Corso di "Sicurezza dei Sistemi di Controllo Industriale"
2024/25

Sistemi di controllo industriale – Produzione integrata – Modello di cybersecurity

Prof. Francesco Montefusco

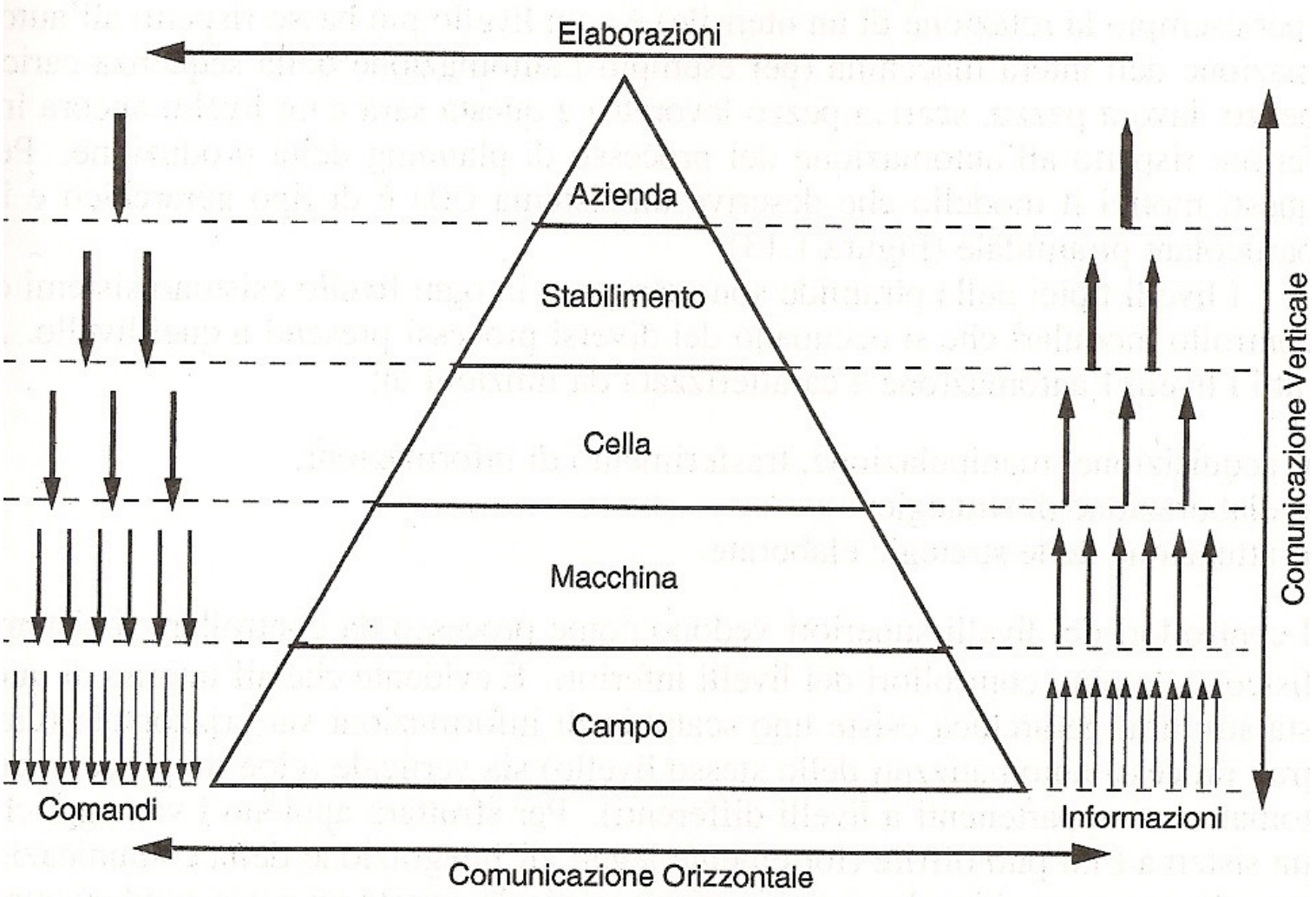
Department of Economics, Law, Cybersecurity, and Sports Sciences

Università degli studi di Napoli Parthenope

francesco.montefusco@uniparthenope.it

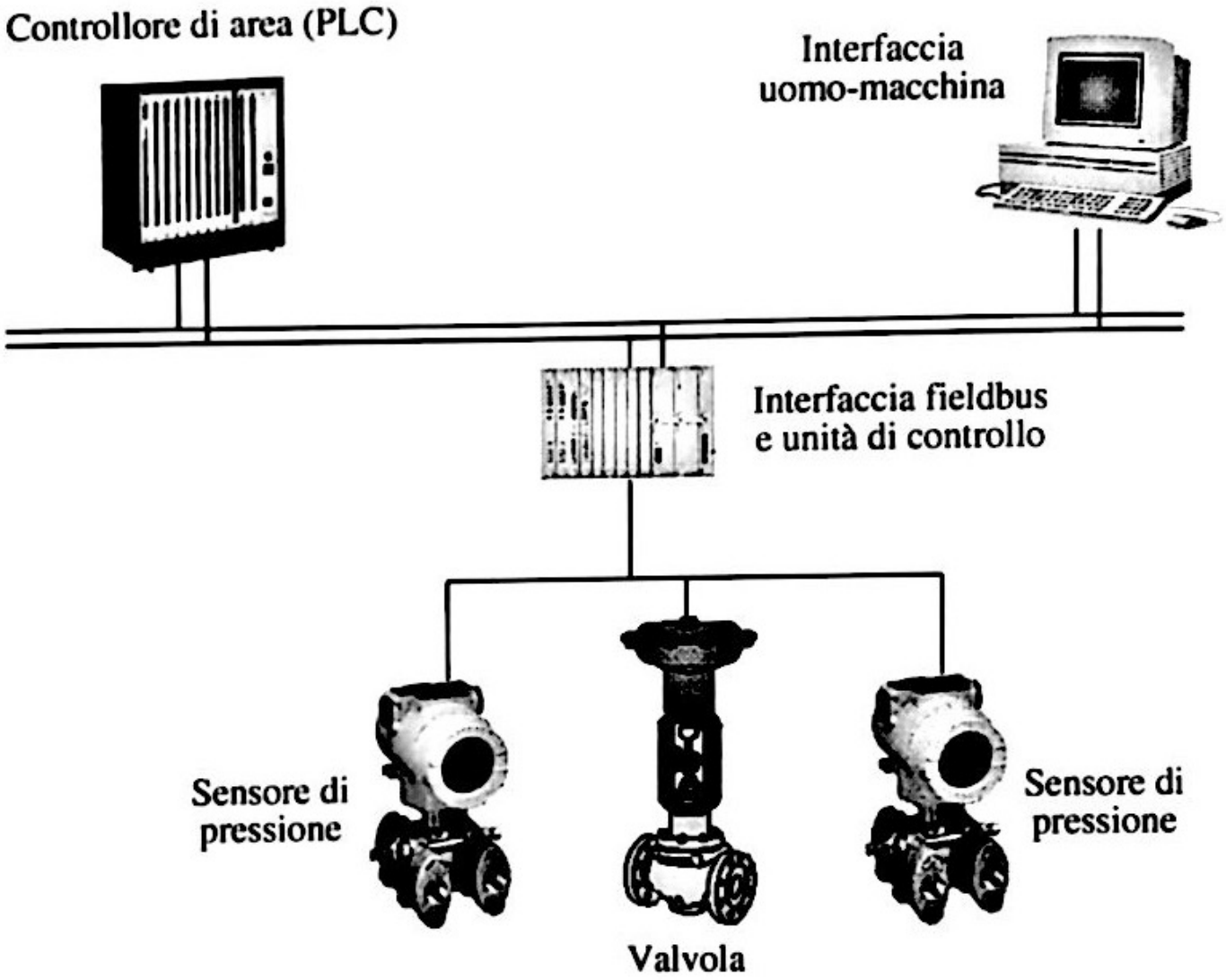
Team code**: 09tkpu5**

Piramide dell'automazione: Computer Integrated Manufacturing (CIM)



