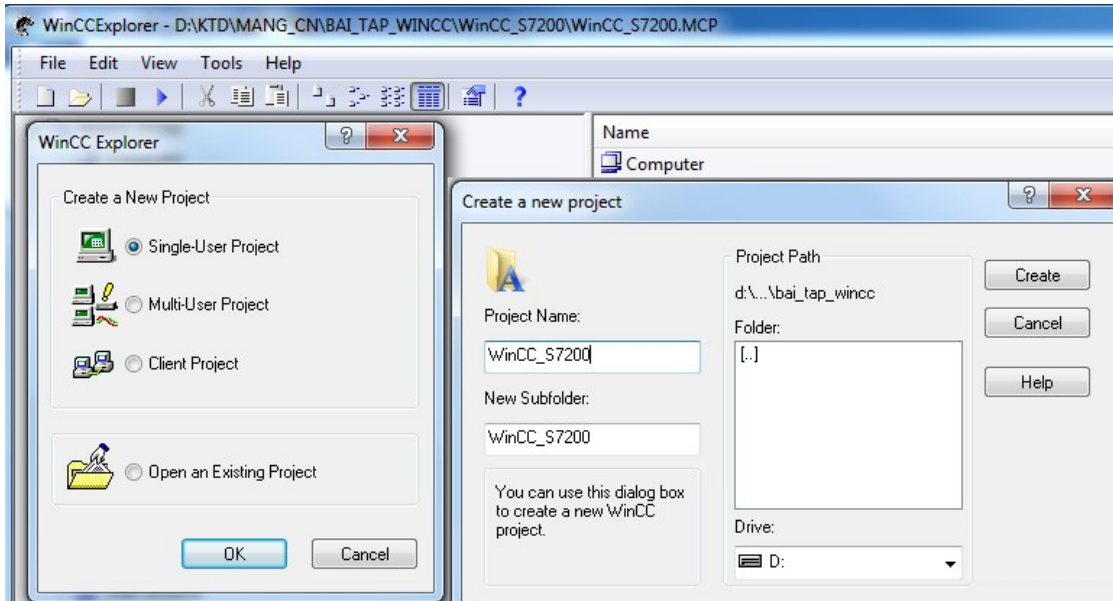
Hình 7.19: Khai báo biến và kết nối mô phỏng với PLC



Lúc này chương trình ứng dụng đã được kết nối tới PLC Simulator thông qua file notepad\_winCC.txt (chương trình Step Micro/Win không cần lúc này).

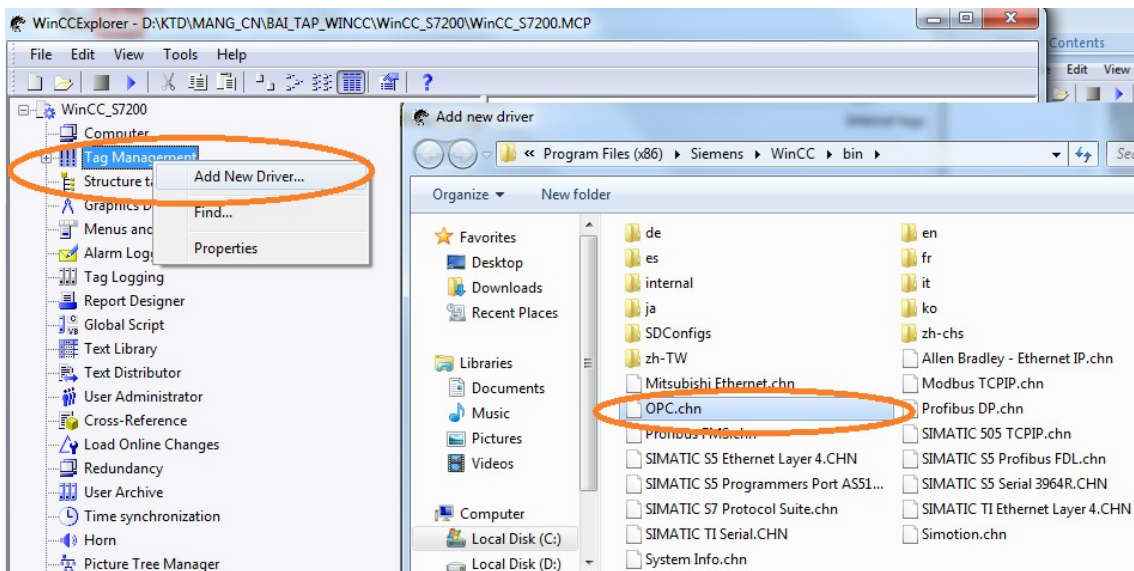
Bước 3: Khởi tạo WinCC và xây dựng chương trình giao diện

Khởi động WinCC và tạo một dự án (project) có tên WinCC\_S7200, từ File/ new đặt tên và chọn đường dẫn



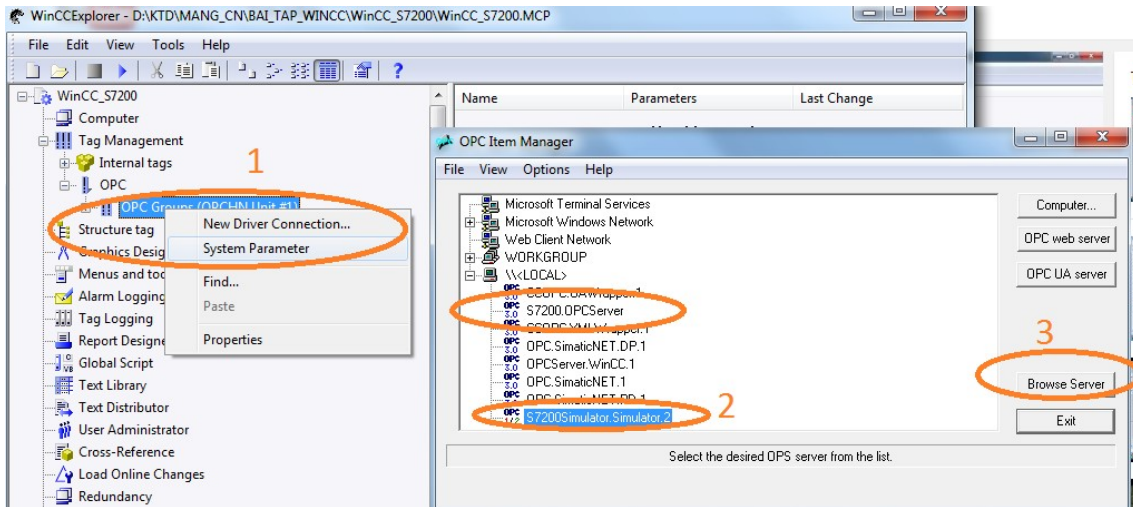
Hình 7.20: Giao diện tạo dự án trên WinCC

- Thiết lập kết nối PLC với WinCC: Trong winCC có 2 loại biến (tag), biến ngoại và biến nội, đối với kết nối cần sử dụng biến ngoại. Vào mục quản lý biến Tag Management, click chuột phải chọn Add New Driver, trong trường hợp này sử dụng S7-200 nên thông qua OPC nên chọn lựa mục OPC (cơ sở dữ liệu).



Hình 7.21: Chọn cấu hình OPC trên WinCC

Từ OPC Group click chuột phải chọn System Parameter để thiết lập tham số cho OPC server. Đối với trường hợp sử dụng cơ sở dữ liệu nhóm, mạng hay trên máy tính có thể lựa chọn cho phù hợp, trường hợp này ta mô phỏng nên chọn S7200Simulator.Simulator.2 (S7200.OPCServer dành cho PLC thực)/ click Browse Server, OK

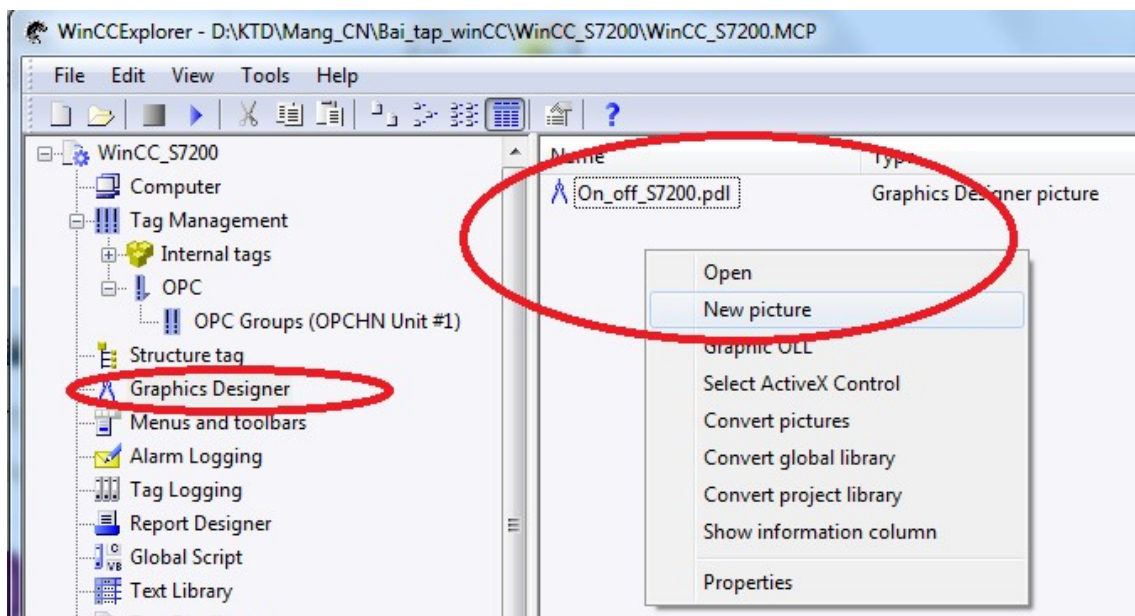


Hình 7.22: Khai báo Tag (biến) cho OPC

Thêm tất cả các biến vào OPC của WinCC

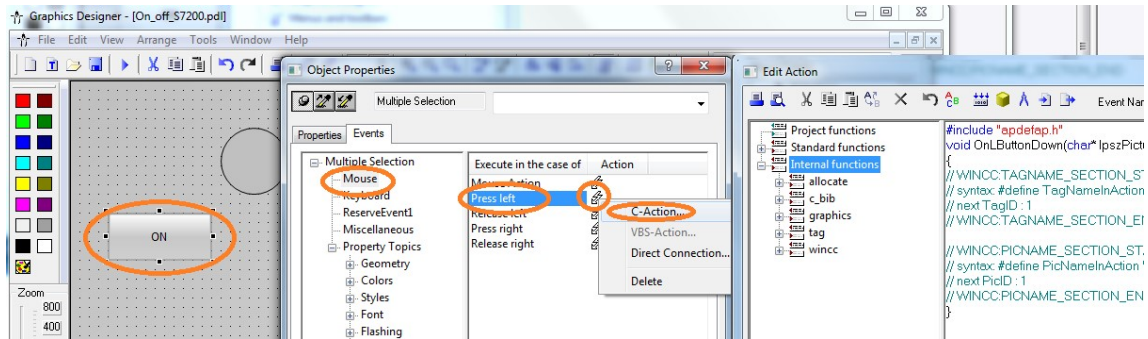
Bước 4: Thiết kế giao diện

Từ thanh menu bên trái chọn mục Graphics Designer/ click chuột phải, New picture, đặt tên On\_of\_S7200, đúp vào tên để mở ra cửa sổ giao diện. và thiết kế giao diện.



