

Le logiche per la gestione della sicurezza delle macchine

di *Gianfranco Ceresini*

Aggiornato al:

1 Logica di sicurezza

Dopo aver studiato nelle guide precedenti l'analisi del rischio, la progettazione della macchine e i dispositivi di protezione utilizzabili come parte sensoristica di sicurezza, andiamo ora a parlare di un'altra parte fondamentale per la costruzione di un'efficace funzione di sicurezza su una macchina: la logica di controllo.

I dispositivi logici giocano un ruolo centrale nei circuiti di comando di sicurezza: infatti effettuano il controllo e il monitoraggio del sistema di sicurezza e consentono l'avviamento della macchina od eseguono i comandi per il suo arresto.

Esiste un'ampia gamma di dispositivi logici in grado di creare un'architettura di sicurezza rispondente alla complessità e alla funzionalità di ogni macchina. Ad esempio, i **piccoli relè di sicurezza** cablati sono più economici e quindi adatti alle macchine più piccole in cui, i **relè di sicurezza modulari** e configurabili sono preferibili dove è necessario un maggior numero di dispositivi di protezione ed un minimo controllo di zona. Le macchine medio/grandi e più complesse devono invece essere gestite da sistemi programmabili (PLC convenzionali o **PLC di sicurezza**) con I/O distribuiti.



Figura 1 – Relè di sicurezza (Sick), Relè di sicurezza modulare (Phoenix Contact) e PLC di sicurezza (Mitsubishi)

In figura 1-b viene sintetizzato in un flow-chart decisionale quale può essere la scelta migliore tra i diversi tipi di logica di sicurezza in base ad una serie di parametri quali il numero di ingressi, le esigenze di comunicazione, la categoria, il software, ecc. I punti indicati nel flow-chart hanno il significato indicato in seguito.

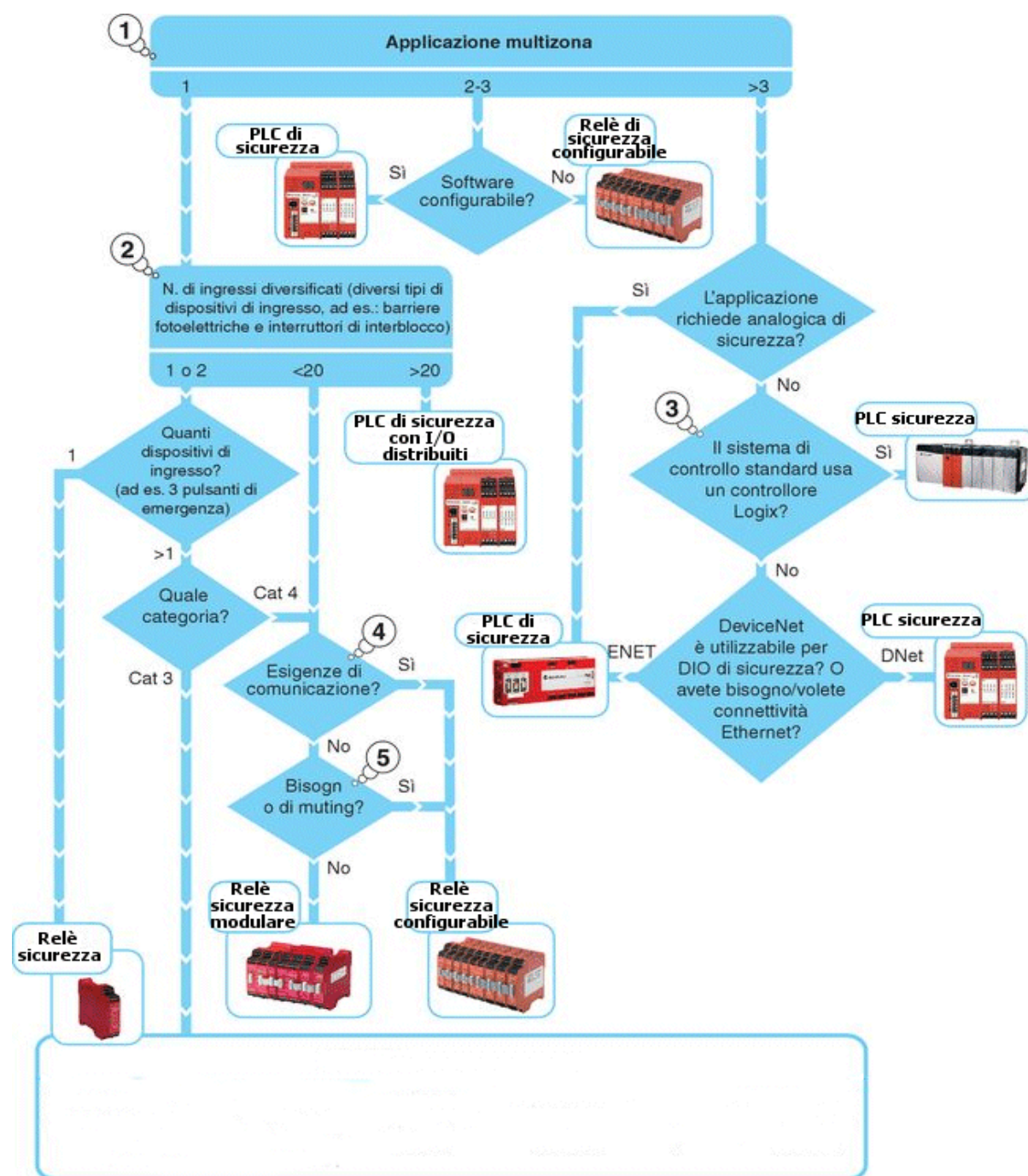


Figura 1-b – Criteri di selezione della logica di sicurezza (Rockwell)

1. **E' una applicazione multizona?** Per conformarsi alle norme di sicurezza e salvaguardare la produttività, i costruttori di macchine hanno iniziato ad integrare nelle macchine caratteristiche di sicurezza funzionale, mediante quello che è stato denominato concetto di "zona." Il concetto di "zona" aumenta sia la sicurezza che la produttività permettendo ad una parte della linea di produzione di rallentare o fermarsi mentre il resto della linea continua a lavorare normalmente. Il pericolo per la sicurezza, in presenza di un blocco o di una anomalia minore delle apparecchiature in linea, può essere eliminato o corretto senza fermare tutta la linea, ovviando a lunghi fermi di produzione e tempi di inattività dei lavoratori. Quando il pericolo viene eliminato, la linea può rapidamente tornare al normale funzionamento. I sistemi con relè a singola funzione e/o espandibili sono adatti solo per il controllo di una singola zona, mentre il controllo multizona per 2...3 zone di un sistema configurabile, quale i relè modulari o preconfigurabili. Per qualunque applicazione che coinvolge il controllo di più di tre zone (con una logica, quindi, più complessa), è più adatto un PLC di sicurezza.
2. **Ingressi diversificati – Numero e tipo:** Per le applicazioni monozona e multizona (< 3 zone), saranno il numero ed il tipo di ingressi (ad es. interruttori di interblocco, pedane di sicurezza, barriere fotoelettriche) a dettare l'uso di relè di sicurezza o di un piccolo controllore di sicurezza preconfigurato. Per 1...2 ingressi, i relè di sicurezza dedicati rappresentano una soluzione semplice e conveniente ma, per le applicazioni che prevedono un alto numero di dispositivi di ingresso, il cablaggio associato ai singoli relè può risultare limitativo. Quindi, in applicazioni che richiedono un limitato numero di dispositivi di ingresso (20 o meno), un sistema di relè espandibile a progettazione modulare e collegamenti plug-in è la soluzione ideale. In ogni caso con i relè di sicurezza, saranno i dispositivi di ingresso utilizzati a decidere i moduli relè da selezionare; quindi, la selezione dei relè per una ampia gamma di dispositivi di ingresso può essere complessa. Le applicazioni che richiedono più di 20 ingressi differenti ed una logica complessa sono maggiormente gestibili con un controllore combinato ad I/O distribuiti. Per le Installazioni più grandi – quelle con un alto numero ed una ampia serie di dispositivi di ingresso – è più adatto un sistema di PLC di sicurezza, dato che la loro capacità di programmazione permette di risolvere le applicazioni di sicurezza mediante il software anziché con sistemi di relè a cascata da cablare.
3. **Il sistema di controllo standard usa un controllore Logix?** Un sistema di controllo di sicurezza può essere un sistema dedicato (solo sicurezza) o integrato, in cui il controllo standard e quello di sicurezza sono combinati per massimizzare il riutilizzo di componenti e strumenti. Un controllore di sicurezza Logix apporta i vantaggi di una piattaforma Logix, ambiente di programmazione comune, reti comuni e comune motore di controllo, e di un controllo di sicurezza integrato, in un ambiente facile da usare che, tra l'altro, consente di raggiungere un SIL 3.

4. **Esigenze di comunicazione?** Un sistema di comunicazione integrato permette al relè di fornire lo stato delle uscite e degli errori attraverso RS232/RS485 o una rete di bus di campo (come DeviceNet ed Ethernet) ad una interfaccia operatore o altro dispositivo. I relè di sicurezza modulari offrono compatibilità a livello di comunicazioni. I controllori di sicurezza programmabili offrono connettività di rete ed un alto livello di diagnostica.
5. **Bisogno di muting?** Talvolta, il processo richiede che la macchina si arresti quando il personale entra nella zona ma che resti in funzione quando il materiale alimentato entra o esce – questa è una tipica situazione in cui è necessaria una funzione di muting. Il muting ha bisogno di una barriera fotoelettrica, di due o quattro sensori di muting e di una unità di controllo per elaborare i segnali e determinare se e quando attivare la funzione di muting. I sensori di muting sono montati davanti e dietro la barriera fotoelettrica e solo una specifica sequenza di uscite dei sensori permetterà di attivare la funzione di muting. Per esempio, quando i due sensori davanti alla barriera fotoelettrica cambiano stato in un determinato periodo di tempo, la barriera fotoelettrica viene “silenziata” e non invia un segnale di arresto alla macchina all’entrata del materiale. A volte i relè di sicurezza modulari includono un modulo appositamente sviluppato per controllare la funzione di muting nelle applicazioni che non hanno specifici requisiti di sequenziamento o temporizzazione. Il muting del relè potrebbe anche essere impostato con il software di configurazione.



Figura 1-c – PLC di sicurezza (Allen-Bradley)

La seguente tabella costituisce, in alternativa al precedente flow-chart, una guida che può essere utile nello scegliere la migliore soluzione. Dati i diversi tipi di protezione previsti per le macchine, per fornire una adeguata protezione ad una macchina o ad un sistema di produzione particolare, è possibile creare un sistema ibrido o una combinazione di architetture.

Caratteristiche	Architettura
Complessità dell'applicazione	
Bassa	Relè dedicati
Media	Relè dedicati o espandibili
Elevata	PLC di sicurezza
Comunicazione	
Stato	Relè espandibili
Controllo	PLC di sicurezza
Diagnostica	
Bassa	Relè dedicati
Media	Relè espandibili
Elevata	PLC di sicurezza
Espandibilità	
Bassa	Relè dedicati
Media	Relè espandibili
Elevata	PLC di sicurezza
Tipi di ingresso	
Speciale	Relè dedicati o PLC di sicurezza
Comune	Relè dedicati o espandibili
Numero di I/O	
Basso	Relè dedicati
Medio	Relè espandibili
Elevato	PLC di sicurezza
Localizzazione I/O	
Contenuta	Relè dedicati o espandibili
Diffusa	PLC di sicurezza
Spegnimento sequenziale	
Nessuno	Relè dedicati o espandibili
Sì	PLC di sicurezza
Controllo di zona	
Poche	Relè dedicati o espandibili
Molte	PLC di sicurezza

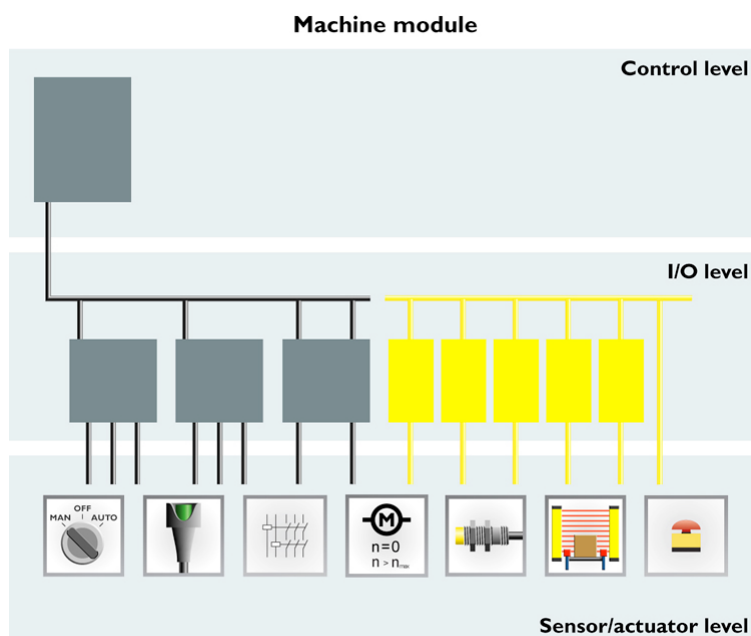
Confronto tra le possibili architetture di un sistema di sicurezza

Moduli di sicurezza elettromeccanici

Le applicazioni strutturate con poche funzioni di sicurezza, ad esempio una macchina per la lavorazione con un controllo finecorsa ripari e un tasto di arresto d'emergenza, dovrebbero essere realizzate con le apparecchiature di sicurezza classiche.

