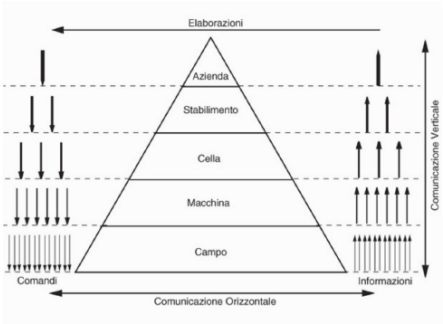
CIM - PRODUZIONE INTEGRATA TRAMITE ELABORATORI

Con CIM - Computer Integrated Manufactoring, si intende un modello di riferimento funzionare per la realizzazione dell'automazione industriale e del controllo di processo basato sul rilevamento, il coordinamento e la trasmissione di informazioni tra i vari sottosistemi di un industria mediante l'utilizzo di reti informatiche.
Solitamente un'industria automatizzata è caratterizzata dalla presenza di celle di lavorazione automatizzate dedicate all'esecuzione di singole lavorazioni che possono però essere non integrate tra loro, realizzate inoltre tramite dispositivi di controllo eterogenei con protocolli di comunicazione spesso incompatibili. Un miglioramento di tale situazione può essere ottenuto tramite una maggiore integrazione tra i sottosistemi a livello aziendale, integrazione che va realizzata attraverso una progettazione metodica, si fa riferimento alla CIM, dell'intero sistema informatico, che comporti l'utilizzo di dispositivi il più possibile standardizzati, gestione dei flussi di informazione e coordinamento di tutti i fattori di produzione incluso l'uomo.

La struttura di riferimento è costituita da 5 livelli:

Si basa su una comunicazione orizzontale e verticale, in modo particolare i comandi vengo dall'alto verso il basso mentre le informazioni dal basso all'alto. Importante che la comunicazione sia veloce.

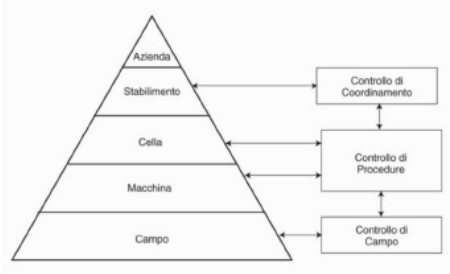


- **Livello DI CAMPO** – è il livello più basso dove si realizzano le funzioni di misura e di comando sui processi produttivi dove troviamo i sensori e gli attuatori.
- **Livello MACCHINA (controllo)** – vengono svolte funzioni di controllo di macchine o processi, oltre alle principali funzioni di sicurezza. In questo livello sono impiegati i dispositivi di controllo diretto PLC che interagiscono direttamente con i sensori e gli attuatori.
- **Livello DI CELLA (Supervisione)** – In una cella viene eseguito un sotto-processo produttivo completo attraverso varie macchine. Operazioni svolte sono la configurazione dei parametri dei sistemi di controllo e il coordinamento delle sequenze di attività da loro svolte. Spesso accompagnate dall'intervento dell'uomo. I dispositivi impiegati sono PC o PLC con maggiore capacità elaborativa.
- **Livello STABILIMENTO (gestione stabilimento)**- Vengono integrati i vari comparti dello stabilimento come la produzione, la logistica, l'amministrazione e la produzione. Ci si occupa della pianificazione della produzione, della gestione delle risorse, e della supervisione. Viene gestita la base di dati e il coordinamento tra le varie celle dello stabilimento. E' prevista l'interazione uomo-macchina attraverso l'utilizzo di workstation o PC superiori attraverso SCADA e MES.
- **Livello AZIENDA (gestione azienda) -** potendo l'azienda essere composta da più stabilimenti. Vengono accolte informazioni dei livelli inferiori per realizzare sistemi di supporto alla decisione che aiutino gli amministratori nelle scelte di pianificazione ai flussi materiali e finanziari, quindi gli investimenti da fare riguardo la produzione, la manutenzione e i miglioramenti.

La forma piramidale tiene conto di vari aspetti:

- Rappresenta un'organizzazione gerarchica, in quanto ogni livello comunica direttamente con quello immediatamente superiore, da cui riceve comandi e cui fornisce informazioni.
- dal livello più basso e proseguendo verso l'alto sono necessari via via minori quantità di informazioni, di maggiore qualità e con frequenze di aggiornamento inferiori;
- Rappresenta, nei livelli inferiori, funzioni più vicine all'impianto, per la cui realizzazione è necessaria una conoscenza dettagliata dei processi da automatizzare, e , nei livelli superiori, funzioni più lontane che realizzano la supervisione e la pianificazione delle attività
- La necessità di interazione con l'uomo è minima ai livelli e massima ai livelli superiori

Anche i sistemi di controllo hanno una architettura gerarchica derivata dalla struttura della CIM che classifica le funzioni di controllo in:



- **Controllo di Campo:** riguarda il controllo dei componenti del livello di campo, implementato su dispositivi dedicati come i controllori embedded o schede dedicate.
- **Controllo di procedure:** si colloca tra i livelli di cella e di macchina e riguarda il controllo *continuo* come la determinazione di segnali e parametri; controllo *logico* per il coordinamento dei sistemi di campo sulla base della lista di operazioni sequenziali che compongono il processo. Ci sono anche controlli di monitoraggio delle prestazioni, diagnostica e dei malfunzionamenti.
- **Controllo di Coordinamento:** riguarda il coordinamento e la gestione delle varie celle dello stabilimento, esegue, ferma e dirige i vari sistemi di controllo in base a dei sistemi intelligenti per il controllo automatico, implementato su calcolatori standard.

Lo scambio di informazioni nella piramide CIM avviene attraverso una infrastruttura di comunicazione informatica che interconnette tutta la fabbrica. Dovrà permettere sia una comunicazione orizzontale tra i componenti di un livello, sia verticale per inviare informazioni al livello e ricevere comandi dal livello subito sopra. La rete è costituita da più sotto-reti:

- **Rete di Campo:** mette in comunicazione dispositivi di livello più basso , sensori e plc. Consente lo scambio di piccoli dati con velocità e determinismo.
- **Rete per il controllo** : comunicazione tra livelli di cella e macchine. I dati sono più strutturati, sono ancora piccoli ma con vincoli real time meno stringenti.
- **Rete Enterprise**: è la rete che circola su tutta azienda e collega i livelli di stabilimento. Le informazioni qui sono molto grandi e strutturate ma non costrette a determinismo.

RETE DI COMUNICAZIONE REAL TIME

Dato che i task coinvolti nei bassi livelli (campo macchina e cella) hanno necessità di soddisfare specifiche real time anche la comunicazione sarà un task real time. Per questo motivo è importante che la rete abbia un comportamento fortemente deterministico. Sono indispensabili proprietà come *interoperabilità* e *interscambiabilità*. Dispositivi di campo diversi tra loro potranno integrarsi, cooperare e interpretare le informazioni scambiate senza bisogno di riconfigurazioni a livello di dispositivo o di rete.
I protocolli delle reti real time devono essere progettati per far fronte alle esigenze di trasmissione di tre tipologie di messaggi:
• Messaggi **periodici** sono generati da task periodici come ad esempio il trasporto di letture di sensori. I vincoli real time sono hard e stretti e occorre garantire i vincoli con determinismo.
• Messaggi **aperiodici** sono generati da task aperiodici, come ad esempio il trasporto di un comando fine ciclo da parte di un operatore. Vengono gestiti con una politica best effort ovvero al meglio delle possibilità del sistema.
• Messaggi **sporadici** sono come i messaggi aperiodici ma con vincoli hard real time e sono ad esempio gli allarmi e i segnali di emergenza.

L'architettura software di una rete real time può essere schematizzata come una pila di protocolli con nodi interconnessi da un canale di comunicazione. Ogni nodo si connette al canale mediante una interfaccia schematizzabile come un buffer in ingresso e un buffer di uscita dei messaggi.
Il vincolo real time non è però sempre realizzabile al 100%, basti pensare ad una connessione in rete geografica molto ampia.

DISPOSITIVI PER IL CONTROLLO

Per Dispositivo per il controllo intende un sistema per l'elaborazione delle informazioni destinato al controllo diretto dei processi fisici. Possono essere di natura diversa ma devono principalmente due qualità essenziali:

- poter rispondere agli stimoli proveniente dal loro esterno sotto forma di eventi o input da sensori,
- e poter agire modificando il comportamento del processo fisico che controllano.

In generale deve poter realizzare diversi compiti come il controllo a ciclo chiuso, delle variabili fisiche e i rispettivi valori di riferimento, il controllo logico-sequenziale, la gestione degli allarmi e anomalie, l'interfaccia operatore e la comunicazione con altri dispositivi. Tali compiti devono essere eseguiti periodicamente, ciclicamente o una sola volta per particolari eventi.
Inoltre, un dispositivo di controllo deve anche permettere il trattamento di un numero elevato di segnali di I/O e dovendo interagire con il mondo fisico deve necessariamente farlo in tempo reale in modo deterministico. Deve rispondere in un modo certo ed entro tempi fissati a eventi esterni non prevedibili.
Se l'applicazione di controllo non è estremamente semplice. i dispositivi di controllo dovranno prevedere un minimo di SO che si occupi della pianificazione, esecuzione e gestione della comunicazione dei processi.
Un'altra caratteristica è la **scalabilità**: poter scegliere le sole funzionalità necessarie, in modo da non appesantire inutilmente il dispositivo di controllo. La **solidità** e la **robustezza** sono altre caratteristiche importanti affinché il sistema possa funzionare in ambienti ostili (resistenza ai campi elettromagnetici)

CONTROLLORI EMBEDDED

Un controllore Embedded è un sistema di controllo realizzato tramite una singola scheda elettronica o tramite un singolo circuito integrato. Contiene al suo interno tutto il necessario per connettere il controllo all'impianto da controllore e per eseguire in maniera opportuna gli algoritmi di controllo definiti dall'utente.
Si identificano sistemi elettronici a microprocessori progettati ad hoc per una determinata applicazione, risulta molto conveniente se i compiti sono noti a priori.
Con la miniaturizzazione dei componenti si è passati a dei *microcontrollori* ma sono usati generalmente in applicazioni che richiedono una riduzione dello spazio, numero di segnali I/O limitati, basso consumo e scarsa interazione con l'uomo.

SISTEMI DI CONTROLLO CON ARCHITETTURA A BUS (+)

Sono sistemi di controllo (microcontrollori) utilizzati quando non bastano dei semplici controllori embedded, ovvero in casi più complessi, come quando c'è necessita di un numero di I/O elevato, necessità dell'interazione con l'uomo o con altri dispositivi o reti informatiche.
Un'architettura a bus permette di connettere ad un bus diversi dispositivi e moduli così da aumentare le funzionalità del sistema di controllo.
La specifica architettura del bus e in particolare i protocolli che gestiscono le comunicazioni, definiscono le caratteristiche del bus stesso, come la possibilità di ospitare più unità di elaborazione per ottenere un sistema multiprocessore, la velocità di trasmissione, l'utilizzo di un bus sincrono o asincrono ecc.
Il vantaggio si basa sulla flessibilità di progettazione del sistema di controllo desiderato mediante la scelta dei moduli, che può essere fatta ad hoc o scelta tra gli standard esistenti.
Necessitano di un sistema operativo sofisticato, che gestisce il sistema, eseguendo gli algoritmi di controllo programmati e assicurando in ogni condizione un funzionamento nel rispetto dei vincoli real time. Controllori basati su questa architettura sono i PLC.

SISTEMI DI CONTROLLO SU PC (+)

Negli ultimi anni, grazie alla notevole evoluzione dell'informatica e dei PC per uso generico e alla forte diminuzione dei loro costi, l'utilizzo di sistemi basati su PC per realizzare dei controllori industriali è sempre più diffuso. I vantaggi che una tale soluzione comporta sono: costi competitivi, ampia disponibilità di hardware e di fornitori differenti, funzionalità avanzate già presenti nel sistema (come interfaccia uomo macchina o sistemi per lo sviluppo e la programmazione del software, semplice interconnessione con reti informatiche ecc). Per essere impiegato per un uso industriale, devono essere più robusti per essere utilizzati in ambienti ostili e devono permettere un'interconnessione con molti dispositivi I/O, risolvibile utilizzando reti informatiche specifiche o schede per gli I/O. Ne fanno parte i **Soft PLC**, ovvero PLC realizzati con PC industriali.

PLC

Il controllore a logica programmabile (o PLC - Programmable Logic Controller) è il più diffuso dispositivo di controllo per l'automazione industriale.
Si tratta di un dispositivo molto flessibile, di concezione modulare con architettura a bus, specializzato soprattutto per il controllo logico/sequenziale. Eredita tutte le caratteristiche di un controllore con architettura a bus e prevede la possibilità di trattare fino a migliaia di punti di I/O con interfacce che accettano segnali di varia natura, ed è in grado di funzionare con ambienti real time (è dotato di sistemi operativi proprietari real-time multi-tasking molto efficienti) ed è di costruzione molto robusta.

Nascono come sistemi utilizzati per cambi diversi, destinati all'uso in ambito industriale, con l'idea di poter essere facilmente programmati e riprogrammati, di facile manutenzione, essere modulare per poter scegliere in base all'applicazione la sua configurazione hardware migliore, deve essere robusto per essere utilizzato in ambienti ostili e competitivo nei costi.
Nasce negli anni 70 come sistema basato su microcontrollore ed è in continua evoluzione da allora.
Attualmente è basato su un sistema multiprocessore, integra possibilità di connessione in rete informatica, è capace di eseguire funzioni molto complesse (come controllo di motori).

I PLC rientrano all'interno dello standard [IEC 61131-1], che lo definisce come un sistema a come sistemi elettronico a funzionamento digitale, destinati all'uso in ambito industriale che utilizza una memoria programmabile per l'archiviazione interna di istruzioni orientate all'utilizzatore per l'implementazione di funzioni specifiche, come quelle logiche, di sequenziamento, di temporizzazione, di conteggio e di calcolo aritmetico, e per controllare, mediante ingressi e uscite sia digitali sia analogici, vari tipi di macchine e processi.
Lo standard fa una distinzione tra un Sistema PLC e un PLC che vengono utilizzati negli stessi modi:

- Sistema PLC: è la configurazione realizzata dall'utilizzatore formata da un PLC e delle periferiche associate necessarie a far funzionare un sistema automatizzato.
- PLC: scheda processore, sia l'intero sistema completo delle sue schede interfaccia

Per quanto riguarda i moduli è composto da :

- **L'armadio o rack**, contiene e racchiude tutti gli altri moduli che sono collegati elettricamente tra loro grazie alla presenza sul lato opposto di una connessione elettrica e il bus che consente la comunicazione di dati, indirizzi, protocolli ecc tra i diversi moduli.
  I moduli sono di un unico proprietario quindi non si ha interoperabilità tra i moduli.
  Deve avere una buona resistenza nell'ambiente, costruzione in base all'ingombro ecc…
- Il **modulo processore** rappresenta il cuore di un PLC ed è costituito essenzialmente da una scheda a microprocessore; controlla e supervisiona tutte le operazioni eseguite all'interno del sistema attraverso l'esecuzione delle istruzioni contenute nella memoria. Avrà una memoria sia per contenere il SO che i programmi specificati dall'utente.
- Il **modulo alimentatore** è una scheda che alimenta tutti gli altri moduli presenti nell'armadio. Connesso alla rete di alimentazione elettrica.
  Quando parliamo di sistemi in ambienti pericolosi (interferenze, gas) l'alimentatore deve essere costruito in maniera attenta. Deve fornire una corrente costante.
  Poiché il PLC dovrebbe funzionare per un lungo tempo e in modo continuo, quando si hanno problemi con l'alimentazione sono previste batterie tampone o PLC di backup. In base al numero di moduli presenti, l'alimentazione fornita sarà diversa.
- I **moduli di I/O**, sono delle schede che permettono l'interfacciamento tra il PLC e il mondo esterno, e devono perciò provvedere al condizionamento dei segnali e all'isolamento. In base al numero di I/O il PLC si adatta per ricevere tutti i dati. Potrebbero avere filtraggi per evitare rumori o rimbalzi dall'ingresso dei sensori; esistono anche altri moduli per convertire i segnali da analogici a digitali.
- I **moduli di rete** sono delle schede che consentono la connessione ad altri dispositivi nella rete, o ad altri sistemi di supervisione e controllo (come i sistemi SCADA) tramite una connessione di rete.
- Il **terminale di programmazione:** per la programmazione e la configurazione del PLC che consente quindi il collegamento con sistemi di sviluppo , ad oggi basati su PC. Sono connessi al PLC o direttamente o attraverso una rete informatica. Consente inoltre di monitore il funzionamento del PLC.

Possono esistere poi una vasta gamma di **moduli speciali** che realizzano delle funzionalità speciali in maniera da rendere il sistema ancora più flessibile e più adeguato a rispondere a diverse esigenze:

- Moduli di I/O remoto per punti di ingresso disposti in superfici estese
- Moduli per la connessione in rete che gestiscono i protocolli di comunicazione per le diverse tipologie di reti informatiche
- Moduli PID Se la regolazione PID non è disponibile
- Moduli interfaccia operatore - attraverso tastiere e display alfanumerici o PC.
- Moduli di backup utile in caso di malfunzionamento poiché sostituiscono il PLC in tempi brevissimi nella gestione degli ingressi e delle uscite

*** Modulo processore:**

Vista la necessità di rispettare specifiche real time nell'ambito dell'automazione industriale, il PLC adotta una modalità di funzionamento nominale ciclica (detta anche a **copia massiva di ingressi e uscite**) che garantisce il funzionamento real time e prevede un ciclo composto da operazioni in sequenza:

- aggiornamento dei dati provenienti degli ingressi fisici
- esecuzione del/dei programma utente, che consentono il salvataggio dei dati nella memoria
- esecuzione di programmi di gestione del sistema per la diagnostica
- scrittura dei dati sull'area di memoria riservata alle uscite

Questo permette un'ottimizzazione delle comunicazioni con moduli di ingresso/uscita, e garantisce che i valori memorizzati degli ingressi restino inalterati durante l'esecuzione dei programmi.
Un primo svantaggio è che si deve attendere la fine del ciclo per leggere un ingresso o scrivere un'uscita.
Se un valore cambiasse due volte all'interno del ciclo, il sistema non memorizzerebbe la modifica.
Altro aspetto è che questo ciclo non ha una durata prefissata quindi potrebbe rallentare il processo.
Per particolari situazioni in cui non è tollerabile l'attesa è prevista la possibilità di eseguire delle operazioni con accesso immediato ai punti di ingresso/uscita da riservare però ai casi di emergenza.
Una alternativa al ciclo può essere rappresentata dalla gestione degli interrupt, che consentono di ricevere una modifica di dato in ingresso nel momento della modifica.

Il **SO** di un PLC è costituito da un insieme di programmi di supervisione memorizzati in maniera permanente nel modulo. Sono dedicati al controllo delle attività, all'elaborazione dei programmi utente e alla comunicazione. Abbiamo anche le funzioni di diagnostica (es. Watchdog) interna su funzioni principali.
Il sistema operativo si occupa anche della gestione di diverse modalità operative attivate attraverso una chiave hardware (usb):
- modalità di *programmazione*: utilizzata per caricare nella memoria del PLC il programma sviluppato.
Il programma viene scritto nel PC, non nel PLC stesso e poi viene memorizzato nel PLC.
- modalità di *convalida e debug* vengono eseguiti i programmi ma l'aggiornamento delle uscite è disabilitato per permettere di testare la correttezza del codice sviluppato senza preoccuparsi degli errori di programmazione.
- modalità di *esecuzione:* i programmi vengono eseguiti e l'aggiornamento degli ingressi e delle uscite viene effettuato permettendo l'effettiva comunicazione con i sensori e gli attuatori.

La **memoria** di un PLC è solitamente organizzata per aree distinte. Una possibilità ripartizione della memoria è la seguente:

- area sistema operativo, riservata alla memorizzazione permanente dei programmi del SO
- area di lavoro del sistema operativo, riservata alla memorizzazione di datida parte dei programmi del SO
- area ingressi/uscite, riservata alla memorizzazione degli stati degli ingressi e delle uscite
- area programmi utente, riservata alla memorizzazione dei programmi utente
- area dati utente, riservata alla memorizzazione dei dati dei programmi utente

Esistono alcuni moduli processore particolari, detti **PLC di sicurezza**, progettati per essere impiegati in applicazioni che richiedono gradi di sicurezza molto elevati, come nell'automazione di presse. Questi moduli processore prevedono una ridondanza di unità di elaborazione, le quali eseguono lo stesso programma e abilitano le uscite solo se vi è pieno accordo tra loro.

Soft PLC o PC Industriale

Sono particolari PLC realizzati tramite PC standard chiamati appunto soft PLC in quanto possono essere visti come personal computer comuni che emulano via software il funzionamento del PLC classico. Sono progettati e costruiti per poter essere utilizzati in ambienti ostili come quelli industriali e presentano moduli I/O come quelli dei PLC che permettono l'interconnessione con un numero elevato di sensori e attuatori. Inoltre, si basano su un principio di funzionamento misto: le funzionalità richieste durante il funzionamento nominale sono eseguite in real time mentre le modalità di interfaccia utente di comunicazione con i sistemi informatici ecc. che non hanno specifiche temporali real time sono gestite come task aperiodici da eseguire in momenti in cui l'elaborazione principale non è impegnata in compiti real time.

IEC 61131

È uno standard per i controllori programmabili, è suddiviso in 7 parti:

1. Informazioni Generali (2003)
2. Requisiti per gli apparecchi e test (1994; 2007)
3. Linguaggi di Programmazione (1993; 2003)
4. Linee Guida per l'utente (1995;2004)
5. Comunicazione (2000)
6. Programmazione per Controllo Fuzzy (2000)
7. Linee Guida per l'Applicazione e l'Implementazione dei Linguaggi di Programmazione per i Controllori Programmabili (1197; 2003)

Lo standard definisce i blocchi da cui *programmi* e *progetti* sono costruiti come Program Organization Units (POUs), cioè piccole unità software indipendenti di un programma utente.
Esistono tre tipi di POU: **funzioni** , **blocchi funzione** e i **programmi**.
Nel momento in cui definiamo diverse POUs diventa importante definire le interfacce di comunicazione (di chiamata) e il loro comportamento. Lo standard predefinisce le interfacce per le chiamate e il comportamento delle più frequenti FUN (come funzioni aritmetiche e di comparazione) e FB (come timer e contatori).
Corrispondono a dei blocchi, che possono essere chiamati tra di loro con o senza parametri.
Le funzioni e i blocchi di funzione costituiscono le "subroutines", dove le POU di tipo PROGRAM costituiscono il programma principale del PLC.

- **Funzioni** – L'idea di base di una **funzione** (FUN) come definita da IEC 61131-3 è che le istruzioni nel corpo di una funzione che sono eseguite sui valori delle variabili di ingresso generano un risultato in un valore in maniera non ambigua, ovvero invocate con i medesimi parametri danno sempre lo stesso risultato.
- **Blocchi Funzione** –Sono i principali blocchi per strutturare i programmi PLC. consente di memorizzare dei parametri, hanno variabili statiche, ovvero quando viene invocato con i medesimi parametri, potrebbe restituire valori che dipendono dallo stato delle sue variabili interne ed esterne, che sono salvati tra un'esecuzione e la successiva del blocco funzione (e. un contatore).
- **Programma** – Rappresentano l'elemento più alto di un programma utente per PLC.
  L'unico POU che ha la capacità di accedere agli I/O del PLC per renderli accessibili alle altre POUs.
  Possono utilizzare variabili di qualsiasi tipo. Tutte le variabili dell'intero programma che sono assegnate a indirizzi fisici devono essere dichiarate in questa POU o al di sopra (nelle sezioni *Configuration* e *Resource*). È consentito l'associazione di un PROG con un task all'interno della configurazione, per eseguire un programma a run-time, i programmi non sono chiamati esplicitamente da altre POUs.

Ogni PLC può essere formato da molteplici unità di processamento, note come "**risorse**" nello standard IEC 61131-3. Diversi programmi possono risiedere nella stessa risorsa, e differiscono per priorità e tipo di esecuzione (periodica, ciclica, aperiodica).
Prima che il programma possa essere caricato in un PLC, diverse informazioni sono necessarie per assicurare che il task associato abbia le proprietà desiderate, queste sono salvate in un file chiamato **configurazione**.

Un **progetto** PLC consiste di diverse POU che possono essere ottenute dal produttore del PLC o create dall'utente. I programmi possono essere usati per creare librerie di POU riutilizzabili. IEC supporta questo aspetto di ri-utilizzo del software, definendo che le Funzioni e i Blocchi Funzione devono rimanere universali.

Dichiarazione delle Variabili: lo standard usa variabili per immagazzinare e processare le informazioni. Variabili corrispondono a flag o a bit di memoria, La loro allocazione viene gestita dal sistema in modo autonomo e ognuna possiede un prefissato tipo di dato (Bool, Byte, Integer, ...). È anche possibile definire nuovi tipi di dato, come le strutture e gli array. E' inoltre possibili delle variabili "persistenti", che possono essere associate ad un indirizzo di I/O e possono mantenere il valore corrente anche in caso di guasto all'alimentazione. La parte della dichiarazione delle variabili può essere scritta in forma testuale indipendentemente dal tipo di linguaggio.

Codice: la parte del codice, o delle istruzioni, segue la parte della dichiarazione delle variabili e contiene le istruzioni che devono essere processate dal PLC. Si usano *linguaggi testuali* , come IL- Istruction List o ST- Structured Text o *linguaggio grafici* , come diagrammi ladder LD e diagrammi di blocchi funzione FBD o gli SFC. I metodi di programmazione del codice sono ovviamente inerenti al tipo di linguaggio scelto.

