Độ tin cậy và tính sẵn sàng trong các hệ thống điều khiển và giám sát

Các chủ đề

- Khái niệm độ tin cậy và tính sẵn sàng
- Các sách lược dự phòng
- Các biện pháp dự phòng nóng
- Cơ chế an toàn
- Cơ chế khởi động lại
- Cơ chế an toàn
- Cơ chế bảo mật
- Cơ chế bảo trì

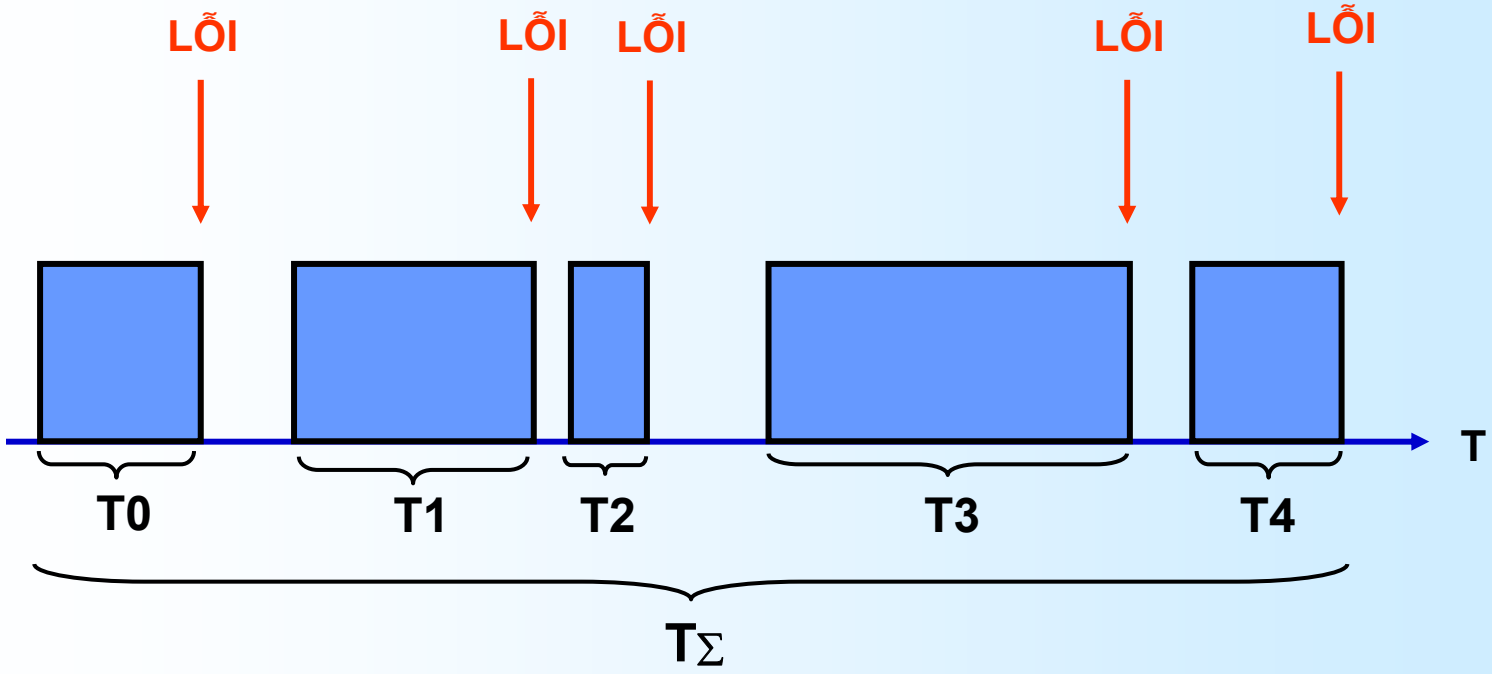
Độ tin cậy

- Khả năng làm việc không gây ra lỗi của hệ thống, được đánh giá qua:
  - Thời gian trung bình tới khi gặp lỗi (Mean Time To Failure, MTTF)
  - Thời gian trung bình giữa hai lần lỗi (Mean Time Between Failures, MTBF) hoặc số lỗi trung bình trên một đơn vị thời gian
- Tính sẵn sàng phụ thuộc vào:
  - Độ tin cậy của từng thiết bị
  - Cấu trúc hệ thống
  - Đặc điểm hệ thống truyền thông
  - Biện pháp dự phòng nóng