Modello di riferimento per la realizzazione dell'automazione industriale basata sul rilevamento, il coordinamento e la trasmissione di informazioni tra i vari sottosistemi mediante l'utilizzo di reti informatiche.

Esempio di implementazione di un sistema di controllo



Componenti base di un sistema di automazione

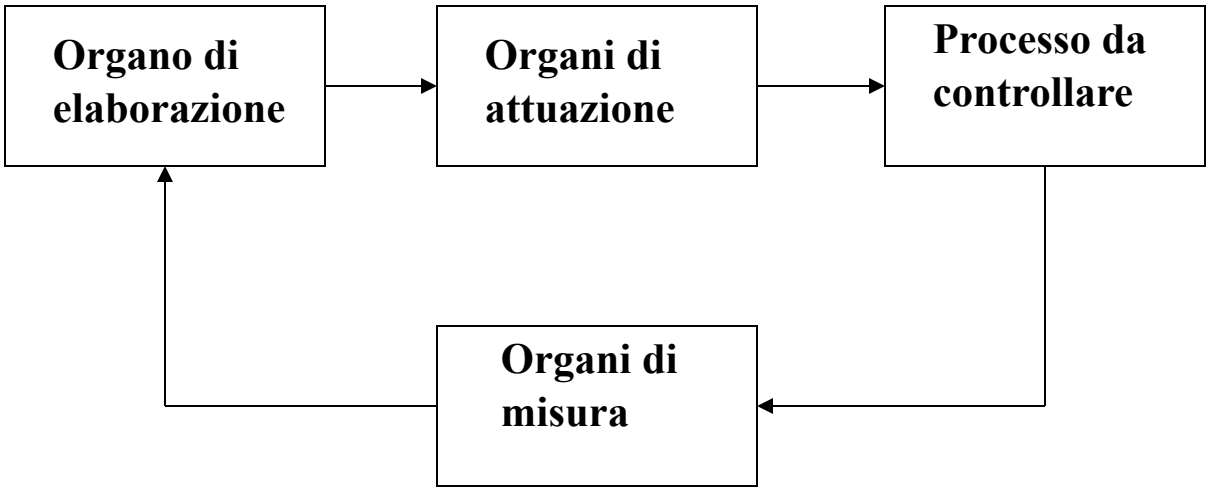
- ***Organi sensoriali:*** svolgono la funzione di misurare le grandezze di interesse per valutare lo stato di avanzamento e/o il corretto svolgimento del lavoro in esecuzione.

- ***Organi di elaborazione:*** sulla base delle misure fornite dagli organi sensoriali e degli obiettivi del lavoro in esecuzione, decidono le azioni da intraprendere.

- ***Organi di attuazione:*** eseguono le azioni comandate dagli organi di elaborazione.

Schema base di controllo in retroazione

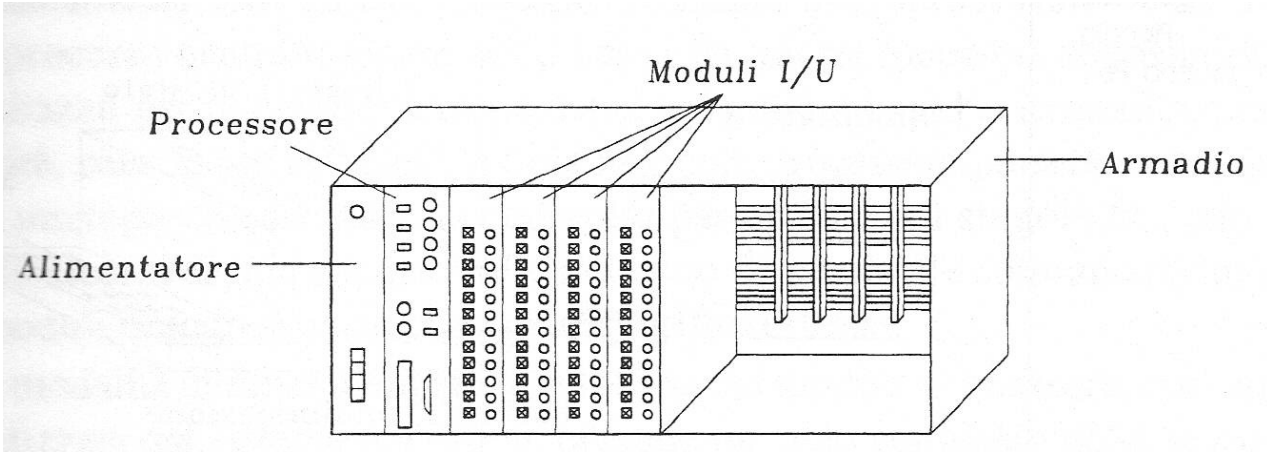
- Uno schema di controllo di base può essere costituito da un insieme di *sistemi* elementari, tra loro interagenti



PLC

- ***«Un PLC è un dispositivo o sistema elettronico a funzionamento digitale, destinato all'uso in ambito industriale, che utilizza una memoria programmabile per memorizzare informazioni o istruzioni, atte a realizzare specifiche funzioni, come quelle logiche, di sequenziamento, di temporizzazione, di conteggio e di calcolo aritmetico e per controllare mediante ingressi ed uscite sia digitali che analogiche, i vari tipi di macchine e processi»***

- Un PLC è composto dai seguenti cinque componenti fondamentali:
  - Armadio
  - Modulo processore
  - Moduli I/O
  - Alimentatore
  - Terminale di programmazione



- Modulo processore
  - Una scheda con uno o più microprocessori che controllano e supervisionano i programmi del sistema operativo e quelli generati dall'utente e una memoria dove questi programmi sono contenuti
  - Modalità di funzionamento più diffusa prevede un ciclo con le seguenti operazioni:
    - Aggiornamento area di memoria riservata agli ingressi fisici
    - Esecuzione programma/i utente
    - Esecuzione programma di gestione del sistema
    - Scrittura sulle uscite fisiche
  - Tempo di scansione
  - Unità di memoria dove sono contenuti i programmi e che può essere ripartita in
    - Area sistema operativo (ROM)
    - Area di lavoro del sistema operativo riservata (RAM)
    - Area ingressi/uscite (RAM)
    - Area programmi utente (di tipo RAM durante lo sviluppo degli stessi, che può essere sostituita da una PROM)
    - Area dati utente (RAM)