Caratteristiche tipiche di questa architettura di sistema:

- separazione classica tra sistema di sicurezza e comando delle funzioni
- rete e periferia I/O diverse

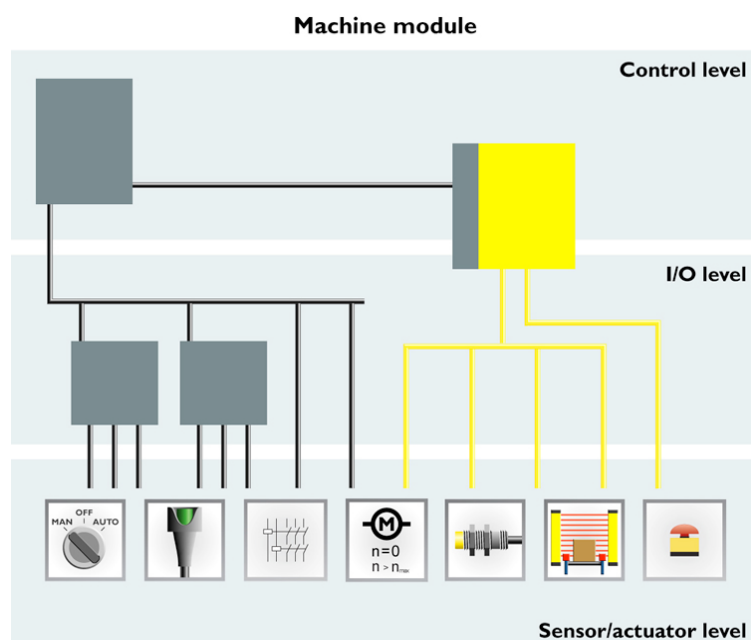


Moduli di sicurezza configurabili

Con l'aumento delle dimensioni degli impianti non cresce solo la quantità delle funzioni di sicurezza; spesso è necessario avere anche altre caratteristiche come l'attivazione/disattivazione temporanea di singoli moduli.

Caratteristiche tipiche di questa architettura di sistema:

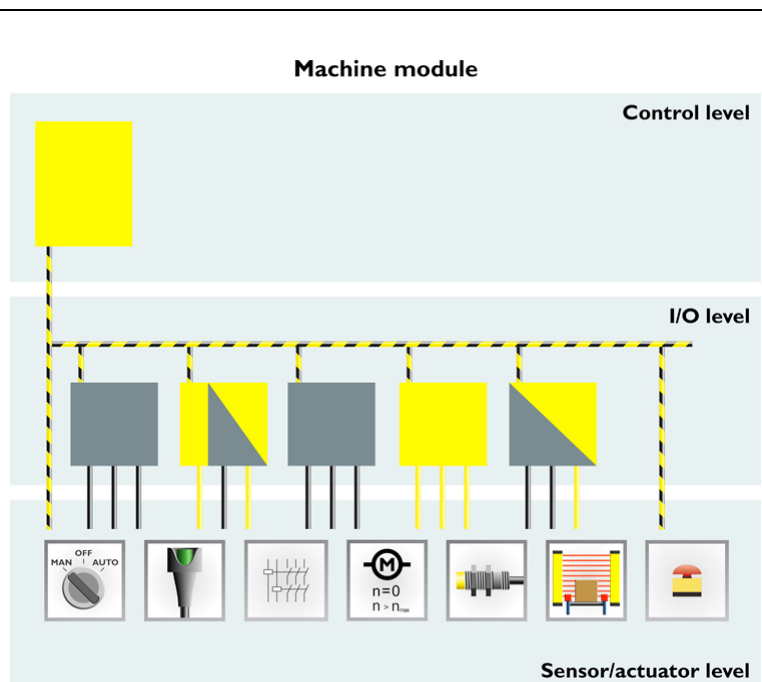
- separazione classica tra sistema di sicurezza e comando delle funzioni
- rete comune per la comunicazione non sicura
- periferia I/O diversa



Moduli I/O di sicurezza

Nelle applicazioni di medie e grandi dimensioni vengono rilevati e generati anche i segnali di sicurezza mediante sistemi bus. Distribuiti in queste reti, i moduli I/O di sicurezza comunicano con il sistema di sicurezza e vengono adattati all'applicazione grazie a una parametrizzazione flessibile. Caratteristiche tipiche di questa architettura di sistema:

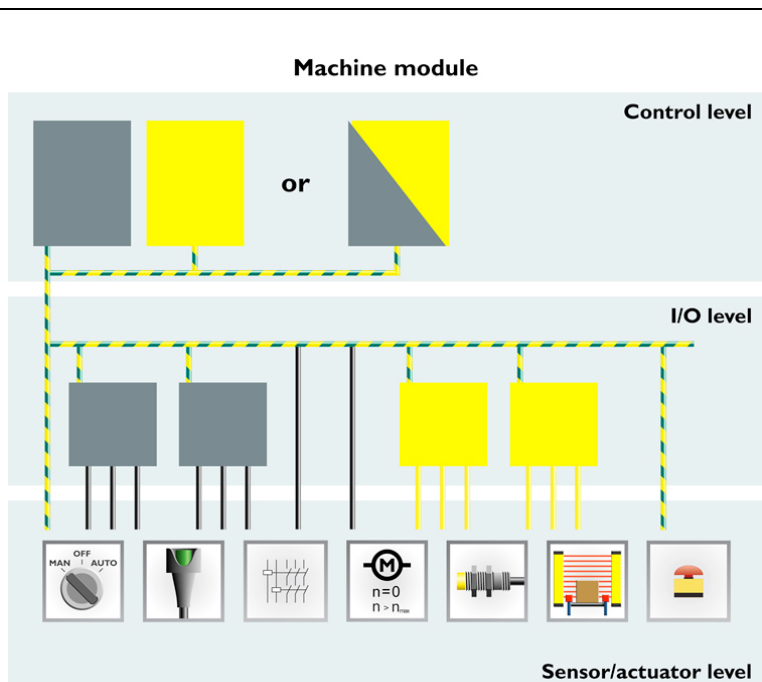
- moduli I/O standard sicuri decentralizzati in combinazione con il sistema di sicurezza
- sistema di comunicazione comune per componenti standard e di sicurezza mediante un bus di campo



Sistemi di sicurezza programmabili

Se si tratta di un'applicazione estesa e non è più possibile gestire il numero delle funzioni di sicurezza con le tecnologie descritte, la scelta migliore sono i PLC di sicurezza in combinazione con un sistema bus sicuro. Sono disponibili due diversi tipi di soluzioni:

1. da un lato vengono offerti sistemi di sicurezza a distanza, quindi separati dal controllore standard, con una rete propria sicura da installare separatamente, una soluzione che aumenta considerevolmente i costi e il tempo necessari.
2. La seconda soluzione integra il controllore sicuro in quello standard e utilizza la rete già esistente per comunicare con le utenze sicure. Nella pratica questa procedura si è rivelata la versione tecnicamente più adeguata ed economicamente migliore.



Caratteristiche tipiche di questa architettura di sistema:

- diversi gradi di integrazione possibili
- sistema di comunicazione comune per componenti standard e di sicurezza

2 Relè (o moduli) di sicurezza

I moduli di monitoraggio con relè di sicurezza (MSR) svolgono un ruolo centrale in molti sistemi di sicurezza. Questi moduli sono generalmente costituiti da due o più relè con contatti a guida forzata e con circuiteria addizionale per garantire le prestazioni della funzione di sicurezza. La guida meccanica (guida forzata) provoca come conseguenza l'impossibilità di chiudere contemporaneamente i contatti ad apertura ed i contatti a chiusura nemmeno in caso di guasto. I relè a guida forzata devono rispondere ai requisiti prestazionali della norma CEI EN 50205. Concezioni più recenti sostituiscono le uscite elettromeccaniche con uscite di sicurezza allo stato solido.

I relè di sicurezza realizzano diversi controlli sul sistema di sicurezza. All'accensione, effettuano l'autodiagnostica sui propri componenti interni. Quando i dispositivi di ingresso sono attivati, il relè confronta i risultati degli ingressi ridondanti. Se accettabili, l'MSR controlla gli attuatori esterni. Se il risultato è positivo, l'MSR attende un segnale di reset per eccitare le sue uscite.

La selezione del relè di sicurezza più appropriato dipende da una serie di fattori: il tipo di dispositivo che deve essere monitorato, il tipo di reset, il numero e il tipo di uscite. In tabella 1 viene indicato come sono gestiti da un relè di sicurezza i vari dispositivi di protezione.

Alcuni relè possono collegarsi a diversi tipi di ingressi ma, una volta scelto il dispositivo, il relè si può interfacciare solo con quel dispositivo. Il progettista deve selezionare un relè che sia compatibile con il dispositivo di ingresso.

Dispositivo di protezione	Cosa fa il modulo di sicurezza
Interruttori elettromeccanici e pulsanti di emergenza: contatti meccanici, a singolo canale con un contatto normalmente chiuso, a doppio canale con entrambi i contatti normalmente chiusi, o a doppio canale, uno normalmente aperto e uno normalmente chiuso.	Il relè deve essere in grado di accettare il singolo o il doppio canale e garantire il rilevamento dei guasti incrociati per la configurazione a due canali
Barriere fotoelettriche, laser scanner, dispositivi senza contatto allo stato solido (es. interruttori magnetici) che hanno due uscite ed effettuano il rilevamento dei propri guasti incrociati.	Il relè deve essere in grado di ignorare il metodo di rilevamento dei guasti incrociati dei dispositivi

Pedane sensibili alla pressione: le pedane creano un cortocircuito tra due canali.	Il relè deve essere in grado di sopportare cortocircuiti ripetuti
Bordi sensibili alla pressione: alcuni bordi sono concepiti come pedane a 4 fili. Alcuni sono dotati di dispositivi a due fili che creano una variazione della resistenza.	Il relè deve essere in grado di rilevare un cortocircuito o la variazione della resistenza
Tensione: misura la forza contro-elettromotrice di un motore durante la decelerazione.	Il relè deve essere in grado di tollerare alte tensioni e di rilevare basse tensioni quando il motore rallenta
Arresto del movimento	Il relè deve rilevare i treni di impulsi da diversi sensori ridondanti
Dispositivo di comando a due mani	Il relè deve rilevare ingressi diversi, normalmente aperti e normalmente chiusi, oltre a fornire la temporizzazione di 0,5 s e la logica sequenziale

Tabella 1 – Gestione degli ingressi da parte di un relè di sicurezza

Un altro fattore importante da considerare è l'impedenza d'ingresso dei relè di sicurezza, la quale determina il numero di dispositivi d'ingresso che possono essere connessi al relè e fino a che distanza essi possono essere montati. Ad esempio, un relè di sicurezza può avere un'impedenza consentita massima di 500 Ohm. Quando l'impedenza d'ingresso è superiore a 500 Ohm, le uscite non vengono attivate. Occorre quindi prestare particolare attenzione per garantire che l'impedenza d'ingresso rimanga al di sotto della massima specificata. L'impedenza d'ingresso dipende dalla lunghezza, dalla dimensione e dal tipo di cavo usato (tabella 2).

Sezione del cavo [mm ²]	Ω per 1000 m
0,5	33,3
0,75	20,95
1,5	13,18
2,5	8,28
4	5,21

Tabella 2 – Resistenza di un cavo di rame usato alla temperatura di 25 °C

Frequenza di controllo dei dispositivi di ingresso

In base alla valutazione del rischio sulla macchina occorre decidere con quale frequenza debbano essere controllati i dispositivi di ingresso collegati al relè di sicurezza per garantire che gli arresti d'emergenza e gli interblocchi della porta siano funzionanti. Ad esempio, per un relè di sicurezza a canale doppio collegato a una porta interbloccata che deve essere aperta a ogni ciclo della macchina (ad esempio più volte al giorno) potrebbe non dover essere necessario nessun controllo. Questo accade perché l'apertura della protezione fa sì che il relè stesso controlli i propri ingressi e uscite (in funzione della configurazione) per verificare la presenza di singoli guasti. Più di frequente viene aperta la protezione, maggiore è l'integrità del processo di verifica.