Tính sẵn sàng

- Khả năng hoạt động liên tục bình thường
  - Đánh giá qua tỉ lệ giữa tổng thời gian duy trì vận hành/ tổng thời gian dừng
  - Độ tin cậy quyết định tới tính sẵn sàng, nhưng không đồng nghĩa
- Tính sẵn sàng phụ thuộc vào:
  - Cơ chế dự phòng
  - Cơ chế an toàn
  - Cơ chế khởi động lại sau sự cố nguồn
  - Cơ chế bảo mật
  - Sách lược bảo trì, khả năng bảo trì
  - ...

Độ tin cậy và tính sẵn sàng



Độ tin cậy ⇔ MTBF ≈ (T0 + T1 + T2 + T3 + T4)/5

Tính sẵn sàng ≈ (T0 + T1 + T2 + T3 + T4)/TΣ

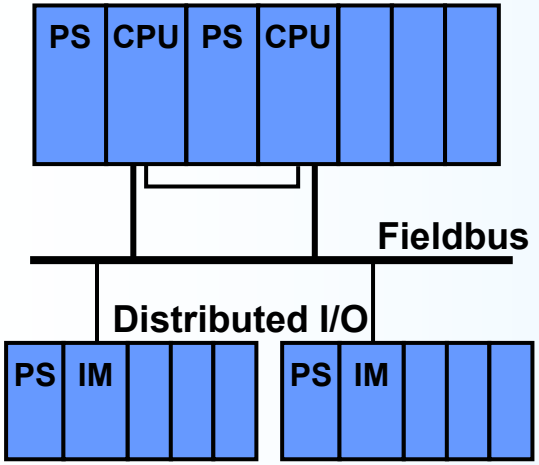
Cơ chế dự phòng

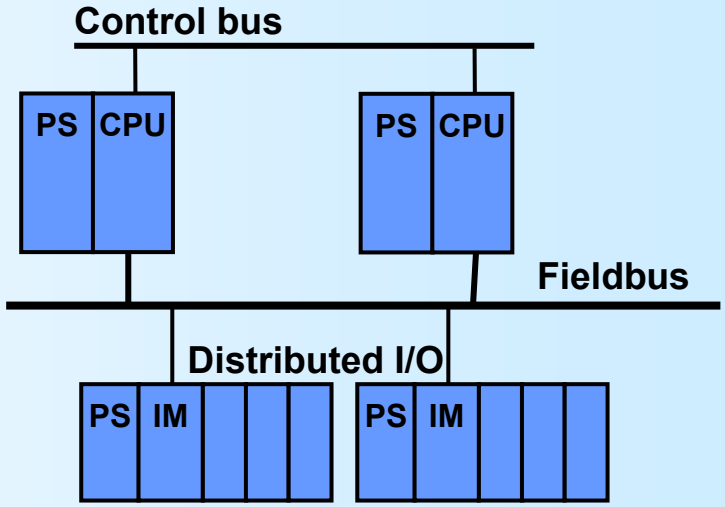
- Yêu cầu dự phòng:
  - Các thành phần quan trọng cần được dự phòng hoàn toàn để trường hợp lỗi một thành phần đơn (phần cứng & phần mềm) không làm mất đi tính năng do nó cung cấp
  - Lỗi mỗi module hoặc card được phép không gây ra tê liệt hơn một trạm vận hành hoặc một vòng điều khiển.
- Sách lược dự phòng
  - Dự phòng lạnh
    - Thay thế thiết bị offline
    - Thay thế thiết bị online
  - Dự phòng nóng
    - Dự phòng cạnh tranh
    - Dự phòng dự trữ