PLC - Moduli speciali

- Moduli di I/U remoto
- Moduli per la connessione in rete
- Moduli PID
- Moduli di servo
- Moduli di backup
- …

PLC – linguaggi di programmazione

- Linguaggi di programmazione grafica
  - Diagramma funzionale sequenziale (Sequential Functional Chart, SFC)
  - Linguaggio a contatti (Ladder Diagram)
  - Diagramma a blocchi funzionali (Functional Block Diagram, FBD)

- Linguaggi testuali
  - Lista di istruzioni
  - Testo strutturato

PLC – classificazione

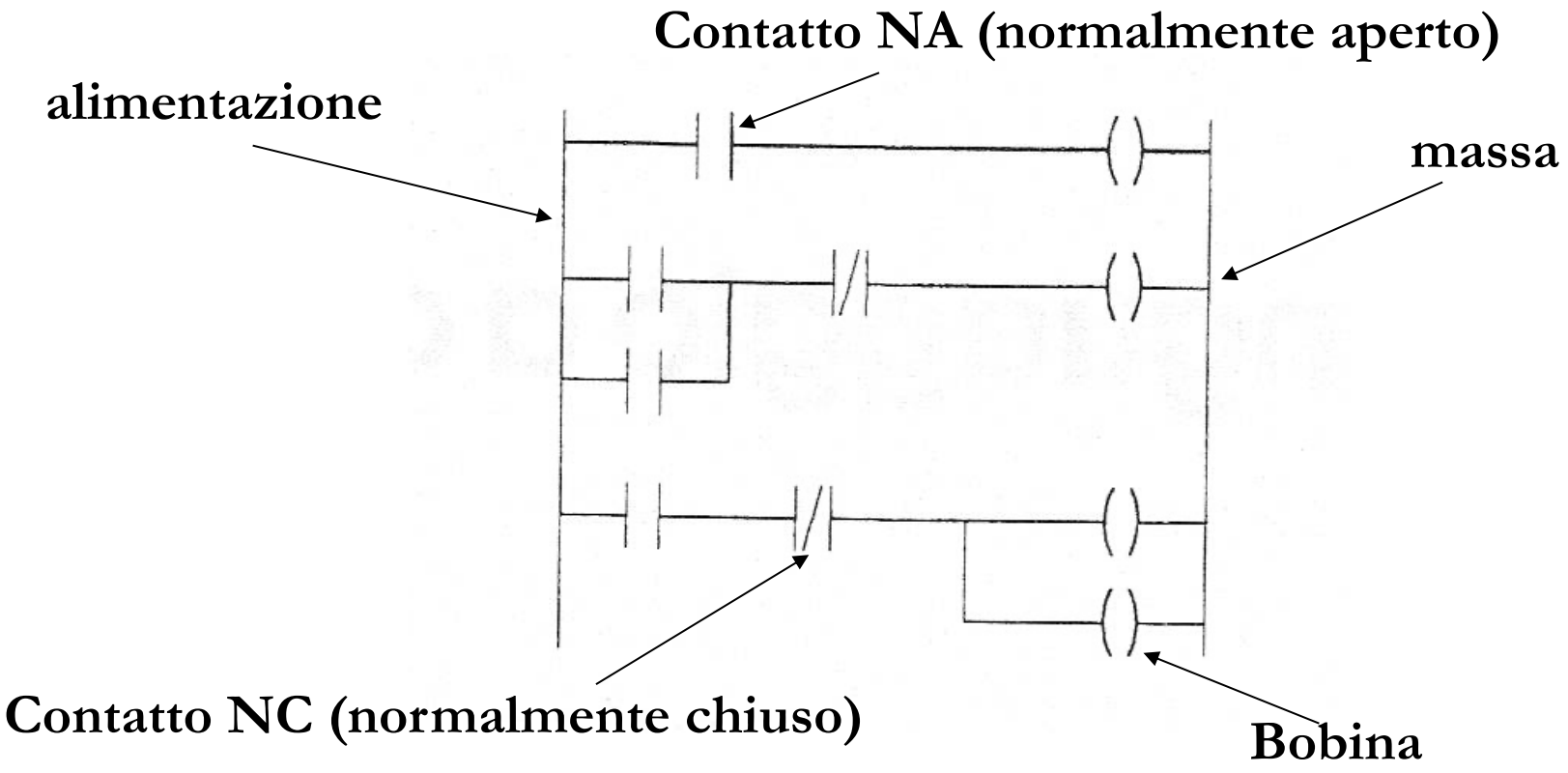
- In base ai punti di ingresso/uscita trattati da un PLC
  - Micro PLC (fino a 64 punti di ingresso/uscita), non modulare
  - Piccoli PLC (fino a 512 punti di ingresso/uscita)
  - Medi PLC (fino a 2048 punti di ingresso/uscita)
  - Grandi PLC (migliaia di punti ingresso/uscita)

PLC – linguaggio a contatti

- Linguaggio più diffuso per la programmazione dei PLC (deriva dalla logica a relè/ elettromeccanica)
  - Istruzioni di base (contatti e bobine)
  - Istruzioni di temporizzazione e conteggio
  - Istruzioni per il controllo di programma
  - Istruzioni per la manipolazione dei dati
  - Istruzioni per la realizzazioni di funzioni speciali

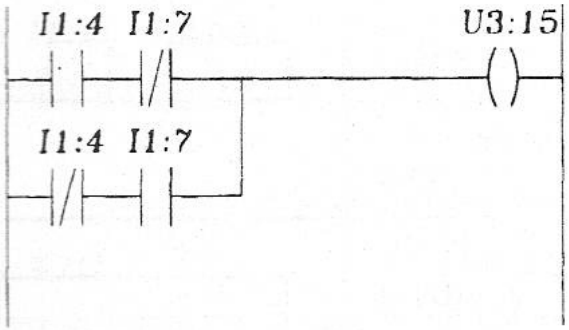
Linguaggio a contatti – esempio di programma

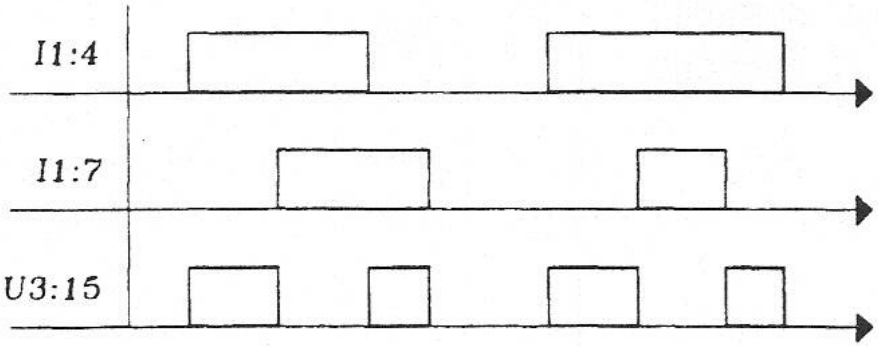
- Due linee verticali (i montanti della scala) che rappresentano l'alimentazione (linea sx) e la massa (linea dx)
- Linee orizzontali (i pioli della scala, *rung*), che alimentano una bobina se una certa combinazione di contatti abilita il flusso di energia