Ricordiamo che per un'architettura del circuito di sicurezza in categoria 2, la frequenza di richiesta (di un'azione legata alla sicurezza) deve essere $\leq 1/100$ della frequenza di controllo (per rilevare avarie). Il controllo in categoria 2 non può quindi essere un controllo qualunque, ma deve essere cento volte superiore, come frequenza, rispetto a quello di richiesta della funzione di sicurezza. Ad esempio se ogni 100 minuti apro un riparo mobile, significa che almeno 1 volta al minuto devo controllare che la funzione di sicurezza (legata al funzionamento del riparo) stia funzionando correttamente. Questo rende la categoria 2 non applicabile per funzioni quali l'emergenza o le porte interbloccate con dispositivi meccanici: infatti un dispositivo meccanico lo posso controllare solo all'apertura del riparo, quando estraggo la chiavetta dal corpo principale dell'interruttore e il cambio dello stato dei contatti viene controllato dal relè di sicurezza; in questo modo però il rapporto tra richiesta e controllo è di 1 a 1 e non di 1 a 100 come richiesto dalla norma EN 13849-1. La conclusione è che con un dispositivo meccanico non posso più realizzare una categoria 2.

Un altro esempio sono gli arresti di emergenza. Poiché tali arresti sono generalmente usati solo per le emergenze, è probabile che siano usati raramente. Occorre dunque stabilire un programma che verifichi gli arresti di emergenza e ne confermi l'efficienza a intervalli pianificati. Questo modo di verificare il sistema di sicurezza è conosciuto come test funzionale e il tempo tra due verifiche successive è chiamato intervallo tra test funzionali. Quanto detto potrebbe essere valido anche per le porte di accesso per la regolazione delle macchine che, come i pulsanti di arresto di emergenza, vengono utilizzate raramente. Anche in questo caso, dovrebbe essere stabilito un programma per verificarne la funzionalità a intervalli programmati.

La valutazione del rischio aiuta a determinare se i dispositivi di ingresso devono essere controllati e con quale frequenza. Più alto è il livello del rischio, maggiore è la frequenza richiesta al processo di verifica. Minore è la frequenza del comando automatico e maggiore deve essere la frequenza della verifica manuale imposta.

Rilevamento dei guasti incrociati dei dispositivi di ingresso

Nei sistemi a due canali, il sistema di sicurezza deve rilevare i guasti di cortocircuito tra i due canali dei dispositivi di ingresso, chiamati anche guasti incrociati. Questo avviene tramite il dispositivo di rilevamento (se di tipo elettronico) o attraverso il relè di sicurezza.

I dispositivi basati sui microprocessori – come barriere fotoelettriche, laser scanner, i sensori senza contatto (es. magnetici) e appunto i relè di sicurezza – rilevano questi cortocircuiti in molti modi. Un modo usato comunemente è quello di rilevare i guasti incrociati attraverso il test con impulsi diversi (figura 2). Gli impulsi dei segnali di uscita sono molto rapidi. L'impulso del canale 1 è sfasato rispetto a quello del canale 2. Se si verifica un corto, gli impulsi avvengono contemporaneamente e vengono rilevati dal dispositivo.

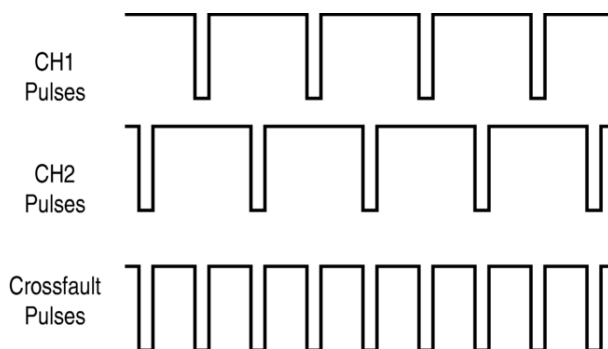


Figura 2 – In caso di guasto incrociato (terza riga di impulsi) gli impulsi dei due canali si sommano
(Allen-Bradley)

I relè di sicurezza elettromeccanici usano un'altra tecnica: un ingresso pull-up (es. + 24 V) e un ingresso pull-down (collegato a terra). Un corto dal canale 1 al canale 2 attiva il dispositivo di protezione dalle sovracorrenti e il sistema di sicurezza procede allo spegnimento (figura 3).

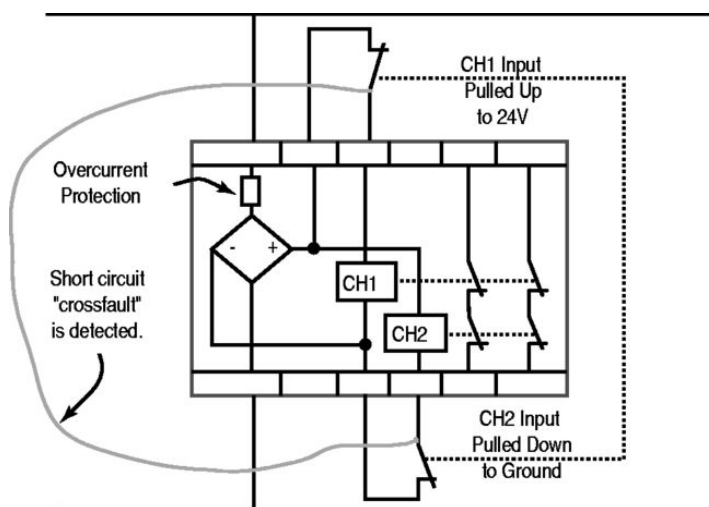


Figura 3 – Diverso modo di rilevare i guasti incrociati (Allen-Bradley)

Uscite

I relè di sicurezza sono disponibili con diversi numeri di uscite. I tipi di uscite aiutano a determinare quale relè usare in determinate applicazioni.

La maggior parte dei relè hanno almeno 2 uscite di sicurezza immediatamente operative. Le uscite di sicurezza sono caratterizzate da contatti normalmente aperti e sono considerate di sicurezza grazie alla ridondanza e al controllo interno. Un secondo tipo di uscita sono le uscite temporizzate usate generalmente negli arresti di Categoria 1 (arresto controllato con l'alimentazione agli attuatori di macchina che rimane a disposizione per raggiungere l'arresto e solo dopo l'arresto avviene il distacco dell'alimentazione), in cui la macchina ha bisogno di tempo per l'arresto prima di permettere l'accesso alla zona pericolosa. La figura 4 mostra i simboli usati per i contatti istantanei (immediate) e ritardati (delayed).

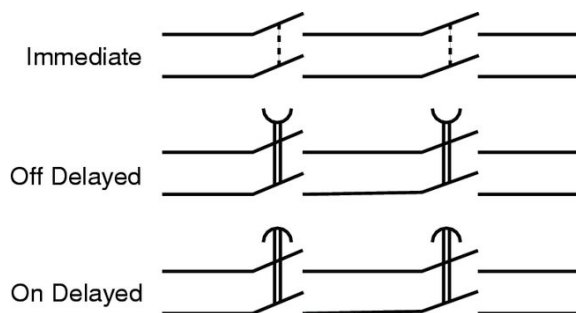


Figura 4 – Simboli per i tipi di contatto di uscita dei relè di sicurezza (Allen-Bradley)

I relè di sicurezza hanno anche uscite ausiliarie. Generalmente si tratta di uscite con contatti normalmente chiusi e sono usati per segnalare al sistema di controllo della macchina che il sistema di sicurezza è spento. La figura 5 mostra tre disposizioni di contatti normalmente chiusi. Il circuito a sinistra permette di utilizzare i contatti normalmente chiusi solo come circuiti ausiliari per segnalare un singolo guasto sul canale 1 o sul canale 2. La disposizione centrale può essere utilizzata come ausiliaria come mostrato in figura, o utilizzata come sicurezza se i contatti vengono connessi in serie. Il circuito a destra mostra i contatti normalmente chiusi in una disposizione ridondante, in modo che possano essere utilizzati in circuiti di sicurezza.

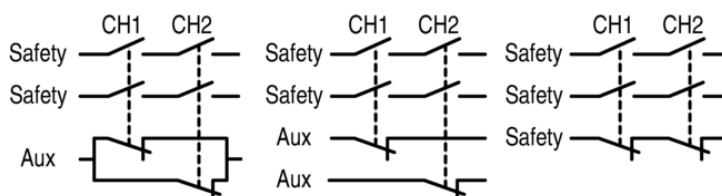


Figura 5 – Contatti normalmente chiusi dei relè di sicurezza usati generalmente come ausiliari (Allen-Bradley)

Caratteristiche delle uscite

Le caratteristiche delle uscite descrivono la capacità del dispositivo di protezione di commutare carichi. Generalmente, le caratteristiche dei dispositivi di carico industriali sono descritte come resistive o induttive. Un carico resistivo può essere un elemento riscaldante. I carichi induttivi sono generalmente relè, contattori o solenoidi che hanno una forte caratteristica induttiva del carico. L'allegato A della norma CEI EN 60947-5-1 (CEI 17-45 - Apparecchiature a bassa tensione Parte 5-1: Dispositivi per circuiti di comando ed elementi di manovra - Dispositivi elettromeccanici per circuiti di comando) descrive le caratteristiche dei carichi (tabella 3).

Designazione	Utilizzo	Corrente termica	Tensione e corrente nominali						VA	
			120V	240V	380V	480V	500V	600V	Chiusura	Apertura
A150	AC-15	10	6	—	—	—	—	—	7200	720
A300	AC-15	10	6	3	—	—	—	—	7200	720
A600	AC-15	10	6	3	1.9	1.5	1.4	1.2	7200	720
B150	AC-15	5	3	—	—	—	—	—	3600	360
B300	AC-15	5	3	1.5	—	—	—	—	3600	360
B600	AC-15	5	3	1.5	0.95	0.92	0.75	0.6	3600	360
C150	AC-15	2.5	1.5	—	—	—	—	—	1800	180
C300	AC-15	2.5	1.5	0.75	—	—	—	—	1800	180
C600	AC-15	2.5	1.5	0.75	0.47	0.375	0.35	0.3	1800	180
D150	AC-14	1.0	0.6	—	—	—	—	—	432	72
D300	AC-14	1.0	0.6	0.3	—	—	—	—	432	72
E150	AC-14	0.5	0.3	—	—	—	—	—	216	36
Corrente continua			125V	250V	—	400V	500V	600V		
N150	DC-13	10	2.2	—	—	—	—	—	275	275
N300	DC-13	10	2.2	1.1	—	—	—	—	275	275
N600	DC-13	10	2.2	1.1	—	0.63	0.55	0.4	275	275
P150	DC-13	5	1.1	—	—	—	—	—	138	138
P300	DC-13	5	1.1	0.55	—	—	—	—	138	138
P600	DC-13	5	1.1	0.55	—	0.31	0.27	0.2	138	138
Q150	DC-13	2.5	0.55	—	—	—	—	—	69	69
Q300	DC-13	2.5	0.55	0.27	—	—	—	—	69	69
Q600	DC-13	2.5	0.55	0.27	—	0.15	0.13	0.1	69	69
R150	DC-13	1.0	0.22	—	—	—	—	—	28	28
R300	DC-13	1.0	0.22	0.1	—	—	—	—	28	28

Tabella 3 - Caratteristiche dei contatti di uscita per la commutazione di un carico induttivo

Le caratteristiche elencate in tabella 3 hanno il seguente significato:

- **Designazione:** è una lettera seguita da un numero, ad esempio A300. La lettera fa riferimento alla corrente termica convenzionale e se la corrente è continua o alternata. Ad esempio, A rappresenta 10 A in corrente alternata. Il numero sta per la tensione di isolamento nominale. Ad esempio, 300 significa 300 V.
- **Utilizzo:** l'utilizzo descrive i tipi di carichi per la cui commutazione il dispositivo è progettato. Ad esempio AC-14 significa controllo di piccoli carichi induttivi (< 72 VA), AC-15 controllo di carichi induttivi di potenza superiore (> 72 VA), DC-13 controllo di elettromagneti.
- **Corrente termica I_{th}:** è il valore della corrente usata per i test di temperatura dell'apparecchiatura, quando è montata in una custodia specificata.
- **Tensione e corrente nominali:** indicano la capacità di chiusura e apertura degli elementi di commutazione in condizioni operative normali.
- **VA:** i valori VA (Tensione x Corrente) indicano i valori nominali degli elementi di commutazione quando si chiude o si apre il circuito. Esempio 1: una caratteristica A150, AC-15 indica che i contatti possono chiudere un circuito di 7200 VA. A 120 V CA, i contatti possono chiudere un circuito con una corrente di spunto di 60 A. Poiché l'AC-15 è un carico induttivo, i 60 A avranno solo una durata limitata come corrente di spunto del carico induttivo. L'apertura del circuito è a soli 720 VA poiché la corrente a regime del carico induttivo è pari a 6 A, ossia la corrente nominale di funzionamento. Esempio 2: una caratteristica N150, DC-13 indica che i contatti possono chiudere un circuito di 275 VA. A 125 V in alternata, i contatti possono chiudere un circuito con un picco di 2,2 A. I carichi induttivi in continua non hanno correnti di spunto come quelli in alternata. L'apertura del circuito è dunque a 275 VA perché la corrente a regime del carico induttivo è pari a 2,2 A, ossia la corrente nominale di funzionamento.