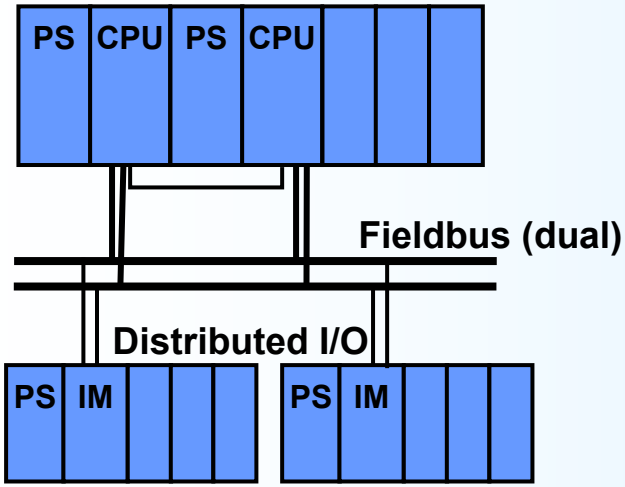
Các biện pháp dự phòng nóng

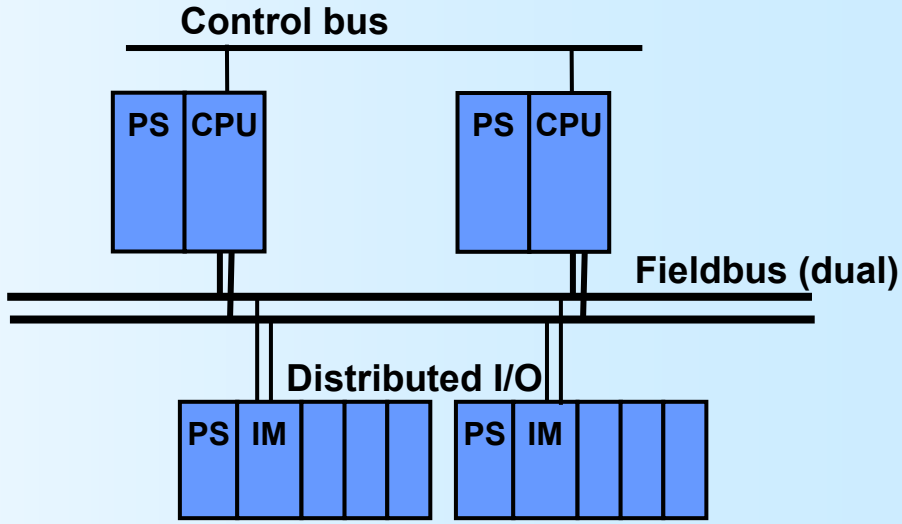
- Dự phòng CPU+nguồn:
  - Dự phòng cạnh tranh
  - Dự phòng dự trữ 1:1
- Dự phòng trạm điều khiển:
  - Dự phòng dự trữ 1:1, chuyển mạch kịp thời, trơn tru
- Dự phòng dự trữ hệ thống mạng:
  - Dự phòng cáp truyền
  - Dự phòng module truyền thông và các thiết bị mạng khác, chuyển mạch kịp thời, trơn tru
- Dự phòng vào/ra
- Dự phòng trạm vận hành 1:n
- Dự phòng trạm server 1:1