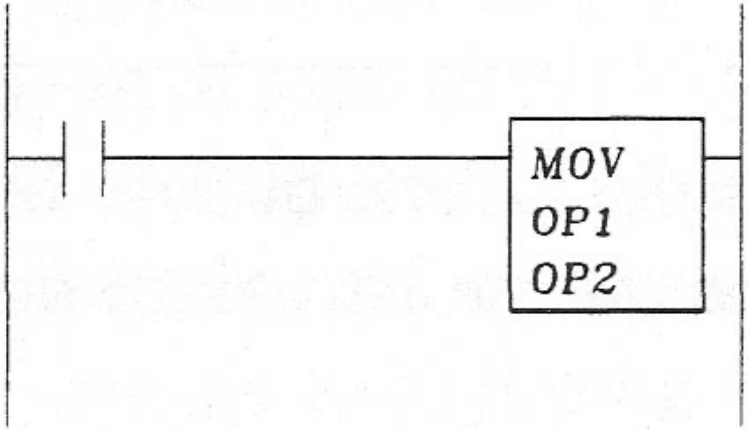
Programmazione di un XOR

OR esclusiva: U3:15 = I1:4 XOR I1:7

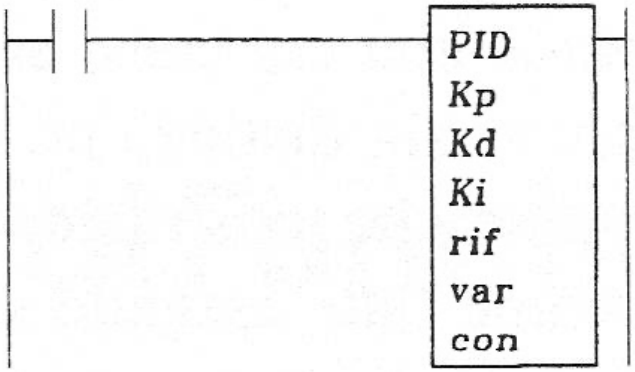




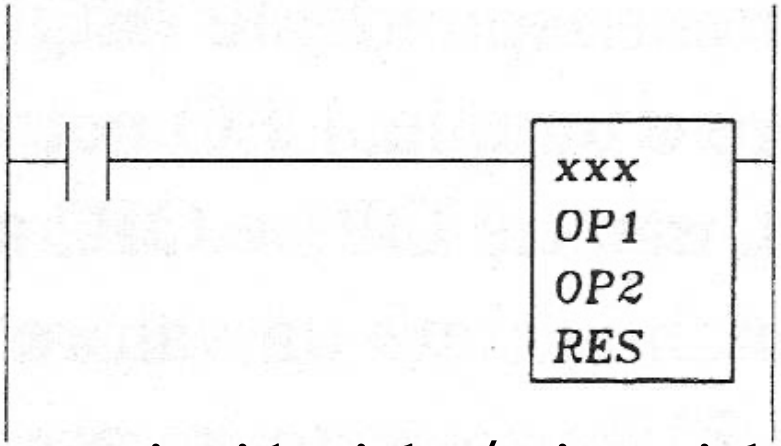
Istruzioni per la manipolazione dei dati e per la realizzazione di funzioni speciali



Istruzione MOV per il trasferimento del contenuto di una parola



Istruzione PID



Operazioni logiche/aritmetiche: xxx = ADD, MUL, SUB, DIV, AND, OR

Sensori

- Sensore: dispositivo che permette di rilevare il livello di una grandezza di interesse, trasformando questa informazione in un segnale di altra natura
- I sensori permettono di monitorare lo stato e/o le uscite del sistema da controllare
- Le prestazioni del sistema di controllo dipendono significativamente da
  - Caratteristiche statiche
  - Caratteristiche dinamiche
  - Localizzazione e modalità di installazione (agiscono su ritardi e rumori di misura)