Riavviamento della macchina

Se, ad esempio viene aperto un riparo interbloccato su una macchina in funzione, l'interruttore di interblocco di sicurezza arresta la macchina. Nella maggior parte delle circostanze, è essenziale che la macchina non si riavvii immediatamente dopo la richiusura del riparo. Uno dei modi più comuni per ottenere questo risultato è affidarsi a un contattore con autoritenuta (figura 6).

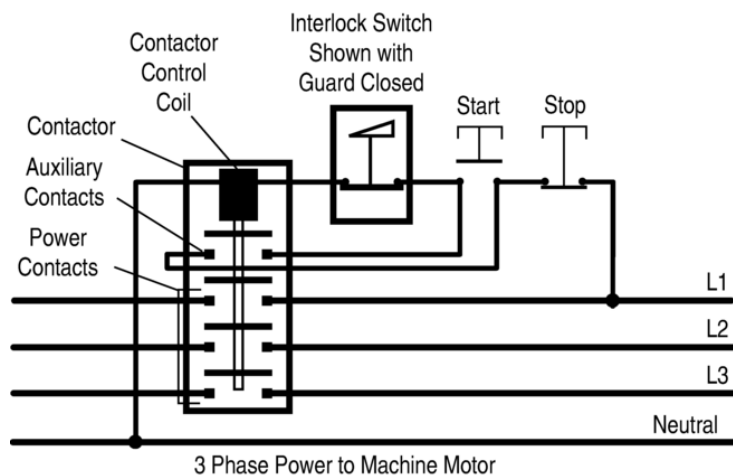


Figura 6 – Semplice circuito di interblocco per evitare il riavvio automatico della macchina alla chiusura del riparo (Allen-Bradley)

La pressione e il rilascio del pulsante di avvio eccita momentaneamente la bobina di controllo del contattore che chiude i contatti di alimentazione. Finché l'alimentazione è presente tra i contatti, la bobina di controllo rimane eccitata (a ritenuta elettrica) tramite i contatti ausiliari del contattore, accoppiati meccanicamente ai contatti dell'alimentazione. Qualsiasi interruzione dell'alimentazione principale o di controllo ha come risultato la diseccitazione della bobina e l'apertura dei contatti dell'alimentazione principale e ausiliaria. L'interblocco del riparo mobile è collegato al circuito di controllo del contattore. Questo significa che il riavvio può essere effettuato solo chiudendo la protezione e quindi impostando su ON il pulsante di avvio, resettando così il contattore e avviando la macchina.

I requisiti per le normali situazioni di interblocco sono definiti dalla direttiva macchine e dalla relativa norma armonizzata EN ISO 14121-1 – Sicurezza del macchinario, principi per la valutazione dei rischi, la quale afferma che “quando la protezione è chiusa, le funzioni pericolose della macchina coperte dalla protezione possono operare grazie ad essa, ma la sola chiusura della protezione non attiva il loro funzionamento”. Molte macchine sono già dotate di contattori singoli o doppi che funzionano nel modo descritto precedentemente (o hanno un sistema che ottiene lo stesso risultato). Quando si installa un interblocco su una macchina esistente è necessario determinare se il sistema di controllo dell'alimentazione risponde a tali requisiti e, se necessario, attuare ulteriori misure.

Funzioni di reset

I relè di sicurezza sono spesso dotati di reset manuale monitorato o reset automatico/manuale. Un reset manuale monitorato richiede la chiusura e l'apertura di un circuito dopo che il riparo mobile è stato chiuso o dopo aver resettato l'arresto di emergenza. La figura 7 mostra tale configurazione.

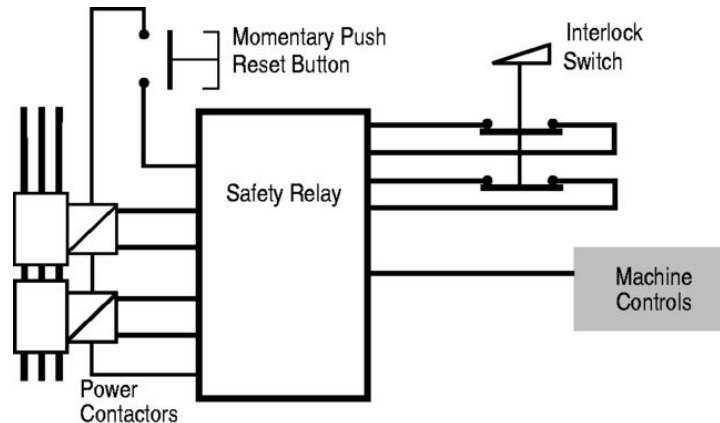


Figura 7 – Reset manuale monitorato (Allen-Bradley)

I contatti ausiliari normalmente chiusi dei contattori di potenza sono connessi in serie con un pulsante “momentaneo”. Una volta che la protezione è stata aperta e chiusa di nuovo, il relè di sicurezza non consente alla macchina di essere riavviata finché il pulsante di reset non sia stato premuto e rilasciato. A questo punto, il relè di sicurezza controlla che entrambi i contattori siano su OFF e che entrambi i circuiti di interblocco (e quindi i ripari) siano chiusi. Se questi controlli sono soddisfacenti, la macchina può essere riavviata con i normali comandi. L'interruttore di reset deve essere posizionato in un luogo che consenta di vedere bene il pericolo, in modo che l'operatore possa controllare che non siano presenti rischi prima di utilizzare la macchina.

Alcuni relè di sicurezza sono dotati invece di un reset automatico/manuale. La modalità di reset manuale non è monitorata e il reset avviene quando il pulsante è premuto. Un cortocircuito o un blocco nel pulsante di reset non viene rilevato. In alternativa, la linea di reset può essere ponticellata, consentendo un reset automatico. L'utente deve quindi fornire un altro meccanismo per evitare l'avviamento della macchina quando la porta si chiude.

Un dispositivo di reset automatico non richiede un'azione di commutazione manuale, ma dopo la disattivazione eseguirà sempre un controllo di integrità del sistema prima di resettare il sistema. Un sistema di reset automatico non deve essere confuso con un dispositivo senza sistemi di reset. In questi, infatti, il sistema di sicurezza sarà attivato immediatamente dopo la disattivazione, ma non sarà effettuato alcun controllo di integrità del sistema.

In sintesi si può affermare che i relè di sicurezza dedicati sono utilizzati per specifiche applicazioni utilizzando moduli di controllo preconfigurati concepiti per interfacciare dispositivi di sicurezza comuni quali pulsanti di emergenza, cancelli di sicurezza, barriere fotoelettriche e pedane di sicurezza. Alcuni relè dedicati forniscono funzioni speciali come temporizzazione, controllo a due mani, muting e attivazione del dispositivo di rilevamento accesso. Essendoci molti tipi di dispositivi di ingresso e funzioni, sono molti anche i tipi di relè di monitoraggio di sicurezza dedicati. I relè di monitoraggio di sicurezza dedicati sono in grado di fornire diagnostica di base mediante LED sul pannello frontale e sono dotati di contatti ausiliari che possono essere collegati a PLC o indicatori luminosi. Le architetture dei sistemi con relè di sicurezza dedicati sono generalmente utilizzate nelle applicazioni a medio ed alto rischio.

E' da osservare che se il rischio è ancora più basso, una funzione di sicurezza può essere realizzata anche senza una logica di controllo: solo da un dispositivo di azionamento e da un dispositivo di controllo. Un pulsante di arresto di emergenza che apre la bobina di un relè ausiliario di sicurezza, per esempio, esegue una semplice funzione di sicurezza.



Figura 8 – Relè di sicurezza a singola funzione (Allen-Bradley)

3 Relè (o moduli) di sicurezza modulari e configurabili

Grazie all'impiego di moduli di espansione I/O digitali di tipo plug-and-play, i relè modulari espandibili supportano fino a decine di ingressi diversi (pedane, barriere fotoelettriche, interruttori e così via) per garantire il controllo di sicurezza di apparecchiature di produzione più grandi e complesse mediante un solo sistema di relè. La struttura basata su microprocessori offre funzionalità di diagnostica e comunicazioni con più protocolli. Consente inoltre al relè di comunicare lo stato delle uscite e di errore ad un'interfaccia operatore attraverso una rete fieldbus. La facilità di collegamento tra i moduli consente la rapida espansione del sistema con un cablaggio ridotto. È possibile creare diverse combinazioni di moduli per il funzionamento con vari tipi di dispositivi di ingresso, riducendo così la necessità di installare più relè di sicurezza a singola funzione (visti al paragrafo precedente), semplificando la configurazione, il cablaggio e la manutenzione e risparmiando spazio prezioso nel quadro elettrico.

I moduli configurabili spesso dispongono di un'interfaccia di diagnosi per la visualizzazione assistita da PC di stati di ingressi, uscite e stati interni in modo da riconoscere rapidamente e facilmente errori di ogni tipo di cablaggio, la mancanza di informazioni e lo stato del sistema.

I relè configurabili hanno, come i PLC di sicurezza, una struttura ridondante, ma a differenza dei PLC non devono essere programmati.

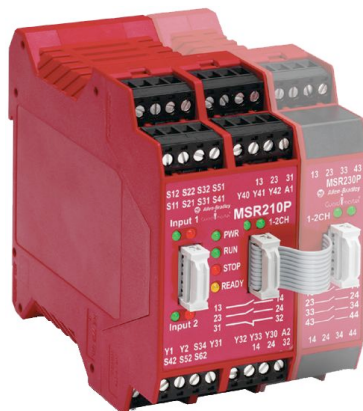


Figura 9 – Relè di sicurezza modulare espandibile (Allen-Bradley)

4 PLC di sicurezza

L'esigenza di applicazioni di sicurezza flessibili è alla base dello sviluppo dei controllori/PLC di sicurezza. I controllori programmabili di sicurezza offrono agli utilizzatori, in un'applicazione di sicurezza lo stesso livello di flessibilità del controllo che avrebbero con controllori programmabili standard. Tuttavia, le differenze tra PLC convenzionali e di sicurezza sono molte. I PLC di sicurezza sono disponibili in varie piattaforme, per rispondere ai requisiti di funzionalità e integrazione dei più complessi sistemi di sicurezza.



Figura 10 – Differenti tipologie di PLC di sicurezza (Allen-Bradley)

Hardware

Ridondanza delle CPU, memoria, circuiti I/O e diagnostica interna sono funzionalità dei PLC di sicurezza che i PLC standard non hanno. Un PLC di sicurezza dedica molto più tempo alla diagnostica interna su memoria, comunicazioni e I/O. Queste operazioni aggiuntive sono indispensabili a raggiungere la certificazione di sicurezza necessaria. Il sistema operativo del controllore gestisce la ridondanza e la diagnostica addizionale, in modo assolutamente trasparente per il programmatore che può quindi procedere alla programmazione dei PLC di sicurezza quasi come farebbe per i PLC standard.

I microprocessori che controllano questi dispositivi effettuano un'esauritiva diagnostica interna per garantire l'operatività della funzione di sicurezza. Lo schema a blocchi di figura 11 offre un esempio di PLC di sicurezza. Sebbene i controllori a microprocessore differiscano leggermente da una famiglia all'altra, i principi applicati per ottenere la classificazione di sicurezza sono simili.

Sono molti i microprocessori utilizzati per elaborare I/O, memoria e comunicazioni sicure. Le analisi diagnostiche vengono realizzate da circuiti watchdog. Questo tipo di struttura è nota come 1oo2D, perché uno qualunque dei due microprocessori può realizzare la funzione di sicurezza mentre, nel contempo, una attenta diagnostica garantisce che entrambi i microprocessori stiano funzionando in sincronizzazione.