Các cấu trúc dự phòng cấp điều khiển





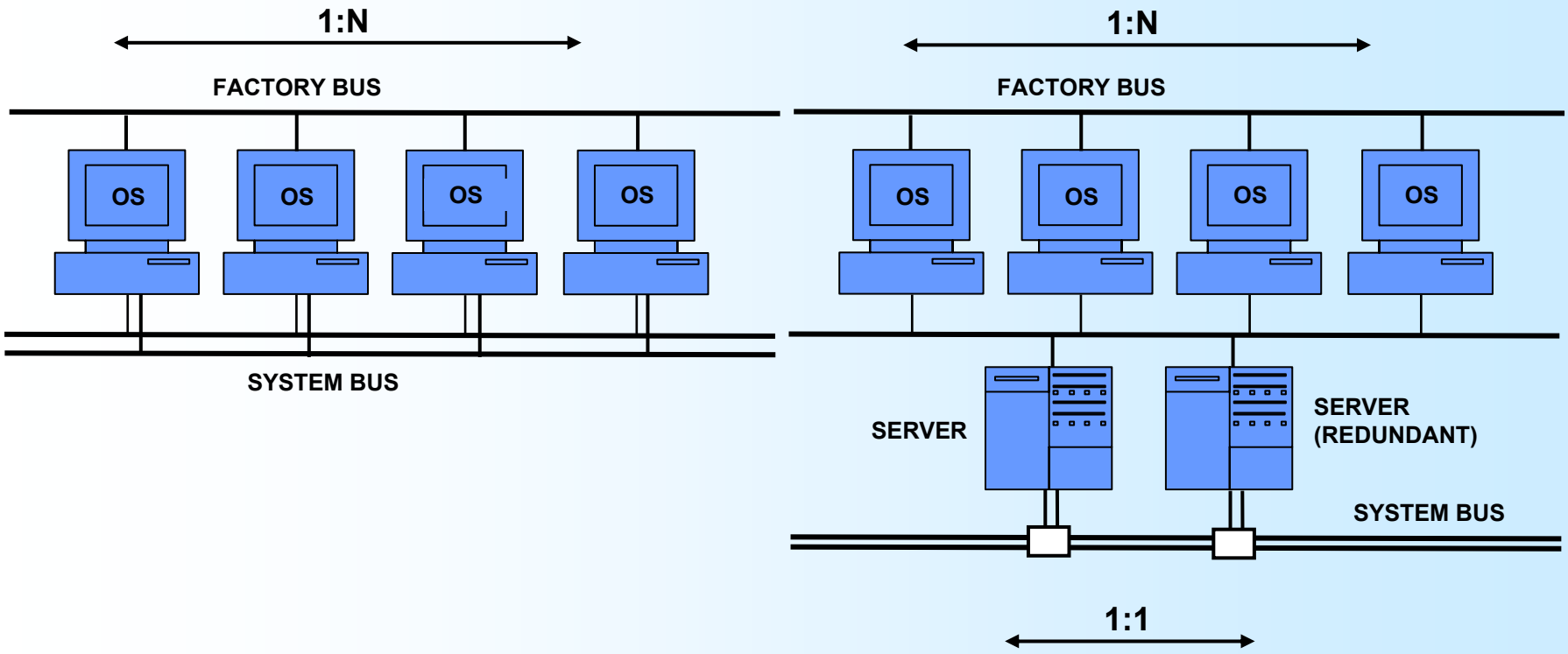




Các tình huống "chuyển mạch"

- Lỗi phần cứng bộ điều khiển tích cực
- Lỗi truyền thông giữa bộ điều khiển tích cực và các I/O
- Lỗi liên kết truyền thông giữa bộ điều khiển tích cực với mạng điều khiển
- Tách bộ điều khiển tích cực ra khỏi giá đỡ
- Yêu cầu chuyển mạch
- Lỗi nguồn cho bộ điều khiển tích cực
- Lỗi bộ nhớ của bộ điều khiển
- Lỗi phần mềm "treo" (phát hiện thông qua cơ chế watchdog và ngắt ngoại lệ).