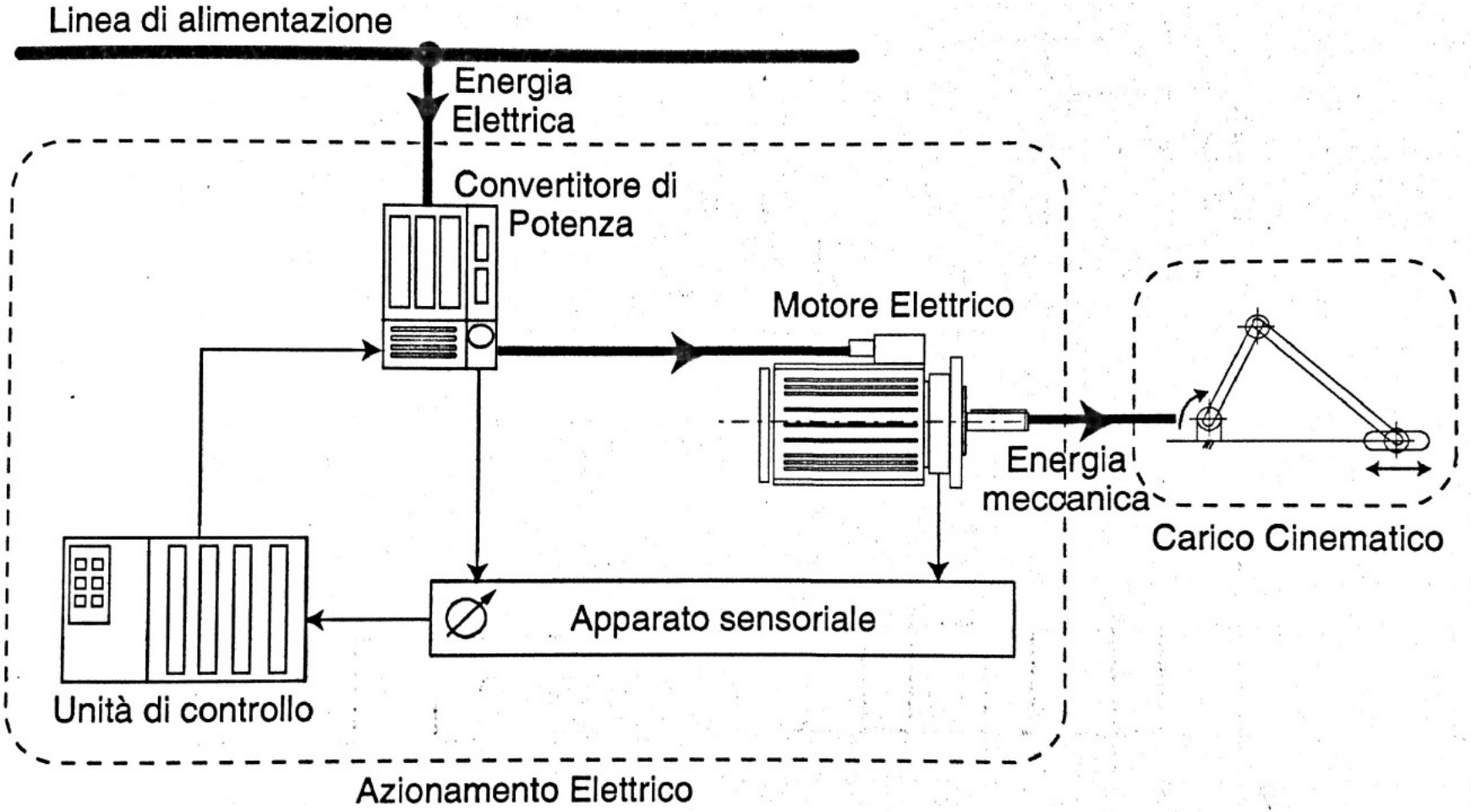
Componenti di un dispositivo di misura

- I dispositivi di misura sono tipicamente costituiti da
  - Elemento sensibile primario: fornisce un parametro o segnale funzione della variabile da misurare
  - Trasduttore: trasforma la grandezza di cui sopra in un segnale di natura diversa, generalmente di tipo elettrico
  - Amplificatore: normalizza il segnale su valori standard (es. 0-5 V)
- In alcuni casi l'elemento sensibile ed il trasduttore coincidono (es. termocoppia)
- I sensori di ultima generazione comprendono anche componenti per la comunicazione su rete
- La misura è influenzata da diversi fattori
  - Qualità del sensore, temperatura, umidità, pressione, vibrazioni e accelerazioni

Criteri di scelta di un sensore

- Principali criteri da prendere in considerazione
  - Campo (range)
  - Accuratezza, precisione, sensibilità e risoluzione
  - Rangeability
  - Caratteristiche dinamiche
  - Affidabilità (Mean Time Between Failure, MTBF)
  - Costi (acquisto, installazione, manutenzione)
  - Materiale di costruzione
  - Problemi specifici di installazione e pericolosità
  - Normative

Attuatore: esempio di un azionamento elettrico



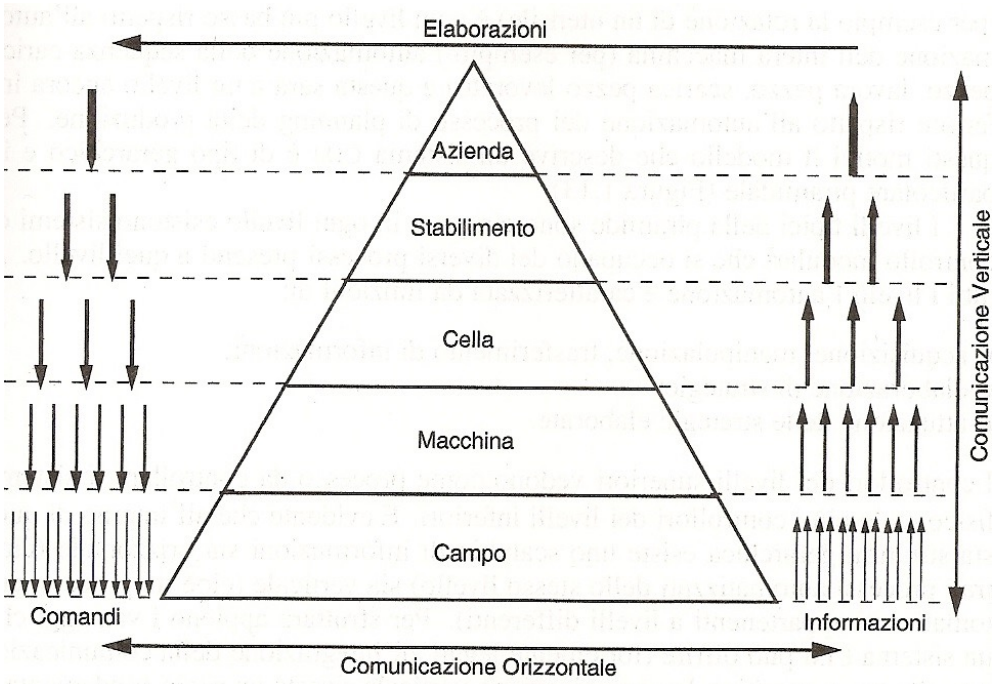
Convertitore di potenza

- Il regolatore fornisce generalmente un segnale di bassa potenza, pertanto è necessario un amplificatore di potenza
- Sistema elettronico di potenza: modula l'energia fornita dalla rete di alimentazione per attuare la tensione richiesta dall'unità di controllo
- Per piccole potenze (decine di Watt) è possibile usare amplificatori di tipo lineare (anche detti di classe A):
  - Amplificatori analogici che richiedono un consumo di potenza non nullo anche a riposo
- Per potenze superiori si utilizzano amplificatori di tipo switching (anche detti di classe D):
  - Il motivo risiede nel maggiore rendimento energetico, principalmente perché non dissipano potenza a riposo

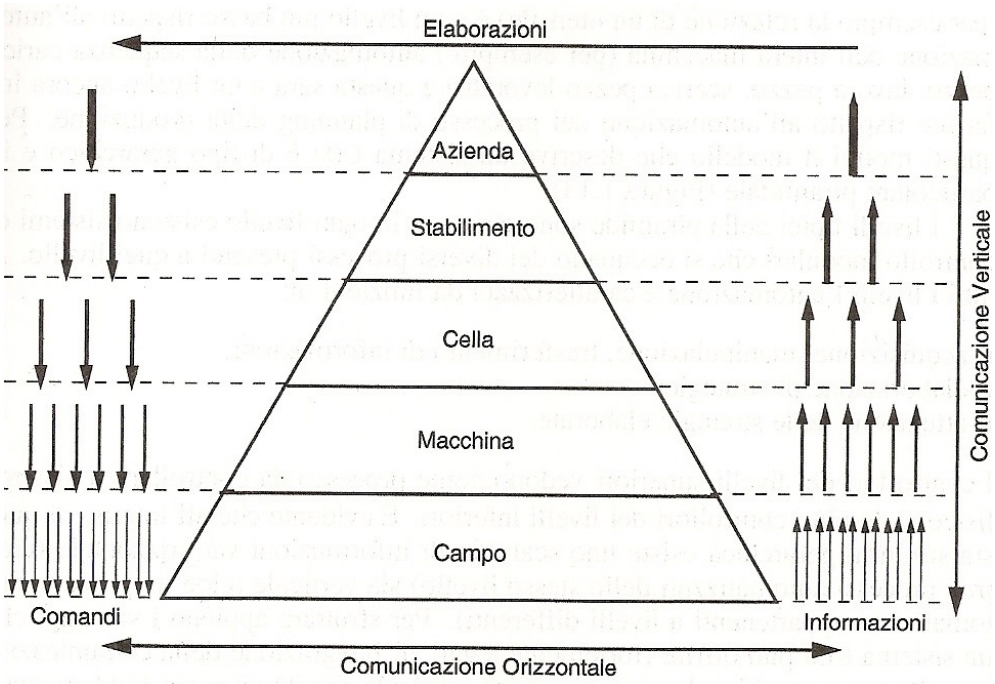
Limitazione fisiche

- Tutti gli azionamenti elettrici presentano limiti di
  - Tensione massima
    - Limiti di isolamento del motore, limiti amplificatore
  - Corrente massima
    - Problemi termici
- Questi limiti si traducono in
  - Velocità massima per il motore
  - Coppia rms e di picco massime erogabili dal motore