Caratteristiche dell'interfaccia: L'interfaccia della POU (come chiamo le POU) viene definita tramite l'assegnamento delle variabili ai tipi nella dichiarazione di ingresso e di uscita. L'interfaccia consente anche variabili globali. L'interfaccia di chiamata e i valori di ritorno di una POU possono essere anche graficamente rappresentati nei linguaggi LD e FBD. Le variabili dell'interfaccia di chiamata sono anche chiamati *parametri formali*. Quando una POU viene chiamata, i parametri di ingresso VAR_INPUT sono sostituiti dai parametri attuali, ossia copie delle variabili (call-by-value). Se invece si usano parametri VAR_IN_OUT si passa l'allocazione di memoria e quindi si potrebbero cambiare i valori.(call-by-reference).
(con VAR_OUTPUT verranno poi restituiti i valori in uscita)
I parametri formali e i valori di ritorno sono visibili anche all'esterno quindi una POU che chiama un'altra POU può utilizzare direttamente i loro nomi espliciti per utilizzarli.

IEC 61131 – 3

Lo standard IEC 61131-3 fornisce 3 linguaggi testuali e 3 linguaggi grafici per la scrittura di programmi utente.

I linguaggi testuali sono:

- Istruction List (IL)
- Structured Text (ST)
- Sequential Function Chart (SFC) in versione testuale

I linguaggi grafici sono:

- Ladder Diagram (LD)
- Function Block Diagram (FBD)
- Sequential Function Chart (SFC) in versione grafica

Lo standard consente l'utilizzo di altri linguaggi come C o BASIC basta che soddisfano dei requisiti fondamentali su cui si basano i linguaggi di programmazione di IEC 61131-3.
I linguaggi grafici utilizzano elementi grafici per formulare il comportamento desiderato del PLC.
Le linee di collegamento o i cosiddetti connettori indicano il flusso di dati tra funzioni e blocchi funzione. La rappresentazione di un POU utilizzando i linguaggi grafici include parti come quelle nelle lingue testuali:

1. Una parte iniziale e finale della POU
2. La sezione di dichiarazione -> può essere sia grafica che testuale
3. La sezione di codice -> divisa in reti. Le reti sono utili per strutturare il flusso di controllo di un POU.

- **Istruction List (IL)** è un linguaggio di programmazione simile ad assembler.
  IL è universalmente utilizzabile ed è spesso impiegato come linguaggio intermedio comune in cui sono tradotte gli altri linguaggi testuali e grafiche.
  Nella sezione del codice del linguaggio testuale IL è costituito da una sequenza di istruzioni, un'istruzione, che è un comando eseguibile per il PLC, è descritta esattamente su una riga.

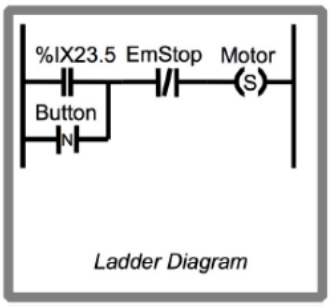
- Lo **Structured Text** (**ST)** è un linguaggio di alto livello, perché non usa operatori di basso livello, orientati alla macchina, ma offre una vasta gamma di affermazioni astratte che descrivono funzionalità complesse in modo molto compresso.

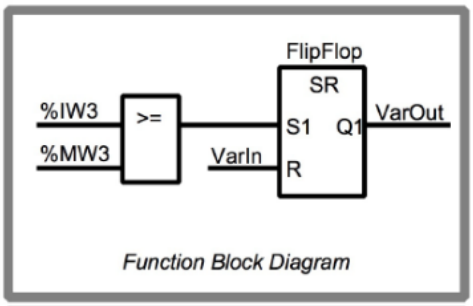
La sezione del codice del linguaggio testuale ST è costituito da una sequenza di dichiarazioni (istruzioni) che consistono in una combinazione di parole chiave, che controllano l'esecuzione del programma e le cosiddette espressioni. Le espressioni, costituite da operatori / funzioni e operandi, vengono valutate in fase di esecuzione.

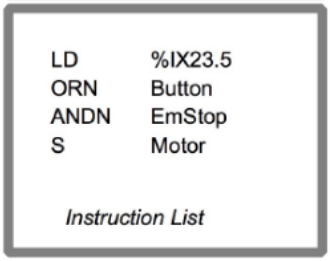
- Il linguaggio **Function Block Diagram** (FBD) deriva originariamente dal campo dell'elaborazione del segnale, e può essere usato per la programmazione con operazioni aritmetiche e binarie tramite rappresentazioni grafiche. Gli elementi grafici di una rete FBD comprendono oggtti-scatole definito magari da un'altra parte come blocco funzione) e istruzioni di flusso di controllo collegate da linee orizzontali e verticali. Gli ingressi non collegati delle scatole possono avere variabili o costanti ad essi collegate. Gli ingressi/uscite possono anche rimanere aperti (liberi).

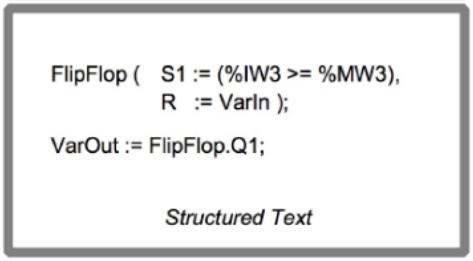
- Il linguaggio **Ladder Diagram** (LD) è adatto ad operazioni logiche binarie o booleane. deriva dal campo dei sistemi elettromeccanici e descrive il flusso di corrente attraverso la rete di un POU da sinistra a destra. Questo linguaggio di programmazione è progettato principalmente per l'elaborazione di segnali booleani (1 TRUE or 0 FALSE).

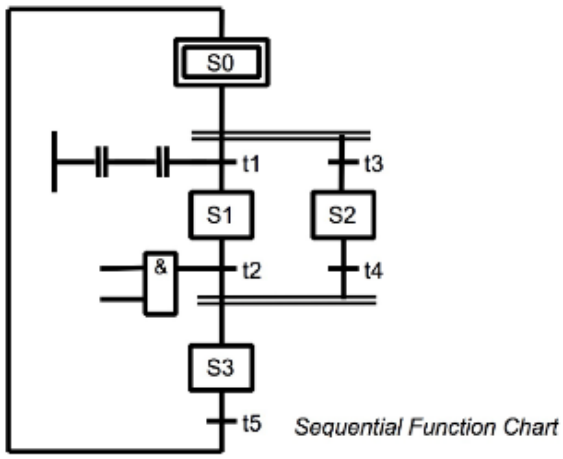
- Infine il linguaggio **Sequential Function Chart SFC** è stato definito per dividere un programma complesso in unità più piccole e più gestibili e per descrivere il flusso di controllo tra queste unità. può essere usato per descrivere la struttura di programma PLC mostrandone l'esecuzione sequenziale e parallela. La metodologia del SFC è stata ottenuta da tecniche ben note come le reti di Petri o la metodologia di sequenze e cascate Le diverse sottodivisioni del programma SFC possono essere programmate indipendentemente usando un qualsiasi linguaggio di programmazione.











SENSORI

Un **sensore** è un dispositivo di input che fornisce un'uscita utilizzabile in risposta a un input fisico specificato. è un particolare tipo di trasduttore (un dispositivo che opera una trasformazione dalla grandezza fisica che ha in ingresso restituendo un'altra grandezza fisica di tipo diverso in uscita) che si trova in diretta interazione con il sistema misurato e che opera una trasformazione da una grandezza fisica in ingresso, di diversa natura, in una grandezza elettrica.
I sensori possono essere digitali o analogici. I sensori che forniscono uscite **digitali** (on/off – T/F – 1/0) possono essere facilmente collegati alle porte di ingresso di un PLC. Un sensore **analogico** (valori continui) invece fornisce un'uscita proporzionale alla variabile misurata, quindi, in questo caso i segnali analogici devono essere convertiti in digitali prima di poter essere immessi nelle porte di un PLC.
Ovviamente rispetto ai sensori che si trovano in commercio hanno caratteristiche strettamente industriali come la robustezza, la longevità e la precisione.

Quando si parla di sensori si parla di una serie di specifiche che ne determinano le caratteristiche:

- **Precisione**: misura in cui il valore indicato da un elemento di misura potrebbe essere sbagliato, ad esempio la precisione di 1° significa che quella misura potrebbe avere un errore di +-1. Errore che ad esempio si presenta nella conversione analogico-digitale.
  Solitamente un sensore è un trasduttore in grado di dare un errore costante o dovuto alla linearità, in realtà non è sempre vero quindi se il sistema non è lineare, si ha un ***errore di non linearità***.
  Un altro errore è l' **errore dell'isteresi** dovuto all'errore che ottengo se raggiungo un certo valore da valori più bassi o più alti.
- **Range**: intervallo tra i valori che posso misurare
- Altre specifiche legate alla **dinamica**, quanto tempo ci vorrà affinché il mio sensore mantenga un valore constante (regime):
  - *tempo di risposta*: t che ci mette il sistema affinché l'uscita corrisponda al 95% del valore a regime
  - *tempo di salita*: t che il sistema passa da 10% a 95%
  - *tempo di assestamento*: t per stabilizzarsi entro una certa percentuale (5%)
- **Sensibilità**: quanto cambia l'uscita data una variazione nell'ingresso, praticamente la relazione uscita-ingresso
- **Stabilità**: capacità di fornire la stessa uscita quando viene usato per misurare un input costante per un periodo di tempo
- **Deriva**: cambiamento di uscita che si verifica nel tempo, una particolare condizione è della deriva zero, come cambia l'uscita se l'ingresso rimane costante
- **Ripetibilità**: capacità di fornire uno stesso valore in uscita ai medesimi valori in ingresso. Ad esempio se il sensore è sensibile ai cambiamenti ambientali (umidità) potrebbe cambiare.
- Affidabilità: probabilità che il sensore lavori in modo specificato

Interruttori meccanici

Un interruttore meccanico è un dispositivo che genera un segnale di attivazione/disattivazione come risultato di un input meccanico che causa l'apertura o la chiusura dell'interruttore. Possiamo usare un interruttore meccanico per indicare la presenza o l'assenza di un pezzo in lavorazione: il pezzo preme contro l'interruttore e quindi lo chiude. (1=true, 0=false se N-Open o al contrario se N-Closed).
Un altro tipo di interruttore meccanico è **l'interruttore di limite** che può essere azionato da una camma, un rullo o una leva che spinge la leva.

Interruttori di prossimità

Gli interruttori di prossimità vengono utilizzati per rilevare la presenza di un oggetto senza venirne a contatto.

- **L'interruttore eddy current** ha una bobina che viene eccitata da una corrente alternata costante che produce un campo magnetico. Quando un oggetto metallico è vicino ad esso, vengono indotte delle correnti parassite, il campo magnetico dovuto a queste induce un ritorno della Forze elettromotrice nella bobina con il risultato che l'ampiezza di tensione necessaria per mantenere la corrente costante cambia. L'ampiezza della tensione è quindi una misura della vicinanza dell'oggetto metallico e può essere usata per attivare un circuito di commutazione elettronico creando un segnale on/off.

- **L'interruttore a lamella** è costituito da due strisce di materiale ferromagnetico sovrapposte ma non a contatto. Quando un magnete o una bobina che porta corrente vengono avvicinate all'interruttore le strisce si magnetizzano e si attraggono andando a chiudere i contatti. Tale interruttore è utilizzato con allarmi antintrusione quando una porta viene aperta.
- **L'interruttore di prossimità capacitivo** è usato con oggetti metallici e non metallici. Sfrutta il fatto che la capacità di una coppia di piastre separate da una certa distanza dipende dalla separazione, più piccola maggiore sarà la capacità (l'interruttore è una delle due piastre). Quindi la prossimità dell'oggetto viene rilevata da un cambiamento di capacità. Questa variazione può essere utilizzata per attivare un circuito elettronico e creare un dispositivo on/off. Oppure per rilevare oggetti di diversa natura come determinare se una torta si trova in una scatola.
- **L'interruttore di prossimità induttivo** consiste invece, in una bobina avvolta attorno ad un nucleo ferroso. Quando una estremità di questo nucleo è posta vicino ad un oggetto di metallo ferroso vi è una variazione nella sua induttanza. Un esempio è quello di rilevare se le bottiglie che passano lungo un nastro hanno tappi metallici.

Sensori e interruttori fotoelettrici

I dispositivi di commutazione fotoelettrica possono funzionare come tipi trasmissivi in cui l'oggetto da rilevare interrompe un raggio di luce (ad esempio in applicazioni che prevedono il conteggio di parti in movimento); oppure come tipi riflettenti in cui l'oggetto riflette il raggio di luce sul rilevatore (utilizzati per rilevare se i contenitori trasparenti contengono liquidi al livello richiesto). Con questi sensori la luce viene convertita in un cambiamento di corrente, tensione o resistenza.

Sensori di temperatura (analogico)

Il sensore di temperatura sfrutta il fatto che due strisce di materiale diverso unite insieme hanno **coefficienti di espansione** diversi in base alla temperatura. Quando la temperatura aumenta la striscia con coefficiente di espansione più alto, che si trova all'esterno, si curva più dell'altro. Quando la striscia di bimetallo viene raffreddata l'effetto di piegatura si inverte. Questo movimento viene usato per creare o interrompere i contatti elettrici, e quindi ad una certa temperatura particolare, per fornire corrente on/off ad un circuito elettrico.

- **Il rilevatore di temperatura resistivo** (RTD) che sfrutta il fatto che la resistenza dei metalli o semiconduttori cambia con la temperatura. Sono molto precisi ma anche molto costosi.
- La **termocoppia** che consiste essenzialmente di due fili che formano una giunzione. Quando la giunzione viene riscaldata in modo che ci sia una temperatura più elevata rispetto alle altre giunzioni nel circuito viene prodotta una EMF correlata alla temperatura di giunzione calda.

Sensori di deformazione (analogico)

I sensori di deformazione sfruttano il fatto che quando un filo o una striscia di semiconduttore viene allungata la sua resistenza cambia. La **resistenza** è proporzionale alla variazione della lunghezza e quindi alla tensione. Tutto ciò viene sfruttato dal fatto che il cambiamento di resistenza di un estensimetro, viene convertito in un segnale di tensione. Un problema che si verifica però è che la resistenza dell'estensimetro cambia anche con la temperatura, quindi, devono essere utilizzati alcuni mezzi di compensazione della temperatura in modo che l'uscita del ponte sia solo funzione della deformazione.

Sensori di pressione (analogico)

I sensori di pressione possono essere progettati per fornire uscite proporzionali alla differenza di pressione tra due porte di ingresso. I sensori di pressione comunemente usati sono a diaframma e a soffietto. I sensori di **pressione** sono progettati per accendersi e spegnersi a una determinata pressione ciò può essere usato per creare degli interruttori.

Il tipo **a diaframma** è costituito da un disco di metallo o di plastica, fissato ai bordi. Quando c'è un cambiamento di pressione il suo centro devia. La quantità di deflessione è proporzionale alla differenza di pressione e può essere rilevata dagli estensimetri attaccati al diaframma. Lo stesso accade con un **soffietto**. La principale differenza è che i diaframmi sono meno sensibili dei soffietti ma possono resistere a pressioni maggiori.

Sensori di livello (analogico)

I sensori di pressione possono essere utilizzati anche per monitorare la profondità o la presenza di un certo livello di liquido in un serbatoio ad esempio attraverso un interruttore a galleggiante che contiene un magnete che si muove in un alloggiamento con un interruttore a lamella. Quando il galleggiante sale o scende, attiva o disattiva l'interruttore a lamella che viene collegato ad un circuito che attiva o disattiva la tensione.

Sensori di flusso (analogico)

Nei sensori di flusso si sfrutta la differenza di pressione che si verifica quando un fluido scorre attraverso un tubo con una restrizione. La differenza di pressione viene calcolata attraverso un diaframma e diventa una misura della velocità del flusso.

Sensori intelligenti (analogico)

Per utilizzare un sensore è necessario aggiungere circuiti che amplificano o convertono segnali per ottenerlo nella forma corretta; tenere conto di non linearità, della deriva o calibrarlo. Alcuni sensori hanno tutto questo incluso in un unico dispositivo chiamato sensore intelligente attraverso cui è possibile fare una prima analisi dei dati programmandoli.

ATTUATORI

Il termine attuatore viene utilizzato per un dispositivo che trasforma un segnale elettrico in un'azione più potente che quindi determina il controllo del processo.
Generalmente il segnale digitale proveniente da un canale di uscita di un PLC viene utilizzato per controllare un attuatore che a sua volta controlla un processo.

- **Relè** : quando una corrente passa attraverso un solenoide viene prodotto un campo magnetico che può attrarre componenti metallici nelle sue vicinanze. Con i relè questa attrazione viene utilizzata per azionare un interruttore. Quindi quando un relè viene collegato all'uscita di un PLC, quando l'uscita si attiva viene generato il campo magnetico del solenoide, che estrae i contatti e chiude l'interruttore.
  Un caso di relè è un **relè a ritenuta** che rimane aperto/chiuso anche se interrotta l'alimentazione.
- **Valvole di controllo**
  Un altro esempio di uso di un solenoide come attuatore è una valvola a solenoide che può essere utilizzata per controllare la direzione del flusso di aria o olio pressurizzato e utilizzarlo per azionare altri dispositivi come un pistone contenuto in un cilindro. Il movimento del pistone può poi essere utilizzato per implementare altre azioni.

MOTION CONTROL

Sensori di posizione

Il termine **sensore di posizione** viene utilizzato per un sensore che fornisce una misura della distanza tra un punto di riferimento e la posizione corrente, mentre un **sensore di spostamento** dà una misura della distanza dalla posizione attuale e la posizione precedentemente registrata.
- I sensori di posizione lineare e angolari sono ampiamente utilizzati e sono generalmente chiamati **potenziometri lineari e rotativi,** per cui in base alla rotazione si avrà un'uscita proporzionale allo spostamento.
- Un'altra forma di sensore di spostamento è il **trasformatore differenziale lineare** costituito da tre bobine posizionate simmetricamente attraverso le quali si muove un'asta ferrosa. Nel momento in cui l'asta si sposta verso una delle bobine si crea una tensione alternata maggiore in una bobina rispetto all'altra. L'uscita è quindi una tensione alternata che viene convertita e amplificata e poi immessa nel canale analogico del PLC.
I **sensori di spostamento capacitivo** invece sono essenzialmente dei condensatori a piastre parallele. La capacità cambierà se la posizione tra le piastre cambia. Questi metodi vengono utilizzati per fornire sensori di spostamento lineare.

Questi sensori di posizione servono perché si utilizzano all'interno di controlli in retroazione per i motori. Ovvero quando voglio che l'oggetto sia posizionato esattamente in un certo punto. Nel caso di servomeccanismi in cui la misura relativa al motore e la posizione di riferimento sono uguali il sistema avrà raggiunto la posizione desiderata.

Sincro

Nei servosistemi (dispositivi per controllare una grandezza meccanica nel tempo) in cui sia necessario rilevare e trasmettere a distanza una posizione angolare variabile si impiegano trasduttori realizzati in modo da consentire la trasmissione continua della posizione angolare, appunto i Sincro, senza alcun fine corsa e senza perdita di potenza; questo accade perché mediamente i potenziometri non girano all'infinito.

Resolver

Il resolver è un tipo di trasduttore, analogo al Sincro, di spostamento induttivo, dispositivo elettromeccanico per la misura di spostamenti angolari che consente di rilevare la variazione di flusso di induzione magnetica, concatenato con un solenoide, in funzione della posizione del solenoide stesso. Alimentato in corrente alternata, è un dispositivo analogico, cioè la tensione misurabile in uscita è una corrente alternata. L'analogo digitale prende il nome di encoder.
Sono impiegati nella strumentazione di bordo di navi ed aerei per i dati relativi alla posizione geografica. Un impiego tipico dei resolver è la trasformazione da coordinate polari a cartesiane e viceversa.

Encoder

L'Encoder è un dispositivo che converte uno spostamento angolare o lineare in impulsi elettrici, quindi in segnali digitali. Un encoder *incrementale* rileva i cambiamenti nello spostamento angolare o lineare da una certa posizione di riferimento; Un encoder *assoluto* fornisce la posizione angolare o lineare effettiva.

- Per quanto riguarda **l'encoder incrementale** un raggio di luce passa attraverso le fessure di un disco ed è rilevato da un sensore di luce. Quando il disco gira il raggio di luce viene trasmesso e interrotto alternativamente, e quindi sarà possibile calcolare lo spostamento.
- **L'encoder assoluto** differisce dall'encoder incrementale per avere un modello di slot che definisce in modo univoco ogni posizione angolare. all''aumentare del numero di tracce si ha una combinazioni univoche delle varie tracce (più preciso). Ad esempio si può utilizzare un codice binario corrispondente ad una particolare posizione angolare. Generalmente però viene utilizzata una forma modificata di codice binario chiamata Gray Code in cui la differenza tra un passaggio e l'altro modifica solo un bit, quindi è necessario utilizzare un circuito per convertire il codice Gray in codice binario.

Motori

Un **motore a corrente continua CC** è costituito da una bobina di filo montata in fessure su un cilindro di materiale ferromagnetico, chiamato armatura. L'armatura è montata su cuscinetti ed è libera di ruotare; è montata nel campo magnetico prodotto da magneti permanenti o corrente che passa in bobine di filo che sono chiamate bobine di campo. Quando una corrente passa attraverso la bobina dell'armatura le forze determinano una rotazione. Vi sono spazzole e un commutatore che sono utilizzati per invertire la corrente ogni mezza rotazione e quindi mantenere la bobina rotante. La velocità di rotazione può essere modificata cambiando la dimensione della corrente e in realtà ciò viene fatto di solito con un circuito elettronico. Generalmente un PLC può controllare la velocità di rotazione di un motore controllando il circuito elettronico.
Molti processi industriali però richiedono un PLC per accendere o spegnere un motore a CC. In questo caso vengono utilizzati i relè. Infatti, un relè controllato da un PLC farà in modo di accendere o spegnere il motore in maniera opportuna; mentre collegando due relè si può fare in modo di invertire la tensione e quindi far sì che il motore possa ruotare in un verso o nell'altro.
Un altro tipo di **motore a CC è quello senza spazzole** che utilizza un magnete permanente per il campo magnetico. Con un convenzionale motore CC è necessario utilizzare un commutatore per invertire la corrente ogni mezza rotazione, con il motore senza spazzole vengono utilizzati i circuiti elettronici. Il motore può essere avviato o arrestato controllando la corrente.
Generalmente i motori a AC sono più economici e più robusti oltre che più affidabili dei motori CC ma il mantenimento della corrente costante o il controllo della velocità sono più complessi del motore a CC. Per questo i motori a CC senza spazzole sono più utilizzati a fini di controllo.

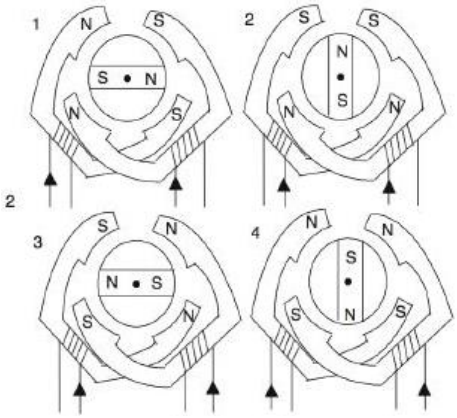
Motori stepper

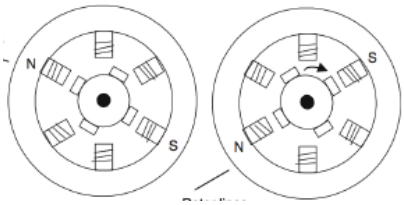
Il motore passo-passo o stepper è un motore sincrono in CC che può suddividere la sua rotazione in un grand numero di passi (step), per ogni impulso digitale fornito in ingresso.
È considerato la scelta ideale per tutte quelle applicazioni che richiedono precisione nello spostamento angolare e nella velocità di rotazione.
I motori passo-passo sono motori che, a differenza di tutti gli altri, hanno come scopo quello di mantenere fermo l'albero in una posizione di equilibrio, se alimentati si limitano infatti a bloccarsi in una ben precisa posizione angolare, solo indirettamente è possibile ottenerne la rotazione: occorre inviare al motore una serie di impulsi di corrente, secondo un'opportuna sequenza, in modo tale da far spostare, per scatti successivi, la posizione di equilibrio.
L'azionamento dei motori passo passo viene realizzato con un computer, un PLC, un microcontrollore o un circuito elettronico. Sostanzialmente si collegano le bobine a dei transistor di potenza e i transistor a ciò che li comanda. Per i motori unipolari, che hanno quattro bobine la corrente deve circolare nelle bobine sempre nello stesso verso. Per i motori bipolari, che hanno due bobine la corrente circola in entrambe le direzioni.

Possono essere a magneti permanenti o a riluttanza variabile o una forma ibrida che li combina.

In quello a **magnete permanente**, con un rotore a magnete permanente, alimentando in maniera opportuna due poli, e quindi le 2 braccia che vanno a costituire i 4 poli, ci sarà una rotazione.

In quello a **riluttanza variabile**, il rotore è realizzato in acciaio e ha un numero di denti, in numero inferiore dei poli sullo statore. Quando viene attivata una coppia di poli, il campo magnetico attrae la coppia più vicina di denti e questi si allineano. È cosi possibile ruotare in passi.
Infine, la versione **ibrida** combina le caratteristiche di entrambi.





SCADA

SCADA sta per **Supervisory Control and Data Acquisition** ovvero acquisizione dati, supervisione e controllo e sintetizza brevemente le tre funzioni svolte da questo sistema. Per distinguere un sistema SCADA da altri sistemi che svolgono funzioni simili occorre descrivere le varie funzioni svolte dal sistema SCADA, il modo in cui queste funzioni vengono svolte e il campo di applicazione.

- Per quanto riguarda **l'acquisizione dati** mette in relazione il sistema con il processo controllato.
  Un sistema SCADA deve eseguire funzioni di supervisione potendo acquisire informazioni sullo stato del processo, in modo da poterne orientare il comportamento e dunque controllarlo, influenzandone lo stato (cambiando valore ai parametri che lo caratterizzano).