Hình 7.23: Tạo giao diện thiết kế

Đặt thuộc tính cho các đối tượng thiết kế trong trường hợp này có 2 nút ON, OFF và đèn hiển thị. Nhấp đúp để đặt thuộc tính, chọn tab Events/ chọn press, sang cột Action (hành động) click chuột phải lựa chọn ngôn ngữ để mô tả thuộc tính (chọn ngôn ngữ C) lúc này ta viết code hoặc có thể đơn giản hơn chọn các hàm có sẵn trong thư mục bên trái Internal functions/ tag/ get ( lấy giá trị biến) và set (thiết lập cho biến).

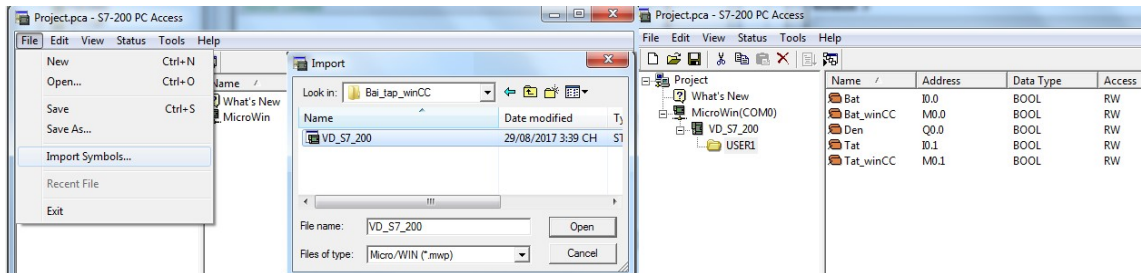


Hình 7.24: Lựa chọn thuộc tính cho đối tượng trong hàm thư viện có sẵn

Thiết lập cho biến bằng cách chọn Tag/ set/ set TagBit (do nút đơn vị là 1 bit)/ Tag\_Name click ... bên phải để chèn biến lúc đầu chèn từ phần mềm mô phỏng PLC Simulator chọn biến tương ứng với giao diện. trường hợp này chọn Bat\_winCC cho nút bật.

Bước 2: Sử dụng PC access để liên kết WinCC với các biến trong S7-200

Khởi động PC access, chọn File/ Import symbol, chọn file lập trình PLC ở trên VD\_S7\_200 (đối với mô phỏng không cần dùng PC access)



Hình 7.25: Kết nối chương trình ứng dụng PLC S7-200 với PC Access

## 7.3 Kết nối Win CC với S7-300

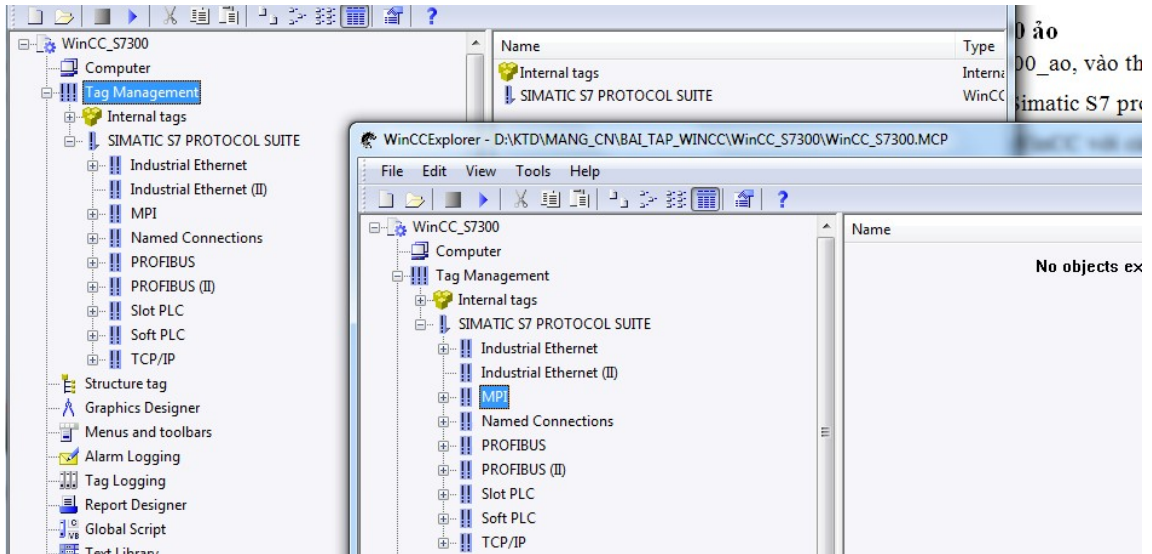
### 7.3.1 Tạo liên kết S7-300 ảo với WinCC qua biến (Tag) ngoại

Bài toán về tạo một dự án cho Tag đơn bit (VD3)

Bước 1: Tạo một dự án tên S7\_300\_ao, vào thư mục Tag Management/ click chuột phải Add New Driver.../chọn lựa Simatic S7 protocol Suite.chn Nếu sử dụng kết nối với S7, tương tự chúng ta kết nối WinCC với các hệ thống khác. Trong giao thức S7



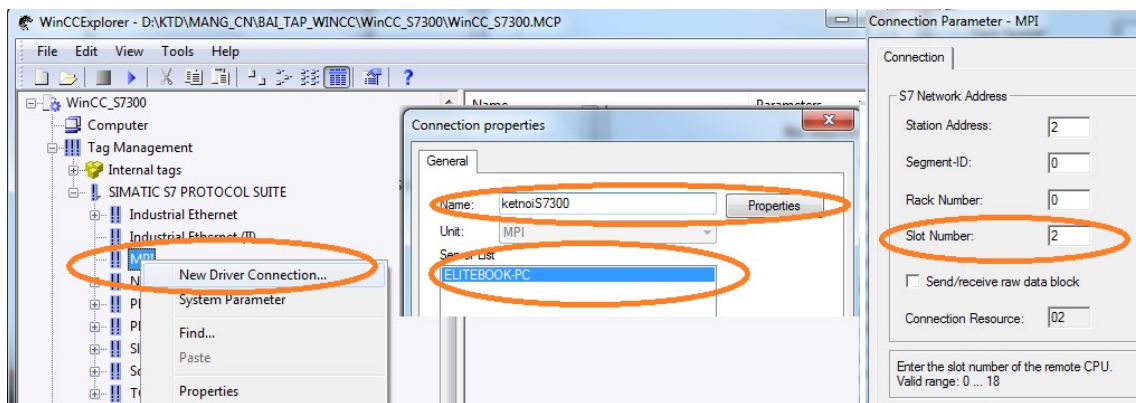
có nhiều giao thức con: Ethernet, MPI, Profibus, Slot PLC, TCP/IP... trong trường hợp này ta chọn giao thức MPI (kết nối PLC S7-300 riêng) không sử dụng biến nội nữa mà lúc này sử dụng biến ngoại [56], [20].



Hình 7.26: Giao diện cấu hình phần S7 với WinCC

### Bước 2: Thiết lập Driver

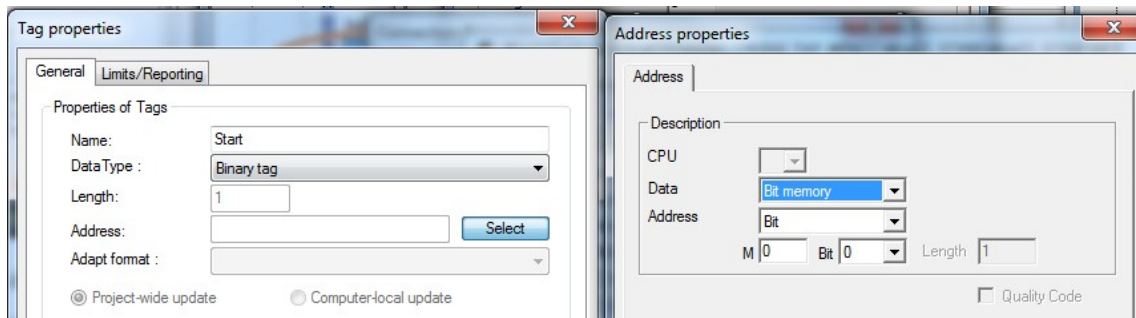
Click chuột phải vào MPI/ New Driver Connection, đặt tên cấu hình kết nối là kết nối S7-300, click Properties/ chọn Slot là 2, tức trùng với địa chỉ trạm. Chú ý trong trường hợp này tên máy tính được chọn làm tên cho Server list, khi dự án được copy sang máy tính khác cần đổi tên server cho phù hợp.



Hình 7.27: Thiết lập cấu hình kết nối máy tính và S7-300

### Bước 3: Thêm các biến vào kết nối

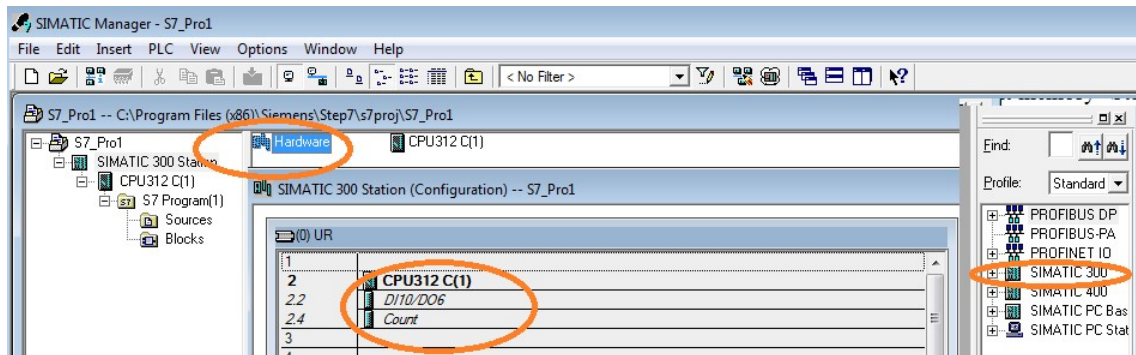
Từ thư mục bên phải click chuột phải, chọn New tag/ đặt tên Tag (Start)/ chọn kiểu dữ liệu, đối với nút nhấn thì chọn 1 bit Binary tag, click Select để lựa chọn Input/Output của PLC S7-300, chọn bit M0.0 làm bit nhớ “bit memory” Start, tương tự cho nút Stop là M0.1 và đèn Lamp là “Output” Q0.0.