- Le attività di controllo costituiscono una gerarchia
- Ad ogni livello è necessario
  - Acquisire, manipolare, trasferire informazioni
  - Elaborare strategie di controllo
  - Attuare le strategie elaborate



- Ai livelli superiori:
  - Dati complessi e strutturati, strategia aggiornata sporadicamente (ad es., modifica volumi di produzione)
- Ai livelli inferiori:
  - Dati semplici, controllo a frequenze elevate, tipicamente real-time (ad es. controllo velocità utensile)



CIM: Livello di campo

- **Livello di campo:**
  - componenti hardware che eseguono fisicamente le azioni necessarie per l'esecuzione dei compiti specifici di produzione/servizio, ossia
  - sensori, attuatori, componenti dell'impianto e semplici anelli di regolazione (di velocità, pressione, livello, etc.)
  - La funzione di questi componenti è quella di fornire un'interfaccia di input/output tra i livelli superiori ed il processo da controllare
  - Esempio:
    - Controllo del livello di un liquido in un serbatoio
    - Il s.d.c. di livello superiore comunica il livello desiderato (set point)
    - Il s.d.c. di campo fa si che tale livello sia mantenuto (regolazione), indipendentemente dai disturbi
    - Il s.d.c. di campo viene visto come un *attuatore virtuale* dal livello superiore
  - Tecnologia: il sistema di controllo a questo livello è tipicamente un *controllore embedded* (ad es., PIC, DSP, Arduino)

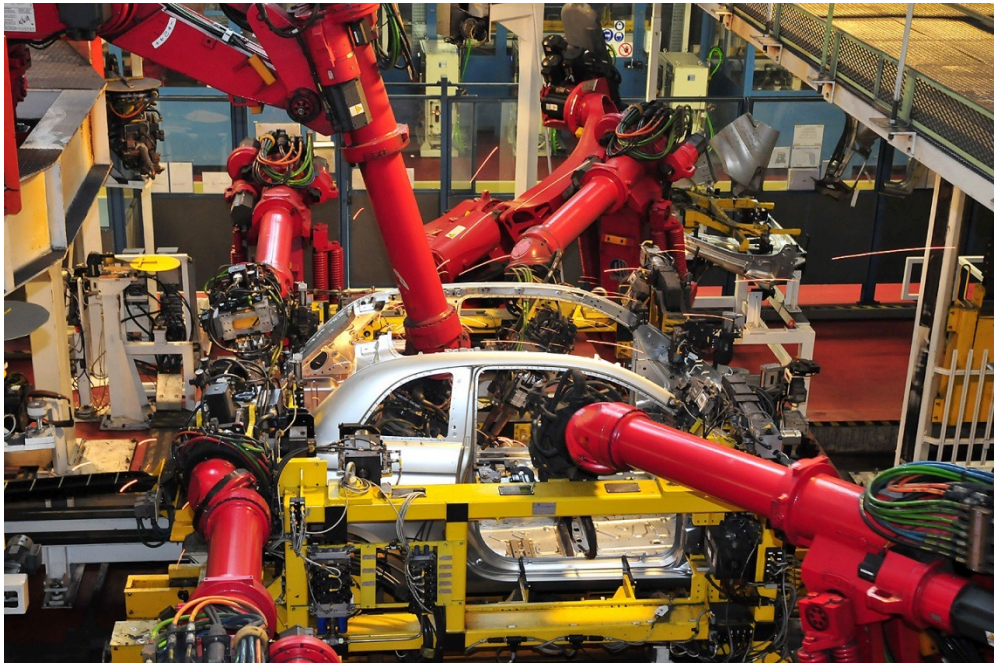
CIM: Livello di macchina

- **Livello di macchina:**
  - Raggruppa i componenti di campo atti a fornire una determinata funzionalità (ad es., macchina utensile o robot industriale)
  - Oltre alla regolazione di variabili analogiche, è necessario il
  - Controllo della realizzazione sequenziale di operazioni

  - Ad es., si pensi ad un robot industriale
    - livello di campo: controllo velocità, posizione dei singoli giunti
    - livello di macchina: pianificazione traiettorie e sequenze di azioni
  - Le operazioni devono essere coordinate con quelle di altre macchine dal livello superiore
  - Tecnologia: la realizzazione sequenziale di operazioni viene controllata tramite appositi sistemi digitali (*PLC, Programmable Logic Controller*) o da sistemi embedded

CIM: Livello di cella

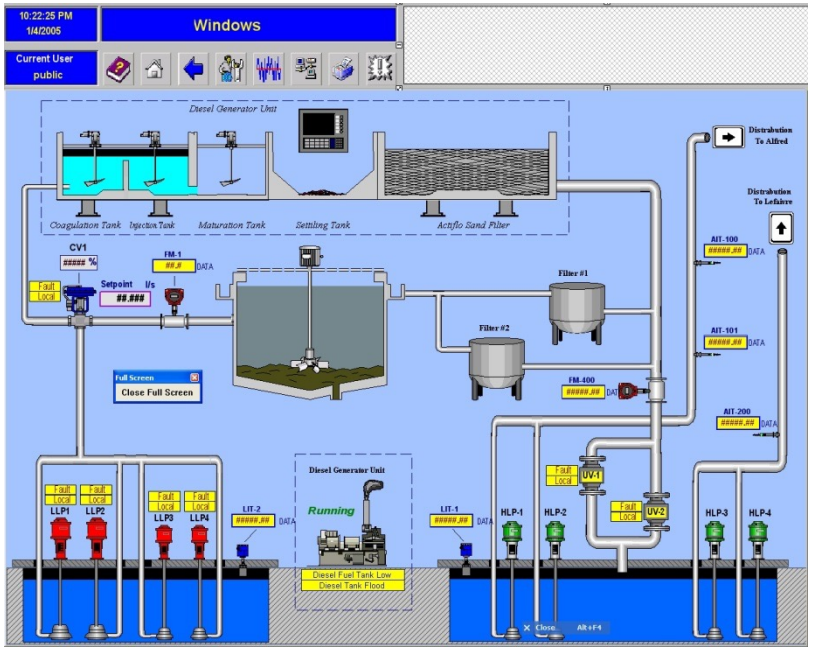
- **Livello di cella:**
  - Cella di produzione: insieme di macchine
    - interconnesse fisicamente da un sistema di trasporto e stoccaggio materiali
    - controllate in maniera coordinata per svolgere uno specifico processo
  - Il s.d.c. di cella regola e supervisiona il funzionamento coordinato di tutte le macchine operatrici della cella

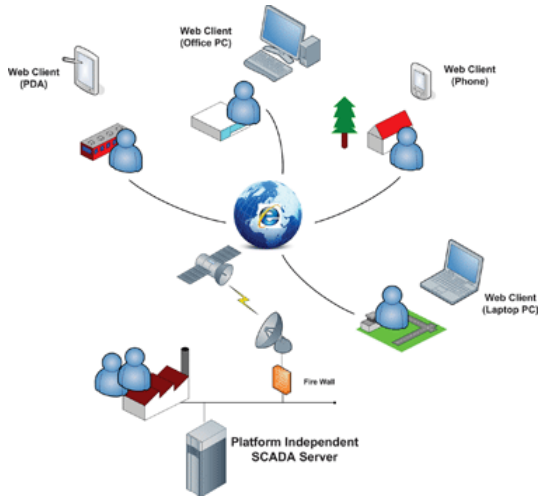


- Le operazioni sono più complesse in quanto coinvolgono un maggior numero di elementi da coordinare
- Tecnologia: anche in questo caso si usano controllori logici e sistemi embedded