- La **supervisione** è la funzione per mezzo della quale un sistema SCADA rende possibile l'osservazione dello stato e dell'evoluzione degli stati di un processo controllato. A questa funzione appartengono le funzionalità di visualizzazione delle informazioni relative allo stato attuale del processo, di quelle storiche, e degli stati che costituiscono delle eccezioni.
  => Un sistema che non permetta di accedere a queste informazioni non può essere considerato un sistema SCADA.

- La funzione di **controllo** rappresenta la capacità di un sistema di prendere decisioni relative all'evoluzione dello stato del processo in funzione dell'evoluzione del processo medesimo. Le funzionalità di controllo sono concentrate nel sistema di elaborazione il quale, una volta eseguite opportune procedure, sfrutta il sistema di acquisizione dati in senso inverso per cambiare valore ad opportuni parametri di stato del processo controllato.

A differenza quindi dei PLC che fanno un controllo puntuale (per esempio di un motore), un *sistema SCADA è in grado di andare a modificare i riferimenti o comunque i parametri del sistema* (che un PLC invece prevede che siano quelli dati).

Caratteristiche funzionali e architetturali

L'analisi del processo controllato produce informazioni che influenzano le scelte progettuali sia dal punto di vista tecnologico sia dal punto di vista organizzativo ed è consigliabile anteporre sempre l'approfondimento della conoscenza del processo prima di definire delle caratteristiche di un sistema di controllo. Vi sono alcuni elementi classici di indagine per la determinazione delle caratteristiche fondamentali del sistema di controllo. La qualificazione del processo rispetto a questi elementi permette di individuale dei vincoli che si traducono negli elementi distintivi del sistema realizzato rispetto a tutti gli altri.

- **Real time** si riferisce alla capacità del sistema di reagire alle sollecitazioni del processo con ritardi trascurabili rispetto alla dinamica evolutiva del processo medesimo.
  Un un primo elemento in contrasto con la caratteristica del sistema di operare in tempo reale risiede nei limiti imposti dalla tecnologia in quanto l'uso delle migliori tecnologie non potrà mai essere in grado di rendere nulli i tempi di trasferimento dell'informazione che creeranno sempre dei ritardi sull'intero sistema.

- Un sistema di controllo è costituito da vari componenti ognuno dei quali caratterizzato da un determinato grado di **affidabilità**, ovvero da un valore di probabilità di malfunzionamento espresso come percentuale del tempo di esercizio. Nella realizzazione di un sistema è necessario tenerne conto per ogni singolo componente, per elaborare eventuali contromisure per contenere l'influenza sull'affidabilità dell'architettura complessiva.

- La **disponibilità** è la percentuale di tempo per la quale deve essere assicurato lo stato di esercizio del sistema, cioè il valore complementare della percentuale di tempo in cui il sistema è fermo a causa di guasti, manutenzioni e aggiornamento. Può essere riferita all'intero sistema o a parti critiche di esso. Questa potrebbe essere una forte esigenza in industrie chimiche, per evitare che un processo chimico possa essere lasciato in stati potenzialmente dannosi.

- La realizzazione delle funzioni di un sistema di supervisione e controllo comporta sempre la definizione di sottosistemi responsabili dell'**interazione uomo macchina** (HMI). I gradi di interazione comprendono funzionalità di semplice osservazione dello stato di esercizio del sistema o funzionalità responsabili dell'esecuzione di procedure manuali gestite dagli operatori. Vi possono essere funzionalità accessorie per la comprensione dello stato del sistema come la notifica di allarmi e la visualizzazione di grafici relativi alle grandezze più importanti.

- occorre tener conto delle **dimensioni geografiche** del sistema SCADA che sono definite dalla collocazione delle apparecchiature di acquisizione dati e dal sistema di elaborazione. Se il processo controllato è limitato geograficamente le dimensioni rimangono limitate alla struttura che ospita il processo. Se invece il processo si estende per un'ampia area geografica (es. sistema di trasporto) la collocazione delle apparecchiature di acquisizione dati segue la struttura del processo, quindi potrebbe avere un numero elevato di postazioni che possono trovarsi in luoghi distinti e molto distanti tra loro. In questo caso è richiesta un'elevata affidabilità in termini di continuità e qualità del servizio.

Protocolli e tecnologie di comunicazione

Lo sviluppo di sistemi SCADA richiede un'analisi delle interfacce di comunicazione e una saggia scelta dei protocolli e tecnologie. La scelta delle tecnologie e dei protocolli di comunicazione ricoprono un ruolo importante nell'efficacia del funzionamento del sistema produttivo.
Tra gli elementi che possono essere oggetto di analisi vi sono:

Velocità di scambio dei dati: analizzando lo scambio dati tra le apparecchiature di acquisizione e i sistemi di controllo bisogna provvedere alla realizzazione di un canale di comunicazione sufficientemente veloce in modo da permettere che l'intero processo di acquisizione, trasmissione, elaborazione e attuazione avvenga in tempi veloci che rendano l'azione di controllo efficace.

Sicurezza: La sicurezza diventa una caratteristica rilevante quando le comunicazioni possono essere esposte a intrusioni indesiderati e potenzialmente pericolose. La sicurezza del sistema di controllo deve rispondere a esigenze che non dipendono solo dalla cattiva fede ma anche dalla probabilità di errore che caratterizza i comportamenti umani.

Servizi supportati: Una caratteristica dei protocolli e tecnologie di comunicazione riguarda il tipo di servizi che vengono erogati. Nell'analisi della comunicazione è necessario valutare correttamente la le caratteristiche e i tipi di dati che bisogna trasferire per scegliere, tra i servizi offerti, quello che meglio si adatta ai bisogni prefissati. Tecnologie diverse e protocolli diversi, infatti, possono erogare servizi identici ma con prestazione totalmente diverse. Occorre quindi valutarne le caratteristiche e valutare l'opportunità di adottarle. (come la valutazione di qualità offerta da un tipo di infrastruttura in termini di robustezza o garanzia di trasferimento dati).

Affidabilità: la trasmissione dei dati è un processo caratterizzato da fenomeni che possono compromettere l'integrità dell'informazione trasportata comportando rischi di valutazione errata dello stato di esercizio del sistema. Architetture protocollari diverse sono dotate di algoritmi di controllo per l'individuazione degli errori causati dalle infrastrutture di trasporto molto diversi tra loro. I due estremi tra le molte soluzioni possibili al problema dell'integrità del flusso informativo sono quelli che realizzano la trasmissione senza alcun controllo, lasciando al fruitore la necessità di intercettare errori e provvedimenti da adottare oppure scegliere soluzioni che garantiscono l'integrità del flusso come elemento caratteristico della trasmissione di dati. La prima soluzione risulta efficace quando il mezzo trasmissivo e le apparecchiature sono caratterizzate da probabilità di errore molto basse con mezzi trasmissivi ad altissima affidabilità. Quando invece il mezzo trasmissivo e le apparecchiature sono caratterizzate da inaffidabilità intrinseca l'uso di architetture protocollari prive di meccanismi di gestione errore è impensabile; in tal caso la scelta ricade sull'usare servizi di trasmissione affidabili oppure realizzare i meccanismi di gestione degli errori.

Disponibilità: nella realizzazione del sistema SCADA è sempre importante valutare gli effetti causati da disservizi nel trasferimento dell'informazione, come interruzione del servizio di trasmissione dati. Solitamente il sistema di comunicazione interno a un sistema di controllo deve essere dotato di una continuità del servizio. Se il sistema attua politiche di controllo necessita di un continuo aggiornamento dello stato di esercizio del processo controllato e al tempo stesso di un canale di comunicazione con disponibilità immediata nel momento in cui si rende necessaria l'attuazione di un'azione di controllo. È necessario quindi scegliere tecnologie e protocolli che prevedano queste caratteristiche. Generalmente si fa ricorso al principio della ridondanza dei dispositivi lungo l'intero canale di comunicazione; ciò permette una riduzione significativa della probabilità di guasto ma non la sua eliminazione definitiva.

Intellegibilità: In questo senso è importante valutare le soluzioni proposte dai produttori di dispositivi e software utilizzati nello sviluppo del sistema di controllo e fare riferimento agli "standard" disponibili, privilegiando quelli che hanno dimostrato di essere soluzioni efficaci al problema delle comunicazioni. Dove per "standard" si considerano tecnologie frutto del processo di produzione di modelli di comunicazione condivisi, condotti da istituti o enti.
(intellegibilità: attitudine degli apparati interessati a una comunicazione corretta e chiara delle informazioni, quindi senza interferenze)

Architettura software di un sistema SCADA

Il cuore di un sistema SCADA è rappresentato dalla sua realizzazione software.
Il sistema presenta una struttura modulare con tecnologia client/server.

Base di dati di processo: è il nucleo del sistema a cui tutti gli altri moduli fanno riferimento.
È importante quindi avere un metodo sistematico per processare le informazioni, conservando insieme con esse tutta una serie di parametri che sono necessari per la loro corretta gestione (TAG, una descrizione, un tipo, un indirizzo, una classe allarme, il tempo di aggiornamento, il valore grezzo e il valore convertito e lo stato dell'allarme). Uno dei grossi vantaggi nel suo utilizzo è che la base di dati provvede a uniformare i dati che contiene, che possono essere di tipo diverso; questo permette agli altri moduli di accedere alla base di dati senza conoscere dettagli su come la variabile è misurata o convertita, ma conoscendo solo la rappresentazione di questa all'interno della base di dati.
Gli altri moduli invece non sono tutti necessariamente presenti:

- **Modulo comunicazione (driver):** si occupa della gestione delle comunicazioni con i vari dispositivi e del controllo del trasporto delle informazioni, in via seriale o rete informatica. In un sistema SCADA deve esserci almeno un modulo di comunicazione, per avere accesso contemporaneamente ai diversi dispositivi che sono connessi con il campo denominati con la sigla RTU – Remote Terminal Unit (es. PLC, regolatori ecc).
  Un modulo di comunicazione può inoltre consentire la comunicazione con altri applicativi in esecuzione sullo stesso elaboratore, ottenuta attraverso gli strumenti tipici dell'ambiente operativo. (Ad esempio, se il sistema SCADA funziona su Windows viene fornito un driver per collegarlo ad altri applicativi come un foglio elettronico o un programma di gestione).

- **Modulo gestione allarmi**: nell'ambito di un sistema SCADA gli allarmi da gestire sono classificati in:
  - *Allarmi a insorgenza*: si attivano al verificarsi di un evento e permangono nel loro stato di attivazione;
  - *Allarmi a insorgenza e riconoscimento*: si attivano al verificarsi di un dato evento e possono venire disattivati quando l'operatore ne effettua il riconoscimento comandandone la disattivazione;
  - *Allarmi a insorgenza, riconoscimento e rientro*: sono come gli allarmi a insorgenza e rientro ma per essere disattivati necessitano oltre che del riconoscimento da parte dell'operatore anche del venir meno della condizione che ha generato l'allarme.

  Il sistema permette di programmare la condizione che genera l'allarme e il tipo di allarme e ovviamente il raggruppamento degli allarmi in differenti classi di priorità. È possibile associare ad ogni allarme o gruppo di allarmi con la stessa classe di priorità una sequenza di operazioni prefissate che il sistema SCADA eseguirà automaticamente qualora un allarme si attivi. I livelli di priorità definiscono ovviamente gli allarmi che devono essere risolti prima.

L'insorgere di un allarme, viene immediatamente comunicata tramite l'interfaccia operatore e viene memorizzata in una memoria non volatile per permettere un'analisi a posteriori del numero, la frequenza e il tipo di allarme. Un'altra possibilità offerta è quella del filtraggio degli allarmi utile per ridurre le segnalazioni allarme a quelle veramente significative.

- **Modulo interfaccia uomo – macchina**: si occupa dell'interfaccia operatore e deve permettere almeno l'accesso alla base di dati con tecniche di selezione per il rintracciamento di variabili, di campi o di ordinamenti. Per una comunicazione efficiente è prevista la possibilità di integrare delle pagine grafiche che rappresentano pannelli di comando o schemi (sinottici) dell'impianto o di parte di esso. I pannelli di comando permettono all'operatore di inviare comandi attraverso simboli grafici: pulsanti, manopole, ecc. Il Sistema SCADA infatti offre una libreria di oggetti grafici predefinita per lo sviluppo di schemi grafici anche complessi.

- **Supporto alla manutenzione**: nelle operazioni di processi produttivi vi sono azioni di manutenzione che possono essere suddivise in due categorie:
  - *manutenzione correttiva o straordinaria* per riparare dispositivi che si guastano. Se il sistema SCADA rileva una condizione anomala di funzionamento permette all'operatore di identificare in maniera abbastanza puntuale l'area del malfunzionamento e le possibili cause, e tenerne traccia per analisi successive.
  - *manutenzione preventiva o programmata*, per mantenere l'impianto in condizioni ottime di funzionamento. Molte operazioni, infatti, devono essere eseguite con cadenza temporale fissata o dopo un certo numero di ore di funzionamento; altre devono invece essere eseguite se si verifica un certo evento, quindi, è chiara l'esigenza di avere una procedura automatica, inglobata nel sistema SCADA, che segnali agli operatori quali sono le operazioni da eseguire generando il cosiddetto ***piano di manutenzione***.

- **Gestione ricette:** si occupa della gestione delle sequenze di operazioni predefinite, dette "ricette", che possono essere eseguite in seguito a scadenze temporali, al verificarsi di eventi o alla richiesta di un operatore. In generale serve ad impostare, in un ambiente multiprocesso/prodotto i dati di impianto per ciascun processo/prodotto, che rappresentano i parametri da fornire alle macchine utili all'esecuzione della lavorazione.

- **Sistema esperto:** è delegato alla decisione sulle modalità di comportamento del sistema in risposta a determinati eventi nel caso in cui non siano state esplicitamente programmate. In linea di principio il modulo deve sostituire l'operatore umano il quale, in queste situazioni, prende delle decisioni in base allo stato dell'impianto o alla sua esperienza. Molto spesso però si preferisce non dare troppa autonomia al sistema ma fargli presentare una serie di ipotesi di comportamento all'operatore umano, al quale poi spetta la decisione finale.

- **Controllo statistica del processo:** costruisce in tempo reale i diagrammi di controllo che rappresentano dati statistici del processo rispetto al tempo, in una forma che rende agevole stabilire se il processo si mantiene in uno stato di controllo statistico oppure se ne sta allontanando.

SCADA vs DCS

La principale distinzione tra SCADA e DCS è la distribuzione dell'intelligenza del sistema. Un sistema SCADA viene considerato come un sistema con funzioni di controllo concentrate nel sottosistema di elaborazione e fisicamente e tecnologicamente distinte dalle funzioni di acquisizione. I sistemi DCS, invece, sono caratterizzati da strutture di acquisizione dotate di elevata capacità elaborativa che hanno condotto alla realizzazione di funzioni di acquisizione e controllo contigue.
Un sistema SCADA è generalmente un sistema **centralizzato** di acquisizione pura, mentre i DCS sono sistemi **distribuiti** con apparecchiature di acquisizione complesse. Infatti, nei sistemi DCS non è possibile parlare di apparecchiature di acquisizione come nei sistemi SCADA perché consistono in veri e propri sistemi di elaborazione complessi in grado di interpretare i dati provenienti dall'osservazione del processo, valutarne le caratteristiche e prendere decisioni orientate al controllo dello stato.
Ad oggi, con lo sviluppo delle tecnologie e delle infrastrutture di comunicazione la distinzione tra sistema SCADA e DCS va affievolendosi.
Un **sistema di controllo distribuito** (DCS) è un sistema di controllo automatico costituito da diversi sottosistemi, in grado di scambiare autonomamente informazioni con il campo (processo o impianto) in architettura distribuita.

SICUREZZA - Safety e Security

I sistemi di comunicazione industriale assumono compiti sempre più importanti, nel momento in cui questi sistemi assumono compiti fondamentali per la sicurezza delle persone o dell'ambiente è necessario raggiungere un certo livello di integrità della sicurezza. Ad esempio, in ambito industriale deve essere possibile arrestare un motore in caso di emergenza, evitare che un motore si avvii in modo improvviso e poterne ridurre la velocità. Il problema essenziale è che il termine italiano *sicurezza* traduce entrambi i termini inglesi *safety* e *security* che però sono due concetti distinti, anche se entrambi hanno l'obiettivo di evitare eventi indesiderati.

- La **safety** riguarda la prevenzione di incidenti non intenzionali (es. malfunzionamenti) che comportino danni a persone o all'ambiente;
- La **security** invece riguarda la protezione del sistema e delle persone da attacchi o minacce di attacchi intenzionali, fatte da persone esterne (hacker).

SAFETY

E' la parte della sicurezza industriale che riguarda la prevenzione di incidenti non intenzionali (es. malfunzionamenti) che comportino danni a persone o all'ambiente, lo standard **IEC 61508** la definisce come "*libertà dal rischio inaccettabile di danno".*
In generale la safety non è una proprietà assoluta: affermare che il rischio relativo a uno specifico sistema è stato ridotto a zero non è una dichiarazione realistica, per questo si parla più di **accettabilità del rischio**: ovvero quale livello di rischio siamo disposti ad accettare.

Un primo passo quando si parla di safety consiste nell' identificare quali sono i pericoli ("*potenziale fonte di danno"*) per controllarli e mitigarne gli effetti. Quando vengono identificati tutti i pericoli e tutte le misure la sicurezza si considera raggiunta. Questo procedimento di identificazione deve essere sempre anteposto allo sviluppo di un sistema. L'importanza dei pericoli e della loro identificazione serve anche per attuare delle azioni preventive.

I problemi di Safety sono anche legati ai **problemi di comunicazione**, quindi bisogna che anche la rete di comunicazione rispetti la sefety desiderata.
I sistemi di comunicazione industriale legati alla safety si ottengono migliorando i sistemi di comunicazione standard tipicamente non sicuri, integrando funzioni di sicurezza, che di solito garantiscono livelli di sicurezza di tipo SIL3. Questi sistemi devono essere implementati in modo tale da poter evitare errori sistematici e rilevare guasti stocastici che portano a rischi come la corruzione di un messaggio. L'idea è quella di avere una ridondanza nei canali di comunicazione, un'architettura chiamata *one-out-of-two* (1oo2), il che significa che esistono due canali distinti che eseguono la trasmissione del messaggio e che, alla ricezione concordare il risultato all'unanimità.
In genere, i sistemi di comunicazione standard includono già alcune misure per la rilevazione dei guasti (come un CRC – *controllo di ridondanza ciclico* nella parte del payload).

Durante la valutazione della sicurezza ci sono due approcci su come trattare il sistema di comunicazione: considerare le misure di rilevamento guasti già disponibili e aggiungere ulteriori misure per raggiungere il livello di integrità desiderato, o considerare il sistema come una scatola nera, quindi lo standard viene considerato non sicuro e viene integrato con sistemi di sicurezza esterni.

- La sicurezza della rete di controllo **CAN** si basa sui meccanismi di rilevamento guasti di Can *standard*; per aumentarne l'integrità di sicurezza i messaggi vengono inviati due volte e il secondo è invertito. Viene utilizzato il protocollo **CANopen** con l'utilizzo di un Watchdog: controllore esterno che consente di capire se il messaggio arriva correttamente. Il CanOpen garantisce un SIL3. Inoltre viene aggiunta un'architettura hardware con due canali.
- **ProfiSafe** invece, che è la versione di sicura di PROFIBUS o ProfiNet, si basa sul concetto di *canale nero*: la rete standard, il protocollo standard e le componenti hardware standard dei nodi sono trattati come una scatola nera e si assume che non siano sicuri. Vengono quindi aggiunti hardware e firmware relativi alla sicurezza esternamente al canale nero.

Al fine di garantire la sicurezza del sistema, esistono degli **standard** che ci consentono di applicare la safety anche a sistemi molto diversi da loro (es. produttori diversi).
Un problema generale riguarda un giusto compromesso tra l'applicabilità e l'utilità di uno standard: uno standard generico, applicabile ad una vasta gamma di sistemi, risulta meno comprensibile per un dominio specifico; al contrario, uno standard più specifico è applicabile ad una gamma di sistemi più limitata. Per questo si differenziano come *generici*, *specifici* del dominio o dell'applicazione.
Tutti questi Standard hanno in comune il fatto di specificare un modello di ciclo di vita in cui un'analisi di rischio, una specifica dei requisiti di sicurezza, un'analisi della Safety e la convalida sono attività cruciali.

SECURITY

Nel contesto delle comunicazioni industriali la **security** può essere definita come una serie di misure che proteggono il sistema da avversari che cercano intenzionalmente di ottenere accessi non autorizzati e dannosi.
L'azione effettiva che un avversario compie per ottenere l'accesso alle funzioni di controllo viene generalmente definita **attacco di sicurezza**. Un attacco di sicurezza è possibile solo se il sistema presenta delle vulnerabilità, cioè dei difetti o punti deboli che possono essere sfruttati. La presenza di vulnerabilità determina delle minacce ovvero delle potenziali violazioni della sicurezza che è necessario identificare.
Ovviamente mentre un attacco alla security è l'azione effettiva che tenta di violare la sicurezza di un sistema, una minaccia alla security è la potenziale violazione della sicurezza e potrebbe non avvenire.
Dal momento che la sicurezza è stata per anni un argomento importante nel mondo IT esistono molti meccanismi di sicurezza già disponibili. Tuttavia, non sempre è possibile utilizzare questi meccanismi nel mondo industriale. I sistemi di comunicazioni industriale hanno infatti requisiti di sicurezza in tempo reale che non possono essere soddisfatti dai protocolli usanti nel mondo IT.

Infine, i sistemi di comunicazione industriale sono sistemi distribuiti in cui la funzionalità di controllo è distribuita su diversi dispositivi. Per interagire tra loro, questi dispositivi, devono essere interconnessi da una rete comune. Pertanto, gli avversari hanno due differenti possibilità di ottenere un accesso non autorizzato alle funzioni di controllo:

- L'avversario può tentare di interferire con lo scambio di dati tra dispositivi e in tal caso si parla di **attacchi di rete**. Oppure
- L'avversario può attaccare direttamente i dispositivi che implementano la funzionalità di controllo e in tal caso parliamo di **attacco al dispositivo**.

Per contrastare questo tipo di attacchi alla security devono essere garantiti diversi obiettivi di security come integrità, disponibilità, riservatezza, autenticazione, autorizzazione e non tracciabilità.

IEC 61508

Lo IEC 61508 è uno standard internazionale che disciplina l'intero ciclo di vita dei prodotti e dei sistemi elettrici, elettronici o elettronici programmabili (E/E/PE) relativi alla sicurezza, inclusi la loro applicazione, progettazione, utilizzo e manutenzione. L'IEC 61508 è uno standard generale che si applica a tutti i settori industriali.
L'idea di base è quella di considerare delle apparecchiature sotto controllo, EUC (Equipment Under Control), che con rischio intrinseco. Al fine di ridurre questo rischio vengono implementati dei sistemi di controllo. Ad esempio, in una fabbrica, delle macchine pesanti potrebbero essere dei EUC, che se non controllate, potrebbero comportare dei rischi per l'operatore.
L'importante è che questi sistemi di controllo funzionino correttamente, nel senso che non creino problemi in caso di malfunzionamenti o errori.

A seconda della necessaria riduzione del rischio, il sistema relativo alla safety è classificato in uno dei 4 livelli di integrità di sicurezza **SIL**.

SIL	Dangerous Failure per Hour
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

I SIL sono definiti in termini di tassi di fallimento accettato relativo a guasti pericolosi all'ora. Si presuppone che un SIL4 sia più sicuro di un SIL1.
In generale, avere un determinato SIL vuol dire far si che il sistema complessivo possa avere dei guasti/malfunzionamento appartenenti ai range in tabella.
Inoltre, a seconda del SIL richiesto esistono dei vincoli nell'architettura del sistema; maggiore è il SIL minore è la tolleranza ai guasti. Inoltre, più è alto il SIL più rigorosi sono i metodi che devono essere utilizzati per la progettazione e lo sviluppo di un sistema, compresa la parte di software.

Oltre ai vincoli, lo standard richiede la produzione di una **documentazione** adeguata necessaria per poter verificare se il sistema ha effettivamente raggiunto il SIL richiesto, come una "prova di sicurezza", che deve essere poi approvato da alcune agenzie di regolamentazione prima che il sistema entri in funzione.

Aree pericolose

Sono quelle porzioni dell'impianto, a rischio, che dovrebbero garantire quindi una maggiore sicurezza. Lo standard **IEC 61158-2** definisce i vincoli necessari per definire i protocolli di comunicazione all'interno delle Aree pericolose.

In industrie come quelle chimiche o petrolchimiche, è intuibile che si deve mantenere un alto grado di cautela a causa della presenza di sostanze infiammabili e del passaggio di corrente nei sistemi di comunicazione. Devono quindi essere attuate misure preventive per salvaguardare la sicurezza in caso di esplosioni/incendi, magari utilizzando custodie a prova di esplosione e spurgo.

Per quanto riguarda la classificazione delle **aree pericolose**, questa si basa sull'identificazione di materiali infiammabili (NFPA) e sulla possibilità che vengano a contatto con archi elettrici provocando esplosioni.
Esistono due tipologie di classificazioni:

- Divisione: un'area pericolosa viene identificata da una classe, una divisione e un gruppo.
  La *classe* = tipo di materiale (gas, polvere…), la *divisione* = probabilità della presenza di materiale infiammabile e del suo utilizzo; e il *gruppo* = proprietà fisiche del materiale infiammabile. (nord America)
- Zone: le aree pericolose vengono divise in zona 0, zona 1 e zona 2.
  La zona 0 è dove effettivamente è presente il liquido infiammabile, la zona 1 è quella direttamente a contatto con una zona 0 e la zona 2 è quella più lontana dove in condizioni normali non dovrebbe essere presente del liquido infiammabile.