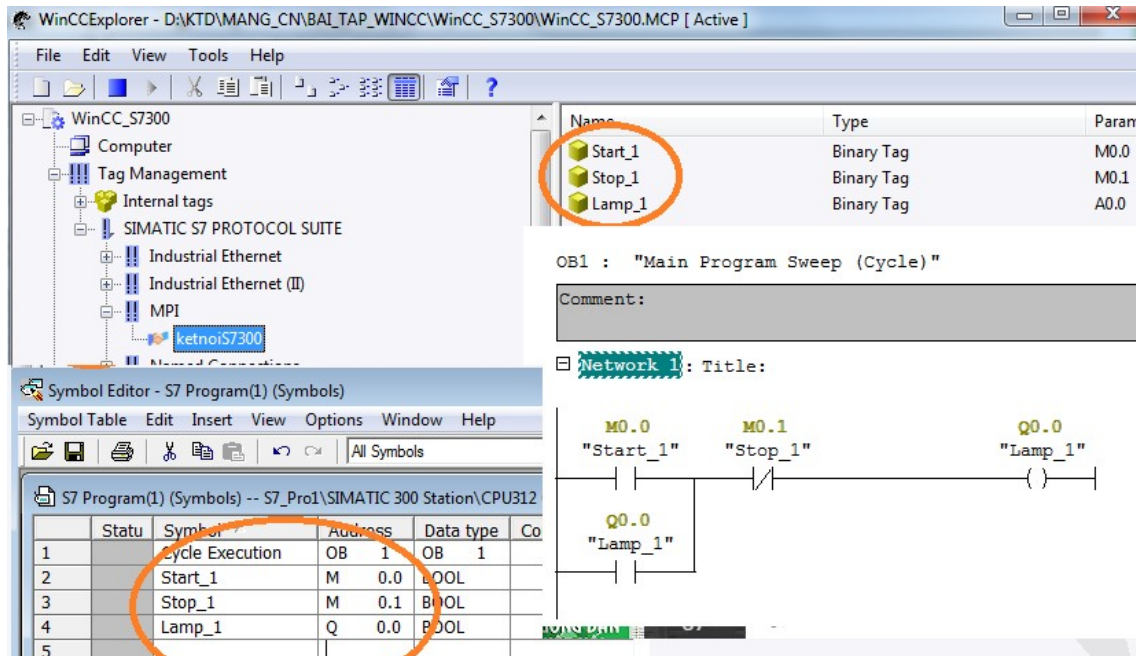
Hình 7.28: Kết nối biến nhớ vào WinCC

#### Bước 4: Xây dựng chương trình S7-300

Khởi động Simatic Step 7/ chọn CPU 312C có hỗ trợ sẵn I/O trên CPU, chọn địa chỉ MPI 2 (liên kết máy tính qua MPI), chọn ngôn ngữ lập trình LAD khối OB1, đặt tên dự án S7-300 là S7\_pro. Thiết lập cấu hình Hardware như Hình 2.29



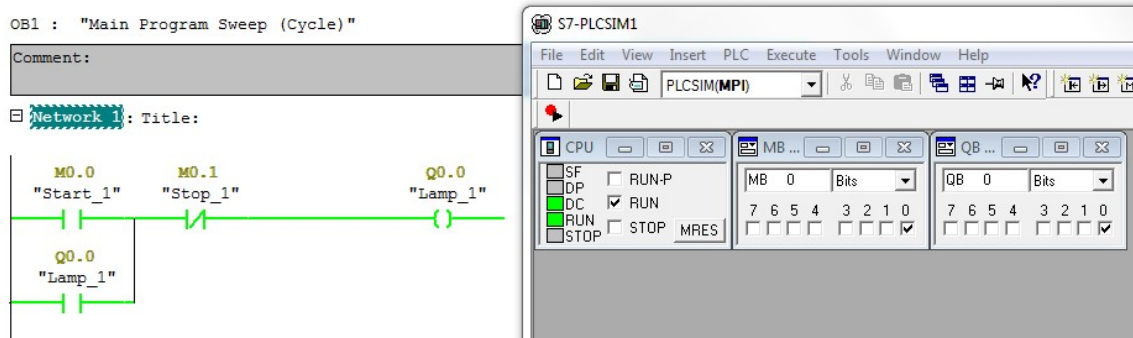
Hình 7.29: Cấu hình Hardware cho S7-300



Hình 7.30: Chương trình trên PLC S7-300 với biến (Tag) trên WinCC

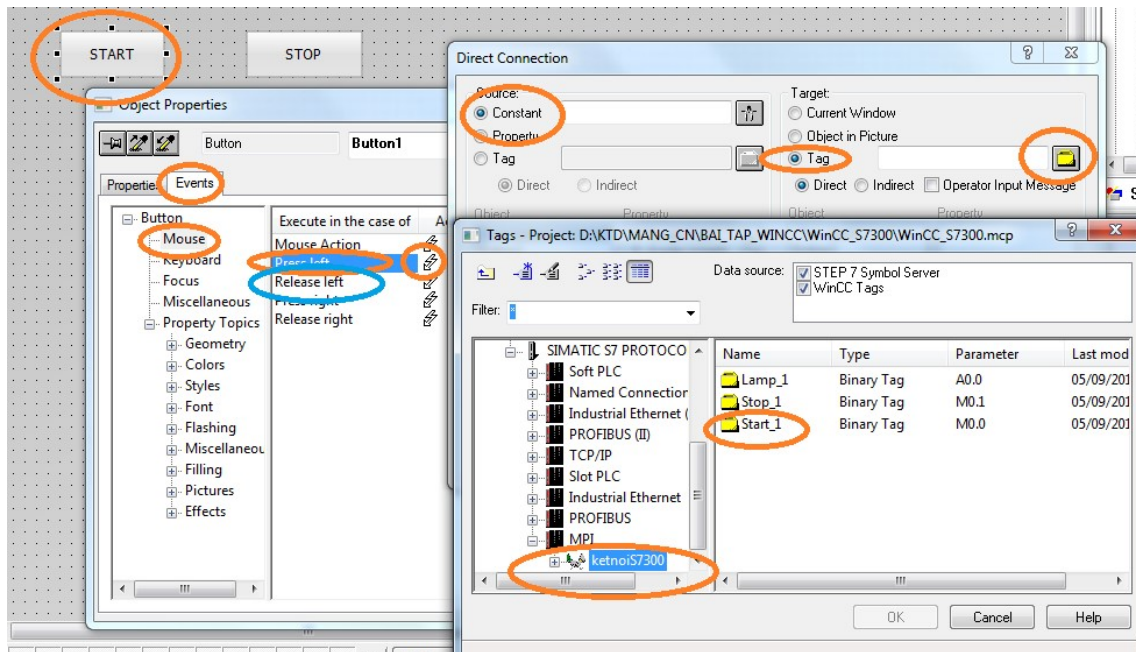
Đối với liên kết WinCC cần thiết lập symbol lần lượt khai báo các biến (Tag) đã thiết kế trong WinCC như Start, Stop, Lamp với các địa chỉ tương ứng M0.0, M0.1 và Q0.0 trong S7-Program và lập trình cho khối OB1.

Mở phần mềm mô phỏng S7-PLCSim, thực hiện Download chương trình vừa lập trình vào PLCSim để mô phỏng, bậc chế độ RUN, thử mô phỏng nguyên lý lập trình có đúng không, chế độ xem Monitor màn hình để thấy trạng thái “điện” trên chương trình.



Hình 7.31: Giao diện mô phỏng cho S7-300 trên PLCSim

#### Bước 4: Kết nối WinCC với S7-300

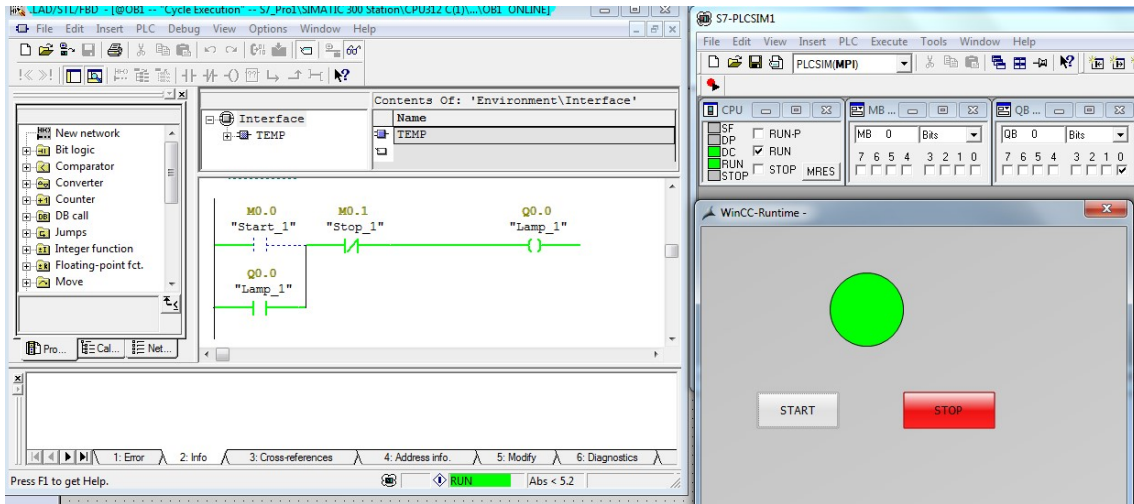


Hình 7.32: Đặt thuộc tính cho biến

Mở WinCC tạo một giao diện trong Graphics gồm 2 nút Start, Stop và đèn Lamp như bài trước. Đặt thuộc tính cho nút bấm, lúc này click chuột phải/ Events/ Mouse/ Press left (bỏ thuộc tính C đã viết trước), đúp vào mũi tên cột Action/ Constant (0/1 đối với Start và 1/0 đối với Stop) và Tag/ mở hộp thư mục Tag/ chọn thư mục chứa

biến là “ketnoiS7300” của MPI và chọn biến Start\_1 đã thiết kế trước. Quá trình này cũng thực hiện cho trường hợp khi nhấn phím “Release left”. Tương tự, thực hiện cho nút Stop và Lamp.

Lưu toàn bộ và chọn chạy chương trình Run/ cửa sổ Runtime hiện ra để lựa chọn giao diện muốn kết nối với phần cứng S7-300.

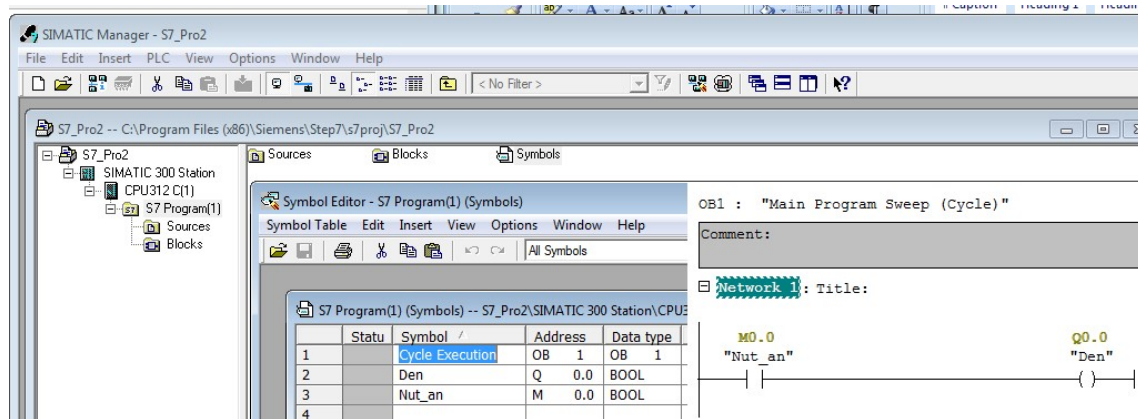


Hình 7.33: Kết quả kết nối PLC S7-300 với WinCC [2], [57]

### 7.3.2 Tạo nút nhấn hai tác động trên WinCC

Bước 1: Thiết kế S7-300

Tạo một chương trình trên S7-300 của Step7 có tên dự án là S7\_Pro2, CPU 312C có hỗ trợ I/O điều chỉnh địa chỉ I/O về 0.x. Khai báo Nut\_an với Den có biến lần lượt M0.0 và Q0.0 trong Symbol