CIM: Livelli di stabilimento ed azienda

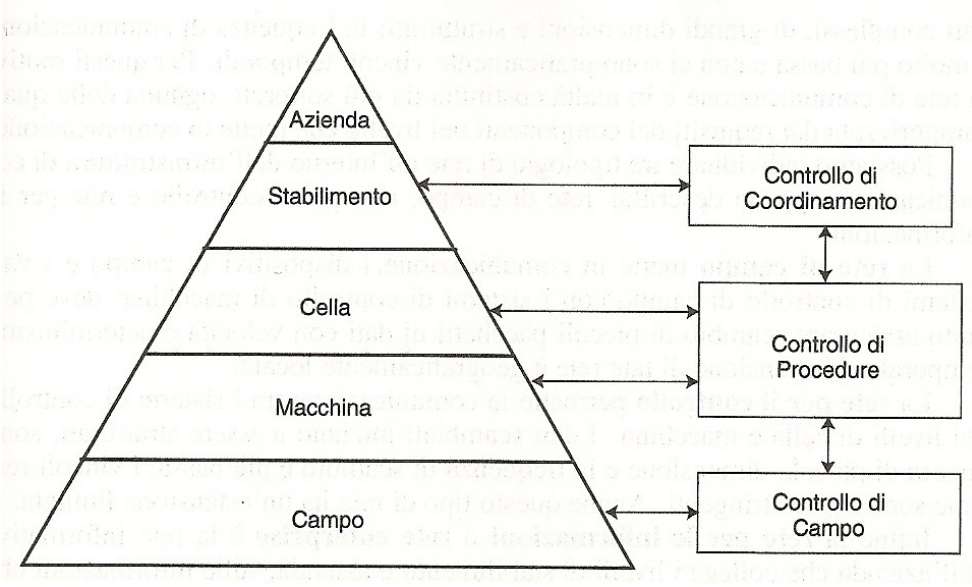
- **Livello di stabilimento:**
  - Questo livello comprende tutte le celle o linee produttive di un impianto industriale
  - Riceve le istruzioni dal livello gestionale (planning, gestione ordini, etc.)
  - Il s.d.c. elabora i piani operativi per la produzione
  - Componente fondamentale: Sistema di supervisione, controllo e acquisizione dati (*SCADA, Supervisory Control and Data Acquisition*)
  - Tecnologia: workstation con struttura client/server
- **Livello di azienda:**
  - Sistema decisionale, processi gestionali di supporto ai livelli inferiori
  - Tecnologia: workstation con struttura client/server connesse al mainframe aziendale





CIM: livelli di controllo

Standard ANSI/ISA-S88.01-1995



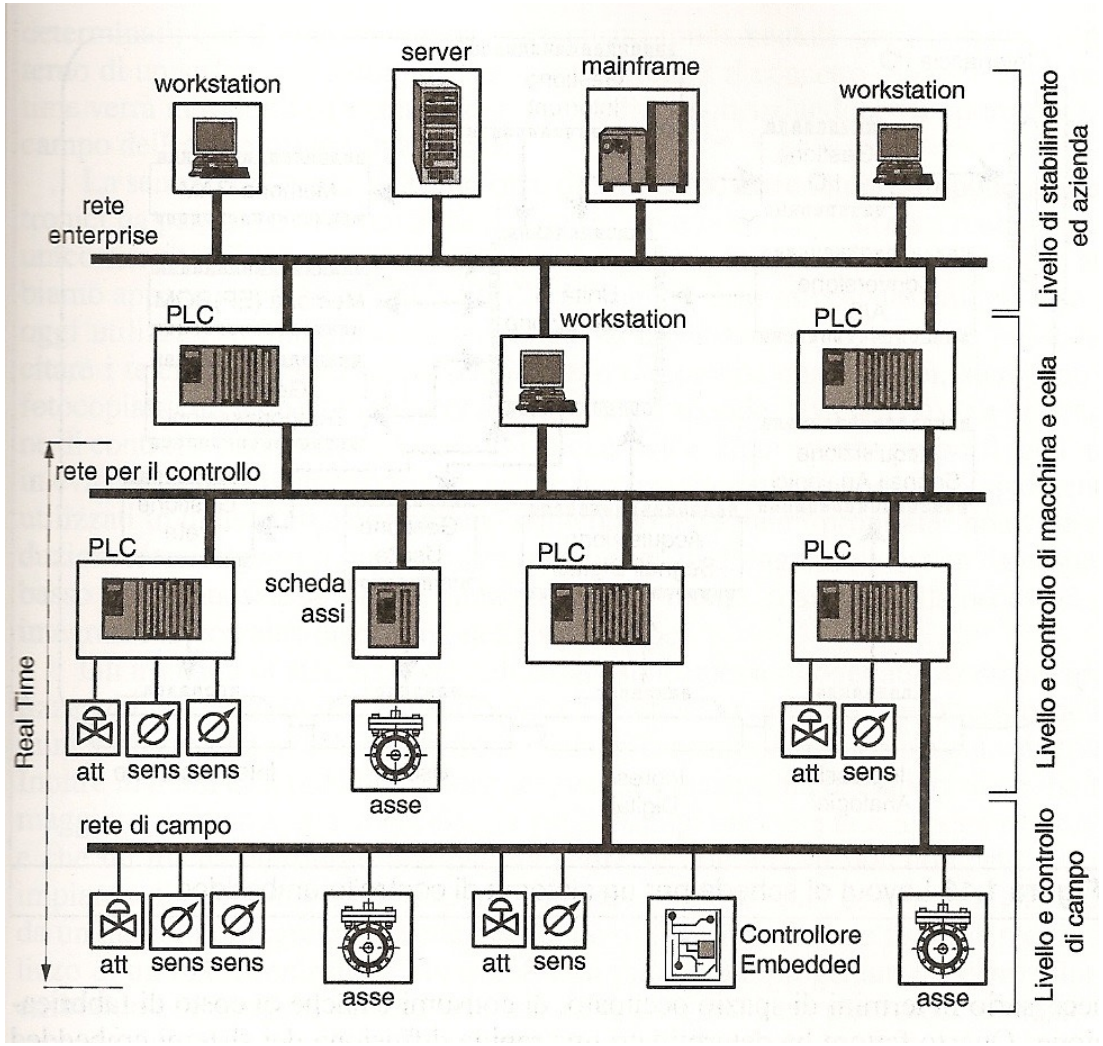
- **Controllo di campo**
  - Controllo continuo
  - Dispositivi embedded o dedicati
- **Controllo di procedure**
  - controllo continuo (es. pianificazione segnali di riferimento, tuning adattativo parametri) e controllo logico sequenziale
  - Controllo logico-sequenziale operazioni, diagnostica
- **Controllo di coordinamento**
  - Algoritmi di ottimizzazione della produzione (ricerca operativa, intelligenza artificiale)