Các cấu trúc dự phòng cấp ĐKGS



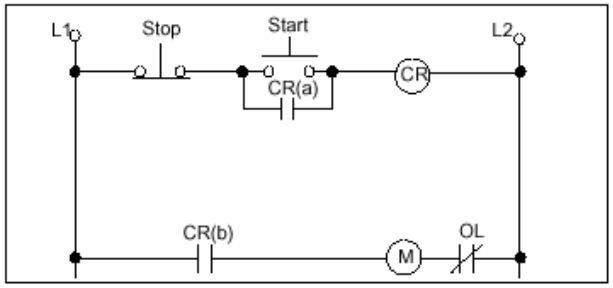
Cơ chế an toàn hệ thống

- Tầm quan trọng:
  - Bảo vệ người và thiết bị trong các tình huống nguy hiểm
  - Chi phí thực hiện phần an toàn nhiều khi vượt xa phần điều khiển thuần túy
- Hai biện pháp chính:
  - Dừng khẩn cấp (Emergency Shutdown) :Thông qua bấm nút dừng khẩn cấp hoặc tự động nhờ các cảm biến chuyển mạch
  - Tín hiệu ra tương tự hỗ trợ chế độ an toàn khi mất liên lạc với trạm điều khiển hoặc khi phát hiện trạm điều khiển có lỗi (giữ giá trị cuối hoặc đưa về giá trị mặc định.
- Các chuẩn thông dụng:
  - EN 60204–1: Safety of machinery – Electrical equipment of machines
  - EN 954–1: Safety of machinery – Safety related parts of control systems
  - EN 418: Safety of machinery – Emergency stop
  - IEC 61508: Standard for Programmable Safety Systems

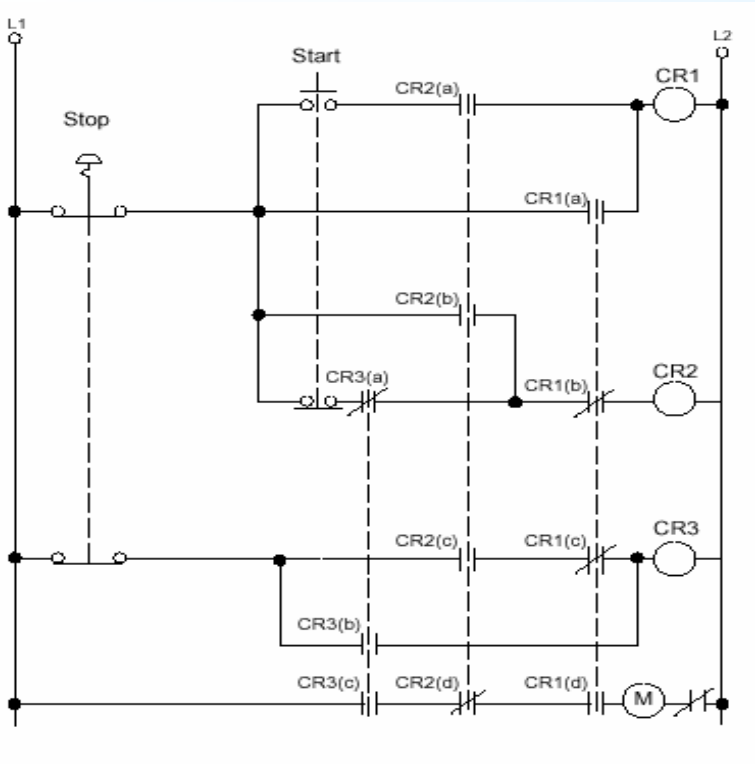
Các biện pháp dừng khẩn cấp

- Thiết bị dừng khẩn cấp (Emergency Shutdown Device, ESD):
  - Các nút dừng khẩn cấp (Emergency Stop Button)
  - Các cảm biến chuyển mạch an toàn (Safety Switch)
  - Các cơ cấu tự động phanh hãm
- Nguyên tắc:
  - Cắt nguồn ra khỏi các hệ truyền động
  - Có khả năng phanh hãm tự động ngay cả khi mất nguồn
  - Các thiết bị dừng khẩn cấp phải hoạt động trong bất kỳ tình huống nào (kể cả khi một tiếp điểm bị dính)

Giải pháp mạch cứng an toàn



Mạch không an toàn



Mạch có dự phòng và tự giám sát

- Phương pháp thực hiện
  - Sử dụng cơ chế dự phòng và tự giám sát
  - Sử dụng các tiếp điểm liên động (positive-guided contacts
- Nhược điểm:
  - Cấu trúc phức tạp, không linh hoạt -> khó khăn trong việc thiết kế và bảo trì
  - Số lượng lớn rơ-le, tiếp điểm
  - Tốn dây dẫn
  - Chiếm nhiều chỗ trong hộp điều khiển