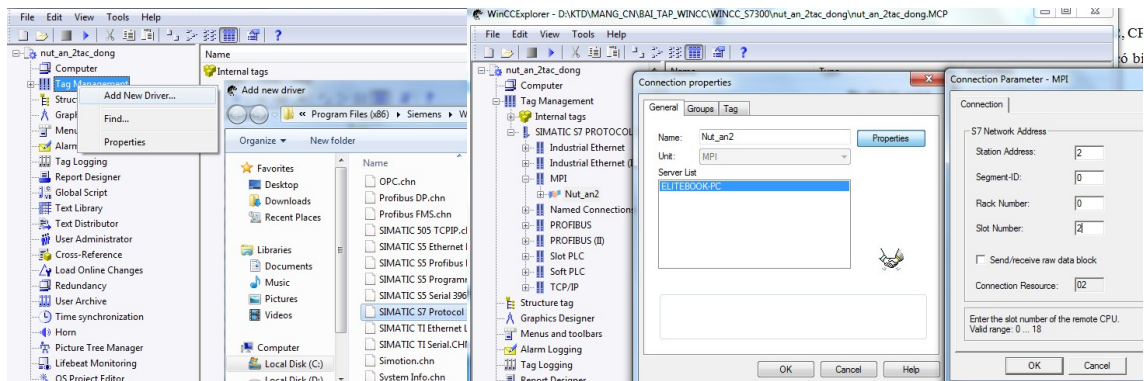
Hình 7.34: Thiết lập dự án trên S7-300 cho nut\_an và den

Bước 2: Tạo dự án trên WinCC

Khởi động WinCC, thiết lập dự án có tên nut\_an\_2tac\_dong , nhấp chuột phải để thêm kết nối giao thức S7 Protocol Suite.chn, Chọn giao tiếp MPI để thiết kế kết nối



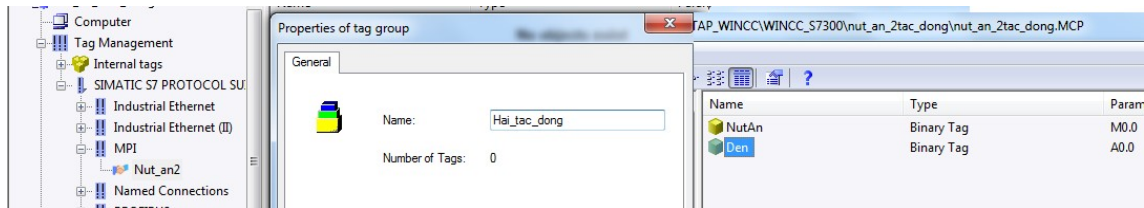
giữa S7-300 và WinCC, đặt tên cho hệ thống kết nối là Nut\_an2/ Properties chọn địa chỉ Slot 2, Ok



Hình 7.35: Thiết lập cấu hình giao tiếp MPI cho nut\_an

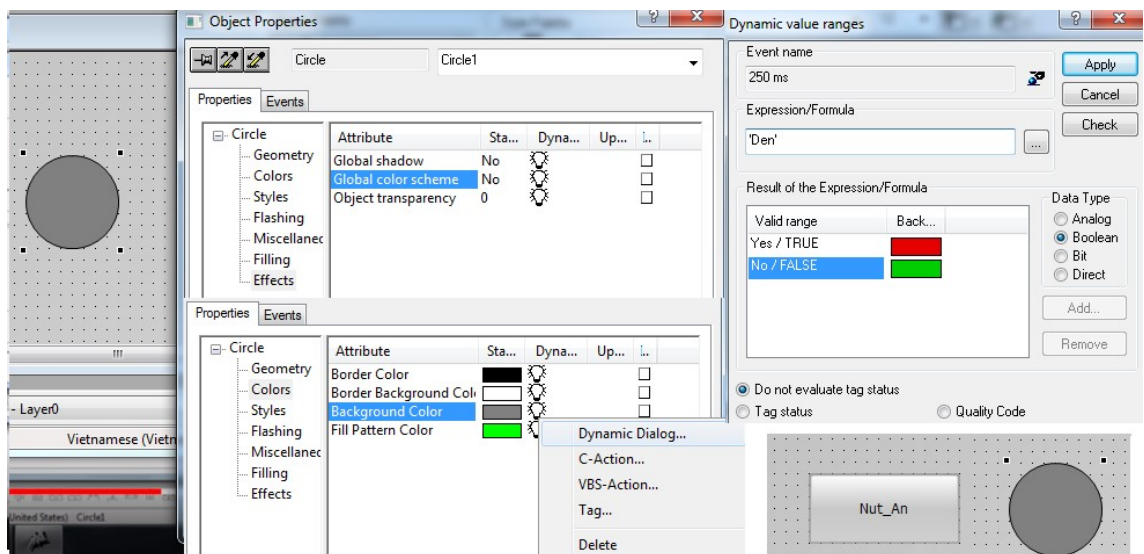
### Bước 3: Đặt thuộc tính cho biến

Từ kết nối Nut\_an2 ta tạo ra nhóm biến có tên Hai\_tac\_dong, từ nhóm biến này ta tạo ra 2 biến là NutAn và Den có địa chỉ ngoài M0.0 và Q0.0 theo kiểu nhị phân bit memory và Output giống như trong chương trình S7-300 đã mô phỏng.



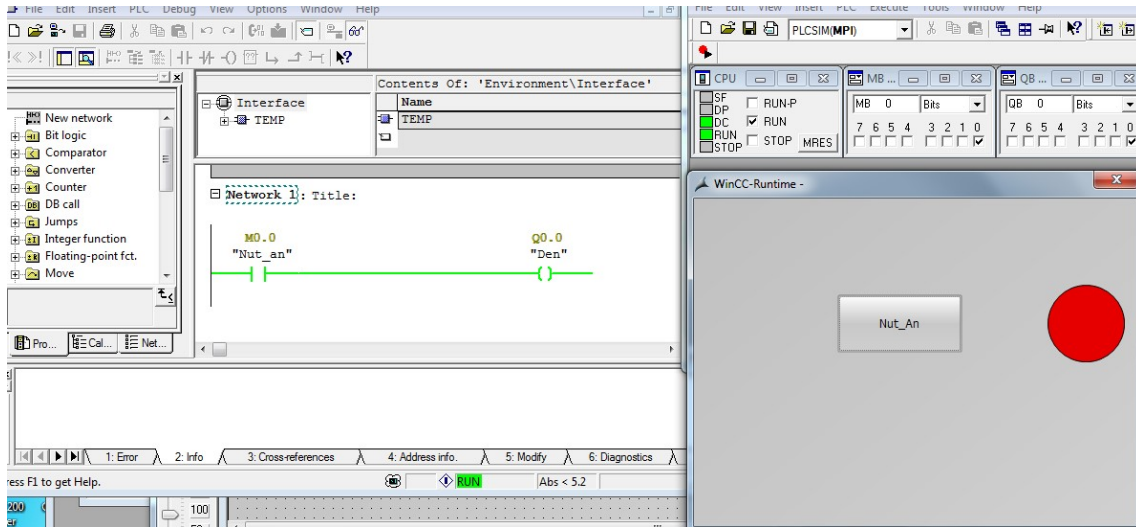
Hình 7.36: Thiết lập biến ngoại

Bước 4: Thiết kế giao diện: Xây dựng giao diện gồm nút bấm và một đèn như các phần trước, thuộc tính Effects đặt No.



Hình 7.37: Thiết kế giao diện hệ thống nút ấn hai chế độ

Còn thuộc tính Colors/ Dynamic Dialog/ chọn màu sắc cho Yes/No, thời gian tác động 250ms, chèn biến 'Den' vào Expression. Tương tự, áp dụng cho nút bấm.



Hình 7.38: Kết quả thực hiện giao tiếp WinCC với S7-300 ảo.

Đối với nút bấm ta viết dạng ngôn ngữ C

BOOL bit; // tao dien 0/1

bit= GetTagBit("NutAn");

if (bit==0)

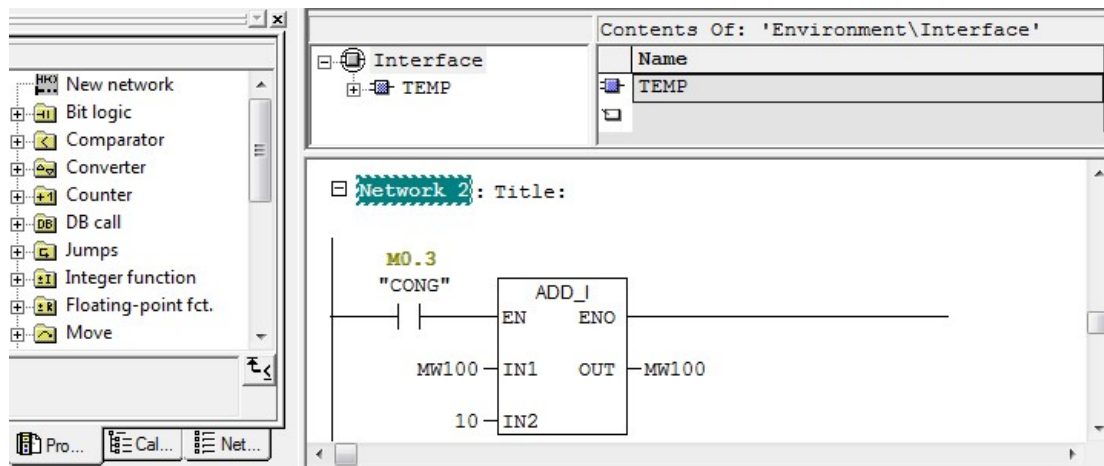
SetTagBit("NutAn",1);

if (bit==1)

SetTagBit("NutAn",0);

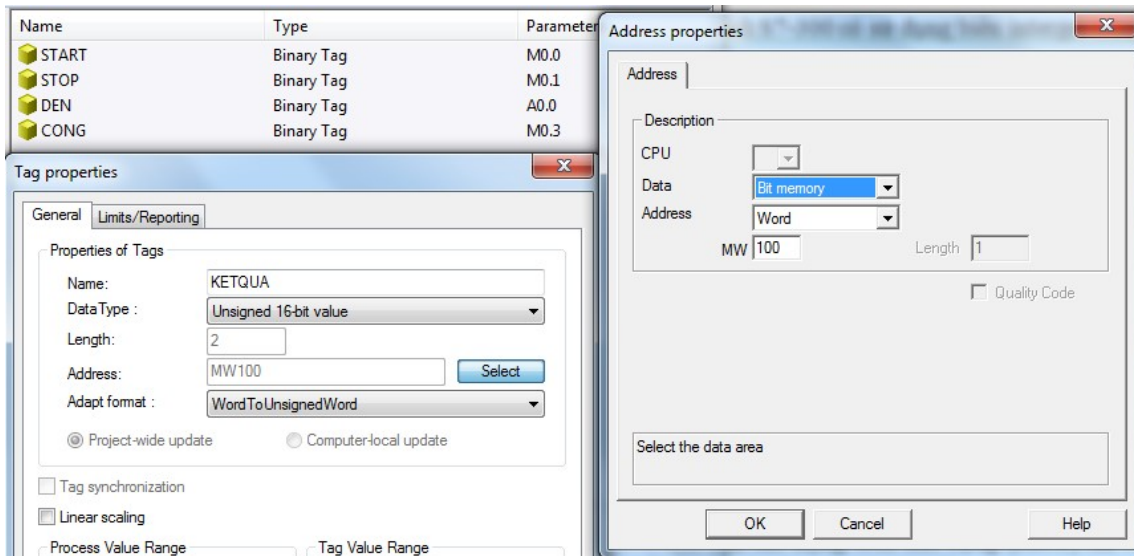
Bài toán về tạo một dự án cho Tag số nguyên (VD3)

Xây dựng chương trình S7-300 có sử dụng biến interger bằng phép cộng số nguyên giữa MW100 với số nguyên 10 và kết quả lưu vào địa chỉ MW100.