CIM: reti di comunicazione

- **Rete di campo**
  - Comunicazioni dispositivi di campo – piccoli pacchetti dati, vincoli temporali su invio pacchetti, estensione locale
- **Rete per il controllo**
  - Comunicazione s.d.c. a livelli macchina e cella – pacchetti piccoli, vincoli temporali meno stringenti, estensione limitata
- **Rete per le informazioni** (o rete enterprise)
  - Comunicazione a livello di stabilimento e azienda – quantità di dati elevate, vincoli di real-time assenti, estensione ampia

Architettura di un sistema di automazione distribuito

- Modulare
- Gerarchica
- Dispositivi interconnessi
- Più reti di comunicazione



Reti di telecomunicazione per l'automazione

- Come si vede nello schema precedente, esistono diverse tipologie di reti, a seconda del livello di controllo
- I modelli di riferimento principali sono :
  - FIELDBUS (IEC 61158)
    - Highway Addressable Remote Transducer (HART)
    - Foundation Fieldbus
    - Profibus
  - Controller Area Network (ISO 11898)
    - Sviluppato inizialmente da Bosch in ambito automobilistico, si è poi diffuso ampiamente in ambito industriale
  - Industrial Ethernet
    - Simile a Ethernet, ma con specifiche a livello fisico adatte ad ambiente industriale

CIM: reti di campo

- L'utilizzo di reti di campo comporta i seguenti vantaggi:
  - Semplificazione architetturale, tali reti sono facilmente espandibili e riconfigurabili (reti «snelle»)
  - Riduzione del cablaggio, con diminuzione dei costi di installazione e di manutenzione dei cavi
  - Possibilità di trasmettere informazioni più complesse e bidirezionali (dispositivi intelligenti che possono operare delle elaborazioni locali
  - Capacità di elaborazione determina una diminuzione della criticità dei tempi di risposta
  - Possibilità di calibrare via software i vari sensori e attuatori da un solo terminale connesso alla rete
  - Maggiore robustezza delle trasmissioni, trasmissione digitale meno sensibile ai disturbi di quella analogica e consente di implementare tecniche per il riconoscimento e correzione degli errori di trasmissione

Sistemi SCADA

- Sensori e attuatori interagiscono con le grandezze fisiche di processo
- I dispositivi di controllo (e.g. PLC) interagiscono con sensori e attuatori, memorizzando i dati in una memoria locale e realizzando le logiche di automazione dell'impianto
- I dispositivi di controllo sono connessi via rete a uno o più dispositivi di supervisione:
  - Sistema SCADA(Supervisory Control And Data Acquisition) è un insieme di componenti software e hardware che consentono di
    - acquisire e storicizzare i dati,
    - presentare i dati all'operatore tramite HMI e/o informazioni riassuntive
    - fornire un supporto alla decisione per la gestione dell'impianto

Sistemi SCADA: funzioni principali

- Acquisizione dati
  - Per poter fornire informazioni sul processo, è necessario che il sistema acquisisca dati da esso mediante opportuni driver di comunicazione
  - Questi dati vengono raccolti in una base dati, che costituisce il nucleo del sistema SCADA
  - Ai dati grezzi possono essere aggiunte altre informazioni come l'identificativo del sensore, stringhe informative, unità di misura e/o conversione del valore in unità standard...
- Controllo di supervisione
  - Tramite uno SCADA, l'operatore può supervisionare il processo ed intervenire su di esso se necessario
  - Questa funzione si realizza tipicamente tramite una Human-Machine Interface (HMI) di tipo grafico

Sistemi SCADA: funzioni aggiuntive

- Rappresentazione dati
- Storicizzazione dei dati
- Gestione di allarmi
  - Programmando la condizione che ne causa l'insorgenza
  - Provvedendo ad informare l'operatore (mediante lampeggianti, SMS, e-mail…)
- Gestione di ricette
  - Eseguendo particolari sequenze di operazioni (ricette) al verificarsi
    - di una scadenza temporale,
    - Eventi particolari
    - Richiesta dell'operatore
  - Provvedendo ad informare l'operatore (mediante lampeggianti, SMS, e-mail…)
- Manutenzione (correttiva o preventiva)
- Interazione con sistemi di livello superiore
  - Domain Controller per la gestione degli accessi e l'autenticazione degli utenti
  - Sistemi MES (Manufacturing Execution System) per gestire il dispaccio di ordini, le scorte di magazzino e in generale per gestire e controllare la produzione
  - Software gestionali ERP (Enterprise Resource Planning)

Evoluzione dei sistemi SCADA

- I primi SCADA erano spesso realizzati su mainframe o minicomputer con sistemi di comunicazione proprietari
- Oggi si va nella direzione di sistemi distribuiti, spesso web-based
- La connessione dei sistemi SCADA a reti aziendali o a internet ha aumentato i rischi per la sicurezza in tali sistemi (e.g. Stuxnet)
- In generale i sistemi di controllo industriale che includono PLC, sistemi SCADA e altri dispositivi sono vulnerabili a vari tipi di minacce, tra cui
  - attacchi informatici
  - malfunzionamenti
  - disastri naturali.

Modello di cybersecurity per i sistemi di controllo industrial (ICS)

- La sicurezza dei sistemi di controllo industriale (ICS) è cruciale per garantire la protezione delle infrastrutture critiche e dei processi industriali e può essere garantita attraverso
  - **Identificazione delle minacce e vulnerabilità**: È fondamentale effettuare analisi dei rischi per identificare vulnerabilità e minacce specifiche per l'ambiente industriale, come attacchi informatici (malware, phishing), guasti hardware e errori umani.
  - **Architettura di sicurezza**: Implementare una struttura di sicurezza multilivello, che includa firewall, sistemi di rilevamento delle intrusioni e segmentazione della rete, separando la rete ICS dalla rete IT aziendale per limitare l'accesso e ridurre il rischio di attacchi.
  - **Autenticazione e Autorizzazione**: Utilizzare metodi di autenticazione forti (come l'autenticazione a due fattori) e controlli rigorosi per garantire che solo gli utenti autorizzati possano accedere ai sistemi di controllo.
  - **Aggiornamenti e Patch**: Mantenere il software e l'hardware aggiornati con le ultime patch di sicurezza per ridurre le vulnerabilità.

- ...
  - **Monitoraggio e Audit**: Implementare sistemi di monitoraggio continuo per rilevare attività sospette e condurre audit regolari per valutare la sicurezza dei sistemi.
  - **Formazione e Sensibilizzazione**: Educare il personale sui rischi di sicurezza e sulle migliori pratiche per ridurre il rischio di errori umani.
  - **Piani di Risposta agli Incidenti**: Sviluppare e testare piani per gestire e rispondere rapidamente a potenziali attacchi o guasti/incidenti di sicurezza, minimizzando il danno e ripristinando le operazioni.

Normative e standard

- Esistono diverse normative e standard che guidano la sicurezza degli ICS, come:
  - NIST SP 800-82: Linee guida per la sicurezza dei sistemi di controllo industriale.
  - IEC 62443: Standard internazionale per la sicurezza dei sistemi di automazione industriale.
  - ISA/IEC 61511: Normativa per la sicurezza dei sistemi di controllo nei processi di processo.