  -> Giá thành tổng thể cao

Cơ chế khởi động lại sau sự cố

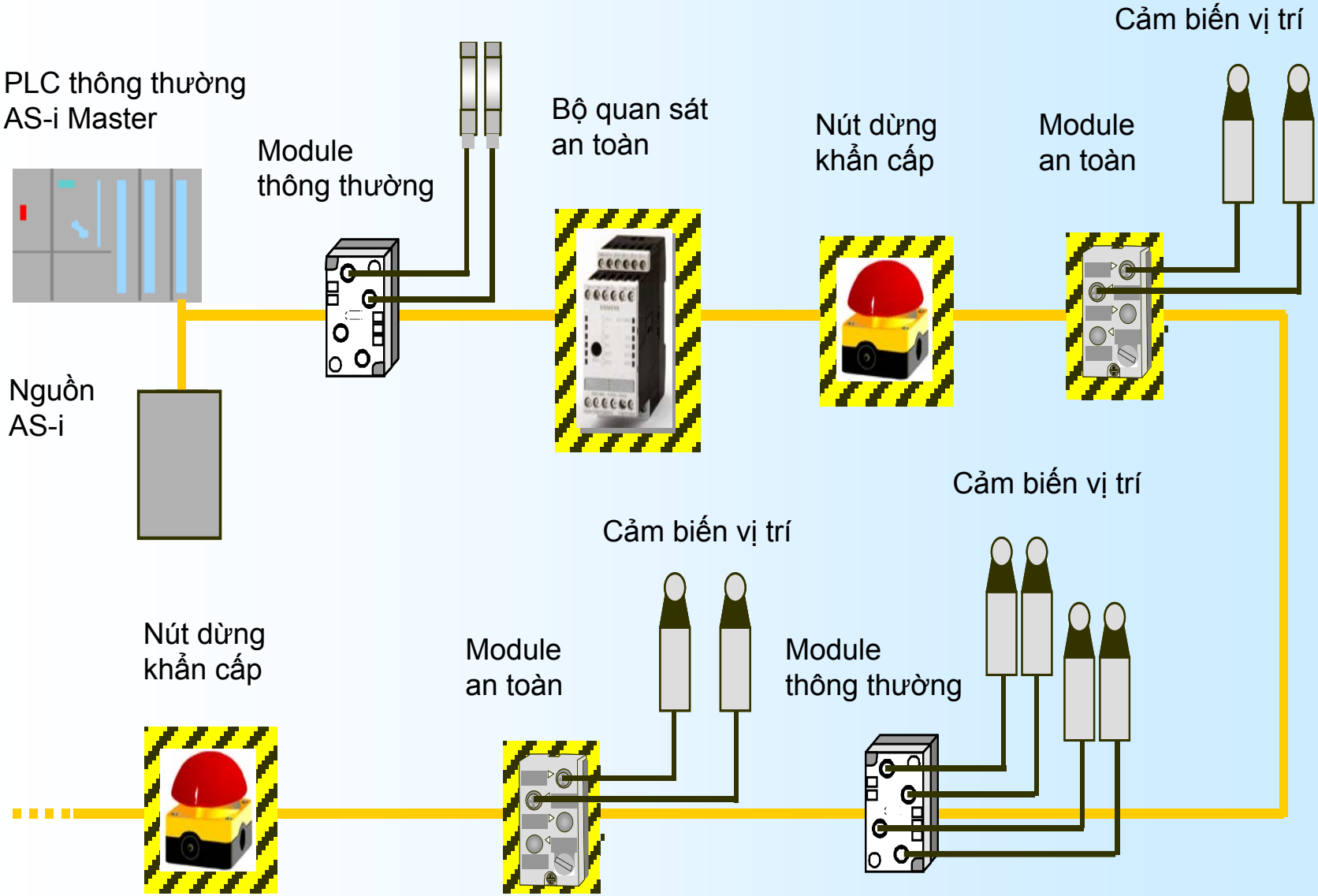
- Yêu cầu:
  - Các trạm điều khiển cần có khả năng tự phát hiện lỗi mất nguồn, thực hiện xử lý và đặt các tín hiệu ra về trạng thái an toàn, sau khi có nguồn trở lại phải có khả năng hồi phục trạng thái cũ
  - Các trạm vận hành phải có khả năng tự hồi phục trạng thái làm việc trước khi xảy ra sự cố
  - Tất cả các nút mạng phải có khả năng tự khởi động một cách độc lập với các nút khác
- Các biện pháp thực hiện:
  - Hệ điều hành tự động lưu giữ liên tục các dữ liệu trạng thái vào các vùng nhớ bền
  - Các trạm có cơ chế bắt tay để đồng bộ hóa dữ liệu và tiếp tục làm việc sau khi khởi động lại