Bus di campo (FieldBus) intrinsecamente sicuri

Il tema della sicurezza oggi è sempre più fondamentale in ambito industriale, anche in relazione ai bus di campo (connessione tra PLC e attuatori-sensori).
Un rete di bus di campo *regolare* e una rete di bus di campo *intrinsecamente sicura* non differiscono topologicamente ma le differenze riguardano il numero di dispositivi per segmento e la presenza di barriere di sicurezza che servono a limitare la potenza di alimentazione dei cavi.
Gli strumenti di campo per sistemi intrinsecamente sicuri sono progettati in modo da non iniettare energia nel bus. Per ciascun segmento viene impiegata una sola fonte di alimentazione elettrica, quindi non è consentita alcuna ridondanza; e le barriere sono collocate in aree sicure, poiché più economiche; e, nel caso in cui c'è l'esigenza di collocarle in aree pericolose, devono essere alloggiate in custodie di sicurezza a prova di fiamma.
Limitando l'alimentazione si avranno meno dispositivi e una lunghezza limitata.
In pratica, tra la parte sicura e quella non sicura, viene collocata una barriera che consente di dividere le due porzioni di rete.
Negli anni sono nati dei metodi di convalida di un'installazione di sicurezza intrinseca che sono serviti ad aumentare la potenza elettrica e il numero di dispositivi per segmento:

- **Concetto di Entità**: vengono valutati tutti i parametri del sistema (tensione, la corrente, la capacità) e, attraverso notevoli calcoli matematici si rilevano i limiti della barriera prevista dallo standard. Limitando la potenza limito anche il numero di dispositivi, in questo metodo molto pochi (2/3 dispositivi per barriera).
- **Modello FISCO**: aumentando la potenza disponibile è possibile aumentare il numero di dispositivi per segmento. La differenza sostanziale con il modello entity è che semplifica i calcoli e i parametri (che diventano standard) di installazione.
  L'idea è quella di mantenere una singola alimentazione per segmento, e di non consentire feedback ai dispositivi sull'alimentazione del cavo.
  Si raddoppia il numero di dispositivi, l'unico problema è che prevede alimentatori molto costosi.
  Modello FISCO ridondante: ha due alimentatori, in modo da garantire una commutazione al secondo alimentatore in caso di guasti. *Modello FISCO multidrop:* più alimentatori collegati ai segmenti
- **Modello HPTC**: aumenta drasticamente il numero di dispositivi per segmento e quindi la potenza. Per fare questo vengono inseriti dei metodi meccanici di protezione contro le esplosioni, effettuati nelle varie zone. è possibile utilizzare alimentatori standard quindi, meno costosi, in configurazione ridondante con due alimentatori in parallelo (in caso di guasto subentra l'altro). Quindi fa si che aumenta la disponibilità e la durata degli alimentatori.

- **Modello DART**: cambia totalmente l'approccio di funzionamento: DART consente una potenza disponibile molto più elevata in condizioni normali (come quelle in ambienti non pericolosi), grazie alla interruzione rapida della comunicazione in caso di scintille o malfunzionamenti.
  L'idea di basa sul fatto che, in caso di un'esplosione, esiste una primissima fase prima della scintilla seguita poi dall'esplosione vera e propria. Nella fase immediatamente prima della fase critica si avrà una notevole variazione della corrente. Si cerca quindi di riconoscere questo cambiamento, in modo da poter disattivare immediatamente l'alimentazione e quindi evitando di arrivare alla scintilla. DART inoltre è di semplice installazione e manutenzione e supporta il numero massimo di dispositivi consentiti per segmento (32). Le infrastutture diventano molto più piccolo e i costi vengono ridotti.

Rete di bus di campo = rete industriale di comunicazione per il controllo distribuito in tempo reale, nel livello di campo.

Protocolli Bus di campo

La comunicazione industriale consiste nel trasportare le informazioni sul campo e nel controllare il processo in modo affidabile ed efficace. Esistono diversi tipi di protocolli di rete a seconda delle esigenze situazionali. Generalmente le reti industriali sono indicate come bus di campo che includono bus di processo e bus di dispositivo, che dipendono dalla dimensione dei dati che viene gestita in una sola volta. Esiste una crescente domanda tra gli utenti dei sistemi di automazione industriale per un protocollo unificato industriale indipendente dai produttori. Lo scopo è di mantenere alcuni aspetti chiave: di avere un sistema che consenta il determinismo (sicuri del caso peggiore) e di andare verso sistemi aperti che comportano riduzione dei costi e una maggiore disponibilità di informazioni dai dispositivi di campo.

I diversi livelli della struttura secondo la piramide CIM si devono gestire diversi requisiti specifici per quel particolare livello. Ad esempio, il livello aziendale deve gestire un grande volume di dati molto più strutturati ma non critici. Nei livelli inferiori invece si hanno informazioni meno strutturate ma con tempi di campionamento molti più stringenti. Quindi si avranno velocità diverse, quantità di informazioni diverse e quindi anche strutture diverse, come lunghezze di cavi ecc.
Per specifiche diverse si avranno protocolli diversi per ogni livello. Questi cambiano in base alla velocità, al volume e alla sicurezza dei dati.
Si userà come standard, o metro di paragone, la struttura della pila ISO-OSI.

RETI A BUS I/O

I dati e le informazioni sullo stato nei livelli più bassi vengono comunicati tramite il bus I/O, ad esempio, le condizioni di un dato macchina o di un processo.
In pratica è la parte della rete che collega i PLC ai vari dispositivi di campo. In generale I PLC saranno collegati ad una LAN, collegata ad un PLC di supervisione che collega poi il resto della rete.
Le reti di bus I/O sono suddivise in due categorie: reti di bus di dispositivo e reti di bus di processo.
Le reti di bus di **dispositivi** si interfacciano con dispositivi di basso livello (dispositivi discreti come interruttori di fine corsa e pulsanti), mentre le reti di bus di **processo** si interfacciano con dispositivi di informazione di alto livello (sensori intelligenti, valvole di controllo, misuratori di pressione, ecc).
Le reti di bus di processo si occupano di dispositivi analogici mentre le reti di bus di dispositivi si occupano principalmente di dispositivi discreti. Oggi però si parla principalmente di reti di campo che riescono a supportare sia dati analogici che discreti.

L'avvento della comunicazione digitali ha fatto ampliare la capacità dell'automazione industriale. Consente a più di un dispositivo fieldBus (es PLC) di comunicare i propri dati sul filo e quindi comunicare con molti altri dispositivi. La trasmissione digitale ha i suoi vantaggi in quanto è meno suscettibile alle interferenze elettromagnetiche ed è molto più facile ripristinare un segnale digitale piuttosto di uno analogico.
Inoltre, un dispositivo di campo intelligente può passare un valore digitale direttamente proporzionale al valore di processo, eliminando la necessità di linearizzare o scalare i dati.
Ovviamente vi è una notevole riduzione del cablaggio, facilità di espansione dell'impianto, risparmi sui costi, sui tempi di fermo, identificazione dei guasti in modo semplice se necessario.

Nel momento in cui inserisco una rete di comunicazione tra dispositivi e PLC posso avere un controllo bidirezionale che raggiunge anche il livello di dispositivi di bordo di tecnologia fieldbus.
Le strutture che vedremo nei protocolli avranno due livelli esistenti: una a livello di campo e una di host.
Esiste ancora la comunicazione analogica 4-20mA.
I dispositivi di campo binari, come interruttori di fine corsa, solenoidi e valvole, sono integrati tramite le schede di I/O binarie dei PLC mediante una connessione punto-punto.

Per altri protocolli come **Modbus** deve esserci invece una interfaccia appropriata nel controllore per l'integrazione.
Per altri segnali come quelli analogici (4-20mA)si avranno collegamenti point-to-point collegata direttamente al PLC.
In **foundation fieldbus** (FF) , si ha una doppia comunicazione, di tipo gerarchica basata su due algoritmi FF H1 (liv. Più basso) e un protocollo di tipo H2 come dorsale, che consente di collegare diversi dispositivi tra di loro, cambiando ovviamente la velocità tra questi.

Nel caso di **PROFIBUS** i dispositivi vengono collegati tramite un segmento (PROFIBUS-PA), che viene poi portato alla rete a velocità più alta (PROFIBUS-DP) tramite un accoppiatore o collegamento di segmento che funge da interfaccia tra i due segmenti.

Esistono anche altri protocolli con strutture analoghe ma caratteristiche particolari.

A livello di Controllo, si trovano fieldbus HSE e PROFIBUS-DP insieme a controlNET regolano il livello di controllo nella gerarchia.
A livello di Gestione si hanno protocolli di diverso tipo, strettamente TCP/IP o Ethernet-base perché magari si scambiano informazioni tramiti file XML, EXCEL che non hanno bisogno di caratteristiche particolari.

Reti HART

HART – *Highway Addressable Remote Tranducer* è un protocollo di rete di controllo di processo aperto introdotto alla fine degli anni ’80. È un protocollo ibrido che utilizza la tecnica **FSK** che consente di sovrapporre un segnale di comunicazione digitale a un segnale di corrente analogico (4-20mA). È supportato dalla HART Communication Foundation (HCF) che consente di creare dispositivi compatibili con il protocollo HART.
Ma permette anche la compatibilità con sistemi già esistenti. Per molti anni, infatti, il settore dell’automazione di processo e controllo è stato dominato dal segnale analogico 4-20 mA per trasportare i segnali di variabili di processo (PV) e di controllo da e verso la sala di controllo. Il protocollo HART estende questa comunicazione analogica a una comunicazione digitali bidirezionali sul medesimo sistema, quindi sul medesimo cablaggio si trasporta sia un segnale analogico che digitale. Questo segnale digitale noto come segnale HART trasporta la configurazione del dispositivo, le informazioni diagnostiche, la calibrazione e qualsiasi altra misurazione del processo.
Quindi alcune delle caratteristiche protocollo HART sono:

- Comunicazione analogica e digitale simultanea
- Compatibile con strumentazioni analogiche convenzionali
- Supporta dispositivi di campo multivariabili
- Possibilità di avere due master
- Standard *aperto di fatto* (non sono standard aperti ma esiste una fondazione che consente di garantire la compatibilità tra diversi dispositivi)
- Retrocompatibile
- Supporta sia operazioni sia point to point che multidrop
- Tempi di risposta molto veloci

L’idea di HART era di supportare la corrente 4-20 mA già esistente con segnali di processo digitali. La capacità di trasmettere informazioni importanti sui medesimi canali ha portato alla sua accettazione.
Il personale di campo, già esistente, quindi non doveva imparare molto e un piccolo master portatile era tutto ciò che era necessario per la taratura in sito dei dispositivi.

All’aumentare dei protocolli, quindi della concorrenza, ha fatto si che siluppassero divrse versioni che ne hanno aumentato le capacità e potenzialità. Ciò ha portato a ulteriori sviluppi sia dal punto di vista degli strumenti che dei protocolli.

Per quanto riguarda le **componenti**, gli strumenti intelligenti hanno funzionalità di: azzeramento, regolazione della distanza e dello span, diagnostica per verificarne la salute e memoria per memorizzare informazioni di stato e configurazione.
Supportano le comunicazioni bidirezionali con il controllore, digitalizzano il segnale di processo e eventualmente correggono le variabili di processo.
Contengono software avanzati che eseguono misurazioni e le azioni di controllo.
Si hanno strumenti che consentono la risoluzione, precisione e affidabilità del processo.

Inizialmente è stato sviluppato pensando al fotovoltaico, successivamente le inforzioni sullo stato sono state incluse per prestare sempre più funzionalità. I dispositivi di campo smart ad oggi supportano la tecnologia HART.

Come avviene la comunicazione:

Il **master** solitamente è un host (es Sistema di controllo distribuiti, PLC, PC …), il master secondario può essere uno strumento di configurazione portatile utilizzato per configurazioni occasionali di diversi parametri di processo. Uno **slave** è un qualsiasi dispositivo nel campo (es. trasmettitore o un posizionatore)

- **Arbitrato (accesso al mezzo)**→ garantisce una corretta trasmissione dei messaggi tra master e slave.
  - Nella modalità **master-slave**: è il master che richiede e avvia la trasmissione dei messaggi, richiedendo il dispositivo slave. Il dispositivo slave a sua volta risponde solo alle richieste del master. In HART possono esserci 2 master sulla rete, un master primario e un master secondario, che consente di aggiungere dispositivi (es uno per analizzare il sistema).
  - La modalità **burst** (bus-slave), come la modalità master-slave, viene avviata da un comando del master. Le risposte vengono generate dallo slave richiesto senza frame richiesti dal master. I dati vengono aggiornati ad un ritmo più veloce poiché lo slave continua a trasmettere senza una richiesta del master. Un frame, da un master o da uno slave, viene trasmesso solo dopo aver verificato che nessuna trasmissione si sta verificando sulla rete in quel momento. Quindi è responsabilità del timer consentire l'accesso alla rete. Se si hanno i due master, hanno uguale priorità nell'acceso al bus. Nel caso in cui entrambi i master dovessero accedere ripetutamente al bus, lo farebbero in alternativa.

- **Modalità di comunicazione** →

- Nella modalità **master-slave** si ha un ciclo di comunicazione, dove ogni master chiede di ricevere dati da tutti gli slave.
- La configurazione della modalità **burst** fornisce al master alcune informazioni su base continua, fino a quando non viene detto di fermarsi. Fornisce una comunicazione più veloce rispetto alla modalità master-slave e viene utilizzata nella configurazione a slave singolo.

Reti HART →

- Nella rete **punto-punto**, il tradizionale segnale corrente 4-20 mA viene utilizzato per controllare il processo e non viene influenzato dal segnale HART. I parametri di configurazione vengono trasferiti digitalmente tramite il protocollo HART. Quindi, ogni dispositivo è collegato direttamente punto-punto al dispositivo master e tutto questo avviene tramite FSK; sulla medesima comunicazione ho la possibilità di aggiungere un secondo master (palmare) che mi consente di ricevere informazioni aggiuntive oltre alla trasmissione dei dati. l segnale digitale HART viene utilizzato per scopi di messa in servizio, manutenzione e diagnostica.
- Le reti di comunicazione **multidrop** vengono utilizzate quando i dispositivi sono ampiamenti distanziati. Sono necessari due fili per comunicare con il master. Se necessario in questa modalità è possibile incorporare barriere di sicurezza intrinseche (Safety) e alimentazione ausiliaria per un massimo di 15 dispositivi.
  Ho quindi un unico cavo che mi consente di collegare i diversi dispositivi; due master, un modem FSK che mi consente di fare lo shift legato alla frequenza e ho l'acquisizione di tutti i dispositivi.

Per quali applicazioni è nato HART:

Applicazioni nei sistemi di controllo → i dispositivi hardware HART possono aggiornare i loro dati due o tre volte in un secondo e questa velocità di aggiornamento nonostante non sia la più veloce è molto più veloce dei limiti di tempo associati alla maggior parte dei processi.
Un trasmettitore di pressione multivariabile HART può avere un sensore di temperatura in grado di monitorare la temperatura del processo eliminando così la necessità di utilizzare un sensore di temperatura separato.
Nello schema di trasmissione di corrente 4-20mA il controller fornisce dati a console operatore, workstation, ecc. in questo schema solo le informazioni sono sottoforma di un segnale analogico. Le architetture successive utilizzano I/O remote, console operatore, controller e workstation tutte collegate da un protocollo di comunicazione aperto.
Inoltre, i sistemi HART ottengono una disponibilità di informazioni sullo stato che possono essere inviate tramite i cavi di rete alla sala controllo, utili per una conoscenza preventiva di una possibile interruzione o per la manutezione.

Applicazioni nei sistemi SCADA → poiché HART supporta i valori di processo digitali, può essere applicato in SCADA. Vari parametri dei PV ottenuti dalla misurazioni HART possono essere utilizzati per la manutenzione preventiva negli SCADA.
Inoltre, le applicazioni SCADA richiedono l'aggiornamento dei dati sul campo in pochi minuti e poiché l'aggiornamento dei dati in HART richiede solo una frazione di secondo può essere applicato in modo sicuro nelle applicazioni SCADA.
Altre aree applicative sono la gestione dell'inventario, la lettura automatizzata dei contatori, il monitoraggio delle condutture situate in luoghi remoti.

Vantaggi: il protocollo HART ha una funzionalità di comunicazione unica e compatibile con le versioni precedenti; infatti, è l'unica struttura di comunicazione che supporta contemporaneamente comunicazione analogica e comunicazione digitale. Conservando il tradizionale segnale 4-20mA, estende la capacità del sistema per la comunicazione digitale bidirezionale con strumenti multivariabili su campo intelligenti. Qualsiasi applicazione di processo può essere indirizzata dai servizi offerti dal protocollo HART. Inoltre, alla base della sua accettabilità c'è la semplicità del protocollo e il costo molto basso dei dispositivi di campo conformi; in più lo standard aperto di fatto, più master che possono controllare lo stesso dispositivo intelligente e la comunicazione su lunghe distanze tramite un convertitore, è possibile aggiungere funzionalità e infine accedere a parametri e diagnostica del dispositivo.

Foundation Fieldbus

Nasce nella FF negli anni 90', basato essenzialmente su due protocolli: ISA/ANSI S50.02 e IEC 61158. L'idea alla base di FF è che il tradizionale segnale analogico viene sostituito con un collegamento di comunicazione digitale. Si hanno due diversi protocolli di rete, facilmente interfacciabili: H1 a velocità più bassa da installare a livello di impianto per sostituire la trasmissione a corrente 4-20 mA mantenendo il cablaggio dell'impianto esistente; a un livello più alto, H2 ad alta velocità che funge da dorsale tra i segmenti H1.
Già nel 99' l'idea era quella di sostituire H2 con un protocollo basato su Ethernet commerciale ad alta velocità COTS (si utilizzavo lo stesso hardware già esistente), e poi nel 2000 fu sostituito con HSE.

FF definisce fieldbus come "*un collegamento di comunicazione digitale bidirezionale multidrop tra dispositivi intelligenti e di controllo*". Le funzionalità associate a FF sono:

- È un protocollo per il controllo di processo e di automazione digitale bidirezionale, semi- duplex
- Se confrontato con il modello di riferimento OSI ha solo 3 livelli: physical layer, data link layer e application layer. Ha un layer 8 aggiuntivo, chiamato *user layer*, per aggiugere funzionalità.
- Ha un'architettura a due livelli composta dal livello inferiore H1 e dallo strato superiore H2.
- Supporta comunicazioni programmate e non pianificate
- Supporta l'interoperabilità, ovvero i dispositivi di diversi produttori possono essere collegati senza interruzioni

Architettura → Ha un'architettura a due livelli: H1 è il bus di livello inferiore che collega insieme i dispositivi di campo e H2 è il bus di livello superiore che interconnette i diversi segmenti di bus H1.
L'architettura supporta il controllo nei dispositivi di campo (posizionamento valvola) senza apparecchiature di controllo. Consente il consente il controllo a cascata dei dispositivi di collegamento e dei loop di controllo nei controller.
In realtà, sia H1 che H2 funzionano sullo stesso protocollo ed eseguono servizi identici, quello che cambia sono i livelli fisici. L'architettura a due livelli di FF è resa possibile dall'implementazione di un livello utente, livello 8, chiamato anche blocco funzione.

Vantaggi H1 → l'applicazione della tecnologia H1 offre una riduzione del numero di cavi e pannelli di smistamento, ridotto numero di I/O, numero ridotto di barriere di protezione e dimensioni ridotte della sala di controllo, poiché si hanno pochissime attrezzature. Inoltre, vi è la possibilità di configurare i dispositivi da remoto, maggiore accuratezza nelle misurazioni, maggiore disponibilità di informazioni per quanto riguarda la salute e lo stato delle apparecchiature, calibrazione e maggiore sicurezza degli impianti. (quello che si poteva fare in HART si può fare in H1)

Vantaggi HSE (aggiornamento di H2 con Ethernet) → in pratica HSE è la dorsale di controllo e consente quindi l'allocazione delle risorse per l'acquisizione di informazioni e le manutenzioni.
Si hanno una serie di vantaggi nell'avere HSE a livello superiore:

- **Interoperabilità dei sottosistemi**: possiamo supporre che la rete industriale abbia diversi sottosistemi. Ogni sottosistema è caratterizzato da un H1 (quindi da un dispositivo di controllo) e questi diversi sottosistemi possono essere collegati tra loro tramite un HSE. Utilizzando HSE è possibile accedere alle informazioni per le diverse operazioni dell'impianto senza la programmazione del cliente, per valutare l'integrità dei dati, il controllo dello stato di dispositivo, la ridondanza, ecc.
- **Blocchi funzione** → a livello più alto si hanno questi blocchi funzione, identici per entrambi i dispositivi H1 e HSE. Questo consente di eliminare la programmazione per la configurazione tramite un linguaggio di programmazione proprietario; invece, lo stesso linguaggio di programmazione viene utilizzato per tutte le operazioni dell'impianto. Sono responsabili degli arresti del circuito, trasferimenti senza strappi ecc..

Dorsale di controllo → L'idea di avere questa dorsale consente ai dispositivi di collegamento di portare dati da singoli segmenti (appartenenti ad H1) alla dorsale di controllo HSE. Pertanto, diverse reti H1 sono collegate da HSE e quindi di avere il controllo di tutto quello che succede.
HSE supporta la capacità di comunicazione peer-to-peer, quindi un dispositivo può comunicare con un altro senza dover passare attraverso il computer centrale, eliminando rischi di guasto di quest'ultimo.

Utilizzo di Ethernet: HSE utilizza cavi Ethernet standard, schede di interfaccia e hardware di rete standard, quindi costi minori. Si possono utilizzare comunicazioni hardware di qualsiasi tipo di produttore, anche non commerciale standard. I componenti Ethernet sono disponibili nella categoria COTS standard.

Processo di comunicazione → il processo di comunicazione prevede il trasporto di dati e messaggi da un dispositivo fieldbus ad un altro. I dispositivi devono avere un **tag** per l'identificazione del dispositivo corretto e un **indirizzo** di rete del dispositivo per fornire correttamente i dati su quello designato. Il funzionamento di diversi blocchi funzione esistenti nel livello applicazione e utente (livello 8) deve essere coordinato e collegato in modo corretto e i dati inseriti sul bus devono essere utilizzati da altri dispositivi, quando richiesto. Quindi è necessario avere una conoscenza delle tecnologie di comunicazione sottostanti.

Funzionamento: ogni dispositivo di campo FF è in grado di eseguire quelle funzionalità incapsulate in blocchi funzione che sono gli elementi base per la programmazione di applicazioni e per l'esecuzione degli algoritmi di controllo e automazione (come controllo PID, operazioni matematiche…). Un'altra caratteristica di FF è la capacità di diagnostica avanzata che definisce anche un formato standard facilmente integrabile nei sistemi di gestione degli asset.
Per garantire che i messaggi scambiati tra blocchi funzione di diversi dispositivi vengano scambiati in maniera corretta FF fa affidamento sugli **orari di pianificazione**. Questi possono essere generati online o offline e vengono utilizzati dal Link Active Scheduler (**LAS**) che gestisce tutti i trasferimenti di messaggi tra diversi dispositivi di campo su un bus ed è inoltre responsabile dell'avvio dell'esecuzione di blocchi funzione in ciascun dispositivo. In caso di guasto un altro dispositivo che esegue il LAS precedentemente assegnato assumerà automaticamente la responsabilità della pianificazione dei messaggi.
Il LAS è importante per il raggiungimento di un comportamento deterministico in tempo reale.
Il traffico di rete del bus di campo è periodico e una singola iterazione di una pianificazione è denominata macro-ciclo. Durante la porzione di comunicazione programmata del macro-ciclo, vengono trasmessi tutti i dati relativi alle strategie di controllo del processo. Una parte del macrociclo viene utilizzata per la pubblicazione periodica dei dati (comunicazioni cicliche) e un'altra parte viene utilizzata per attività di background acicliche (messaggi di supervisione e di gestione della rete). I dati periodici sono considerati ad alta priorità e i loro requisiti di temporizzazione devono essere rispettati durante l'esecuzione dell'applicazione di controllo. Le richieste asincrone hanno priorità inferiore e vengono trasmesse solo se non ritardano le comunicazioni periodiche.

Ridondanza → la ridondanza è inclusa nel sistema a diversi livelli per garantire la disponibilità delle risorse in periodi di guasti. Può essere aggiunta a livello di host, di dispositivo, di supporto e di rete. HSE ha una robustezza integrata per garantire tolleranze ai guasti e localizzazione dell'errore.
In pratica il FF garantisce la ridondanza grazie al decentramento delle operazioni.

PROFIBUS

PROFIBUS è uno standard di bus di campo aperto, sviluppato nell'89 inizialmente da Siemens per soddisfare le esigenze dell'automazione di processo e dell'automazione di fabbriche. E' particolarmente adatto per applicazioni veloci, critiche nel tempo e implica anche comunicazioni complesse. Aderisce al modello ISO/OSI per la comunicazione.
PROFIBUS supporta due tipi di dispositivi:
master - chiamato "s**tazione attiva**", e slave - chiamato "**stazione passiva**". Un dispositivo master ha il diritto di controllare il bus quando ha l'accesso al bus, può trasmettere messaggi senza alcuna richiesta remota. Trasmettitori, sensori e attuatori sono invece esempi di dispositivi slave. Un dispositivo slave riconosce qualsiasi messaggio ricevuto e alla ricezione di una richiesta del master può inviare messaggi a quel master.

Sono disponibili tre versioni:

- **PROFIBUS – DP** gestisce processi di comunicazione veloci come azionamenti, I/O remoti a livello di dispositivi di sistemi di automazione del processo, come nelle industrie chimiche, alimentari, automobilistiche ecc.. E viene utilizzata la versione DP in soluzioni in cui è importante rispondere in tempi certi (time-critical). In questa modalità vengono usati i multimaster, nel qual caso uno slave viene assegnato ad un solo master, quindi più master possono leggere gli input da un dispositivo specifico ma solo un master può scrivere output su quel dispositivo.

- **PROFIBUS – PA** è la versione per la gestione dei sistemi di automazione e controllo dei processi, utilizzata per per collegare solitamente i dispositivi di campo.
  I vantaggi che derivano dall'utilizzo di PA sono ad esempio sistemi di sicurezza guasti, autodiagnosi, trasferimento affidabile delle informazioni, raggiungibilità delle apparecchiature, misurazione ad alta risoluzione ed integrazione al controllo discreto ad alta velocità. Che si traduce in una riduzione dei costi di installazione, minori tempi di fermo macchina, maggiore affidabilità delle operazioni, più funzionalità nella sicurezza ecc.
  Il collegamento tra DP e PA in una stessa rete avviene attraverso un accoppiatore che mi consenta di passare da DP a PA. Differisce da DP poiché i dispositivi possono essere alimentati sul cavo bus, quindi può essere utilizzato anche in aree a rischio di esplosione, e i trasferimenti di dati avvengono tramite IEC 61158-2.