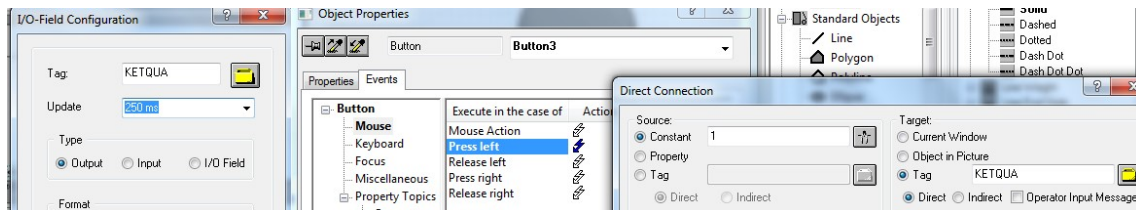
Hình 7.39: Chương trình S7-300 với số nguyên (interger)

Như vậy, khi có lệnh tác động trên nút cộng (M0.3) thì vùng nhớ MW100 được tăng thêm 10 đơn vị. Chuyển sang WinCC tại nhóm Tag ta tạo thêm 2 Tag, Tag CONG kiểu bool 1 bit – M0.3 và Tag ô chứa KETQUA kiểu unsigned 16 bit – MW100.



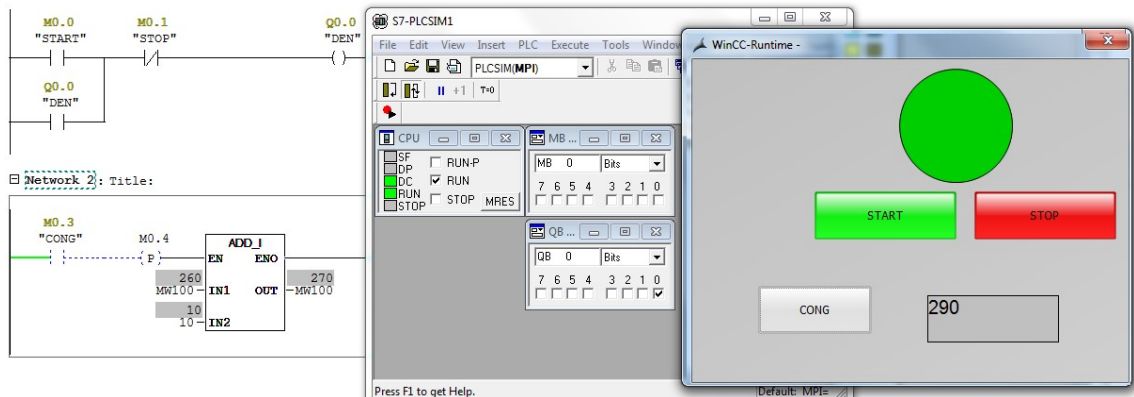
Hình 7.40: Tạo Tag interger cho phép cộng trên WinCC

Qua cửa sổ giao diện thiết kế tạo một nút CONG và một vùng nhớ I/O field, đặt thuộc tính cho nút cộng tương tự như nút START, STOP trên và thuộc tính cho I/O field.



Hình 7.41: Thiết lập thuộc tính của nút CONG và KETQUA

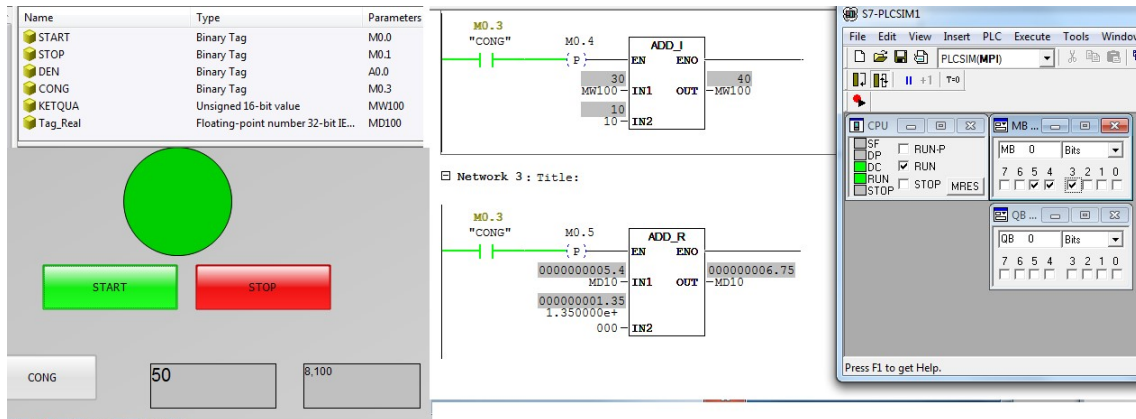
Các kết quả được thực hiện cho số nguyên như sau



Hình 7.42: Kết quả xây dựng Tag số nguyên cho phép cộng 10

Bài toán về tạo một dự án cho Tag số thực (VD3)

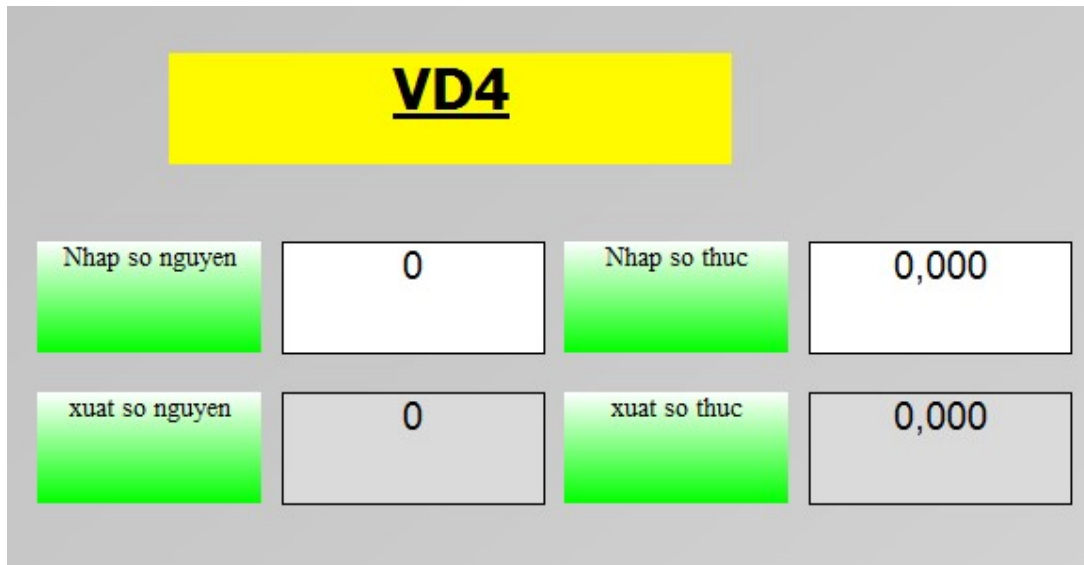
Tương tự như Tag interger (biến số nguyên), Tag real được thực hiện tương tự, trong đó MW thay bằng MD.



Hình 7.43: Kết quả thiết kế giao tiếp PLC S7-300 với Tag real

### 7.3.3 Nhập xuất số thực và số nguyên trong WinCC

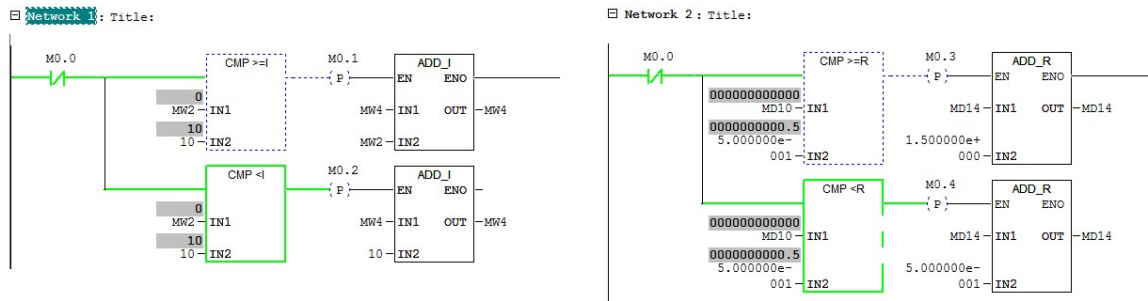
Tạo dự án VD4, thiết kế giao diện Vd4 với vùng xuất nhập bằng cách, chọn I/O field với tên nhãn kèm theo là nhập tương tự cho vùng xuất. Đặt thuộc tính cho vùng nhập dữ liệu bằng cách Click chuột phải vào I/O field/ Effects/ Global.../ No. sang mục Colors/ Background chọn màu trắng vùng nhập và màu nâu cho vùng xuất.



Hình 7.44: Thiết kế giao diện nhập xuất giá trị số nguyên và số thực

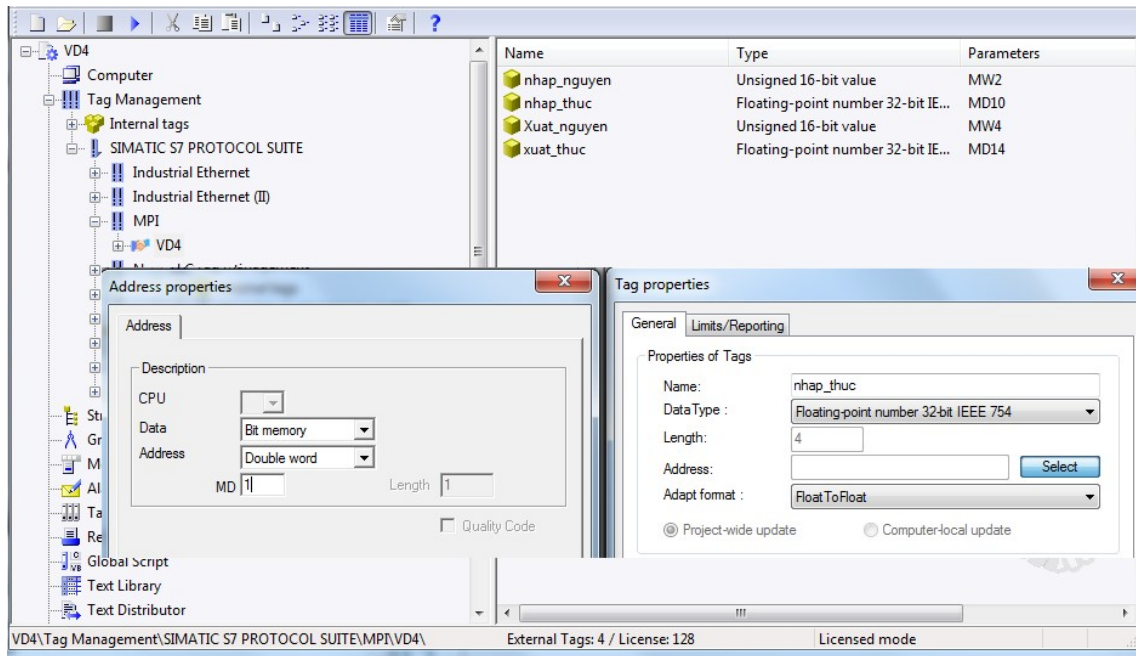
Xây dựng chương trình S7-300, chương trình nhập vào số nguyên và số thực. Nếu vùng nhập số nguyên MW2 có giá trị lớn hơn 10 thì vùng hiển thị MW4 = MW4+MW2 và nếu nhỏ hơn 10 thì MW2= MW2+10. Tương tự số thực nếu vùng nhập MD10 >0.5 thì vùng hiển thị MD14=MD14+1.5, nếu nhỏ hơn thì MD14=MD14+0.5