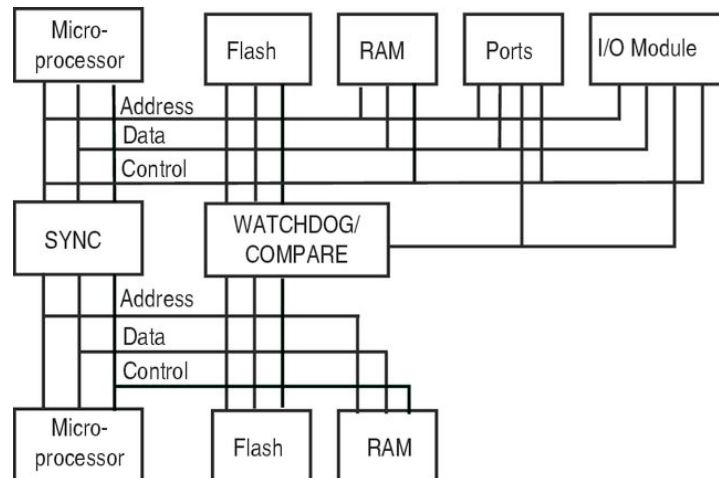


Figura 11 – Architettura 1oo2D di un PLC di sicurezza (Allen-Bradley)

Inoltre, ogni circuito di ingresso è testato internamente diverse volte al secondo, per verificarne il corretto funzionamento (figura 12). Grazie a questi continui test, ad esempio, anche se un pulsante di emergenza è premuto una sola volta al mese, il circuito sarà in grado di comunicare correttamente con il PLC di sicurezza.

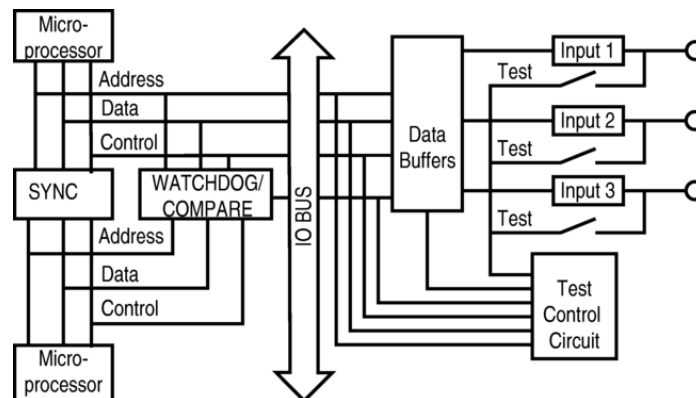


Figura 12 – Diagramma a blocchi di un modulo di ingresso di sicurezza (Allen-Bradley)

Le uscite del PLC di sicurezza sono elettromeccaniche o allo stato solido. La figura 13 mostra contatti multipli in ciascun circuito di uscita di un PLC di sicurezza. Come i circuiti di ingresso, anche i circuiti di uscita sono testati diverse volte al secondo per verificare che possano disattivare le uscite. L'uscita delle tre che non dovesse rispondere correttamente viene disattivata dalle altre due e il guasto viene riportato dal circuito di monitoraggio interno.

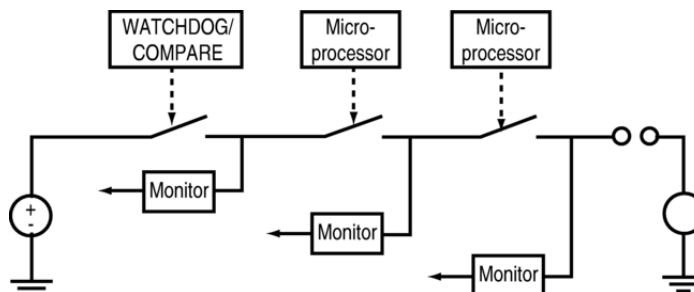


Figura 13 – Diagramma a blocchi di un modulo di uscita di sicurezza (Allen-Bradley)

Quando si usano dispositivi di sicurezza con contatti elettromeccanici (pulsanti di emergenza, interruttori di porta, ecc.), l'utilizzatore può applicare segnali di prova a impulsi per rilevare i guasti incrociati. Per limitare i costi legati alle uscite di sicurezza, molti PLC di sicurezza sono dotati di specifiche uscite a impulsi che possono essere collegate a dispositivi a contatto meccanico. Un esempio è mostrato in figura 14, in cui le uscite O1, O2, O3 e O4 inviano impulsi sfasati fra di loro.

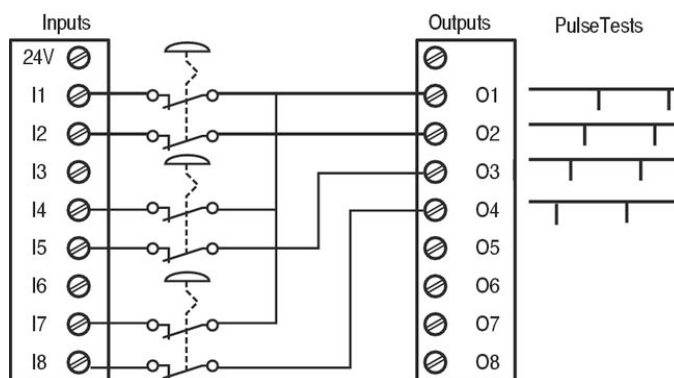


Figura 14 – Prova ad impulsi di due ingressi elettromeccanici NC (Allen-Bradley)

Il PLC di sicurezza si aspetta di vedere questi differenti impulsi riflettersi agli ingressi. Se vengono rilevati tassi di impulsi identici, si è verificato un guasto incrociato e si adottano misure adeguate nel PLC di sicurezza.

Software

La programmazione dei PLC di sicurezza è molto simile a quella dei PLC standard. Il sistema operativo gestisce la diagnostica aggiuntiva e il controllo degli errori, in modo che tale compito non spetti al programmatore. Per molti PLC di sicurezza, sono utilizzate speciali istruzioni di scrittura del programma per il sistema di sicurezza e queste istruzioni tendono a replicare la funzione dei relè di sicurezza. Ad esempio, l'istruzione per il pulsante di emergenza in figura 15 funziona in modo molto simile a un relè di sicurezza. Anche se la logica dietro ognuna di queste istruzioni è complessa, i programmi di sicurezza sembrano relativamente semplici perché il programmatore non fa altro che collegare tra di loro questi blocchi. Queste istruzioni, insieme ad altre istruzioni logiche, matematiche, di manipolazione dati, ecc. sono certificate da terzi per assicurare che il loro funzionamento sia coerente con gli standard applicabili.

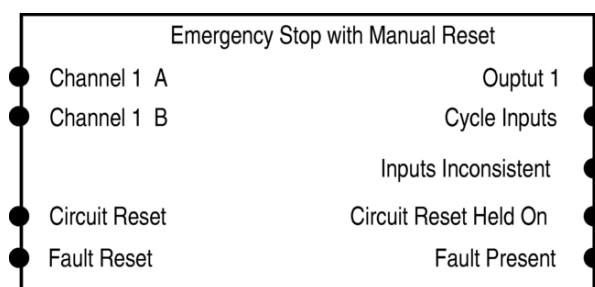


Figura 15 – Blocco funzione software per l'arresto di emergenza (Allen-Bradley)

I blocchi funzione sono il metodo predominante di programmazione delle funzioni di sicurezza. Oltre ai blocchi funzione e alla logica ladder, i PLC di sicurezza forniscono anche istruzioni applicative di sicurezza certificate. Le istruzioni di sicurezza certificate servono a gestire applicazioni specifiche. L'esempio di figura 15 mostra una istruzione di arresto di emergenza. Per compiere la stessa funzione in logica ladder sarebbero necessari circa 16 rami di logica ladder. Poiché il comportamento logico è integrato nell'istruzione per l'arresto di emergenza, la logica integrata non deve essere testata. I blocchi funzione certificati possono interfacciare quasi tutti i dispositivi di sicurezza. Di seguito un esempio di istruzioni per applicazioni certificate disponibili nei PLC di sicurezza.

1.	Ingressi differenti (1 N.O. + 1 N.C.) con reset automatico
2.	Ingressi differenti (1 N.O. + 1 N.C.) con reset manuale
3.	Arresto di emergenza con reset automatico
4.	Arresto di emergenza con reset manuale
5.	Ingresso ridondante (2 NC) con reset automatico

6.	Ingresso ridondante (2 NC) con reset manuale
7.	Uscita ridondante con retroazione positiva
8.	Uscita ridondante con retroazione negativa
9.	Dispositivo di abilitazione con reset automatico
10.	Dispositivo di abilitazione con reset manuale
11.	Comando a due mani con pin attivo
12.	Comando a due mani senza pin attivo
13.	Barriera fotoelettrica con reset automatico
14.	Barriera fotoelettrica con reset manuale
15.	Selettore a cinque posizioni
16.	Test singolo a impulsi per l'uscita
17.	Test ridondante a impulsi per l'uscita

I PLC di sicurezza generano una firma che consente di tracciare le eventuali modifiche apportate. Questa firma è di solito una combinazione di programma, configurazione ingressi/uscite e registrazione cronologica. Quando il programma è terminato e convalidato, l'utente dovrebbe registrare questa firma tra i risultati di convalida, per futuro riferimento. Se il programma ha bisogno di modifiche, è richiesta una nuova convalida e la registrazione di una nuova firma. Per impedire modifiche non autorizzate, il programma può anche essere bloccato con una password.

Il cablaggio dei sistemi a logica programmabile è semplificato rispetto a quello dei relè di sicurezza. Anziché essere cablati a terminali specifici dei relè di sicurezza, i dispositivi di ingresso sono collegati a qualunque terminale di ingresso e i dispositivi di uscita a qualunque terminale di uscita. I terminali sono poi assegnati mediante software.

In sintesi, i PLC di sicurezza apportano alle architetture di sicurezza programmabilità, elevato numero I/O, controllo distribuito ed un alto livello di comunicazione. Apportano anche delle funzioni speciali prima non disponibili nei sistemi dedicati: contatori ad alta velocità e segnali analogici. Le architetture con PLC di sicurezza sono spesso utilizzate nelle applicazioni complesse ad alto rischio.

5 Scelta tra modulo di sicurezza e PLC di sicurezza

Considerazioni tecniche

Inizialmente, il relè di sicurezza è stato la scelta di base in molti impianti industriali. E per molti sistemi è ancora una buona soluzione. Sono molto veloci (da 30 a 50 ms il tempo di risposta) e sono dedicati ad un solo compito: controllare gli ingressi e disattivare le uscite. Sono dotati di logica sufficiente per analizzare gli ingressi e le uscite del circuito e determinare se un dispositivo sta eseguendo correttamente il suo compito, e disattivarlo se non lo sta facendo. Tuttavia, un relè di sicurezza in genere è in grado di gestire correttamente solo una o due funzioni.

Successivi miglioramenti hanno portato ad una maggiore flessibilità nel tentativo di permettere all'utente finale non solo di impostare il comportamento del relè, ma anche di utilizzare lo stesso di relè per funzioni di sicurezza differenti.

Un'altra variante è la ASi (interfaccia sensore-attuatore), un dispositivo di rete che, invece di essere cablato ai sensori, designa gli ingressi di una rete che controlla in modo sicuro i dispositivi tramite un bus di comunicazione. Sebbene si possa già definire intelligente, un dispositivo del genere è ancora, fondamentalmente, un relè di sicurezza più flessibile e in grado di offrire capacità diagnostiche.