- **PROFIBUS – FMS** ha un formato di messaggistica *peer-to-peer*. Ciò consente ai master di comunicare tra loro, fino a 126 nodi (e tutti possono essere master).
  Oltre ai tre tipi precedenti, a volte viene utilizzata una "**modalità combinata**" che utilizza contemporaneamente FMS e DP nella stessa rete. FMS è il primo protocollo di comunicazione ed è progettato per operazioni a livello di cella dove normalmente comunicano PLC e PC., nel qual caso il master primario comunica con il master secondario FMS

DP può indirizzare compiti di comunicazione estremamente critici; PA è particolarmente orientato a soddisfare le esigenze della comunicazione di automazione dei processi.
In entrambi i casi, al livello 2 corrisponde al protocollo di accesso al bus che consente la comunicazione master-slave e il metodo del token per i multimaster.
Esiste anche un livello 7, o livello applicazione, funge da interfaccia tra i programmi applicativi e i diversi protocolli FMS, DP, o PA esistenti nel livello utente.

→ le tre versioni FMS, DP, PA utilizzano tutti un protocollo di accesso al bus standard implementato dal layer 2 di OSI che qui è definito Field Data Link (**FDL**) che garantisce che tutte e tre le versioni funzionino correttamente e determinino una comunicazione deterministica a liv. di campo.
Oltre a gestire i protocolli di trasmissione FDL gestisce sia la sicurezza dei dati che il rilevamento degli errori; gestisce la procedura di comunicazione tra master/slave e il metodo di passaggio token per il sistema multimaster.
Il protocollo è progettato in modo tale che le tre varianti funzionino perfettamente insieme offrendo operazioni ad alta velocità e alta deterministica a livello di campo; riduzione dei costi mediante la connessione a due fili per PA e una capacità estesa a livello di controllore per FMS.

Esistono diverse tecnologie di trasmissione vengono utilizzate per PROFIBUS:
- **seriale**; in cui la struttura del bus consente l'aggiunta e la cancellazione di una stazione senza influenzare altre stazioni; ci sono 32 dispositivi per segmento e i lati del segmento sono terminati con terminatore di bus attivo.
- **intrinsecamente sicuro** viene utilizzato in aree potenzialmente esplosive; quando si utilizza questa tecnologia è necessario rispettare i livelli massimi di corrente e tensione per evitare situazioni esplosive.
- MBP sta per la codifica **Manchester** con il bus alimentato sullo stesso cavo, anche in questo caso è un metodo utilizzato in particolari situazioni come industrie chimiche, in questo caso si trasmette sul fronte di salita/discesa di modo che il voltaggio resti costante.
Industrie con alti disturbi elettromagnetici o dispositivi a distanze considerevoli impiegano schemi di trasmissione a **fibra ottica**. Ovviamente i dispositivi nella rete devono essere in grado di integrarsi con questa tecnologia.

Ridondanza → la ridondanza garantisce una maggiore disponibilità del sistema. Essa può essere applicata in diversi modi:

- La **ridondanza master** assicura la disponibilità di un secondo master nel caso in cui il primario non funzioni.
- La **ridondanza dei supporti** garantisce che il cablaggio sia progettato con ridondanza (es. un doppio cavo).
- La **ridondanza degli accoppiatori di segmenti** si ha un doppio gateway che consente di passare DP-PA. Se un gateway non riesce l'altro assume la sua funzione.
- La **ridondanza ad anello** garantisce la ridondanza dei supporti sul lato PA (in aree pericolose).
- La **ridondanza slave** garantisce l'installazione di dispositivi di comunicazione con comunicazione ridondante. I dispositivi Slave contengono due interfacce, una primaria e una di backup, quando lo slave primario fallisce lo slave secondario riprende perfettamente o ne prede posto il master

ProfiNet → oltre alle versioni elencate sopra esiste una versione più aggiornata chiamata ProfiNet **c**he utilizza la tecnologia di comunicazione basata su Ethernet con opportuni adattamenti. Ethernet ha i seguenti vantaggi:

- È un sistema aperto
- Implementa gli standard IT
- È una tecnologia di comunicazione indipendente dal fornitore che favorisce l'interoperabilità
- Comunica dal livello 1 al livello 5 in modo coerente
- Integra i segmenti PROFIBUS senza bisogno di cambiamenti

ProfiNet è disponibile sia come software per le specifiche che per il SO indipendente. Ha un modello di ingegneria e un modello di comunicazione.
Il **modello di ingegneria** è un concetto indipendente dal fornitore che si inserisce in ProfiNet utilizzando uno strumento di configurazione intuitivo. Il modello supporta anche espansioni funzionali personalizzate dal produttore. Il **modello di comunicazione** definisce una specifica per il trasferimento dei dati tramite Ethernet utilizzando procedure IT convenzionali.

MODBUS

Modbus è un protocollo di comunicazione seriale inizialmente sviluppato da AEG-Modicon e inizialmente progettato per funzionare con i PLC.
Si tratta di un **protocollo di messaggistica** a livello di applicazione (livello 7) e fornisce una comunicazione **CLIENT-SERVER** tra dispositivi connessi su diversi tipi di rete. E un protocollo **MASTER-SLAVE** su livello Data Link.
Per Modbus non è richiesta alcuna interfaccia, è un protocollo molto leggero, ma è più lento di altri protocolli, per questo viene utilizzato più a sistema SCADA che PLC.
Il protocollo descrive il modo in cui un dispositivo accede ad un altro, come vengono ricevute le informazioni e in che modo vengono fornite le risposte. In caso di errore il protocollo fornisce un meccanismo per inviare il comando corrispondente all'utente.
La **comunicazione** può avvenire su una rete Modbus o su altre reti come Ethernet incorporando il protocollo Modbus come pacchetti di dati nel protocollo delle altre reti.
Non esiste un modo formale per certificare che un protocollo sia compatibile con Modbus, è responsabilità dei produttori confermare che i loro prodotti sono compatibili con altri dispositivi Modbus

ARCHITETTURA→ Consente di comunicare con altri Modbus diversi tramite dei Gateway opportuni.

l protocollo di **comunicazione seriale Modbus** si basa sul principio **master-slave** con il master che avvia una trasmissione e lo slave risponde fornendo i dati necessari al master, ad esempio dei dati dai sensori, prendendo misure adeguate o informando il master che l'azione richiesta non può essere eseguita. Ad esempio perché potrebbe esserci stato un errore. In questo caso la risposta è composta da l'indirizzo dello slave, l'azione richiesta e un indicazione del motivo del perché non può essere svolta.

Alcune caratteristiche di Modbus sono fisse altre sono selezionabili dagli utenti. Le caratteristiche fissate sono legate alla struttura del **pacchetto** (il formato del frame, la sequenza dei frame, la gestione degli errori di comunicazione e delle condizioni di eccezione e le funzioni eseguite). Le caratteristiche selezionabili sono il mezzo di trasmissione e le caratteristiche di trasmissione.
La parte principale del protocollo non è tanto la comunicazione ma quanto la struttura del **MESSAGGIO**:
Per quanto riguarda la struttura del messaggio in ModBus, è stato utilizzato per testare la capacità dei protocolli di resistere agli attacchi cyber e quindi non ha una protezione da **attacchi cyber** perché trasmette dati in chiaro senza crittografia e senza autenticazione.

- ADU che contiene tutto il pacchetto (indirizzo + check errori + PDU)
- PDU che contiene i dati veri e propri

1) Versione su **trasmissione seriale asincrona** come Fibra ottica.

2) Modbus TCP/IP nasce dall'idea di trasformare il protocollo Modbus strettamente seriale in un protocollo basato su una comunicazione digitale, tendando di rendere Modbus più aperto possibile. L'idea per fare questo è quella di sfruttare Ethernet standard, che riduceva i costi e consentiva una maggiore apertura del protocollo. Questo ha fatto si di essere implementato su TCP senza preoccuparsi della sicurezza.
Andando ad utilizzare Modbus TCP/IP verranno usati i livelli ISO/OSI 1,2,3,4 e 7. E l'architettura master- slave di Modbus viene modificata in **client-server** in Modbus su TCP/IP.
I diversi PLC, HMI e I/O possono essere collegati a Modbus TCP/IP tramite gateway e i diversi protocolli Modbus avviano la comunicazione usando TCP/IP.

3) Modbus Plus è un protocollo più recente che non è più un protocollo aperto, ma **proprietario**.
Modbus plus nasce per superare i problemi di **sicurezza**, di attacchi cyber di Modbus.
Ha come caratteristica principale quella di avere un passaggio di **TOKEN** invece di master-slave.
Usa una rete LAN in cui i dispositivi situati in posizioni geografiche diverse possono condividere informazioni per scopi di misurazione, controllo e monitoraggio.
Si rivolge alle reti Modbus collegandole tra loro.

CANBUS

CAN sta per *Controller Area Network* ed è stato sviluppato da Bosch nel 86' per occuparsi della crescente domanda di sistemi di controllo elettronico nell'industria automobilistica (nelle centraline delle auto). È un protocollo di comunicazione **seriale** standardizzato da ISO e utilizza un unico metodo di accesso al bus particolare chiamato **ARBITRAGGIO BITWISE NON DISTRUTTIVO.**
Si tratta di un protocollo di comunicazione molto semplice, affidabile e **prioritario**, utilizzato tra sensori, attuatori e dispositivi intelligenti. Viene applicata una tecnica **produttore-consumatore** per accedere al supporto fisico basato sul metodo di accesso **CSMA/CD**. È un metodo **deterministico**, per risolvere la contesa per l'accesso al bus, per questo sfrutta l'intera larghezza di banda del mezzo.
CANbus si riferisce a una rete di controllori indipendenti, supporta il controllo distribuito in tempo reale con un livello molto alto di sicurezza. CAN è diventato uno standard per la rete di veicoli ed è stato applicato in diversi campi per scopi di controllo.
Le unità collegate al bus, sensori e attuatori, possono inviare messaggi quando il bus è libero; cioè il sistema è di tipo **multimaster**.
Arbitraggio → Quando più di un'unità inizia ad inviare messaggi allo stesso tempo, la loro priorità viene risolta da un identificatore di messaggio (ID) che risiede nel frame dati che è stato assegnato durante la configurazione della rete; quindi una particolare unità vince la contesa del bus e invia il messaggio. Le altre unità che hanno perso possono inviare il loro messaggio quando il bus entra in uno stato di inattività.
Inoltre, il protocollo Can ha funzionalità di rilevamento, notifica, ripristino e confinamento degli errori.
Il numero di unità che possono essere collegate non ha limiti logici ma quando vengono aggiunte più unità al sistema la velocità diminuisce.

Frame CAN → esistono 5 tipi di frame per la comunicazione CAN:

1. **Frame dati**: frame che viene trasmesso dalle unità mittenti per inviare messaggi alle unità riceventi
2. **Frame remoto**: usato dalla unità ricevente che risponde ad una trasmissione di un messaggio con lo stesso ID della unità trasmittente
3. **Frame di errore**: quando un errore viene rilevato viene inviato questo frame per notificare alle altre unità che è stato riconosciuto un errore
4. **Frame di sovraccarico**: è usato dall'unità ricevente per notificare che non è preparata a ricevere altri frame
5. **Spazio interframe**: per distanziare i messaggi che vengono inviati

I primi due vengono impostati dall'utente mentre il resto è impostato nella parte hardware di CAN.

Bus di Campo: Ethernet Industriale

Nel mondo industriale, a partire dagli anni 70-80' sono stati creati una serie di standard, proprietari che poi sono stati resi aperti, facenti parte dello standard IEC 61158. Tuttavia quello che si è cercato di fare è stato quello di trovare un protocollo quanto più comune ai diversi produttore (cosa non successa), ma nel frattempo Ethernet è diventato uno standard per quanto riguarda le comunicazioni classiche. Si è cercato di unire queste due esigenze, anche perché utilizzare Ethernet ha un costo molto minore.
Si è pensato che Ethernet non potesse essere utilizzato fino a questo momento perché utilizza un metodo non deterministico di accesso al mezzo (CSMA-CD) che non soddisfa i requisiti dei sistemi di controllo in tempo reale. Per ovviare a questo i produttori hanno sviluppato diverse soluzioni che vanno sotto il nome di **Ethernet industriale** (adattamenti di Ethernet all'industria).

L'idea è quella di una segmentazione della rete; e ovviamente, mentre nei livelli alti, Ethernet è uno standard utilizzato senza problemi, ai livelli più bassi potrebbe comportare delle problematiche perché le informazioni sono critiche rispetto al tempo.
Quindi l'Ethernet industriale nasce per soddisfare i requisiti della LAN industriale della rete di automazione e dei bus di campo dove le applicazioni sono critiche e a tempo reale.

Si hanno tre possibili utilizzi di Ethernet in ambito industriale:

- utilizzare solo prodotti standard Ethernet, incluse schede di interfaccia di rete (NIC), switch e cavi (come nei cellulari);
- utilizzare hardware standard Ethernet ma con NIC specifiche;
- O usare cavi Ethernet e tutto il resto specifico.

Diversi tipi di Ethernet industriali non è detto che possano coesistere tra loro.
Tutta la parte hardware ovviamente deve essere certificata per lavorare in ambienti industriale.

Si devono avere **garanzie di servizio**. Poiché Ethernet utilizza CSMA/CD per gestire l'accesso al mezzo, non garantisce determinismo. Per essere utilizzato nel campo industriale le soluzioni devono quindi fornire in qualche modo alcune garanzie:

Nei sistemi di controllo, soprattutto a livelli più bassi, si ha bisogno di **garanzie riguardo ai tempi**, in quanto devono essere più vicini a un tempo reale.
Ethernet anche utilizzando collegamenti full duplex non può garantire un tempo di trasferimento limitato né la riduzione del jitter. Una delle possibilità è quello di utilizzare LAN virtuali.
Per il traffico che invece richiede un tempo di trasferimento inferiore o deterministico Ethernet deve essere modificato ulteriormente, in questo caso è possibile trovare due soluzioni:

- modificare il protocollo (non utilizzando CSMACD)
- utilizzare componenti di rete che implementano specifiche funzioni di gestione della comunicazione

In entrambe le soluzioni la modifica è basata sul principio di accesso multiplo a divisione di tempo **TDMA**.

Ethernet, in secondo luogo, non supporta funzioni di **ridondanza** del mezzo fisico; nel momento in cui una macchina si spegne, di solito il protocollo utilizza il cosiddetto Spanning Tree che identifica il percorso che esiste tra due macchine. Tuttavia, il tempo necessario per la riconfigurazione della rete con questo protocollo è molto lento. Di conseguenza è stato sviluppato il *Rapid Spanning Tree* più veloce. tuttavia, in caso di errore nel percorso di comunicazione può essere ancora troppo lento per le reti di sistemi di controllo.
Di conseguenza, i fornitori hanno sviluppato soluzioni proprietarie e cioè anelli virtuali basati su specifici dispositivi, oppure il protocollo MRP Media Redundancy Protocol.

Lo standard IEC61784-3 specifica protocolli dedicati alla **sicurezza**. Attualmente solo due soluzioni industriali Ethernet hanno profili nello standard della safety e sono **Ethernet/IP** (CIP Safety) e **ProfiNet I/O** (ProfiSafe). Altre soluzioni Ethernet industriali hanno un profilo di sicurezza ma non standardizzato come **Safety over EtherCAT**.

Quattro categorie per classificare le soluzioni Ethernet Industriale in base alla tecnologia utilizzata:

1. **Full Ethernet**: queste reti utilizzano lo standard Ethernet IEE 802.3 in tutte le sue componenti e, per evitare incertezza dovuta alle collisioni i collegamenti vengono usati in full duplex (funzionano in entrambe le direzioni). MA non si ha garanzia sul funzionamento. Possono essere basate sulla prioritizzazione standard dei dati su Ethernet e sulla creazione di VLAN. Il vantaggio è che posso usare dispositivi di rete commerciali COTS che possono coesistere con altre soluzioni Ethernet industriali o con stazioni Ethernet standard; lo svantaggio è che non ho nessuna garanzia di servizi deterministici. In questa soluzione rientrano Modbus TCP/IP, Ethernet/IP, ProfiNet e FF HSE.

2. **Ethernet compatibile**: questa soluzione è compatibile con Ethernet ma utilizza dispositivi specifici per garantire prestazioni durature e in tempo reale. Il vantaggio è che può coesistere con le stazioni Ethernet standard e può fornire garanzie deterministiche (perché modifico il protocollo usando hardware specifico); lo svantaggio è che utilizzando dispositivi di rete specifici aumentano i costi. In questa soluzione rientra **ProfiNet I/O real-time**.

3. **Implementazioni su dispositivi Ethernet comuni**: caso opposto al precedente, queste reti possono usare hardware standard Ethernet. Usano i livelli definiti in IEEE 802.3 ma gli strati superiori vengono modificati per gestire il traffico di rete in modo da poter fornire servizi garantiti. Ad esempio **Ethernet PowerLink**.
   In questo caso, si garartisce il determinismo, si utilizzano dispositivi commerciali COTS (economici). Lo svantaggio si ha bisogno di livelli di gestione delle comunicazioni fatti per adattare stazioni Ethernet industriali o Ethernet standard.

4. **Nuovi fieldbus che usano collegamenti Ethernet come accesso al mezzo**: richiedono l'uso di dispositivi specifici ovvero i fieldbus di ultima generazione. Si ha il vantaggio di avere garanzie specifiche, determinismo, prestazioni in tempo reale ma lo svantaggio è che utilizza dispositivi di rete specifici e stazioni specifiche che non possono coesistere con altre stazioni Ethernet industriale o Ethernet standard. In questa soluzione rientrano **EtherCAT** e **SERCOS**.

I profili Ethernet Industriali sono stati inclusi nello standard IEC 61158 e IEC 61784 (specifiche del bus di campo e reti di comunicazione industriale). Quello che è successo è che protocolli standard già esistenti si sono adattati a introdurre profili basati su Ethernet (come FF).

Ethernet/IP: Ethernet/IP utilizza un protocollo CIP (Common Industrial Protocol) di messaggistica. Lo stack Ethernet/IP utilizza Ethernet TCP/IP come mezzo per trasportare la messaggistica CIP. Mentre CIP invece, è il protocollo di livello superiore e si basa sull'approccio orientato agli oggetti forzando i livelli più bassi ad operare in maniera deterministica. L'uso della messaggistica CIP fornisce una serie di funzionalità che includono:

- CIPSync, che consente la sincronizzazione degli orologi
- CIPSafety, che è uno strato superiore per la sicurezza delle applicazioni CIP
- Servizi per scambi ciclici di variabili, detti trasferimenti impliciti, basati sul traffico multicast in UDP/IP.
- Servizi per lo scambio di messaggi basato su eventi, chiamati trasferimenti espliciti, basato sul traffico TCP/IP.

I messaggi basati su eventi TCP/IP vengono utilizzati sia per la trasmissione di informazioni di sistema (diagnostica) sia per informazioni di applicazioni che non richiedono tempi di risposta rapidi, questo perché TCP/IP è più lento di UDP poiché basato su protocollo di handshaking (con gli acknowledgement)

FF HSE - **Foundation Fieldbus High-Speed Ethernet** → è un protocollo di livello applicativo (7) che utilizza UDP/IP piuttosto che TCP/IP per le comunicazioni in tempo reale e TCP/IP per altri scambi. FF HSE è un adattamento del FF per Ethernet. Consente la ridondanza offerta dalle topologie ad anello logico ed implementa le comunicazioni pianificate per garantire che due componenti non pubblichino dati nello stesso momento. Questo meccanismo è appunto implementato nel livello applicativo per consentire l'utilizzo di protocolli Ethernet e TCP/IP standard.

SERCOS → SERCOS III è supportato da associazioni commerciali chiamate SERCOS. Traduce i livelli applicativi del bus di campo SERCOS su Ethernet e implementa meccanismi simili a EtherCAT. Si concentra su applicazioni hard real time nel controllo di movimento. Per garantire il determinismo questa soluzione utilizza solo cavi Ethernet e si basa su una topologia a linea in cui solo un frame circola tra i dispositivi. C'è un master che invia frame con tutti i dati richiesti per essere letti dagli slave. I dispositivi ricevono questo frame uno dopo l'altro, leggono i dati di cui hanno bisogno e scrivono i dati se necessario.

EtherCAT

EtherCAT (Ethernet per la tecnologia di controllo dell'automazione) è un sistema bus di campo basato su **Ethernet ad alte prestazioni**. Il suo principale obiettivo è quello di applicare Ethernet alle applicazioni di automazione che richiedono tempi di cortocircuiti jitter molto bassi.
E' una soluzione popolare per connettere applicazioni di controllo ai dispositivi di campo in ambienti industriali, comprese le applicazioni di controllo del movimento. Inoltre le apparecchiature e i dispositivi sono facilmente reperibili sul mercato.
EtherCAT è uno standard **aperto** e le sue specifiche sono state recentemente integrate negli standard internazionali di bus di campo. Si basa su un approccio **master- slave** in cui un solo master è ammesso nella rete e fa affidamento su una **tecnologia ad anello** fisico. Può interagire con entrambe le reti basate su TCP/IP e altre soluzioni basate su Ethernet come Ethernet/IP o ProfiNet.

EtherCAT supporta due diversi tipi di layer fisici: **Ethernet** ed **EBUS**

- **Ethernet** viene utilizzato per una connessione a una rete Ethernet esterna; viene in genere utilizzato per la connessione tra il segmento di rete master e slave. In effetti una rete EtherCAT può essere vista come un singolo dispositivo Ethernet che riceve e invia frame Ethernet, tuttavia questo dispositivo non è costituito da un singolo controller Ethernet ma include un numero ampio di slave EtherCAT.
- **EBUS** può essere utilizzato come bus di backplane (presente nei PLC) e in particolare EBUS è uno strato fisico progettato per ridurre i ritardi di passaggio all'interno dei nodi. Utilizza la codifica Manchester e incapsula i fotogrammi tra identificatori di inizio frame (SOF) e di fine frame (EOF). Il protocollo EBUS incapsula semplicemente i frame Ethernet; quindi EBUS può trasportare qualsiasi frame Ethernet.

Per quanto riguarda la **TOPOLOGIA** del sistema normalmente in Ethernet si ha una topologia a stella che porta a maggiori sforzi di cablaggio e costi infrastrutturali, in EtherCAT la disposizione dei nodi slave rappresenta un **anello aperto**. In una delle estremità aperte, il dispositivo master, che controlla completamente il traffico attraverso la rete avviando la trasmissione. invia frame, direttamente o tramite switch Ethernet, e li riceve dall'altra parte dopo che sono stati elaborati. Tutti i frame vengono inoltrati da ogni slave al successivo. Ogni slave, quando riceve un frame, lo elabora e poi lo inoltra allo slave successivo nell'anello fisico. I frame non sono gestiti secondo una schema store-and-forward ma ogni frame viene elaborato al volo e ritrasmesso nel livello data-link (**modify on the fly**). Poi l'ultimo slave nella rete restituisce il frame al master.
Questa struttura ha la funzionalità **full-duplex** di Ethernet, che utilizza due coppie di fili per eseguire contemporaneamente comunicazioni in entrambe le direzioni, entrambe le direzioni di comunicazione sono gestite indipendentemente per ottenere le massime prestazioni e i frame Ethernet devono essere elaborati al volo. La topologia risultante assomiglia visivamente a una linea ma è di fatto un anello perché l'ultimo slave manda dati al master.
Inoltre, viene fornita **un'unità di gestione della memoria fieldbus** (**FMMU**) in ogni dispositivo slave che legge/scrive porzioni di dati incluse nel frame mentre viene inoltrato al dispositivo successivo.

Il protocollo di COMUNICAZIONE EtherCAT punta a massimizzare l'utilizzo della larghezza di banda Ethernet. Il meccanismo di accesso al mezzo si basa sul principio **master/slave**, in cui il nodo master invia frame Ethernet ai nodi slave sull'anello fisico e ciascuno degli slave estrae i dati da e in questi frame. I frame inviati sulla rete sono frame **Ethernet standard**, il cui campo dati incapsula anche il **frame EtherCAT**, che a sua volta è costituito da un'intestazione e da uno più datagrammi EtherCAT o unità di dati del protocollo (PDU). In modo da ottenere un uso efficiente del grande campo di dati Ethernet disponibili.

Dal punto di vista del master, l'intero segmento EtherCAT è visto come un singolo dispositivo Ethernet, che invia a riceve frame Ethernet standard con il campo **EtherType** per distinguerlo da altri frame Ethernet. In questo modo EtherCAT può coesistere con altri protocolli Ethernet. L'unico vincolo è che l'ultimo dispositivo slave EtherCAT nel segmento invia il frame completamente processato e lo stesso avviene per ogni dispositivo.

Sono disponibili diverse modalità di **INDIRIZZAMENTO** per l'accesso agli slave. L'intestazione della PDU EtherCAT viene utilizzato sia per **l'indirizzamento del nodo fisico** che per **l'indirizzamento logico**.
Indirizzamento fisico: il campo dell'indirizzo all'interno di ciascuna PDU EtherCAT è suddiviso in un:

- **indirizzo di dispositivo slave**, indirizza in modo univoco un singolo dispositivo slave. Esistono due diversi meccanismi di indirizzamento:
  - **della posizione**: utilizzato per indirizzare ciascun dispositivo slave tramite la sua posizione fisica all'interno del segmento. Ogni dispositivo slave incrementa il capo indirizzo mentre il datagramma transita attraverso il dispositivo slave
  - **del nodo**: gli slave vengono indirizzati tramite indirizzi di nodo configurati assegnati dal master durante la fase di avvio del collegamento dati. Ciò garantisce che, anche se la topologia del segmento viene modificata o i dispositivi vengono aggiunti/rimossi, i dispositivi slave possono essere indirizzati tramite gli stessi indirizzi configurati.
  - **modalità per Broadcast**: viene indirizzato ogni slave EtherCAT, l'indirizzamento broadcast viene utilizzato per l'inizializzazione di tutti gli slave e per controllare lo stato di tutti gli slave.
- **indirizzo fisico** all'interno del dispositivo slave.