Giải pháp "Bus an toàn"

- Một hệ thống bus an toàn
  - Cho phép các thiết bị ESD (*emergency shutdown devices*) sử dụng chung mạng với các thiết bị vào/ra thông thường.
  - Hỗ trợ mức SIL (*Safety Integrity Level*) phù hợp với yêu cầu của chức năng an toàn (theo chuẩn IEC 61508: *Standard for Programmable Safety Systems*)
- IEC 61508 yêu cầu một hệ bus an toàn
  - Truyền dẫn tin cậy tín hiệu từ các cảm biến an toàn để thực hiện ngắt mạch khi cần thiết
  - Tự động ngắt mạch cũng trong trường hợp lỗi thiết bị vào/ra hoặc lỗi bus

  ➔Thêm khả năng phát hiện lỗi bus và lỗi thiết bị so với bus thông thường
- Lợi thế của giải pháp bus an toàn
  - Độ linh hoạt cao, tiết kiệm dây dẫn, công nối dây, tích hợp khả năng chẩn đoán.

ASI – Safety at Work®



Cơ chế bảo mật

- Mục đích: Hạn chế và kiểm soát các quyền
  - Sửa đổi chương trình, chẩn đoán hệ thống
  - Truy nhập màn hình
  - Truy nhập dữ liệu
  - Điều khiển (đặt giá trị)
  - Xác nhận và xóa cảnh báo/báo động
- Đặt chế độ bảo mật
  - Theo trạm vận hành / trạm kỹ thuật
  - Theo người sử dụng hoặc theo nhóm người sử dụng
  - Theo từng phân đoạn
  - Theo từng cửa sổ, trang màn hình
  - Theo từng tag riêng rẽ
- Biện pháp:
  - Phần cứng: khóa an toàn (ví dụ trạm kỹ thuật)
  - Phần mềm: Đăng nhập tên sử dụng + mật khẩu

Sách lược bảo trì

- Phát hiện lỗi (*Fault Detection*):
  - Tình trạng lỗi, vị trí lỗi
  - Càng gần hiện trường càng tốt
- Chỉ thị lỗi (*Fault Indication*):
  - Chỉ thị lỗi tại chỗ: Mỗi thiết bị hoặc thành phần thiết bị cần được trang bị đèn chỉ thị trạng thái vận hành
  - Gửi thông báo lỗi thông qua hệ thống cảnh báo/báo động
- Chẩn đoán lỗi (*Fault Diagnosis*):
  - Chẩn đoán trực tuyến / chẩn đoán ngoại tuyến
  - Chẩn đoán tại chỗ / chẩn đoán từ xa
- Khắc phục lỗi (*Fault Recovery*):
  - Chế độ bảo trì: Cho phép người vận hành đưa trực tiếp giá trị biến quá trình, giá trị điều khiển
  - System back-up: Lưu trữ phần mềm công cụ và phần mềm ứng dụng, các tài liệu kỹ thuật.

Bảo trì phòng ngừa

- Bảo trì phòng ngừa (preventive maintenance):
  - Phát hiện các tình trạng nguy cơ lỗi, trước khi lỗi xảy ra
  - Thực hiện các biện pháp cần thiết (thay thế thiết bị, bảo dưỡng thiết bị, căn chỉnh,..)
- Các biện pháp chủ yếu:
  - Sử dụng các hệ thống phần mềm quản lý thiết bị, hỗ trợ lập lịch bảo dưỡng định kỳ
  - Sử dụng các thiết bị đo (nhiệt độ, dòng, áp, tốc độ, độ rung, tiếng ồn,...)
  - Sử dụng hệ thống phần mềm phân tích và chẩn đoán lỗi (các hệ chuyên gia, các tác tử di động)