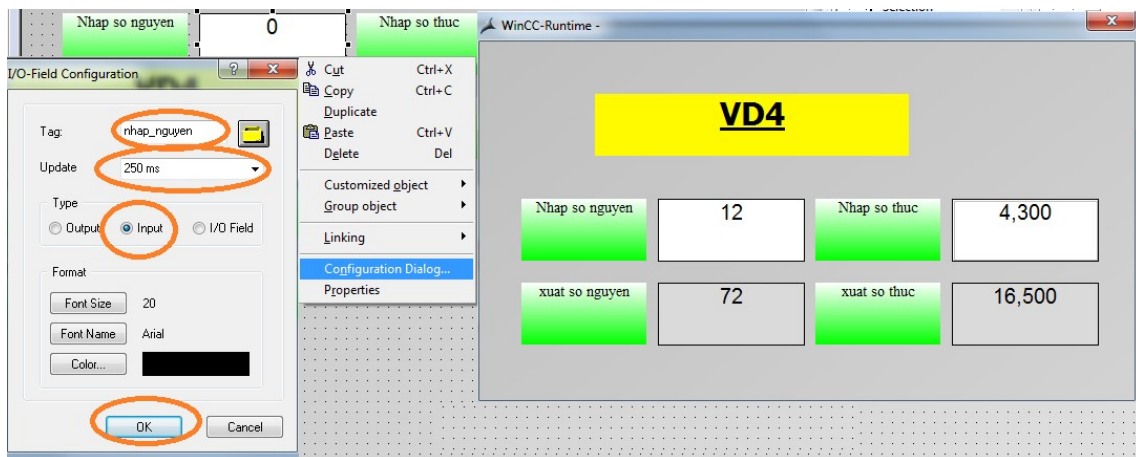


Hình 7.45: Chương trình cho VD4

Xây dựng các Tag cho chương trình bao gồm 4 Tag: nhap\_nguyen, nhap\_thuc, xuất\_nguyen, xuất\_thuc, tương ứng với các địa chỉ, MW2, MW4, MD10, MD14



Hình 7.46: Cấu hình Tag cho WinCC

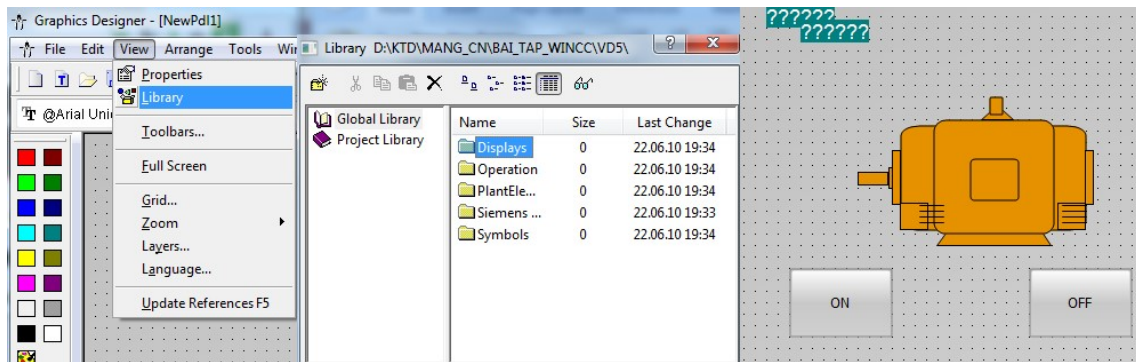


Hình 7.47: Kết quả thực hiện xuất nhập số nguyên và số thực trên WinCC

Gán biến Tag cho giao diện thiết kế, từ vùng nhập Field I/O click chuột phải vùng nhập số nguyên/ Configuration Dialog/ chọn Tag nhap\_nguyen, thời gian cập nhật 250ms, chọn Type Input. Tương tự cho nhập số thực với Tag nhap\_thuc và vùng xuất thì Type chọn iutput. Ngược lại hai vùng xuất thay đổi Input thành Output tương ứng với các biến xuất và chạy kết quả

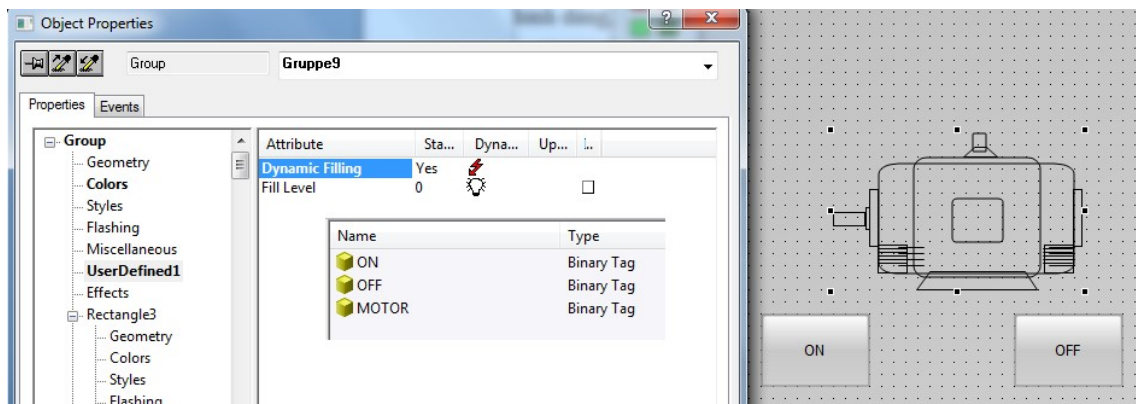
### 7.3.4 Khai thác đối tượng thư viện trong WinCC

Tạo một dự án VD5, mở một Graphics VD5, View/ Library/ Displays, tại thư viện này có nhiều đối tượng thiết kế sẵn như đồng hồ đo, các thang chia độ, các cảnh báo, các logo, hiển thị số, kim... chúng ta có thể kéo thả và thay đổi các thuộc tính Properties. Ví dụ thay đổi thuộc tính động cơ trong thư viện PlantElements/ Motors này, thay đổi thuộc tính cho động cơ bằng cách click chuột phải Properties/ màu sắc, hình dáng, hiệu ứng...



Hình 7.48: Khai thác thư viện có trong WinCC

Thực hiện On/off ứng với động cơ đổi màu trạng thái Xanh/Đỏ. Tạo thiết kế giao diện gồm động cơ và hai nút nhấn ON/OFF.



Hình 7.49: Xây dựng thuộc tính cho đối tượng thư viện

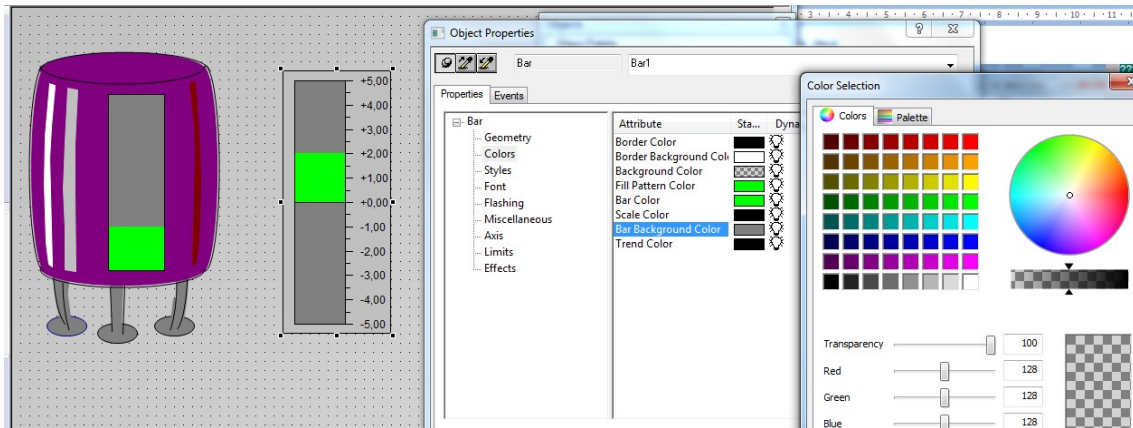
Tạo 3 biến nội trong Tag nội: ON, OFF, MOTOR đều kiểu Binary Tag. Xây dựng hiệu ứng như trường hợp đèn đường tròn, ở đây lựa chọn UserDefined1 để cho phép

thay đổi hình nền đối trong thư viện. thay đổi một số thuộc tính cần thiết như màu sắc, giá trị max, min, giá trị ban đầu, màu nền, màu viền cần thiết...

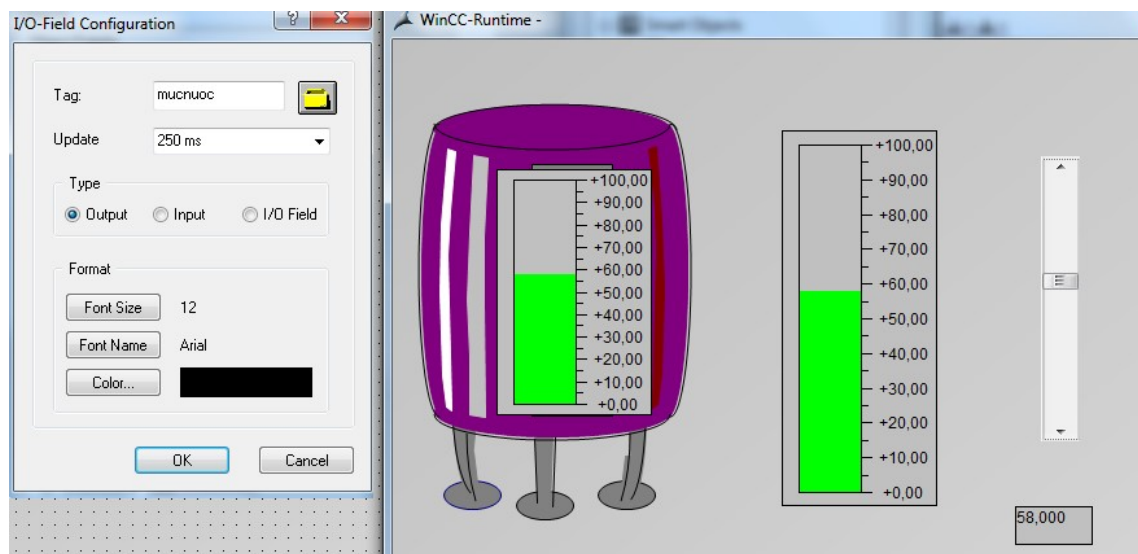
### 7.3.5 Tạo thanh trượt trong WinCC

Tạo một dự án mới, với VD6, thiết kế thanh Bar trong Smart Object/ Bar, kết hợp với một bồn nước có trong thư viện để kéo lên xuống, đặt các thuộc tính màu sắc, màu nền, màu khung viền và giá trị min, max, giá trị khởi đầu cho thanh bar trong Miscellaneous.

Tạo một Tag nội có tên “mucnuoc” kiểu số thực, trở lại với giao diện thiết kế, chọn Bar, click chuột phải để vào Bar Configuration chèn Tag “mucnuoc” cho tất cả các đối tượng cần lên xuống. Để cho mức nước lên xuống ta cần một thanh trượt Slider trong Windows Object, chọn thuộc tính cho Sider giống với các Bar vừa rồi cũng Tag “mucnuoc”, thời gian update 250ms, giá trị min, max.