Indirizzamento logico: diversi dispositivi EtherCAT possono essere indirizzati separatamente tramite un singolo frame Ethernet, che porta ad un miglioramento significativo della larghezza di banda del sistema. Tuttavia, per terminali di input di piccole dimensioni, il sovraccarico di un singolo comando EtherCAT potrebbe essere eccessivo. La FMMU riduce questo problema inoltre converte un indirizzo logico in uno fisico tramite una tabella interna.

Tutti i protocolli basati su Ethernet hanno un **problema basato sulla SINCRONIZZAZIONE** dell'accesso alla memoria slave. In questo caso EtherCAT fornisce un meccanismo per sincronizzare l'accesso alla memoria slave chiamato **SyncManager,** che consente di avere scambi di dati coerenti e sicuri tra master EtherCat e l'applicazione locale, generando interrupt per informare entrambi i lati delle modifiche. È configurato dal master EtherCAT e utilizza un buffer situato nell'area di memoria per lo scambio di dati e controlla l'accesso a questo buffer. Tutti gli accessi al buffer iniziano dall'indirizzo iniziale; dopo l'accesso all'indirizzo iniziale è possibile accedere all'intero buffer. Un accesso al buffer termina accedendo all'indirizzo finale.
Due modalità di comunicazione sono supportate da SyncManager:

1. **Modalità Bufferizzata**: ciascuna entità può eseguire l'accesso in qualsiasi momento, fornendo sempre i dati più recenti. Nel caso in cui il buffer sia scritto più velocemente di quanto viene letto, i vecchi dati vengono eliminati. Questa modalità è in genere utilizzata per dati di processo ciclici. Il meccanismo utilizza 3 buffer identici: 1 per la scrittura, 1 per la lettura, e 1 di riserva aiuta come archivio intermedio.
2. **Modalità Mailbox**: implementa un meccanismo di handshake per lo scambio dati, in modo che nessun dato vada perso. Un'entità riempie i dati e non può accedere all'area finché l'altra entità non legge i dati. Viene in genere utilizzata per i protocolli a livello applicazione.

La sincronizzazione si porta come concetto collegato quella del **CLOCK:** per mantenere la sincronizzazione tra i vari dispositivi si deve avere anche la sincronizzazione distribuita dell'orologio che consente a tutti i dispositivi (master e slave) di condividere lo stesso tempo di sistema con precisone.
In genere il riferimento clock è il primo slave con capacità di clock distribuito dopo il master all'interno del segmento e viene utilizzato come orologio di riferimento per sincronizzare gli orologi slave di altri dispositivi e del master stesso. Il processo di sincronizzazione dell'orologio è composto da 3 passaggi:

1. Il master invia un frame di sincronizzazione a intervalli e ogni slave lo memorizza; il master legge tutti i timestamp e calcola i ritardi di propagazione degli slave.
2. Il master misura il tempo di ritardo tra l'orologio di riferimento e gli orologi slave e viene compensato l'offset di entrambi i clock.
3. la deriva naturale di ogni orologio locale deve essere compensata da un ciclo di controllo del tempo. Questo meccanismo regola nuovamente l'orologio locale misurando regolarmente le differenze.

A livello applicazione si ha una sorta di macchina a strati Ethernet responsabile del **coordinamento** delle applicazioni master e slave all'avvio e durante il funzionamento. Le modifiche di stato sono in genere avviate dalle richieste del master. La macchina a strati viene controllata e monitorata utilizzando alcuni registri presenti sullo slave. Il master richiede cambiamenti di stato scrivendo sul registro di controllo. Lo slave indica la scrittura dello stato nel registro di stato e inserisce possibili codici di errore nel registro del codice di stato.

Ethernet PowerLink – EPL

EPL è una rete **Ethernet Real Time RTE**. Il protocollo EPL è stato sviluppato per fornire cicli di comunicazione molto veloci con un jitter basso e allo stesso tempo mantenendo la compatibilità con Ethernet (classico).
In cima allo stack di comunicazione, a livello applicazione è stato introdotto il protocollo CANopen, garantendo in tal modo la compatibilità con un ampio numero di sistemi di comunicazione già implementati. In questo contesto EPL viene spesso chiamato *CANopen over Ethernet*.
Per quanto riguarda l' ARCHITETTURA a livello Data Link si utilizza Ethernet in particolare CSMA/CD mentre a livello fisico si utilizza una trasmissione di tipo full-duplex.

EPL definisce due tipi di **STAZIONI**, ovvero il

- nodo gestione **MN** (management node – master) → rappresenta di solito il controllore di un sistema di automazione
- nodi controllati **CN** (controlled node – slave)→ sono in genere dispositivi di campo come ad esempio sensori e attuatori.

Ogni rete contiene esattamente 1 MN e CN collegati in diverse topologie.
EPL può essere impiegato in diversi campi e in particolare per **applicazioni con vincoli temporali molto stretti**, come sistemi di controllo si movimenti coordinati. La DLL di EPL si basa su una tecnica di accesso a **multiplo a divisione di tempo TDMA** gestita dal MN che consente alle stazioni di accedere in modo ordinato al supporto fisico e quindi evitare collisioni anche se vengono utilizzate configurazioni ethernet non commutate. In pratica l'operazione di rete si basa su un ciclo periodico (**CICLO EPL**) con durata costante. EPL. Il ciclo EPL è suddiviso in 4 sezioni:

1. **Start Period** viene avviata dal MN che trasmette il frame di inizio per sincronizzare tutti i CN.
2. **Periodo Isocrono**, in cui i MN e i CN si scambiano dati ciclici. In cui il MN fa una richiesta di poll a un CN che dopo un periodo elaborazione invia la risposta contenente i dati richiesti. Tale ultimo frame non viene inviato esclusivamente al MN ma sulla rete in modo che tutti i CN lo ricevano. Dopo aver ricevuto il frame, l'MN attende un tempo di silenzio, quindi si sposta sul prossimo CN.
   Lo standard supporta **due classi di comunicazione** che specificano il modo in cui vengono indirizzati i CN: **continua**: viene interrogato un CN ad ogni ciclo, **multiplex** viene eseguito il polling di un CN ogni n cicli.
3. Alla fine del periodo isocrono, il MN trasmette il frame informando tutti i CN che il **Periodo Asincrono** viene avviato. In questo periodo, un solo messaggio asincrono può essere inviato dal MN o da uno dei CN. Durante il periodo isocrono, il MN può raccogliere richieste di trasmissione asincrone e quindi, secondo uno schema di priorità, seleziona il nodo a cui è concesso di trasmettere. Solitamente possono essere messaggi di allarmi o messaggi Ethernet utilizzati per una comunicazione generica.
4. Infine, vi è un **Periodo di Inattività** inserito alla fine del periodo asincrono per garantire che non vi siano superamenti di messaggi nei confini del ciclo EPL.

La corretta esecuzione del ciclo EPL richiede che tutte le stazioni connesse alla rete siano conformi al protocollo

Le funzioni di **RIDONDANZA** di EPL sono esplicitamente definite dai servizi di alta disponibilità PowerLink che rappresentano un'estensione delle specifiche di base e che mantengono la piena compatibilità con esso. Questi servizi hanno l'obiettivo di fornire funzionalità di rete complete anche in caso di guasti singoli imminenti su qualsiasi componente PowerLink (MN, CN e infrastruttura fisica). L'elevata disponibilità di PowerLink si basa su due aspetti specifici, ovvero la ridondanza del mezzo e la ridondanza MN.

- **Ridondanza del mezzo**: fornita introducendo un secondo cablaggio fisico nella rete. Tutti i dispositivi sono collegati a entrambi i cavi e tutte le informazioni possono essere trasmesse su entrambi i collegamenti da ciascun nodo (MN e CN) implementando il set di servizi ad alta disponibilità.
- **Ridondanza MN**: Nella rete sono presenti nuovi nodi **R-NM**: Il nodo gestione attivo **AMN** che ospita ed esegue le funzionalità del MN. Il nodo di gestione stand-by **SMN** in stato di attesa relativo alle funzionalità MN, che si comporta come un CN, con la differenza che monitora costantemente la rete e In caso di guasto dell'AMN, uno degli RMN acquisirà immediatamente la funzionalità dell'AMN.

Infine, un ulteriore modo di fornire un servizio di ridondanza consiste **nell'utilizzare una struttura ad anello** per l'architettura di cablaggio. Un anello chiuso offre la possibilità di avere due percorsi di trasmissione indipendenti da ogni nodo ad ogni altro nodo nella rete.

Bus di Campo Wireless

Nasce dalla tendenza del mondo di utilizzare le comunicazioni wireless. Il più grande vantaggio si basa sul fatto che è una comunicazione mobile, senza cavi ne fili, quindi potrebbe essere una valida soluzione da aggiungere a sistemi industriali già esistenti.
In generale, offrono una straordinaria opportunità per quanto riguarda le comunicazioni a corto raggio e sono semplici da aggiungere nel mondo industriale; ma ci sono anche degli svantaggi in termini ad esempio di affidabilità, sicurezza o disponibilità delle informazioni, non possiamo avere la medesima garanzia di affidabilità, sicurezza, scalabilità di connessioni cablate.

Nella comunicazione wireless, non vi è alcun collegamento fisico tra trasmettitore e il ricevitore. Si dice che i media non sono "guidati" quindi ma vengono trasmesse onde elettromagnetiche tra questi due. Di solito si utilizza un'antenna per trasmettere e ricevere informazioni, questa irradia un campo magnetico nell'aria. Solitamente sono sistemi **multicast**, quindi ogni ricevitore può raccogliere più onde elettromagnetiche trasmesse.

Nella comunicazione wireless vengono utilizzati due tipi di trasmissione:
Direzionale: l'antenna trasmittente emette un raggio elettromagnetico solo in una porzione dell'area, quindi è focalizzato, pertanto in questo caso entrambe le antenne trasmittenti e riceventi devono essere accuratamente allineate in modo che il ricevitore possa ottenere la massima potenza trasmessa.
Omnidirezionale l'antenna trasmittente diffonde in tutte le direzioni e quindi ogni antenna ricevente può riceverlo.

I segnali non guidati possono raggiungere il ricevitore tramite diversi metodi:
propagazione del terreno: i segnali sono di bassa frequenza e viaggiano in tutte le direzioni seguendo la parte più bassa dell'atmosfera, quindi seguendo la curvatura della terra. Questo fa si che la distanza che possono percorrere dipende dalla potenza emanata dall'antenna trasmittente. **propagazione nel cielo**: consente una corsa del percorso relativamente più lungo con meno potenza dell'antenna trasmittente. In questo caso le onde radio relativamente più elevate vengono irradiate nella ionosfera dove vengono respinte nuovamente nell'antenna ricevente.
propagazione della linea di mira: le antenne sono direzionali e i segnali ad altissima frequenza vengono trasmessi in linea retta. Le antenne devono essere molto alte o abbastanza vicine l'una all'altra in modo tale che la propagazione non sia influenzata dalla curvatura della terra.

Ovviamente all'aumentare della frequenza aumenta la capacità di trasmissione dati.
Quando si tramettono i dati c'è una prima fase di inizializzazione in cui l'antenna del trasmettitore e quella del ricevitore si sintonizzano. I dati devono essere codificati e c'è bisogno di una serie di simboli di partenza che indicano qual è il momento di inizio e di sincronizzazione; una volta in possesso di queste informazioni vengono trasmessi i dati e ricevuti in modo tale da poter essere decodificati. Inoltre, per ridurre la latenza non viene usato un protocollo di handshaking ma una struttura a pipeline (trasmissioni continua).

La rete **LAN wireless** è regolata da una serie di standard. Oltre allo standard IEE 802.11 per wifi esistono altri standard che soddisfano esigenze di comunicazione wireless.

WiFi → tecnologia locale che aggiunge mobilità alle LAN private cablate e supporta un raggio massimo di poche centinaia di metri; utilizza un protocollo MAC denominato CSMA/CA. Le configurazioni sono half-duplex, le stazioni di trasmissione ricezione scambiano informazioni sullo stesso canale radio. Pertanto, una stazione non può trasmettere e ricevere allo stesso tempo, ma prevede un meccanismo di prevenzione delle collisioni è chiamato controllo distribuito DCF.

WiMax → viene utilizzato per accedere alle reti di sensori wireless in modo migliore rispetto ad altri in termini di copertura e capacità delle celle. WiMax gestisce gateway tra reti di sensori wireless WSN e internet. VoIP e video che sono il traffico time-sensitive hanno priorità in WiMax.
WiMax opera in condizioni dove tra l'antenna e il ricevitore ci possono essere ostacoli (es. tra edifici). Utilizza un meccanismo di richiesta/concessione che presuppone canali separati per le trasmissioni in entrata e in uscita. In WiMax la trasmissione dei messaggi è di tipo full duplex.
Le architetture del traffico WiMax possono essere sia *point-to-point* che *point-to-multipoint*. Infine, WiMax utilizza sia le

frequenze con licenze che quelle senza licenza. La sicurezza è gestita tramite un meccanismo di crittografia (al contrario del WiFi).

Bluetooth → il bluetooth è un protocollo di comunicazione wireless aperto e destinato alle reti personali PAN, utilizzato per applicazioni office a bassa potenza e a corto raggio. Utilizza uno schema *channel-hopping* che supporta bassa latenza e throughput elevato che aumenta l'affidabilità del sistema. Non può essere applicato in ambienti industriali a causa della sua incapacità di fornire un ritardo di comunicazione end-to-end e una copertura a basse distanze.
È una comunicazione molto limitata. Funziona bene in comunicazioni molto ridotte come tra PC e tastiere ecc.

ZigBee → nasce come protocollo per reti PAN, progettato per applicazioni wireless a potenza ultra-bassa in aree per il monitoraggio e il controllo (Wireless Sensor Network). È un protocollo di trasmissione a bassa potenza, bassa velocità di trasmissione dati e a basso.
ZigBee non può però fornire affidabilità contro interferenze e ostacoli per questo motivo non può essere applicato nell'ambito industriale sebbene abbia una comunicazione sicura, basata su un algoritmo di crittografia. Il lato positivo è che utilizza la topologia *mesh* (sistemi molto veloci) e usa la tecnica DSSS spettro diretto a sequenza diretta.

WHART (Wireless Highway Addressable Remote Transmission): è una rete di protocollo *mesh* gestita tramite IEEE 802.15.4 ed è un'estensione del protocollo di comunicazione HART retrocompatibile con i dispositivi e le applicazioni HART esistenti. È considerato il primo protocollo standard aperto per WSN nell'area dell'automazione e del controllo dei processi.
Utilizza la tecnologia TDMA (time-division-multiple-access) ed è interoperabile e supporta il *channel hopping* tra due canali adiacenti. Utilizza una banda di frequenza ISM non crittografata.
I servizi di sicurezza industriale sono forniti dal livello MAC e dal livello di rete tramite un algoritmo AES. L'affidabilità dei sistemi WHART è ottenuta utilizzando la frequenza, la diversità di percorsi e i metodi di consegna dei messaggi. Il consumo energetico è ottimizzato gestendo correttamente il programma di comunicazione.

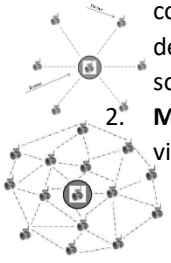
ISA 100.11a basato sull' IEEE 802.15.4 e fornisce comunicazioni wireless affidabili e sicure per il monitoraggio non critico e il controllo dei sistemi di automazione industriale. Alcune delle sue caratteristiche sono a basso costo, basso consumo energetico, robustezza alle interferenze RadioF, bassa complessità, scalabilità e interoperabilità.
A differenza di WHART, non è retrocompatibile. Funziona in uno schema *channel hopping* sincronizzato nel tempo per evitare interferenze RF e anche per ridurre il consumo energetico.
Può funzionare sia in topologia a stella che a maglie. Il primo viene utilizzato per una risposta rapida, necessaria per alcune applicazioni industriali critiche nel tempo. La topologia mesh viene utilizzata per una maggiore robustezza del sistema, un maggiore tolleranza alle interferenze RF e una maggiore affidabilità. I messaggi infine sono protetti tramite crittografia AES. Il suo basso consumo è dovuto a TDMA che consente di non consumare energia nel momento in cui i router non stanno trasmettendo.

Affinché avvenga una comunicazione corretta è necessario accedere al mezzo di trasmissione, cioè all'aria. Se i trasmettitori cercano di **accedere al mezzo** nello stesso tempo nessuna ricezione sarebbe possibile ai corrispondenti ricevitori. Varie tecniche sono utilizzate per l'accesso al mezzo e ognuna ha le sue caratteristiche:

- Il più semplice tra loro è che i dati siano modulati da una **frequenza fissata**. Sebbene richieda meno larghezza di banda è più suscettibile alle interferenze.
- In **TDMA (time division)** tutte le stazioni che partecipano alla trasmissione dei messaggi ricevono diversi intervalli predefiniti per evitare collisioni.
- In **CSMA** la collisione viene evitata introducendo un tempo di ritardo casuale dopo il riconoscimento del canale libero. Quando la trasmissione è terminata il canale risulta libero e tutti gli altri aspetteranno che il canale sia libero per evitare collisioni.
- Nello **spettro diffuso di hopping di frequenza**, la frequenza del trasmettitore salta da una frequenza all'altra secondo un programma predefinito noto al ricevitore, che consentono di evitare interferenze.

Tre **topologie** sono normalmente utilizzate per il collegamento in rete di sensori wireless nell'automazione industriale

1. **Stella**: nella topologia a stella ho un nodo centrale HUB e una serie di dispositivi a corolla della stella. La comunicazione tra i diversi dispositivi avviene tramite l'HUB e quindi dipende fortemente dalla capacità dell'elemento centro stella del sistema. Viene applicata quando il consumo di energia è limitato e le fonti di dati sono confinate in un intervallo geografico limitato è però la modalità più veloce per la trasmissione dei dati.
2. **Mesh**: comunicazione in cui ogni elemento può comunicare con un certo numero di elementi che sono nel suo vicinato. È particolarmente adatta per una rete in cui i sensori sono distribuiti su un'ampia area geografica con



ridondanza elevata. Vengono determinati automaticamente i percorsi migliori per i messaggi da portare al gateway e il sistema bypassa automaticamente un sensore guasto. Deve però essere disponibile energia sufficiente per trasmettere i messaggi.

3. **Stella-Mesh**: la topologia stella e mesh sono combinate insieme. Ho quindi una struttura gerarchica, quindi la comunicazione dei dispositivi avviene tramite i router e poi i gateway. Questa topologia combinata presenta l'alta velocità della topologia a stella e la capacità di riparazione automatica delle reti mesh.

Wired (cavo) vs Wireless:

nel caso di una comunicazione Wireless si punta ad eliminare le problematiche inerenti alle reti cablate, che hanno bisogno di cavi e opere di muratura.
costi di installazione e manutenzione sono inferiori nelle reti wireless rispetto a quelli cablati, in quanto quest'ultime hanno più hardware.
Per quanto riguarda invece le reti in ambienti ostili, le reti cablate hanno bisogno di particolari attenzioni, richiede tempo, richiede più risorse umane e può essere soggetto a disconnessioni. Cosa che invece risolvono in parte le reti wireless, che riducono gli angoli ciechi nella visibilità del processo, portando a rese più elevate a un costo inferiore, ma nello stesso tempo hanno bisogno di più personale per il controllo.
I problemi relativi alle parti wireless sono quelle legate alle interferenze elettromagnetiche, quindi risultano impossibili da utilizzare in campi soggetti alle onde elettromagnetiche; inoltre ha problemi di interferenza di canali vicini (cross-talk), o problemi dovuti a comunicazioni che potrebbero essere non così affidabili come in connessioni via cavo.
Nel caso della rete cablata si hanno problemi di sovraccarico, la rete wireless non ne è influenzata ma non sono esenti da problematiche di interruzioni o poca copertura di segnale.

Wireless Sensor Network – WSN

La tecnologia wireless applicata alle industrie di processo sta diventando sempre più utilizzata anche perché l'utilizzo di sensori che raccolgono le informazioni non sempre ha la possibilità di avere comunicazioni via cavo. Quindi ovviamente vengono utilizzati comunicazioni wireless, che hanno minori costi e tempi di istallazioni più rapidi.
Si possono utilizzare sensori intelligenti, che raccolgono capacità intrinseche, che combinano rilevamento, calcolo e comunicazione in un singolo dispositivo.

Sebbene derivino numerosi vantaggi dall'implementazione della tecnologia di reti wireless nelle operazioni degli impianti di processo le problematiche e preoccupazioni più importanti derivano dall'interferenza RF tra le varie tecnologie wireless. Questo è noto come problema di **coesistenza**.
Il problema può verificarsi quando due messaggi con energia sufficiente si scontrano o si sovrappongono tra loro nel tempo o nella frequenza.
La coesistenza è definita come la capacità di un sistema di eseguire un'attività in un dato ambiente condiviso in cui altri sistemi hanno la capacità di svolgere i propri compiti e possono o meno utilizzare lo stesso insieme di regole. La coesistenza di diversi protocolli wireless implica l'invio affidabile di messaggi appartenenti a ciascun protocollo in presenza di interferenze RF.
Sono state adottate diverse tecniche per combattere e ridurre al minimo il problema della coesistenza che includono: diversità di frequenza, diversità temporale, diversità di potenza, diversità di codifica, diversità spaziale, lista nera e valutazione del canale.

Quindi, quando si parla di Wireless si parla di WSN. L'idea è quella che nell'automazione di processo i sensori vengono impiegati in diverse posizioni all'interno dell'impianto per le misurazioni dei parametri di processo e il loro successivo controllo. I dati dei sensori vengono elaborati e le azioni di controllo vengono eseguite in modo tale che le variabili di processo rimangano all'interno dei valori impostati.
La struttura gerarchica di un sistema di automazione di impianti di industriali comprende fasi in cui vengono prese decisioni specifiche relative a tale livello (piramide CIM). Quello che succede è che si hanno diversi

approcci possibili. In generale uno convenzionale, che è quello di avere diversi dispositivi e componenti (moduli, rack…); nelle reti di campo si ha invece un sistema più compatto dove gli elementi del campo collegati alla parte di alimentazione in modo diretto. Quando invece si parla di ambienti **Wireless** i singoli dispositivi hanno una alimentazione e delle antenne che ne consentono la trasmissione e dei gateway che ricevono informazioni dagli AP. Quindi non si hanno più connessioni via cavo ma tramite aria e cioò ne comporta tutti i benefiti in termini di costi e manutenzione. Durante la progettazione di una rete wireless industriale, però, è necessario prestare attenzione al fatto che i dati inviati dalle stazioni , via aria, devono essere crittografati e protetti da intercettazioni.
La rete deve rimanere connessa indipendentemente dal fatto che i nodi siano statici o mobili e il consumo di energia in ogni stazione deve essere mantenuto il più basso possibile; la trasmissione deve essere priva di interferenze fornite da fonti o rumori RF vicini e infine dovrebbe esserci la ritrasmissione dei dati in caso di perdita dei pacchetti.

Benefici → ci sono numerosi vantaggi che si accumulano nell'applicare le reti di sensori wireless nell'automazione industriale. Sebbene esistano problemi di coesistenza che devono essere affrontati durante l'implementazione delle WSN, i vantaggi superano di gran lunga gli inconvenienti: non sono necessari cavi, la modernizzazione di un impianto esistente è abbastanza semplice; costi ridotti di manutenzione e di costruzione, maggiore produttività e sicurezza e meno requisiti di personale in loco.

Requisiti per i protocolli per i sistemi SCADA: DNP3 e IEC 60870

Quando il concetto di sistema SCADA viene collegato a grandi infrastrutture come reti elettriche, ferroviarie, idriche, ecc. i protocolli diventano fondamentali soprattutto quando le infrastrutture che hanno una dimensione anche a livello nazionale, e che quindi hanno bisogno di maggior controllo e supervisione. Oppure quando si hanno infrastrutture intese come critiche occorre quindi una conoscenza dei protocolli che supervisionano o comunque vengono utilizzati dai sistemi informatici.
L'infrastruttura per eccellenza quando si parla di sistemi SCADA è la rete elettrica perché ha una conoscenza del processo fisico molto dettagliata e ha una struttura per sua natura fortemente eterogenea. È divisa in 3 macro-parti: Generazione – Trasmissione - Distribuzione che di solito hanno società di riferimento diverse ma devono interagire tra di loro con una sincronizzazione delle informazioni quanto più precisa possibile. La rete elettrica è composta da molteplici unità interconnesse tra loro e quindi diventa importante mantenere la stessa frequenza, avere una sincronizzazione delle informazioni quanto più precisa possibile.

Le reti elettriche consistono in sistemi di trasmissione e sistemi di distribuzione.
Il **sistema di trasmissione** è costituito da linee elettriche e ad alta tensione e un numero di sottostazioni di grandi dimensioni. Fornisce energia alle stazioni terminali dove i trasformatori abbassano la tensione e immettono energia nella rete di distribuzione.
Le **reti di distribuzione** includono un gran numero di sottostazioni e trasformatori più piccoli che convertono ulteriormente la potenza in tensione di rete e la riflettono sui consumatori domestici e commerciali.