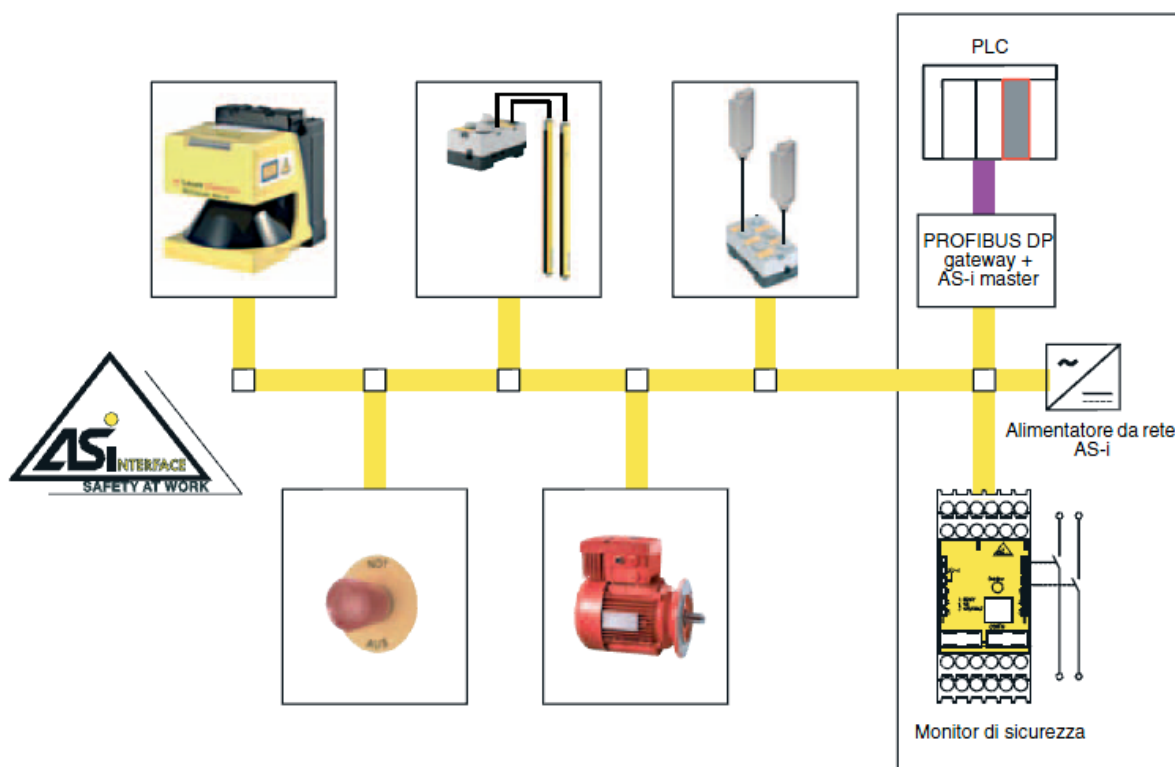


Figura 16 – Collegamento in rete con AS-Interface a livello sensore-attuatore e connessione a bus di campo (Profibus) di livello superiore (Leuze)

Se si cercano maggiori capacità, ma non si necessita di un alto livello di prestazioni come quelle offerte da un PLC di sicurezza, si può prendere in considerazione un relè di sicurezza modulare. Anche se hanno bisogno di programmazione, sono più semplici da utilizzare e non necessitano del rigore richiesto per sviluppare una applicazione con un PLC di sicurezza.

Alla sommità della scala di performance c'è il PLC di sicurezza, per impianti che trattano un gran numero di funzioni o con requisiti complessi. Il PLC di sicurezza può assumere compiti che vanno al di là della capacità del relè, il che rende più facile la costruzione della logica di controllo per garantire che un dispositivo stia facendo esattamente ciò che un utente richiede. Il PLC di sicurezza può tuttavia non essere sempre in grado di raggiungere i tempi di risposta garantiti da un relè di sicurezza. Anche se il PLC di sicurezza non è la risposta per ogni situazione, offre diversi vantaggi. Per esempio:

- Con un PLC di sicurezza, la logica è gestita da un software, non è cablata. La sua flessibilità consente di risparmiare denaro e aumentare la produttività diagnostica.
- Un PLC di sicurezza offre un sistema di sicurezza più sofisticato. Le funzionalità comprendono la modularità, la capacità di essere riconfigurato, e diversi modi di funzionamento, come la capacità di prestare attenzione a determinate funzioni in un modo e ad altre funzioni in altri modi.
- Il cablaggio è più semplice. Insieme di relè di sicurezza potrebbero essere ingombranti. Con un PLC di sicurezza i dispositivi sono cablati singolarmente ai moduli d'ingresso. Le distanze di cablaggio sono brevi, le interconnessioni sono per via logica. Parti di un sistema possono essere facilmente isolate per la diagnostica e le modifiche.
- La diagnostica è più completa. Poiché ogni dispositivo può essere ricondotta a un modulo di I / O, i guasti sono più facili da individuare.
- I PLC di sicurezza e i PLC convenzionali possono essere combinati in un unico sistema, favorendo le comunicazioni, la diagnostica e la risoluzione di problemi

Il vantaggio fondamentale invece dei relè di sicurezza è la flessibilità nel voltaggio, infatti può essere comandata quasi ogni tipica tensione di controllo. Tensioni tipiche includono: 5 V DC, 12 V DC, 24 V DC, 120 V AC e 230 V AC. La corrente nominale a 24 V DC è di circa 6 A per un carico resistivo. Confrontiamo questa situazione con quella di un PLC di sicurezza. Un controllore di sicurezza è un dispositivo a stato solido. Ciò significa che le sue uscite sono "transistorizzate" e pensate solo per contatti a 24 V DC con un massimo di 2 A. Se si ha intenzione di controllare un relè di potenza superiore o un contattore, queste uscite possono anche andare bene. Tuttavia, se si utilizza un relè di sicurezza per il controllo diretto del carico finale con tensioni diverse da 24 V DC, allora il PLC denota limiti.

I PLC di sicurezza sono in genere modulari, quindi possono essere aggiunti I/O di sicurezza. I moduli di espansione possono essere aggiunti anche ad un sistema di relè di sicurezza modulare. La larghezza e lo spazio sono fattori importanti se, come sempre accade, lo spazio sulla guida DIN all'interno dei quadri è prezioso. I relè di sicurezza generici sono larghi in genere 22,5 mm. e possono arrivare a 45 mm o più. La larghezza dei relè di sicurezza è direttamente proporzionale al numero dei contatti di uscita di sicurezza e della funzionalità complessiva. Tradizionalmente, i

controllori di sicurezza hanno una larghezza di 140 mm. Tuttavia, versioni più piccole sono ora sul mercato. Ad esempio, un controllore di sicurezza con una quantità standard di I/O è ora disponibile in un formato compatto di 67,5 mm. Quindi è facile capire che se l'applicazione richiede tre o più relè di sicurezza di 22,5 mm, lo spazio diventa un fattore importante.

Il numero degli I/O di sicurezza è la considerazione successiva. Un modulo di sicurezza di base 22,5 mm ha di solito due o tre uscite di sicurezza NA e due ingressi di sicurezza. Per i gradi più elevati di sicurezza, come Performance Level "e" secondo la norma ISO 13849-1, per ogni porta di sicurezza o ogni arresto di emergenza sarebbe necessario un relè di sicurezza proprio per mantenere il massimo livello di sicurezza. Per confronto, si consideri un PLC di sicurezza con 20 ingressi e 4 uscite di sicurezza. Con 20 ingressi, il progettista potrebbe collegare 10 pulsanti di emergenza a doppio canale al PLC stesso e mantenere una categoria di sicurezza 4.

Per un progettista abituato ad usare relè di sicurezza, il software di configurazione di un PLC di sicurezza è una delle principali incognite. Molti trovano l'idea di utilizzare un prodotto di sicurezza basato sul software non tranquillizzante. Si preoccupano del necessario livello di competenza di programmazione e dei costi aggiuntivi. Tuttavia l'utilizzo del software può avere un aspetto positivo. Aumenta la flessibilità e offre funzionalità avanzate che un circuito multiplo di relè di sicurezza non è in grado di fornire.

Un software di configurazione pensato per "non programmatori" permette di semplificare il processo di progettazione. Infatti software con funzionalità "drag-and-drop" migliora la facilità d'uso del software. Nel software esistono dei blocchi funzionali di sicurezza pensati per la maggior parte delle applicazioni di sicurezza più importanti. Gli esempi includono l'arresto di emergenza, la porta di sicurezza, la barriera, barriera fotoelettrica con muting, il selettore, gli interruttori di abilitazione, i comandi a due mani e i sensori di sicurezza. Questi blocchi funzionali di sicurezza possono essere mescolati per creare qualsiasi cosa, da funzioni di sicurezza molto semplici a quelle di logica avanzata per il controllo di zone multiple. Il vero potere del software risiede nell'abbondanza di "funzioni logiche di sicurezza." Esempi di funzioni logiche di sicurezza comprendono AND, OR, ritardo all'eccitazione, ritardo alla diseccitazione, generatore di impulsi, ecc. Questi blocchi funzionali di sicurezza prendono il posto dei singoli relè di sicurezza, e le funzioni logiche di sicurezza prendono il posto di funzionalità speciali.

Un altro aspetto potente del PLC di sicurezza è la possibilità di disporre di una modalità di simulazione della sicurezza. Questa modalità è ideale per la progettazione di un sistema di sicurezza alla scrivania potendo entrare in modalità di simulazione per validare il progetto di sicurezza prima di andare sul posto e scaricare il programma per il PLC di sicurezza stesso. Quando una installazione sul campo ha bisogno di un cambio rapido del progetto della sicurezza o di funzionalità aggiuntive, il progettista è in grado di sviluppare il cambiamento, validare in modalità di simulazione, spedire via e-mail il suo progetto sul campo per il download tramite una connessione USB.

Un PLC di sicurezza in genere richiede due password per la sicurezza. La prima password protegge la sicurezza del progetto (software) stesso. Senza questa password, non è possibile apportare modifiche

al progetto di sicurezza. Il PLC di sicurezza dispone anche di una password hardware. Questa password è necessaria per scaricare/caricare da/al PLC di sicurezza controller. I costruttori di macchine possono decidere quanto e quale tipo di accesso concedere ai loro clienti. Per ogni progetto di sicurezza, viene fornita una somma di controllo CRC. Se all'utente finale è concesso l'accesso al software e apporta modifiche, la somma di controllo CRC rifletterà la modifica. Contrasto questi pensieri ad un circuito cablato relè di sicurezza.

Considerata la capacità diagnostica del software, ciò consentirà di risparmiare tempo durante la ricerca guasti che invece può rivelarsi un compito arduo nei relè di sicurezza a causa di tutto il cablaggio e la varietà di relè di sicurezza utilizzati. Con un controllore di sicurezza, è possibile collegare il software tramite USB, caricare il progettare e andare online. A questo punto, il software indicherà il motivo per cui un circuito non si è attivato.

Considerazioni economiche

Per un confronto sui costi, useremo una moduli di sicurezza con funzionalità di base. Tenete a mente che la sicurezza relè con funzionalità avanzate va aggiunta al costo della soluzione con il relè di sicurezza di base. Un prezzo di listino standard per un relè di sicurezza può variare notevolmente. Si assuma che un prezzo equo per un relè di sicurezza con canali a doppio ingresso e due uscite di sicurezza NA è di circa 150 €. Inoltre si può ipotizzare che un PLC di sicurezza abbastanza ragionevolmente costi circa 550 €.

La considerazione successiva è il costo potenziale del software di controllo di sicurezza. I prezzi per un pacchetto di sicurezza del software di controllo di configurazione possono variare da un "senza alcun costo," download libero a circa 1400 €! Anche i costi di licenza sono anche critici. Possono aggiungere centinaia di euro per ogni macchina che utilizza un PLC di sicurezza. Per quanto possibile si raccomanda pacchetto software di configurazione liberamente scaricabile senza costi di licenza e con modalità di simulazione. Dal momento sono disponibili delle opzioni gratuite, non si includerà il software di configurazione negli esempi di prezzo.

1° esempio: con tre moduli di sicurezza standard a 150 € ciascuno, il costo totale è di 450 €. Per il controllore di sicurezza è di 550 €. La soluzione con relè di sicurezza costa 100 € in meno, e lo spazio occupato è lo stesso (figura 17). Poiché il prezzo dei relè di sicurezza è direttamente proporzionale al numero di contatti di sicurezza e di funzionalità, il relè di sicurezza avrebbe dovuto avere un costo medio di 184 euro ciascuno prima che il progettista vedesse un vantaggio di costo nella scelta del PLC. Tuttavia, la sicurezza, la flessibilità di controllo, e altri benefici potrebbero essere abbastanza attraenti per effettuare il cambio della piattaforma di sicurezza.

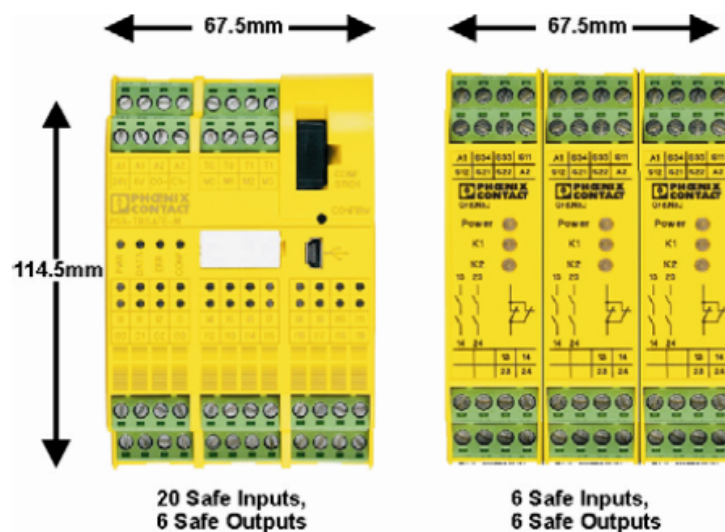


Figura 17 – Esempio 1 di confronto tra soluzione con relè e soluzione con PLC (Phoenix Contact)

2° esempio: con cinque moduli di sicurezza standard a 150 € ciascuno, il costo totale è di 750 €. Il controllore di sicurezza è di 550 €. La soluzione con relè di sicurezza è di 200 € (27%), più costosa e utilizza il 67% di spazio in più sulla guida DIN (figura 18). Se 6 uscite di sicurezza sul PLC sono sufficienti, allora è senza dubbio il PLC di sicurezza diventa una valida opzione a questo punto.