Hình 7.50: Cài đặt thuộc tính màu sắc thanh Bar



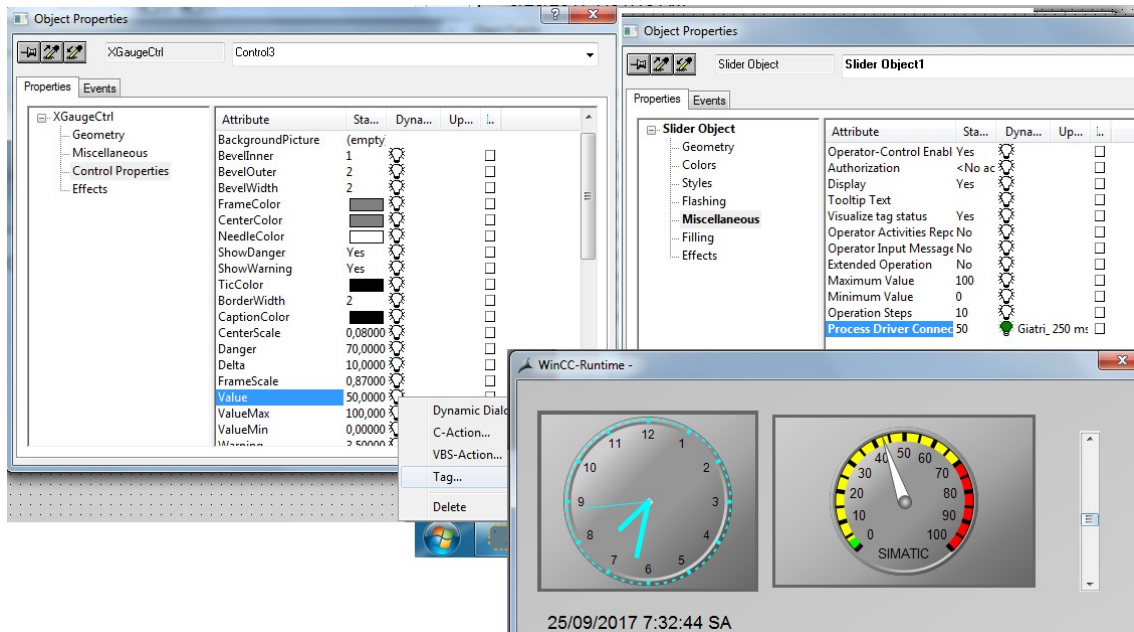
Hình 7.51: Kết quả sử dụng thanh trượt

Thêm I/O field với các thuộc tính cấu hình Configuration giống như các đối tượng trên, Type chọn Output.

### 7.3.6 Xử lý timer trong WinCC

Tạo dự án VD7, mở giao diện Graphics Designer, tại thanh công cụ bên phải Objects, chọn sheet Controls/ chọn WinCC Digital/Analog Clock đặt vào giao diện thiết kế, nhấp đúp để thay đổi các thuộc tính cho đồng hồ, hình dạng số hoặc kim thù thích, khi chạy đồng hồ sẽ thực hiện thao thời gian thực, là thời gian máy tính.

Loại thứ hai là đồng hồ hiển thị giá trị theo biến Tag nào đó, như thang đo, giá trị đo nhiệt độ... chọn từ mục WinCC Gauge Control. Trường hợp này tạo Tag có tên Giatri\_dongho kiểu số thực, thay đổi các thuộc tính trong Properties về hình dáng màu sắc... gán Tag bằng cách click chuột phải, Properties/ control Properties/ Value, click chuột phải Dynamic tại giá trị Value/ Tag chèn Tag Giatri\_dongho vào, thay đổi thời gian 250ms. Tương tự ta tạo một thanh Bar để kéo thanh trượt thay đổi biên nội Tag Giatri\_dongho để đồng hồ đo giá trị.



Hình 7.52: Đặt thuộc tính sử dụng đồng hồ trong WinCC

### 7.3.7 Tạo nút ấn hai tác động

Tạo một dự án mới VD8, mở giao diện thiết kế, thiết kế động cơ trong thư viện, với một nút nhấn. Tạo một Tag nội có tên DONGCO kiểu nhị phân, sau đó viết code C cho nút nhấn:

```
BOOL bit;
bit=GetTagBit("DONGCO");
```

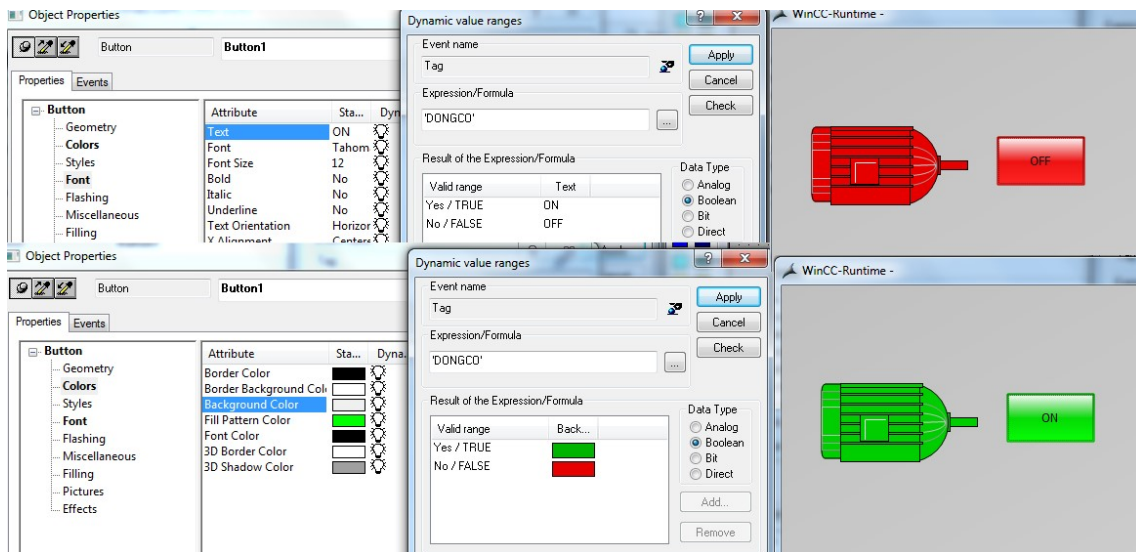


```

if (bit==0)
SetTagBit("DONGCO",1);
if (bit==1)
SetTagBit("DONGCO",0);

```

Tiếp theo đặt thuộc tính hiển thị Text của nút nhấn ON/OFF bằng cách vào Properties/ Button/ Font Text, click chuột phải vào Dynamic/ Dynamic Dialog, chèn Tag DONGCO vào, thời gian 250ms, chọn Data type là kiểu Boolean tại No/False đổi thuộc tính thành OFF, tương tự cho màu sắc, của nút ấn và cả động cơ.



Hình 7.53: Kết quả xây dựng một nút hai tác động trên WinCC

### 7.3.8 Tạo chuyển động thẳng trong WinCC

Tạo một dự án có tên VD9, tạo Tag nội LEN, XUONG, DUNG cho 3 nút nhấn kiểu Binary. Bên cửa sổ thiết kế Graphics ta chèn một đối tượng có trong thư viện để chuyển động theo hướng lên xuống như Oto trong thư viện Siemens HMI/ Vehicles, đặt tên cho đối tượng là “XE” bằng cách Properties/ SymbolLibrary/ Object Name và tạo 3 nút nhấn lên xuống và dừng.

Tiến hành viết code C cho các nút nhấn: Đối với viết nút ấn “Lên 1” thì “Reset 2” nút còn lại về “0”

```

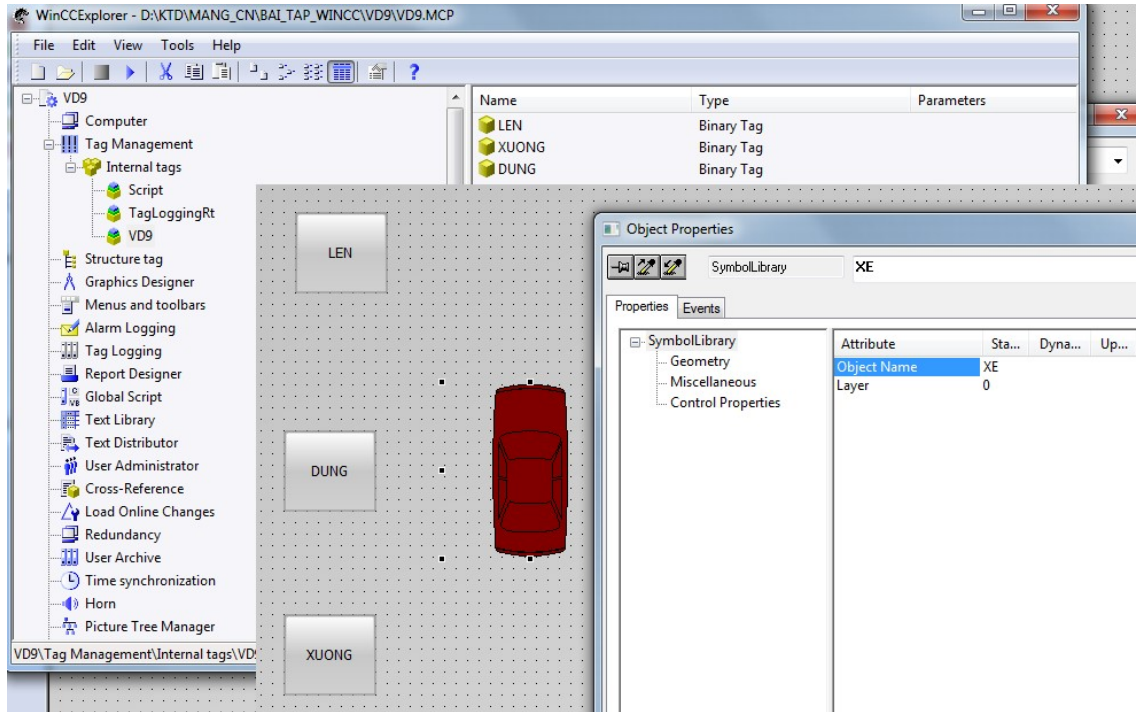
{
BOOL bit
bit=GetTagBit("LEN");
if(bit==0)
{

```

```

SetTagBit("LEN",1);
SetTagBit("XUONG",0);
SetTagBit("DUNG",0);
}

```



Hình 7.54: Thiết kế giao diện và Tag cho hệ thống chuyển động lên xuống

Tương tự, viết code C cho hai nút còn lại, có thể thay đổi màu sắc cho các nút bấm khi chạy như trong các ví dụ trước.

## 7.4 Câu hỏi ôn tập chương

Câu 7.1: Thiết kế hệ thống SCADA mở máy động cơ?

Câu 7.2: Thiết kế hệ thống SCADA cho hệ lưu lượng, mức?

Câu 7.3: Thiết kế hệ thống SCADA cho máy biến biến áp?