Le stazioni di grandi dimensioni si collegano direttamente al sistema di trasmissione e le stazioni di generazione più piccola possono connettersi alle reti di trasmissione o di distribuzione.
Le moderne sottostazioni includono apparecchiature per controllare e proteggere il sistema di alimentazione. Questi sistemi monitorano molte qualità come tensioni, correnti, flussi di alimentazione, lo stato degli interruttori e di altre apparecchiature.
Alcuni dispositivi nelle sottostazioni eseguono funzioni per disconnettere automaticamente l'alimentazione nel caso i cui si verifichino problemi quali sovraccarichi, cortocircuiti o guasti. Che possono disconnettere intere porzioni di rete. Quindi le sottostazioni di trasmissione sono i siti maggiormente monitorati e protetti.
Le sottostazioni sono solitamente monitorate dai sistemi **SCADA** che comunicano i loro dati ad un centro di controllo in cui le informazioni vengono utilizzare per consentire al personale operativo di monitorare e controllare da remoto la rete elettrica.
Le caratteristiche dinamiche della rete elettrica (estrema velocità) portano a far si che anche il Sistema SCADA fornisca un rapido aggiornamento dei dati monitorati e supportare un ritardo minimo nell'emissione delle richieste di controllo dal centro di controllo all'apparecchiatura da campo.
Inoltre, il controllo del sistema di alimentazione richiede un'elevata integrità relativa al trasferimento dei dati, ovvero bisogna garantire che i dati arrivino in maniera corretta anche all'operatore. L'idea è quella che l'operatore deve essere in grado di fidarsi dell'accuratezza delle informazioni riportate al centro di controllo al fine di dedurre rapidamente le risposte richieste.
Il sistema deve rispondere correttamente a qualsiasi comando dell'operatore e attivare solo esattamente l'attrezzatura richiesta dall'operatore.
In generale quindi, quando parliamo di protocolli di comunicazione dobbiamo da un parte garantire l'integrità delle informazioni che viaggia in generale dai sensori o comunque dai sistemi di monitoraggio ai sistemi SCADA, è valido anche il contrario: ossia le informazioni che vengono trasmessi dal sistema SCADA devono essere in qualche modo validate e eseguite in maniera corretta.
Quando si verificano guasti nel sistema, le apparecchiature di protezione automatica installate nelle sottostazioni di solito agiscono per indentificare il guasto e prendere misure per minimizzare i danni al sistema. L'idea è quella che a volte (quando non si può aspettare una risposta da SCADA) un sistema elettrico possa funzionare anche senza SCADA tramite dei sistemi di protezione automatica.
Ovviamente l'azione automatica verrà poi riportata all'operatore, per far si che questo possa cercare una risoluzione al problema e per analizzare a posteriori i dati.
La segnalazione dei dati con data e ora a un sistema che archivia tutte le informazioni viene talvolta denominata segnalazione **sequenza di eventi** o **SOE**.

In quanto ai sistemi SCADA il problema principale è relativo alle durate dei servizi, in quanto

Le apparecchiature di controllo e i sistemi di comunicazione associati hanno in genere una vita utile proporzionale, nell'ordine dei 10 anni. Ci sono quindi sistemi SCADA che operano su sistemi relativamente vecchi o con vecchie architetture che hanno una larghezza di banda limitata e possono presentare tassi di errore più alti rispetto all' IT.
Un aspetto fondamentale è la registrazione temporale (sincronizzazione) dei dati. Considerando che le reti elettriche basano la maggior parte dei loro SCADA e la loro sincro tramite il GPS, che è facilmente hackerabile.

Tradizionalmente i sistemi SCADA nascono con protocolli proprietari con interfacce di comunicazioni che soddisfano specifiche richieste. In tempi recenti sono stati sviluppati e adottati numerosi standard aperti a questo scopo. I moderni sistemi SCADA adottano quasi universalmente interfacce standard dei settori delle telecomunicazioni come per le **seriali** o per **Ethernet su TCP/IP**.

Nell'industria elettrica i protocolli SCADA più comunemente utilizzati sono **IEC 60870.5** utilizzati in Europa e **DNP3** comune nei paesi in lingua inglese.

- La serie **IEC 60870-5** comprende due profili per le attività di base di **telecontrollo** su collegamenti seriali (**T101**) e TCP/IP (**T104**). Sono riconosciuti come gli standard internazionali per i protocolli di trasmissione SCADA di energia elettrica e non vengono quindi utilizzati in altri ambiti. Il loro scopo è stato obbligato dalla legge in molti paesi europei.
  T101: specifica un profilo per quanto riguarda la base del telecontrollo su queste regole, include la definizione di oggetti di dati generici e specifici del sistema di alimentazione e funzioni direttamente applicabili alla sottostazione al collegamento SCADA del centro di controllo. **T104** adatta tutto quello che è stato definito dal T101 su TCP/IP con aggiunta di alcune funzioni come tag temporali.

- **DNP3** è un protocollo SCADA per uso generico basato sulle regole di progettazione che si trovano già in IEC 60870-5 con l'aggiunta di alcuni concetti diversi definiti in alcune parti dell'IEC. L'idea è di definire tipi di dati e funzioni per la trasmissione di dati SCADA generici. Sebbene sia stato progettato per l'applicazione del sistema elettrico, non include gli oggetti dati specifici del sistema elettrico. DNP3 è ora considerato uno standard di fatto, quindi un po' più generico rispetto a IEC, applicabili in più settori.
  E' considerato uno standard di fatto per le comunicazioni SCADA di energia elettrica nei paesi Anglosassoni. La creazione di DNP3 sembra essere stata influenzata come una risposta pragmatica alle richieste del mercato delle utility che ritenevano IEC un po' troppo limitato. E' un protocollo aperto.

Elementi in comune:

- Si basano sul paradigma **Report-by-Exception** (**RBE**), in cui, durante il normale funzionamento, vengono riportate semplicemente le modifiche, e i dati che non sono stati modificati non vengono riportati, aumentando quindi l'efficacia della segnalazione dei messaggi eliminando la segnalazione non necessaria di dati non modificati. Quello che succede è che all'inizio RBE richiede la raccolta iniziale di tutti i dati da un dispositivo di campo, ma dai passaggi successivi verranno mandate solamente le modifiche. Questo permette di mantenere la perfetta sincronizzazione delle informazioni che saranno le stesse sul campo e sul sistema SCADA.
- Utilizzano più o meno la stessa struttura, adottano il modello di riferimento **EPA (enhanced Performance Architecture)** che utilizza i livelli fisico, data-link e applicazione della pila ISO-OSI evitando gli elementi intermedi come nella maggior parte dei bus di campo. DNP3 estende il modello con una "funzione di trasporto" (pseudo-layer) che consente l'assemblaggio di messaggi più grandi in un singolo frame di collegamento dati.
- Per quanto riguarda il controllo includono un meccanismo di **controllo in due passaggi** (es. seleziona/esegui) che fornisce una migliore sicurezza nell'invio dei comandi evitando errori casuali dei dati introdotti ad esempi da interferenze nel sistema di comunicazione. (integrità dei comandi di controllo)
- T101 e DNP3 la parte di gestione del frame di frame è la stessa, definita in IEC 60870, che fornisce una buona efficienza dei messaggi con un buon rilevamento e rifiuto degli errori. (integrità e efficienza dei messaggi)
- Gli oggetti includono **flag di qualità** che forniscono informazioni aggiuntive per qualificare o convalidare i dati che vengono segnalati.
- **Data e ora** sui dati delle modifiche che indicano il tempo di misurazione dei dati segnalati.
- Si hanno una serie di **oggetti di dati** di informazione supportati da entrambi i protocolli (oggetti binari, contatori, comandi di controllo, lettura/scrittura dai dispositivi di campo …)
- Modalità opzionali di funzionamento in cui il dispositivo di campo può segnalare i dati di modifica senza essere interrogato dal master
- …

Ovviamente qualsiasi dispositivo che implementa questi protocolli può scegliere di implementare solo quelle parti del protocollo necessarie per supportare il funzionamento di quel dispositivo. Ogni protocollo ha alcune funzionalità obbligatorie come la pulizia dei dati o la manutenzione del sistema.

Differenze: Queste differenze sono evidenti nell'oggetto dati e nei formati dei messaggi scambiati utilizzati per manipolare gli oggetti.
È importante sapere che le descrizioni dei due standard potrebbero utilizzare termini diversi per descrivere la stessa cosa o termini uguali per descrivere cose diverse. Bisogna fare un po' di attenzione.
(es. stazione di controllo (IEC) = master (DNP3))

- T101 è strettamente utilizzabile su collegamenti seriali, T104 è strettamente utilizzabile su TCP/IP. Il frame di T101 viene sostituito in T104 insieme a diverse regole di conferma dei messaggi.
  DNP3 utilizza sempre il frame di collegamento dati seriale e quando viene utilizzato con TCP o UDP il frame di collegamento dati seriale viene incapsulato in un pacchetto TCP o UDP.
- I messaggi T101 e T104 possono contenere solo un singolo **tipo di dati** (ingressi binari a bit singolo o misurazioni analogiche in interi). I messaggi DNP3 possono contenere più tipi di dati in un unico messaggio, purché la stessa funzione (lettura, comando di controllo, risposta al rapporto) si applichi a tutti i dati nel messaggio. Per questo motivo la risposta a un comando può essere costituita da diversi messaggi più piccoli in T101 o T104 e un numero ridotto di messaggi di grandi dimensioni in DNP3.
  Ciò influisce sull'efficienza della segnalazione dei diversi protocolli. DNP3 risulta quindi molto più efficiente in quanto capace di trasmettere più tipi di dati
- I messaggi T101 e T104 sono limitati alla dimensione massima di un singolo frame di collegamento dati. I messaggi DNP3 non hanno limiti di dimensione logici. Infatti, DNP3 utilizza la funzione di trasporto e la frammentazione del livello applicazione per creare messaggi di qualsiasi lunghezza e li trasmette come una serie di frammenti di applicazione suddivisi in molti segmenti di trasporto per adattarsi ai dati frame di collegamento.
- DNP3 utilizza un meccanismo di conferma esplicito per verificare la segnalazione dei dati dell'applicazione. T101 deduce la corretta segnalazione delle applicazioni facendo affidamento sulla conferma del collegamento dati di ciascun frame del collegamento. T104 si basa sulla conferma di un numero di messaggi trasmessi.
- Poiché i messaggi IEC possono solo riportare un singolo tipo di dati o funzione in un singolo messaggio, la risposta ad alcune funzioni dell'applicazione consiste in una serie di messaggi che iniziano con una sequenza di comando iniziale ACTCON seguito da uno o più messaggi di dati e termina con una sequenza di comando finale ACTTERM. In DNP3 la stessa funzionalità richiede in genere solo un singolo messaggio di risposta.
- I messaggi T101 e T104 includono un valore di causa di trasmissione COT che serve per assistere il controllo di più passaggi della risposta a un comando ed è in parte utile per indicare il motivo per cui i dati vengono inviati. Ad esempio, il COT può distinguere tra un cambiamento che si è verificato spontaneamente (lo scatto di un interruttore dovuto ad un'azione di protezione) o perché un operatore ha emesso un comando di controllo per causare la modifica. DNP3 non include questo tipo di informazioni e non indica il motivo per cui si è verificato un cambiamento.
- Per quanto riguarda i tipi di dati, DNP3 definisce oggetti generici senza assegnare un significato specifico a tali oggetti. T101 e T104 definiscono oltre a questi tipi di base, un numero di oggetti specifici del mondo elettrico.
- DNP3 consente l'uso di segnalazioni non richieste su qualsiasi canale in cui i dispositivi sono in grado di rilevare l'attività del canale al fine di evitare collisioni. In questa modalità di segnalazione, una stazione periferica può inviare una notifica di evento a una stazione master senza essere interrogata.
  La modalità equivalente per T101 richiede l'uso delle regole di collegamento dati bilanciate e richiede un collegamento full- duplex point-to-point dedicato tra la stazione master e ciascuna stazione di distribuzione in modo che sia possibile trasmettere entrambi i dispositivi in qualsiasi momento senza possibilità di collisione di messaggi.

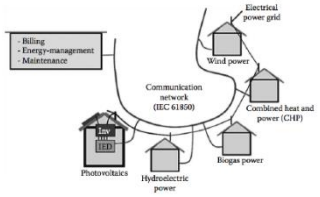
Quando si opera su TCP/IP la differenza tra T104 e DNP3 è meno pronunciata e più difficile da valutare.

IEC 61850 per Smart Grid

Protocollo per sistemi SCADA strettamente legato alle smart grid ovvero le reti elettriche intelligenti. Dovuto al fatto che le reti elettriche hanno bisogno di un telecontrollo da remoto, di informazioni proveniente da dispositivi; e come già visto, per quanto riguarda SCADA, il problema principale è che a differenza di altre infrastrutture, queste hanno una una dinamica molto veloce che fa si che anche i protocolli debbano essere sufficientemente veloci.
Negli ultimi anni le reti elettriche stanno cambiando notevolmente, grazie all'introduzione di fonti rinnovabili all'interno della rete. Si parla in genere, non solo del singolo dispositivo ma anche di farm (solar farm, wind farm…) che potrebbero produrre lo stesso quantitativo dei generatori tradizionali, ma con più fattori da considerare come le rispettive strutture da realizzare.
Ovviamente è nato anche il bisogno di monitorare e controllare questi tipi di fonti rinnovabili.

Rispetto alle vecchie tecnologie e dispositivi, quelli rinnovabili presentano una serie di "svantaggi" legati al fatto magari di non essere completamente prevedibili, di essere più complessi a livello di programmazione ecc…

Un altro problema è che, nel momento in cui queste fonti sono presenti nelle reti comuni (es. casa), i sistemi per l'automazione, la protezione e il monitoraggio di questi dispositivi sono sviluppati e realizzati da molte piccole e medie imprese, quindi diventa complicato da gestire.
Per la gestione del flusso di energia in questa rete elettrica, per la manutenzione degli impianti e per la fatturazione elettrica, la maggior parte delle risorse energetiche deve essere integrata anche in una rete di comunicazione comune. Uno standard richiesto per questa rete di comunicazione è fornito nella IEC 61850, che ha quindi il compito di far interagire tra di loro diversi generatori in una rete distribuita.



- pale eoliche - turbine a biogas - centrali idroelettriche
- fotovoltaico - centrali combinate di calore e potenza

Tutti queste case che hanno una parte di rinnovabili avranno al loro interno quello che IEC definisce come Intelligent Electronic Device (IED), che consente la comunicazione con il protocollo e l'operatore.

Lo standard **IEC 61850** nasce esclusivamente per le reti elettriche ed è stato originariamente sviluppato per l'automazione delle sottostazioni, in seguito è stato utilizzato per risorse energetiche distribuite (fonti rinnovabili). Consiste nelle seguenti parti:

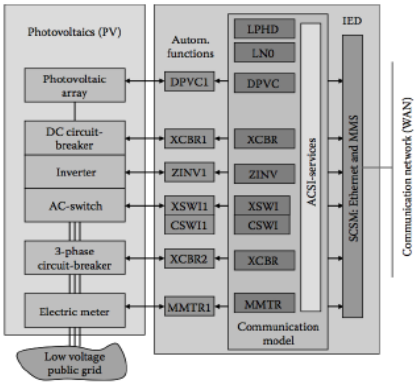
- Modellazione delle informazioni che devono essere scambiate
- Selezione dei servizi astratti di comunicazione (ACSI) della IEC 61850-7-2 che consente di definire in maniera astratta gli elementi della comunicazione.
- Selezione di protocolli reali per i servizi di comunicazione

In sistesi:
Il protocollo nasce esclusivamente per le reti elettriche, in particolare per il controllo dei sottostazioni e le fonti rinnovabili e si hanno delle funzioni di automazione:

2- i valori del campionamento dati analogici

LA comunicazione avviene tramite una struttura particolare simile a XML, abbiamo una serie di nodi logici che ci consentono la trasmissione di info per diverse fonti rinnovabili.

Il concetto base dello standard IEC 61850 per la sua applicazione in risorse energetiche distribuite (DER) può essere descritto con un esempio di un piccolo impianto fotovoltaico.



La struttura reale prevede il pannello fotovoltaico e una parte per la comunicazione (rete elettrica di distribuzione). Tra questi due elementi c'è:
- interruttore a CC che alimenta il pannello,
- un inverter che ci consente di trasformare la corrente da CC a CA,
- un interruttore CA,
- un interruttore automatico 3-fase
- un contatore elettrico che ci consente di capire quanta energia si sta producendo.
Sono di fatto 5 componenti, oltre al pannello fotovoltaico, che vengono trasformati in una serie di oggetti che sono necessari per la comunicazione.

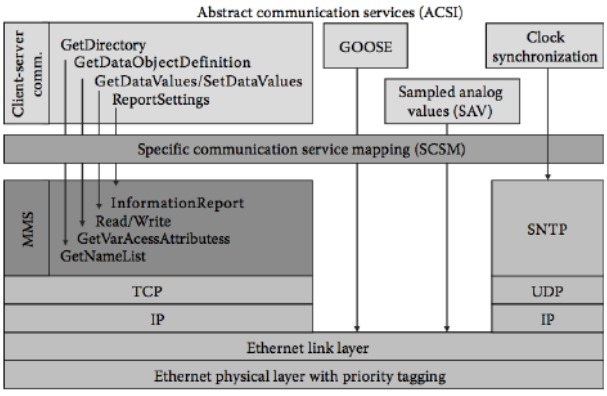
Per l'integrazione di tale sistema in una rete di comunicazione sono richiesti microcontrollori chiamati *Intelligent Electronic Device* **IED**.
IEC 61850 fornisce classi di oggetti standardizzate chiamati Nodi Logici LN per descrivere le informazioni prodotte e consumate dalle funzioni di automazione di un IED (=che ci consentono la trasmissione di informazioni per diverse fonti rinnovabili).
(Per l'esempio utilizzato le classi di nodi logici utilizzate sono: LPHD, LLNO, DPVC, XCBR …)

In generale le **funzioni di automazione** nelle reti elettriche possono essere classificate in tre macro categorie:

1. Le funzioni di **protezione:** evitano pericoli per le persone, danni ai componenti della rete di alimentazione e guasti alla rete elettrica. (eseguite entro 10ms).
2. Le funzioni di **monitoraggio:** supervisionano lo stato dei dispositivi e delle apparecchiature primarie (interruttori automatici, trasformatori, ecc.) all'interno della rete elettrica.
3. Le funzioni di **controllo:** consentono il funzionamento locale o remoto dei dispositivi.

Queste funzioni possono essere suddivise in sotto funzioni ed elementi funzionali.
Per **modellare** le funzioni di automazione nel modello di comunicazione, gli oggetti sono standardizzati a livello degli elementi funzionali LN (Logical Node). (es. un motore, rotore…), che possono poi essere raggruppati in dispositivi logici LD.

I **servizi di comunicazione** richiesti in un IED sono descritti in un modello di comunicazione dai cosiddetti servizi **ACSI** (***Abstract Communications Service Interface***). Questi servizi astratti devono essere implementati utilizzando i protocolli di comunicazione concreti esistenti (**SCSM** – *Specific Communication Service mappings*). Questa mappatura può essere realizzata con protocolli Ethernet TCP/IP e MMS (Manufacturing Message Specification).



Nella struttura standardizzata abbiamo una serie di elementi a basso livello (Ethernet Physical Layer e Ethernet Link Layer per i livelli 1-2 ISO/OSI), IP, TCP o UDP e poi abbiamo due porzioni:
- Da una parte SNTP che serve per la sintonizzazione
- E dall'altra MMS che è un protocollo di comunicazione client-server

Abbiamo poi altre funzioni come GOOSE per la comunicazione con le sottostazioni, e SAV per i dati analogici; che si trovano nella parte alta (servizi di comunicazione astratta). Tutto questo viene fatto tramite la mappatura di specifici servizi di comunicazione SCSM.

I servizi ACSI più importanti per le risorse energetiche distribuite sono i servizi di comunicazione *client-server*. Includono servizi come:

- *GetDirectory*: quando un client desidera comunicare con un altro IED, può recuperare un elenco completo dei nomi di tutti accessibili in un IED, che sono LD, LN, DO e attributi di dati.
- *GetDataObjectDefinition*: un client può recuperare i tipi di dati per tutti gli oggetti.
- *GetDataValues, SetDataValues*: i valori degli oggetti possono essere letti e scritti
- *Reporting*: consente uno scambio di dati basato su eventi di valori impacchettati o dopo un tempo di buffer.

- *Logging*: il server offre la possibilità di archiviare i dati per il successivo recupero da parte dei client.

→ I servizi di **comunicazione client-server** devono essere associati al protocollo di **MMS** basato su Ethernet TCP/IP, che definisce una struttura per ricevere ed inviare messaggi richiesti per controllare e monitorare i dispositivi su una rete; e non riguarda il modo di trasferimento: per questo viene utilizzato Ethernet e TCP/IP. Gli oggetti dati nell'IEC 61850 sono mappati su MMS.

→ Un altro servizio ACSI specificato dallo standard IEC 61850 è il cosiddetto **Generic Object Oriented Substation Event (GOOSE)**. È un meccanismo per la trasmissione rapida di eventi come comandi, allarmi e indicazioni. Si mandano messaggi Broadcast inviati da un IED che possono essere ricevuti e utilizzati da più destinatari che si trovano nella stessa sottorete. Quindi non si ha più una struttura client-server ma publisher-subscribers. E' implementato direttamente di Ethernet link layer e supporta il comportamento in tempo reale.

→ il servizio ACSI denominato ***trasmissione di valori analogici campionati*** (**SAV)** supporta anche una comunicazione time critical, utilizzata principalmente per lo scambio di misure di corrente e tensione dai sensori. Le caratteristiche dei valori possono essere trasmesse come messaggi broadcast in tempo reale da un IED publisher a IED subscribers. Il publisher scrive i valori insieme ad un timestamp in un buffer di invio. Dopo la trasmissione, i subscribers possono leggere i valori dai rispettivi buffer di ricezione.

→ Per la **sincronizzazione dell'orologio** si utilizza il protocollo **SNTP** (standard network Time Protocol) specificato per le applicazioni non cruciali. La sincronizzazione separata è richiesta per il processo SAV ed è consentita l'implementazione dell'uso di un servizio di diffusione nel tempo, come ad esempio il **GPS**. Il problema di GPS è che queste informazioni vengono scambiate in chiaro.

La comunicazione tra uno IED e un sistema avviene tramite una struttura particolare simile a XML adattato alle informazioni che devono essere trasmesse, chiamata **SCL (System Configuration Language)** nel quale le informazioni prodotte vengono modellate in un file SCL; che include in una struttura gerarchica le seguenti informazioni: Punto di accesso per l'IED nella rete di comunicazione - Servizi ACSI supportati da IED - Modello delle funzioni di automazione di LD (LN e blocchi di controllo) - Modelli di tipi di dati (tipi di dati utilizzati nel file SCL).

Lo standard IEC 61850-420 include delle estensioni per i seguenti tipi di risorse energetiche distribuite.

Trends e Sfide per i sistemi di comunicazione industriali:

Nell'era della connettività si hanno processi industriali con un numero sempre più elevato di sensori, reti e infrastrutture di automazione per migliorare l'efficienza, la sicurezza e la trasparenza. Ciò porta, a seconda del requisito specifico del dominio, a tecnologie e metodi specifici.
Si vorrebbe arrivare ad una soluzione universale, ancora molto lontana. Fatto sta che esistono nel mondo dei protocolli di nicchia che stanno diventando sempre più specifici per un determinato problema.
Le principali sfide che i sistemi di comunicazione industriale futuri ICS dovranno affrontare sono:

- **Onnipresenza connettività globale e identità digitale**
  La connettività Internet IP è un dato di fatto. Questo ci porta a pensare che sia possibile anche a livello di comunicazione M2M. Connettività globale in questo contesto significa connettività mobile (senza cavi) su una determinata regione e forse anche oltre i confini.
  Un normale requisito per la connettività globale è l'abbonamento a un determinato tipo di piano di servizio. Quello che si è deciso di fare, anche in sistemi SCADA, è stata quella di fornirsi di servitori come provider Internet, una compagnia telefonica, un dipartimento IT aziendale o qualche altro operatore IT. L'idea è quella per cui alcune macchine difficili da raggiungere vengono, tramite SIM o ID, collegate ad una rete internet pubblica. La scheda SIM non hanno una definizione di identità stabilita: ogni fornitore ha il suo modo per far accedere le macchine o le persone. Ad esempio un sistema di comunicazione industriale ha infatti a che fare con un mix eterogeneo di tecnologie come IP Proxy Router…. Quindi non esiste uno standard SSO (Single Sign-On) per l'infrastruttura ICS che possa essere paragonato a SSO nel mondo IT.
  Ci si può aspettare però che IT, telecomunicazioni e comunicazioni industriali possano ulteriormente convergere, così che le soluzioni IT saranno adottate per ICS.

- **Integrazione verticale** (la piramide CIM diventa un pilastro in cui tutti è connesso con un protocollo)
  quando si parla di sistemi di comunicazione industriale questi sono ed erano visti nella maggior parte dei casi come una struttura piramidale. L'idea è quella per cui questi sistemi potessero essere in qualche modo interconnessi ma più distanti possibili (sistemi a livelli inferiori e superiori). Questo ha portato da una parte a una protezione di questi sistemi, dall'altra si sta comunque cercando di avere una versione più integrata in modo da poter ottenere una riduzione dei costi e una maggiore efficienza.
  Questa tendenza è rafforzata dai vincoli ecologici o di una maggiore efficienza energetica, quindi è importante integrare le diverse parti dell'azienda per fare analisi di altro tipo.
  Anche se i vari sistemi IT sono in qualche modo interconnessi, di solito mancano di una gestione comune e di un linguaggio comune per lo scambio di informazioni. Quindi l'idea è quella di poter trasmettere i dati dall' I/O al CEO (amministratore delegato), ma non è solo un problema di realizzazione fisica ma di semantica e traduzione dei vari sistemi.
  Tuttavia tutto questo sta cambiando perché i protocolli attuali stanno cercando di essere utilizzati nella gestione del processo ma anche in livelli più alti.
  Questa integrazione verticale comporta problematiche di tipo cyber in quanto la maggior integrazione facilita l'accesso a reti meno protette.