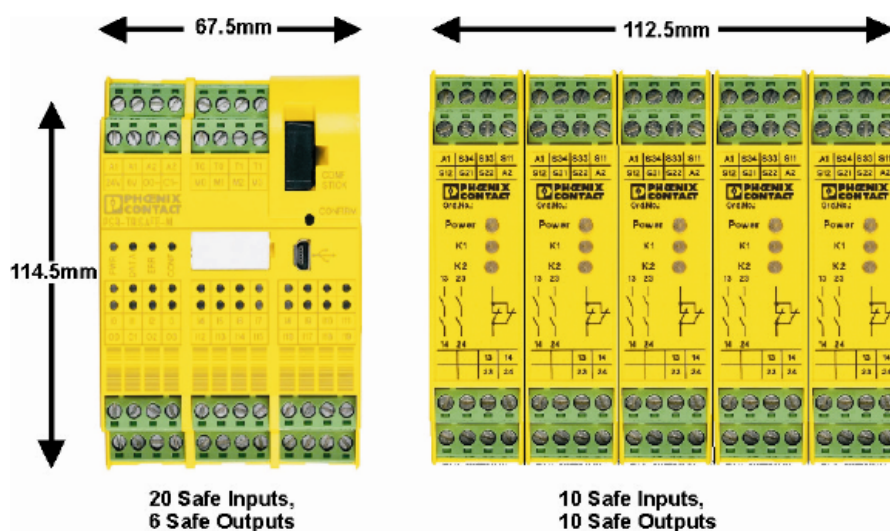


Figura 18 - Esempio 2 di confronto tra soluzione con relè e soluzione con PLC (Phoenix Contact)

In sintesi quando un'applicazione richiede almeno tre relè di sicurezza, ha senso, anche dal lato economico, considerare il passaggio ad una piattaforma di controllo con PLC di sicurezza. Più sono i relè di sicurezza che sono coinvolti, tanto più la soluzione con PLC ha senso.

6 Scelta tra PLC convenzionale e PLC di sicurezza

Ci sono molte applicazioni in cui il sistema di automazione gestito da un PLC convenzionale (standard) è stato impiegato per controllare attrezzature, comprese le parti di sicurezza del sistema di comando. In genere i PLC standard utilizzati in applicazioni di sicurezza sono configurati a coppie. Il PLC ridondante viene utilizzato per gestire un arresto sicuro nel caso in cui il PLC primario fallisca. Oltre all'uso di più di un controllore, le applicazioni di sicurezza progettate utilizzando PLC standard utilizzano I/O aggiuntivi al fine di controllare i segnali di uscita del sistema di sicurezza, e altre uscite di test ad impulsi per la sicurezza dei moduli di ingresso del sistema. Inoltre, le applicazioni, progettate attorno a un PLC standard richiedono software personalizzato per il monitoraggio, il controllo e la diagnosi del sistema di sicurezza. Per riassumere, la progettazione di sistemi di sicurezza con controller standard necessita di maggior tempo di progettazione, I/O hardware, e cablaggio e per sostenere la porzione di sicurezza dell'applicazione, oltre all'hardware e al software necessari per eseguire l'applicazione.

Esistono dei pacchetti ridondanti basati su PLC che riducono drasticamente lo sforzo progettuale ed eliminano la fase di certificazione fornendo un kit completo di software / hardware certificati per l'utilizzo, ad esempio, nelle applicazioni di controllo di una pressa.

L'utilizzo di due PLC fornisce la ridondanza per migliorare l'integrità della sicurezza del sistema. Gli ingressi e le uscite sono collegati in modo incrociato per ottenere il monitoraggio e la verifica del funzionamento come mostrato dallo schema a blocchi di figura 19.

Ci sono tre differenze fondamentali tra un PLC di sicurezza e un PLC standard in termini di architettura, di ingressi e di uscite.

La figura 20 mostra un confronto fra gli schemi a blocchi delle due architetture. Il PLC dispone di un microprocessore che esegue il programma, una memoria Flash che immagazzina il programma, una RAM per eseguire calcoli, porte per la comunicazione e I/O per controllare la macchina. Al contrario, un PLC di sicurezza ha microprocessori ridondanti, memorie Flash e RAM che sono continuamente monitorate da un circuito watchdog e un circuito di rilevamento della sincronia.

La figura 21 mette a confronto un ingresso di un PLC standard con un ingresso di un PLC di sicurezza. Gli ingressi di un PLC standard non forniscono mezzi interni per la verifica della funzionalità della circuiteria di ingresso. Al contrario, i PLC di sicurezza hanno un circuito interno 'di uscita' associato ad ogni ingresso al fine di testare la circuiteria di ingresso.

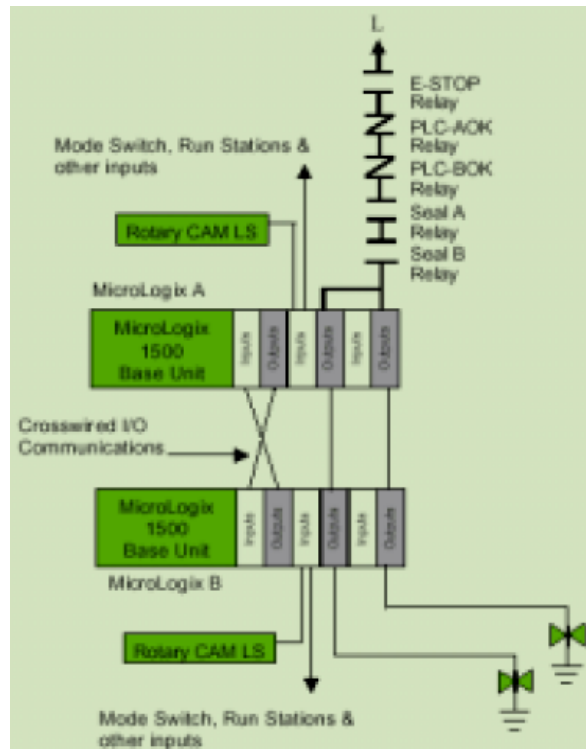


Figura 19 - Esempio di utilizzo di due PLC standard per funzioni di sicurezza (Rockwell)

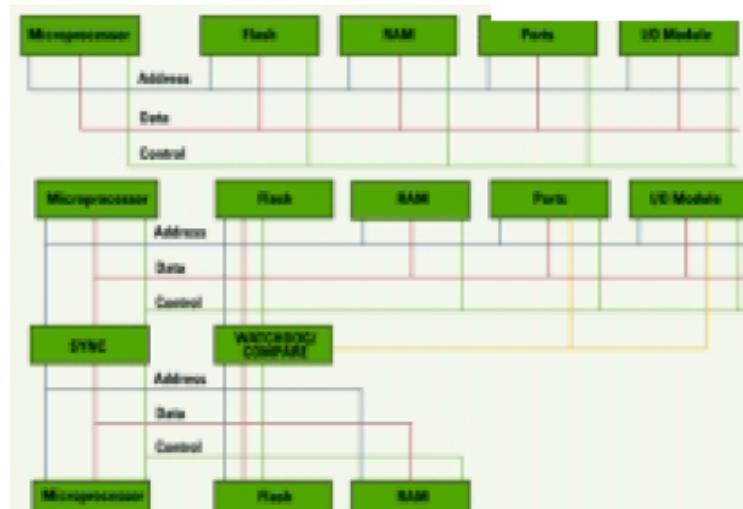


Figura 20 – Confronto fra le architetture di un PLC standard e di un PLC di sicurezza (Rockwell)

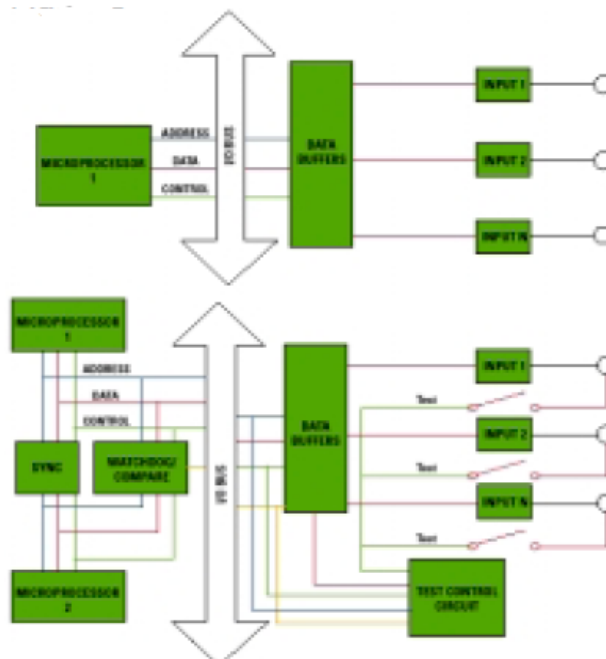


Figura 21 – Confronto fra i circuiti di ingresso di un PLC standard e di un PLC di sicurezza (Rockwell)

La figura 22 confronta i circuiti digitali di uscita di un PLC standard con quelli di un PLC di sicurezza. Il PLC standard dispone di un dispositivo di commutazione di uscita, mentre il circuito di uscita digitale di un PLC di sicurezza contiene un punto di test dopo ciascuno dei due interruttori di sicurezza che si trovano dietro il driver di uscita ed un terzo punto di test a valle del punto di prova del driver di uscita. Ciascuno dei due interruttori di sicurezza è controllato da ogni microprocessore. Se viene rilevato un guasto a uno dei due interruttori di sicurezza a causa di un microprocessore guasto, il sistema operativo del PLC di sicurezza riconosce automaticamente l'errore di sistema.

I PLC di sicurezza sono adatti per applicazioni a SIL 2 e SIL 3 dove possono essere certificati per l'utilizzo nelle più comuni applicazioni di sicurezza.

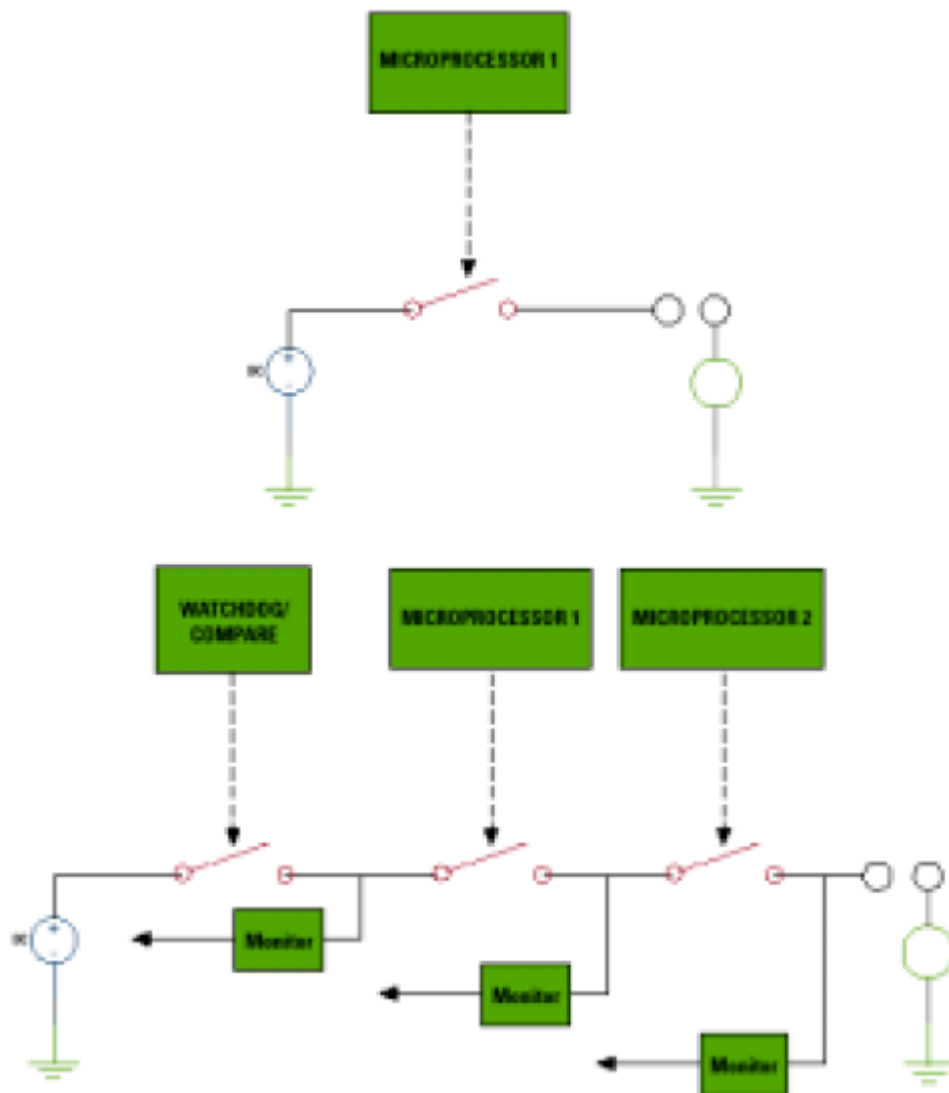


Figura 22 – Confronto fra i circuiti di uscita di un PLC standard e di un PLC di sicurezza (Rockwell)

La ridondanza e l'auto-controllo, funzionalità delle quali un PLC di sicurezza è dotato, fanno sì che i PLC di sicurezza costino circa il 25% e il 30% in più rispetto ai loro omologhi convenzionali. Tuttavia, essi forniscono un notevole risparmio rispetto al costo totale di un sistema con un doppio PLC standard. Analogamente, questo differenziale di costi, se confrontato con un sistema di sicurezza basato su relè di sicurezza, è compensato da costi di cablaggio ridotti, dal minor spazio richiesto nel quadro e nella migliorata flessibilità.