### Tài liệu tham khảo

- [1] Hoàng Minh Sơn, “Mạng Truyền Thông Công Nghiệp,” in *Nhà xuất bản khoa học và kỹ thuật*, 2004, p. 153.
- [2] K. Stouffer, J. Falco, and K. Kent, *Guide to supervisory control and data acquisition (SCADA) and industrial control systems security*, vol. Technology, no. Special Publication Special Publication 800-82. 2006.
- [3] F. Y. Wang, Y. H. Ni, Z. X. Liu, and Z. Q. Chen, “Fully distributed containment control for second-order multi-agent systems with communication delay,” *ISA Trans.*, no. xxxx, 2019.
- [4] Y. Wang, T. L. Nguyen, Y. Xu, and D. Shi, “Distributed control of heterogeneous energy storage systems in islanded microgrids: Finite-time approach and cyber-physical implementation,” *Int. J. Electr. Power Energy Syst.*, vol. 119, no. May 2019, p. 105898, 2020.
- [5] H. Q. K. Lu, “Network smart card review and analysis,” *Comput. Networks*, vol. 51, no. 9, pp. 2234–2248, 2007.
- [6] P. Spieth, T. Roeth, and S. Meissner, “Reinventing a business model in industrial networks: Implications for customers’ brand perceptions,” *Ind. Mark. Manag.*, vol. 83, no. August 2018, pp. 275–287, 2019.
- [7] M. Hussain, A. W. Abdul Wahab, A. T. S. Ho, N. Javed, and K. H. Jung, “A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement,” *Signal Process. Image Commun.*, vol. 50, pp. 44–57, 2017.
- [8] I. Özçelik and H. Ekiz, “Building an interconnection between PROFIBUS and ATM networks,” *J. Netw. Comput. Appl.*, vol. 30, no. 2, pp. 800–817, 2007.
- [9] E. A. Mossin, G. S. Sestito, R. V. Torres, and D. Brandão, “Fuzzy system for calculating the Target Rotation Time in Profibus networks,” *IFAC-PapersOnLine*, vol. 49, no. 30, pp. 272–277, 2016.
- [10] Y. Lu, X. Hong, J. Liu, L. Xu, C. Guo, and S. He, “IRZ-Manchester coding for downstream signal modulation in an ONU-source-free WDM-PON,” *Opt. Commun.*, vol. 284, no. 5, pp. 1218–1222, 2011.
- [11] T. Huang and J. Sun, “NRZ to Manchester code conversion based on nonlinear optical fiber loop mirror,” *Opt. Commun.*, vol. 285, no. 16, pp. 3524–3528, 2012.
- [12] W. hong-you and Z. san-ping, “The Predigest Project of TCP/IP Protocol Communication System Based on DSP Technology and Ethernet,” *Phys. Procedia*, vol. 25, pp. 1253–1257, 2012.
- [13] P. Plesowicz, “Secure signal tunneling for SCADA and PLCs using SSH protocol,” *IFAC Proc. Vol.*, vol. 37, no. 20, pp. 88–93, 2004.
- [14] S. Senthivel, I. Ahmed, and V. Roussev, “SCADA network forensics of the PCCC protocol,” *DFRWS 2017 USA - Proc. 17th Annu. DFRWS USA*, vol. 22, pp. S57–S65, 2017.
- [15] H. Zhang, Y. Li, and H. Zhu, “Development for protocol conversion gateway of Profibus and Modbus,” *Procedia Eng.*, vol. 15, pp. 767–771, 2011.
- [16] E. Baccarelli, P. G. Vinueza Naranjo, M. Shojafar, and M. Scarpiniti, “Q\*: Energy and delay-efficient dynamic queue management in TCP/IP virtualized data centers,” *Comput. Commun.*, vol. 102, pp. 89–106, 2017.
- [17] P. Drahoš and I. Bélai, “The PROFIBUS protocol observation,” *IFAC Proc. Vol.*, vol. 9, no. PART 1, pp. 258–263, 2012.



- [18] D. J. Kang, J. J. Lee, B. H. Kim, and D. Hur, "Proposal strategies of key management for data encryption in SCADA network of electric power systems," *Int. J. Electr. Power Energy Syst.*, vol. 33, no. 9, pp. 1521–1526, 2011.
- [19] S. Vitturi, "Some features of two fieldbuses of the IEC 61158 standard," *Comput. Stand. Interfaces*, vol. 22, no. 3, pp. 203–215, 2000.
- [20] T. CHERIFI and L. HAMAMI, "A practical implementation of unconditional security for the IEC 60780-5-101 SCADA protocol," *Int. J. Crit. Infrastruct. Prot.*, vol. 20, pp. 68–84, 2018.
- [21] Z. Lin, X. Liu, and M. Collu, "Wind power prediction based on high-frequency SCADA data along with isolation forest and deep learning neural networks," *Int. J. Electr. Power Energy Syst.*, vol. 118, no. January, p. 105835, 2020.
- [22] K. P. Q. H. TS. Lê Ngọc Bích, "Mạng Truyền Thông Công Nghiệp Scada Lý Thuyết - Thực Hành," in *Nhà xuất Bản Thanh Niên*, 2019, p. 446.
- [23] E. Chacón and O. Llanes Santiago, "Definition of a control service in the application layer of the ISO/OSI reference model for control stations," *Comput. Ind.*, vol. 20, no. 2, pp. 187–192, 1992.
- [24] M. P. Vigliassi, J. A. D. Massignan, A. C. B. Delbem, and J. B. A. London, "Multi-objective evolutionary algorithm in tables for placement of SCADA and PMU considering the concept of Pareto Frontier," *Int. J. Electr. Power Energy Syst.*, vol. 106, no. August 2018, pp. 373–382, 2019.
- [25] Hoàng Minh Sơn, "Mạng truyền thông công nghiệp," in *Nhà xuất bản kHoa học và Kỹ thuật*, no. NXB kHoa học và Kỹ thuật, 2014, p. 153.
- [26] J. Pena Ramirez, E. Garcia, and J. Alvarez, "Master-slave synchronization via dynamic control," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 80, p. 104977, 2020.
- [27] T. Pfeifer, H. Thrum, and H. Seong Park, "Open Model for the Integration of Various Fieldbus Systems," *IFAC Proc. Vol.*, vol. 30, no. 15, pp. 105–110, 1997.
- [28] Siemens, "Simatic WinCC flexible," in *Flexibility in any HMI applications – from the Micro Panel to the PC*, no. March, 2010, p. 32.
- [29] N. Tekin and V. C. Gungor, "The impact of error control schemes on lifetime of energy harvesting wireless sensor networks in industrial environments," *Comput. Stand. Interfaces*, vol. 70, p. 103417, 2020.
- [30] R. Štohl and S. Šedivá, "Using a Hierarchical Industrial Communication Model via the Common Industrial Protocol in a Small Distillation Column," *IFAC-PapersOnLine*, vol. 52, no. 27, pp. 484–489, 2019.
- [31] Z. Latif, K. Sharif, F. Li, M. M. Karim, S. Biswas, and Y. Wang, "A comprehensive survey of interface protocols for software defined networks," *J. Netw. Comput. Appl.*, vol. 156, p. 102563, 2020.
- [32] D. Bailey and E. Wright, *Practical SCADA for Industry*. 2003.
- [33] J. B. Almeida, J. S. Pinto, and M. Vilaça, "Token-passing Nets for Functional Languages," *Electron. Notes Theor. Comput. Sci.*, vol. 204, no. C, pp. 181–198, 2008.
- [34] A. Ciuffoletti, "Secure token passing at application level," *Futur. Gener. Comput. Syst.*, vol. 26, no. 7, pp. 1026–1031, 2010.
- [35] J. Woo Park, D.-W. Kim, and W. Hyun Kwon, "Analysis of the IEEE 802.4 Token Passing Bus Network with Finite Buffers and Single Priority," *IFAC Proc. Vol.*, vol. 28, no. 22, pp. 129–134, 1995.

- [36] R. Ranjan, D. Swain, and B. Paikaray, “Efficient Key Management and Cipher Text Generation Using BCD Coded Parity Bits,” *Procedia Comput. Sci.*, vol. 57, pp. 703–709, 2015.
- [37] X. Hu, D. Wang, Y. Lin, W. Su, Y. Xie, and L. Liu, “Multi-channel time frequency shift keying in underwater acoustic communication,” *Appl. Acoust.*, vol. 103, pp. 54–63, 2016.
- [38] N. Marriwala, O. P. Sahu, and A. Vohra, “Design of a hybrid reconfigurable Software Defined Radio transceiver based on frequency shift keying using multiple encoding schemes,” *Egypt. Informatics J.*, vol. 17, no. 1, pp. 89–98, 2016.
- [39] F. Obite, E. T. Jaja, G. Ijeomah, and K. I. Jahun, “The evolution of Ethernet Passive Optical Network (EPON) and future trends,” *Optik (Stuttg.)*, vol. 167, pp. 103–120, 2018.
- [40] V. M. Ijure, S. A. Laughter, and R. D. Williams, “Security issues in SCADA networks,” *Comput. Secur.*, vol. 25, no. 7, pp. 498–506, 2006.
- [41] D. T. Bình and V. M. Trí, “Hệ thống SCADA cho mạng điện cơ quan, doanh nghiệp,” *Can Tho Univ. J. Sci.*, vol. 49, p. 21, 2017.
- [42] Siemens, “Simatic Controllers,” in *The innovative solution for all automation tasks*, no. April, 2011, pp. 1–10.
- [43] Office of the Manager National Communications System, *Supervisory Control and Data Acquisition (SCADA) Systems*, no. October. 2004.
- [44] X. Zhang, H. H. Chen, Z. Zhang, and Y. Liu, “Electric-field assisted spin torque nano-oscillator and binary frequency shift keying modulation,” *J. Magn. Magn. Mater.*, vol. 452, pp. 458–463, 2018.
- [45] E. AB, “Soft starter instruction manual,” in *Valid for the following Soft starter Models: MSF-017 to MSF-1400*, 2001, pp. 1–86.
- [46] M. Tabaa, B. Chouri, S. Saadaoui, and K. Alami, “Industrial Communication based on Modbus and Node-RED,” *Procedia Comput. Sci.*, vol. 130, pp. 583–588, 2018.
- [47] X. Wu and L. Xie, “Performance evaluation of industrial Ethernet protocols for networked control application,” *Control Eng. Pract.*, vol. 84, no. November 2018, pp. 208–217, 2019.
- [48] M. Müller, J. Klöckner, and W. Fengler, “Bit accurate timing analysis on a frame based CAN model,” *IFAC Proc. Vol.*, vol. 4, no. PART 1, pp. 114–119, 2009.
- [49] I. V. Sita and A. C. Fărcaș, “Interfacing city resources management system with SIMATIC WinCC,” *IFAC Proc. Vol.*, vol. 2, no. PART 1, pp. 113–118, 2013.
- [50] R. Pribiš, L. Beňo, and P. Drahoš, “Implementation of Micro embedded OPC Unified Architecture server-client,” *IFAC-PapersOnLine*, vol. 52, no. 27, pp. 114–120, 2019.
- [51] A. G. Finogeev and A. A. Finogeev, “Information attacks and security in wireless sensor networks of industrial SCADA systems,” *J. Ind. Inf. Integr.*, vol. 5, pp. 6–16, 2017.
- [52] T. Zheng *et al.*, “High-performance potassium sodium niobate piezoceramics for ultrasonic transducer,” *Nano Energy*, vol. 70, p. 104559, 2020.
- [53] D. Chen *et al.*, “An optimization design strategy of 1–3 piezocomposite ultrasonic transducer for imaging applications,” *Mater. Today Commun.*, vol. 24, 2020.

- [54] A. Alekseev, “Young Professional’s In-house Communication Features at Industrial Enterprises of Russia,” *Procedia - Soc. Behav. Sci.*, vol. 236, no. December 2015, pp. 301–304, 2016.
- [55] Siemens, “WinCC flexible 2008 - Creating Projects,” in *use WinCC flexible and install a license with the Automation License Manager*, 2008, pp. 1–21.
- [56] Siemens, “Sinumerik Machine data and parameters,” *Mach. data parameters Param. Man. 03/2013, 6FC5397-7AP40-3BA1*, vol. Parameter, pp. 1–1728, 2013.
- [57] T. V. Bhaskarwar, S. S. Giri, and R. G. Jamakar, “Automation of shell and tube type heat exchanger with PLC and LabVIEW,” *2015 Int. Conf. Ind. Instrum. Control. ICIC 2015*, no. Icic, pp. 841–845, 2015.