- **Reti locali ibride e Quality of Service QoS**
  La maggior parte degli ICS sono stati progettati tenendo conto di un particolare dominio applicativo (acquisizione dati, allarmi…). Il dominio dell'applicazione ha prodotto caratteristiche specifiche come bassa latenza, intervalli di tempo garantiti, buona scalabilità o bassi costi.
  Non esistono reti "universali" in grado di soddisfare ogni possibile esigenza di connettività, ma l'idea è quella di avere reti ibride. Una rete ibrida è composta da più canali di comunicazione anche molto diversi.
  Un'altra possibilità è quella invece di spostarsi verso le reti universali in cui le caratteristiche di diversi domini sono state combinate. In particolare, ciò è accaduto sul livello di controllo di accesso ai media nel caso di reti come IEC 61580. In genere una parte della larghezza di banda è riservata al traffico deterministico (slot isocroni) mentre il resto può essere arbitrato con CSMA. Con questo design ibrido è possibile ottenere due qualità di rete molto diverse: scalabilità semplice per servizi non in tempo reale e servizio garantito per applicazioni in tempo reale.
  Un fattore importante per i progetti ibridi è il modo in cui viene implementata la **qualità dei servizi** QoS. In generale ICS sono sensibili a tutti e quattro gli aspetti di QoS:
  Larghezza di banda - Latenza (ritardo pacchetto) - Variazione della latenza (jitter) - Perdita di pacchetti

- **Comunicazione machine-to-machine M2M**

  Abbiamo macchine sempre più utilizzare e che interagiscono con l'essere umano; l'idea è quella di avere un processo decisionale e compiti più soft.

  Quello che succede è che i programmi per computer che agiscono per conto di determinati individui o ruoli comunemente chiamati *agenti software*, che proprio come gli esseri umani, devono comunicare con altri agenti, l'ambiente e gli esseri umani per essere in grado di svolgere i loro compiti. A differenza degli umani però non sono persone fisiche. Questa distinzione è molto importante quando si tratta di sicurezza delle informazioni e gli aspetti giuridici per la responsabilità.

  Il problema di sicurezza è ridotto alla protezione di una determinata chiave di crittografia durante l'installazione e il funzionamento. Questa chiave potrebbe essere protetta da PIN o altri canali laterali che possono essere forniti solo da una persona specifica.

  Trasferire queste procedure alla comunicazione M2M non è banale. L'unico metodo conveniente al giorno d'oggi consiste nell'utilizzo di chip card elettroniche ad esempio smart card, moduli di piattaforma affidabili TPM o altri chip che contengono la chiave e gli algoritmi per utilizzare la chiave.

  La seconda sfida per la comunicazione M2M è la gestione della rete: man mano che le reti diventano più grandi è necessario che le tradizionali attività di amministrazione della rete siano automatizzate. Gli ingredienti sono quindi: ricerca dei servizi e tabelle di ricerca, autodescrizione di servizi e capacità, profili di applicazione. L'ideale sarebbero macchine plug-and-play, che comunicano in maniera automatica. Naturalmente è sempre presente la supervisione umana.

- **Scalabilità di hardware e software**

  L'ideale sarebbe la totale integrazione del mondo industriale, cioè la connessione di diverse applicazioni e reti. Le loro diverse caratteristiche che sono state adattate alle specifiche aree di applicazione, potrebbero rappresentare un ulteriore barriera per l'integrazione.

  Un altro aspetto riguarda le dimensioni, sia fisiche che dei codici degli stack di protocollo, le dimensioni del silicio e quindi anche dei costi.

  Quindi la combinazione di reti di sensori a basso costo co potenti reti multimediali a tempo reale non sempre funziona immediatamente. E' necessaria quindi un'architettura scalabile in cui, in termini di hardware, protocolli e software, nodi molto diversi che possono interagire, tramite un piccolo insieme di servizi comuni.

  . . .

Questo è un riassunto sui problemi che si stanno affrontando attualmente, ci sono speranze che il 5G possa risolvere molti dei problemi elencati.

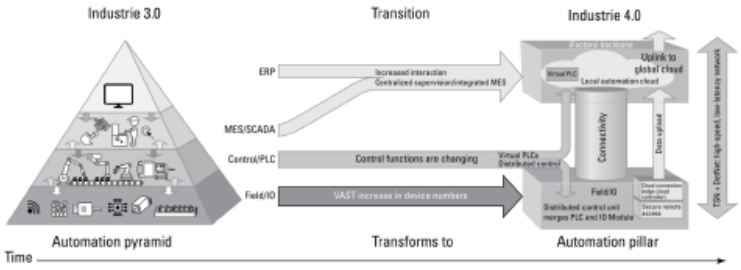
Time Sensitive Networking – TSN

E' uno tra i più promettenti nuovi protocolli, che si adatta ai nuovi cambiamenti sia industriali sia delle comunicazioni in generale.
Rientra più o meno in tutte quelle comunicazioni dell'Ethernet Industriale, in cui si cerca di adattare protocolli classi basati su Ethernet al mondo industriale. L'idea generale nei sistemi automatizzati è quella di avere protocolli, e quindi comunicazioni, sempre più vicini alle caratteristiche real time che garantiscano comunicazioni deterministiche.
L'idea è quella di avere un protocollo che garantisca compatibilità e possa garantire l'aumento della larghezza di banda in futuro.
Il time-sensitive networking TSN supera tre limitazioni attuali:

- Comunicazione affidabile e in tempo reale quindi con tempi ritardo molto brevi
- Larghezza di banda elevata per ospitare grande quantità di dati diversi
- Compatibilità con le versioni precedenti con i dispositivi Ethernet (non TSN)

Verso il futuro…

L'automazione industriale è attualmente in fase di transizione da ciò che viene definita industria 3.0 all'industria 4.0, o la fabbrica intelligente, parte del IIoT Industrial Internet of Things. Quindi l'idea dell'utilizzo di una combinazione di dispositivi intelligenti, analisi avanzate e apprendimento automatico per rendere gli impianti di produzione più intelligenti e dinamici.
Questa transizione viene comunemente rappresentata come passaggio dalla piramide dell'automazione al pilastro dell'automazione.
L'idea è quella di avere un mondo che non è più gerarchicamente costituito ma in cui tutti sono collegati con tutto. La principale modifica per questo scopo è quella di non avere più protocolli distinti per i bus di campo, per la comunicazione tra PLC e sistema SCADA, per la comunicazione a livello aziendale. È necessario quindi che siano una serie di funzionalità che devono essere distribuite all'interno del sistema.



Quindi un'idea è quella di utilizzare un protocollo, come appunto **TSN**, che consente di poter comunicare, sullo stesso mezzo, diversi tipi di traffici. Che consente di avere, in una stessa struttura, connettività diverse con priorità diverse.

La rappresentazione del pilastro prevede: il livello basso, il livello alto e in mezzo sistemi interconnessi. Il pilastro di automazione ha ancora un livello di campo ma il numero totale di sensori è più alto per consentire un'analisi e un controllo molto più rigorosi delle funzioni di produzione (con sistemi di controllo distribuiti che garantiscono tempi di esecuzione veloci e affidabili); e una parte della gestione e del controllo viene spostata a livello più alto come unità di controllo centralizzate. Quindi la pianificazione delle risorse aziendali (ERP), il sistema di esecuzione della produzione (MES), il controllo di supervisione e l'acquisizione dati, che fanno parte della dorsale, vengono spostati nel cloud.
L'idea inoltre è di trasformare i PLC in PLC virtuali ospitati nel cloud e che interagiscono direttamente con il processo di produzione attraverso il livello di connettività. La connettività deve avere però come vincoli principale quello di poter garantire il medesimo determinismo che ci garantirebbero i PLC nella configurazione tradizionale a piramide.
Questo consente di avere totale flessibilità dei sistemi, quindi di avere PLC disposti dovunque.
Sia il livello di campo che il livello di connettività richiedono prestazioni di rete ad alta velocità e bassa latenza. Il livello di connettività trasferisce il traffico in background con priorità più bassa in modo da non dover rallentare il traffico time-critical. È qui che entra in gioco TSN.

In generale, l'idea è che le reti di automazione partono dal sensore che è direttamente collegato ad un infrastruttura cloud presso il backbone di fabbrica, e i messaggi su questa rete di comunicazione possono essere un po' meno urgenti

(mission-critical). Il ciclo di controllo mission-critical viene utilizzato per gestire il processo di produzione e vengono utilizzati i dati del sensore meno urgenti per analizzare e ottimizzare il processo. La parte centrale del pilastro è una "superstrada" dell'informazione in cui il traffico è costituito da dati time-critical e dati meno urgenti.

Quindi, quali sono i possibili approcci:

- Utilizzare TSN, che consente ai dati urgenti e meno urgenti di condividere la connessione di rete, impedendo al traffico meno urgente di ostacolare il flusso del traffico più urgente
- Costruire reti separate per le diverse applicazioni (come in CIM)
- Sovradimensionare l'infrastruttura di rete: un approccio ampiamente utilizzato ma estremamente costoso
- Vivere con i ritardi del traffico nei dati mission-critical (opzione non praticabile)

TSN

Con TSN, tutti i dati viaggiano sulla stessa struttura, con dati urgenti con priorità più elevata, dati meno urgenti con priorità meno elevata. L'idea è come avere un autostrada in cui, c'è una corsia dedicata ai dati urgenti come quelli di emergenza.
Quindi si cerca di ottimizzare il traffico ottimizzando la larghezza della banda disponibile.
TSN è una buona opzione per quanto riguarda il passaggio dall'industria 3.0 a 4.0 non sonlo perché funziona meglio e riesce a rappresentare questa idea di pilastro, ma perché ha un costo totale di proprietà inferiore (anche se bisogna cambiare tutti gli switch esistenti).

TSN è un insieme di sub-standard Ethernet IEE 802, ognuno dei quali definisce le specifiche per una distinta funzione TSN.
L'idea è quella di garantire comunicazioni affidabili ad alte prestazioni, con bassa latenza e mimino jitter nel caso di comunicazioni di dati ad alta priorità.
TSN è ancora in corso di lavorazione ma è tuttavia un miglioramento del protocollo Ethernet ereditandone i vantaggi.

Sincronizzazione del tempo → il termine *time-sensitive* è un omaggio al fatto che il tempo giochi un ruolo importante in TSN. Con TSN tutti i dispositivi della rete devono essere sincronizzati per garantire che tutto arrivi in tempo, cioè devono operare in un orario concordato.
TSN può utilizzare una serie di profili per garantire la sincronizzazione degli orologi:

- *Precision Time Protocol PTP*: tutti i dispositivi compatibili utilizzano il Best Master Clock Algorithm per identificare il dispositivo con l'orologio più preciso, al quale verranno sincronizzati tutti gli altri dispositivi. (= Master dei clock)
- *Protocolli IEEE 1588*, per restringere le opzioni possibili e fornire un'implementazione specifica per i casi d'uso.

2 - Gestione del traffico → il TSN utilizza diversi meccanismi di pianificazione per coordinare attentamente le comunicazioni attraverso la rete. L'idea è quella di garantire un jitter (ritardi) basso.

Uno dei meccanismi più utilizzati è quello dello **Scheduler Time-Aware** che aiuta a prevenire colli di bottiglia nella trasmissione dei dati e minimizza l'effetto di accomodamento nella trasmissione degli switch Ethernet che contribuisce alla latenza e al jitter. Per ridurre al minimo la latenza e soprattutto il jitter, le code di trasmissione negli switch Ethernet sono idealmente vuote quando il traffico ad alta priorità passa.
Poiché si dispone di un solo cavo Ethernet bisogna pensare a un metodo per garantire che i pacchetti time-critical arrivino in un momento in cui la rete viene considerata vuota: questo si fa attraverso dei "cancelli" (interruttori chiamati *Time-Aware Gate*) per la trasmissione dei dati che garantiscono che il traffico ad alta priorità non venga interrotto lungo il percorso. Quindi ci sono dei dispositivi terminali che devono sapere quando i gate della trasmissione si stanno aprendo negli interruttori in modo da poter temporizzare la trasmissione di telegrammi ad alta priorità.
Tutti i frame Ethernet all'interno di ogni switch vengono elaborati fino a raggiungere i gate di trasmissione, dove i frame in ogni coda devono attendere fino all'apertura della rispettiva porta di trasmissione, che a sua volta è determinata dalla lista di controllo della porta. L'elenco di controllo della porta è ciò che l'utente della rete deve configurare affinché gli switch funzionino come previsto e per aprire le porte corrette nel momento giusto.

Ovviamente le reti che utilizzano Time-Aware Scheduler non sono più plug-and-play (come Ethernet) ma devono essere configurate.

Infine, non tutte le applicazioni richiedono la latenza e il jitter bassi quindi è possibile prendere in considerazione anche altre opzioni di pianificazione. Per questo sono stati sviluppati ulteriori standard, come **IEE 802.1Qch-2017 (accodamento)**. Questo approccio fornisce meno accuratezza di latenza e jitter rispetto a Time-Aware Scheduler, ma richiede uno sforzo di configurazione molto inferiore. L'idea è quella in cui l'accodamento e l'inoltro ciclico dei messaggi garantiscono la trasmissione dei frame per un solo hop (salti tra switch) di rete per ciclo. Il vantaggio è che non è necessario configurare intervalli di tempo all'interno del ciclo. Se si conosce il numero di hop di rete lungo il percorso di comunicazione e la lunghezza del ciclo, il calcolo della finestra del tempo di arrivo è relativamente semplice. In sostanza non posso avere un orario preciso ma posso avere un'idea di quello che è il caso peggiore.

Oltre all'utilità Time-Aware Scheduler e all'accodamento, gli standard specificano un numero di utilità di pianificazione (shaper del traffico) per diversi scenari applicativi. Un **traffic shaper** è uno strumento che influenza direttamente i flussi di dati attraverso una rete.
Una possibilità è uno shaper di **IEEE802.1Gav-2009** progettato come standard AVB (Audio Video Bridging) prima di TSN, basato su un "credito" per distribuire uniformemente i fotogrammi per la trasmissione audio e video nel tempo, che mi consente in pratica una trasmissione costante senza ritardi, più armoniosa.

Nella maggior parte dei casi, tutti questi metodi potrebbero essere utilizzati e combinati nella rete, tuttavia la loro combinazione richiede sforzi di configurazione per tutti i dispositivi e l'aggiunta di sistemi automatizzati di configurazione per la rete.

3- Comunicazione affidabile → il TSN deve garantire una comunicazione affidabile. il TSN viene spesso definito come Ethernet deterministico, il che significa che la rete è prevedibile. La sincronizzazione e la pianificazione di TSN sono molto importanti e consentono di ottenere Ethernet deterministico. Questi standard non sono correlati alla sincronizzazione e alla pianificazione ma soddisfano diversi requisiti per la tolleranza agli errori e la protezione del traffico.
- In alcuni casi, se un frame è troppo grande, potrebbe non essere finito alla fine del ciclo assegnato ma potrebbe andare a sovrapporsi all'inizio del ciclo successivo o all'invio dei messaggi a priorità più alta. In una situazione come questa si potrebbe perdere il determinismo della rete. Per evitare ciò il Time-Aware Scheduler utilizza una banda di guardia, che blocca il grande frame in modo che venga eseguito all'inizio del ciclo successivo. Ha uno svantaggio in quanto questa banda di guardia blocca tutti i frame a priorità più bassa, sprecando una parte di larghezza di banda. Quindi quello che fa TSN è ottimizzare la banda: invece di evitare l'invio del frame può ad esempio dividere un frame (grande) in pacchetti più piccoli.

Ridondanza per la tolleranza ai guasti → In generale è fondamentale che le trasmissioni siano affidabili, ancora più importante per le comunicazioni mission-critical su reti sensibili al fattore tempo. In generale le reti utilizzano vari protocolli di ridondanza, che si basano sul consentire alla rete di recuperare automaticamente l'errore, quindi di non avere un operatore che deve controllare e riconfigurare la rete. Un'idea è che i protocolli di ridondanza funzionano utilizzando diversi percorsi di trasmissione secondari attraverso la rete per mantenere la comunicazione mentre il percorso principale viene riparato. I protocolli di ridondanza sono generalmente raggruppati in:

- ***Ridondanza senza interruzioni*:**
  TSN può utilizzare esempio **HSR** o **PRP** e altri standard di IEEE 1CB-2017 che basano sulla trasmissione simultanea di frame su percorsi di trasmissione disgiuntivi. Ogni volta che viene inviato un frame mission-critical, viene duplicato e instradato su almeno due percorsi ridondanti. Quando i frame duplicati arrivano a destinazione, uno viene accettato e l'altro viene eliminato. Se un percorso di comunicazione fallisce, l'altro è in grado di sostenere l'applicazione senza interruzioni.
- ***Ridondanza non interrotta*** (failover): non tutte le applicazioni TSN richiedono ridondanza continua. Potrei avere meccanismi di ridondanza in cui sono accettate delle interruzioni come nel Rapid Spanning Tree, che consentono

comunque di considerare altri percorsi.
In un contesto TSN, oltre ai tempi di latenza e jitter vengono considerati anche i tempi di ripristino della rete in caso di guasto.
Se il tempo di ripristino del protocollo ridondante è inferiore alla latenza massima tollerata, il protocollo può essere utilizzato in un contesto TSN per proteggere l'applicazione in esecuzione. Anche quando il tempo di ripristino del protocollo di ridondanza è superiore alla latenza massima tollerata dell'applicazione, il protocollo di ridondanza può essere ancora utilizzato.

Uno degli aspetti principali quando si parla di TSN sono le problematiche relative alla **costruzione e la sicurezza**. TSN Ethernet non è più plug-and-play e ha bisogno di essere configurato. Gli switch TSN e i dispositivi finali devono essere abilitati e configurati per sincronizzare strettamente le comunicazioni tra dispositivi. La configurazione include l'abilitazione dei meccanismi TSN, come la sincronizzazione dell'ora e il Time-Aware Scheduler quindi la regolazione dei tempi di ciclo delle fasce orarie, delle priorità dei fotogrammi e di altri parametri in base ai requisiti dell'applicazione.
La differenza tra Ethernet plug-and-play e TSN è malamente vista come un problema, è anche vero che dipende dal tipo di configurazione che va fatta. TSN aumenta la configurazione necessaria per far funzionare una rete, ma offre anche molti vantaggi.
Il primo passo per costruire una rete TSN è scegliere il modello di configurazione TSN che si desidera seguire. Si hanno 3 scelte:

1. **Centralizzato**: abbiamo due oggetti, uno trasmette e l'altro riceve con all'interno degli switch TSN. Si ha un'unità centrale (Central User Configuration) e una Centralized Network Configuration). Il CUC aggrega tutte le informazioni e i requisiti dei dispositivi, il CNC assembla tutte le informazioni dall'infrastruttura di rete (come il numero degli switch, la topologia, la largehzza di banda presente ecc). Allora il CUC calcola una configurazione di rete che ospita tutti i dispositivi finali e trasferisce la configurazione all'infrastruttura di rete attraverso il CNC. Se CUC non è in grado di calcolare una configurazione di rete che soddisfi tutti i requisiti TSN dell'applicazione, comunica all'utente l'errore.
   Il vantaggio è che supporta grandi infrastrutture di rete con movimento dinamico della rete;
   Lo svantaggio è che richiede un'infrastruttura dedicata che ospita CNC e CUC.
2. **Decentralizzato**: nel modello TSN decentralizzato, i dispositivi terminali trasmettono i loro requisiti per l'invio e la ricezione di flussi di comunicazione al primo switch TSN a cui sono connessi. Questo switch riceve le informazioni, le valuta e la distribuisce attraverso la rete attraverso qualsiasi altro switch. Quindi la configurazione avviene in maniera autonoma tra i diversi switch. Questo approccio ha il netto vantaggio che richiede una configurazione manuale minima o nulla e si avvicina di più ad un approccio plug-and-play. Lo svantaggio è che su reti più grandi i conflitti tra i requisiti di diversi dispositivi e flussi diventano sempre più difficili da risolvere. Inoltre, non ha un CUC o CNC per coordinare le attività tra i dispositivi.
3. **Ibrido**: è l'idea di combinare i modelli mantenendone i vantaggi. Il vantaggio del modello ibrido è che i dispositivi terminali devono supportare solo un protocollo di configurazione, sebbene l'utente abbia il vantaggio di una vista di rete centralizzata (CNC) proprio come il modello centralizzato.

Mescolare Ethernet TSN e non TSN → TSN è completamente retrocompatibile con Ethernet.
I dispositivi con capacità TSN possono essere collegati a dispositivi Ethernet-non-TSN e viceversa senza la necessità di protocolli di conversione o gateway. Tuttavia, quando utilizziamo una rete mista, con dispositivi TSN e non, non possiamo più garantire determinismo.

- Quando abbiamo **reti parzialmente conformi** il vantaggio è che non si deve cambiare tutta la rete ma solo in parte. Ma è anche vero che tutti i vantaggi che si hanno con TSN diminuiscono dalla presenza di elementi che non garantiscono il determinismo.
- **Integrazione con altre soluzioni Ethernet?**
  TSN non può sostituire le soluzioni di fornitori consolidati perché queste applicazioni dispongono di protocolli che non rientrano nell'ambito di applicazione di TSN.
  Le soluzioni Ethernet industriali esistenti possono però beneficiare delle tecnologie TSN come tecnologia di trasporto.

Per quanto riguarda la **sicurezza** TSN non include specificamente i meccanismi di sicurezza informatica poiché la sicurezza non rientra nell'ambito di base di Ethernet. TSN però, presenta nuove *superfici di attacco*, cioè la possibilità di poter attaccare diversi e maggiori elementi rispetto Ethernet. Il problema principale è quello della sincronizzazione temporale, poiché un attacco a questo distrugge completamente TSN, che non può funzionare senza orologi sincronizzati.
Un altro aspetto è che molti meccanismi di sicurezza nel mondo IT introducono ulteriore latenza e jitter nelle reti (ad esempio i firewall), che potrebbe essere inaccettabile per il mondo industriale.
Fortunatamente sono disponibili metodi per proteggere le reti, uno degli approcci è il protocollo **IEC 62443** che divide le reti sensibili e industriali in:

- **Zone**: è un gruppo di dispositivi fisici o logici che condividono requisiti di sicurezza comuni.
- **Condotti**: è un percorso di comunicazione che conduce dentro o fuori una zona.

Per garantire che nessun dispositivo possa sovraccaricare una rete TSN lo standard (IEC 62443) specifica un insieme di funzioni di supervisione sulle porte degli switch TSN di filtraggio e controllo per flusso, che consentono di monitorare se un dispositivo finale si comporta correttamente o sta consumando una larghezza di banda eccessiva. In caso di comportamento scorretto lo switch può eliminare completamente il traffico o arrestare l'accesso per il malfunzionamento.

Riassumendo tutte le caratteristiche di TSN:

TSN è un Ethernet Plus → TSN non è una nuova tecnologia quanto più un aggiornamento di Ethernet (che funziona perfettamente nel mondo classico ma non nel mondo industriale) in cui si aggiungono le tempestive garanzie di consegna che mancavano in Ethernet.

TSN è retrocompatibile → Continua la tradizione Ethernet di rimanere retrocompatibile con le tecnologie precedenti; non è necessario installare gateway speciali o protocolli di traduzione per farlo funzionare in un ambiente esistente.

In TSN il tempismo è tutto → si occupa strettamente di sincronizzare le attività su una rete, quindi la tempistica è fondamentale, come si riflette nei due requisiti di TSN più importanti:

- Sincronizzazione dell'ora che devono concordare tutti i dispositivi
- Pianificazione in tempo reale: è necessario garantire la latenza (il tempo richiesto per il trasferimento di dati dal punto di partenza al punto di destinazione) per garantire che i dati arrivino in tempo.

Ovviamente migliore è la sincronizzazione, migliore è la pianificazione e più efficiente sarà la rete.

TSN è modulare → TSN non è un singolo standard ma una raccolta di vari standard. Alcuni protocolli nascono per altri motivi. I produttori di dispositivi possono implementare gli standard in modo selettivo, a seconda del caso d'uso del dispositivo, ma devono dichiarare quali standard ogni dispositivo supporta.

La configurazione è fondamentale → sebbene Ethernet sia progettato per essere plug-and-play, TSN non lo è. È necessario, infatti, configurare i dispositivi TSN per coordinare attentamente le loro operazioni di invio e ricezione. Su reti più piccole la configurazione manuale potrebbe essere una opzione; su reti più grande di solito è necessario un meccanismo per automatizzare il processo di configurazione (dipende anche dall'architettura scelta).

TSN è l'ideale per applicazioni industriali → TSN nasce per funzionare nelle applicazioni industriali, quindi, consente comunicazioni tempestive tra tutti i sensori, attuatori e macchinari. E quindi lo rende ideale per le applicazioni di automazione industriale e automazione di veicoli. Oltre che ovviamente in qualsiasi applicazione che richieda una trasmissione affidabile di diverse priorità di traffico su una singola rete (stesso approccio di 5G).

Latenza garantita → ciò che è importante in TSN è garantire latenze e tempi di jitter specifiche in modo che i dati vengano consegnati esattamente quando previsto.

TSN può funzionare su dispositivi non TSN → Ethernet-TSN può funzionare anche su reti combinate, quindi anche non-TSN e può migliorare le prestazioni generali di qualsiasi rete Ethernet anche se uno o più dispositivi terminali non lo supportano. L'idea è quella per cui TSN riesce a garantire latenze predefinite tra i dispositivi e benché la rete ethernet non sia ottimizzata per TSN beneficerà comunque di comunicazioni più efficienti su parti della rete.

TSN introduce problematiche di sicurezza → poiché TSN si basa molto sulla sincronizzazione e sulla programmazione dell'orario, e introduce quindi problemi di sicurezza esclusivi, tra cui:

- partecipanti malintenzionati sulla rete potrebbero introdurre frame di dati aggiuntivi o modificare le priorità dei frame per interrompere o ritardare il traffico mission-critical
- le misure di sicurezza stesse potrebbero eliminare i tempi consumando cicli aggiuntivi di CPU necessari per garantire l'elaborazione tempestiva di frame di dati

-> è importante che siano utilizzate le migliori tecnologie e pratiche per la protezione delle reti TSN

Miglioramento delle soluzioni esistenti → Attraverso piccole modifiche specifiche TSN può interagire con soluzioni Ethernet Real Time specifiche del produttore (EtherCAT, profinet…) questa flessibilità consente il suo utilizzo per migliorare i sistemi senza doverli sostituire completamente.