7 Sicurezza integrata

Attualmente, le soluzioni di controllo di sicurezza offrono la completa integrazione in una singola architettura di controllo, in cui le funzioni di controllo di sicurezza e quelle standard risiedono e lavorano insieme. La capacità di realizzare task di movimento, azionamento, processo, batch, sequenziali ad alta velocità e sicurezza SIL 3 in un controllore offre notevoli vantaggi. L'integrazione di controllo standard e di sicurezza consente di utilizzare strumenti e tecnologie comuni che riducono i costi associati a progettazione, installazione, messa in servizio e manutenzione. La possibilità di utilizzare, sulle reti di sicurezza, hardware di controllo, dispositivi o I/O di sicurezza distribuiti e dispositivi di interfaccia operatore comuni riduce i costi di acquisto e manutenzione, oltre ai tempi di sviluppo. Tutte queste funzioni aumentano la produttività e la velocità della ricerca guasti e favoriscono la riduzione dei costi di formazione.

Lo schema di figura 23 mostra un esempio dell'integrazione di controllo e sicurezza. Le funzioni di controllo non legate alla sicurezza standard risiedono nel Main Task. Le funzioni di controllo legate alla sicurezza risiedono nel Safety Task.

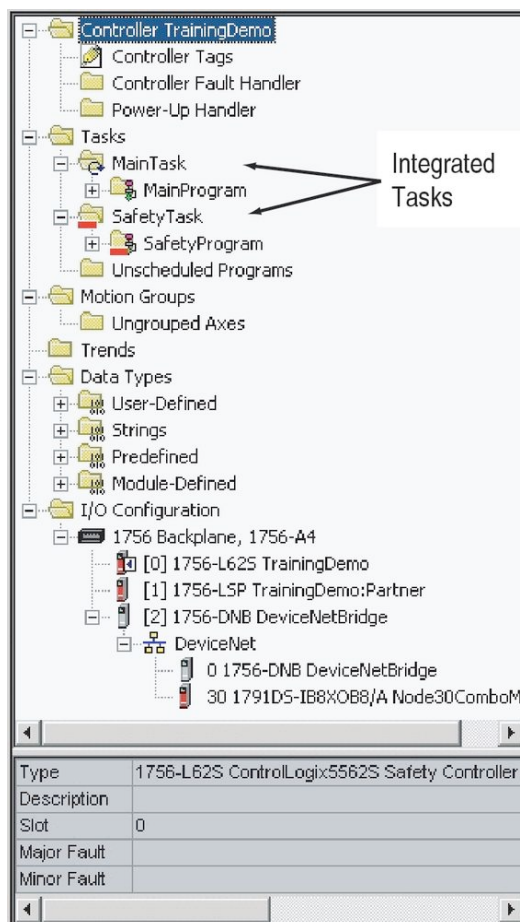


Figura 23 – Sicurezza integrata e Task non di sicurezza (Allen-Bradley)

Tutte le funzioni standard e di sicurezza sono isolate una dall'altra. La figura 24 mostra un diagramma a blocchi della possibile interazione fra la parte standard e quella di sicurezza dell'applicazione. Ad esempio, i tag di sicurezza possono essere letti direttamente dalla logica standard. I tag di sicurezza possono essere scambiati tra i controllori su EtherNet, ControlNet o DeviceNet. I dati dei tag di sicurezza possono essere letti direttamente da dispositivi esterni, interfacce operatore (HMI), personal computer (PC) o altri controllori.

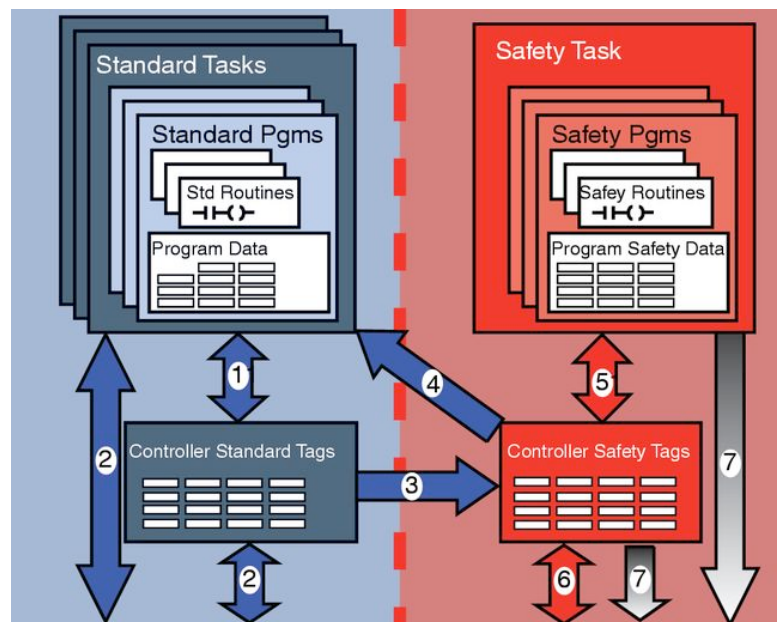


Figura 24 – Interazione fra compiti (tasks) standard e compiti di sicurezza (Allen-Bradley)

1. Logica e tag standard si comportano allo stesso modo.
2. Tag standard, analizzati dal programma o dal controllore e dispositivi esterni, interfacce operatore, PC, altri controllori, ecc.
3. Mappatura dei tag standard nei tag di sicurezza da usare per task di sicurezza.
4. I tag di sicurezza possono essere letti direttamente dalla logica standard.
5. I tag di sicurezza possono essere letti o scritti dalla logica di sicurezza.
6. I tag di sicurezza possono essere scambiati tra i controllori su EtherNet.
7. I tag di sicurezza, analizzati dal programma o dal controllore, possono essere letti da dispositivi esterni, interfacce operatore, PC, altri controllori, ecc. Dopo essere stati letti, questi dati sono considerati dati standard, non di sicurezza.

8 Reti di sicurezza

Le reti di comunicazione a livello di impianto hanno permesso ai fabbricanti di migliorare la flessibilità, aumentare le capacità di diagnostica e le distanze, ridurre i costi di installazione e cablaggio, facilitare la manutenibilità e, in generale, migliorare la produttività delle loro operazioni di produzione. Le stesse motivazioni sono alla base dell'implementazione delle reti di sicurezza industriali. Queste reti di sicurezza consentono ai fabbricanti di distribuire I/O e dispositivi di sicurezza sui macchinari mediante un semplice cavo di rete, riducendo i costi di installazione, migliorando la diagnostica e installando sistemi di sicurezza di maggiore complessità.

Permettono, inoltre, la comunicazione sicura tra PLC e controllori di sicurezza, dando agli utilizzatori la possibilità di distribuire il controllo di sicurezza tra diversi sistemi intelligenti.

Le reti di sicurezza non impediscono l'occorrenza di errori di comunicazione. Le reti di sicurezza hanno una maggiore capacità di rilevamento degli errori di trasmissione per cui, successivamente, i dispositivi di sicurezza adottano le misure adeguate. Tra gli errori di comunicazione rilevati, ci sono i seguenti: inserimento di messaggi, perdita di messaggi, corruzione di messaggi, ritardo di messaggi, ripetizione di messaggi e sequenza non corretta dei messaggi.

Per molte applicazioni, quando viene rilevato un errore, il dispositivo entra in uno stato di diseccitazione, tipicamente chiamato "stato di sicurezza." Il dispositivo di ingresso o di uscita di sicurezza deve rilevare questi errori di comunicazione e poi entrare, se necessario, in stato di sicurezza.

Le prime reti di sicurezza erano legate a un particolare tipo di supporto o schema di accesso ai supporti e, di conseguenza, i fabbricanti dovevano usare cavi, schede di interfaccia di rete, router, ponti, ecc. specifici, che diventavano parte integrante della funzione di sicurezza.

Queste reti erano limitate per il fatto che supportavano solo la comunicazione tra i dispositivi di sicurezza. Ciò significava che i fabbricanti dovevano usare due o più reti per la loro strategia di controllo delle macchine (una rete per il controllo standard e un'altra per il controllo di sicurezza), con l'aumento dei costi di installazione, formazione e dei pezzi di ricambio.

Le moderne reti di sicurezza consentono di comunicare con dispositivi di controllo standard e di sicurezza mediante un unico cavo di rete. CIP (Common Industrial Protocol) Safety è un protocollo standard aperto, pubblicato da ODVA (Open DeviceNet Vendors Association), che permette la comunicazione di sicurezza tra i dispositivi di sicurezza su reti DeviceNet, ControlNet e EtherNet/IP. Dato che CIP Safety è una estensione del protocollo CIP standard, i dispositivi di sicurezza e quelli standard possono risiedere tutti sulla stessa rete. Gli utilizzatori possono anche collegare tra loro a ponte reti contenenti dispositivi di sicurezza, con la possibilità di suddividere i dispositivi di sicurezza per regolare con precisione i tempi di risposta o, semplicemente, per facilitare la distribuzione dei dispositivi di sicurezza. Dato che il protocollo di sicurezza è di esclusiva responsabilità dei dispositivi finali (PLC di sicurezza/controller, moduli I/O di sicurezza, componenti di sicurezza), tutti i componenti quali cavi, schede di interfaccia di rete, ponti e router sono standard e quindi esclusi dalla funzione di

sicurezza oltre a non richiedere hardware di rete specifico. La figura 25 mostra un esempio semplificato di un sistema I/O distribuito. L'operatore apre il cancello. L'interruttore di blocco, collegato al modulo di sicurezza I/O (Safety I/O Block), invia i propri dati di sicurezza sulla rete DeviceNet per il PLC di sicurezza. Il PLC di sicurezza invia un segnale al modulo di sicurezza I/O per fermare le apparecchiature all'interno del cancello e invia un'uscita standard alla torretta luminosa per segnalare che il cancello è aperto. L'operatore (HMI) e il PLC standard monitorano per prendere eventuali misure di controllo aggiuntive, come l'esecuzione di un arresto ciclo di apparecchiature adiacenti.

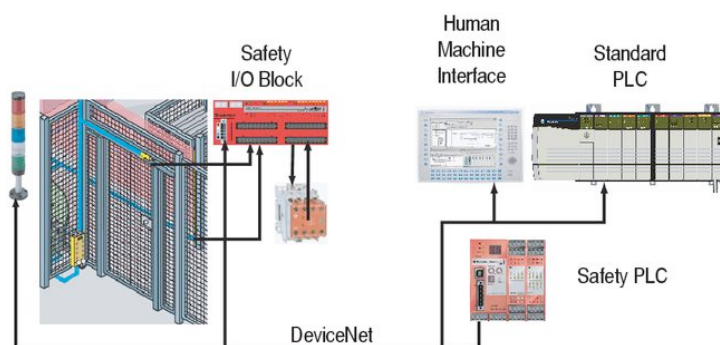


Figura 25 - Esempio di una semplice rete distribuita di sicurezza

Per i sistemi di produzione più grandi, in cui le informazioni di sicurezza e di controllo devono essere condivise, può essere utilizzato Ethernet/IP. La figura 26 mostra un esempio di comunicazione tra due PLC di sicurezza mentre DeviceNet viene utilizzato per la distribuzione locale di I/O all'interno di un sottosistema più piccolo.

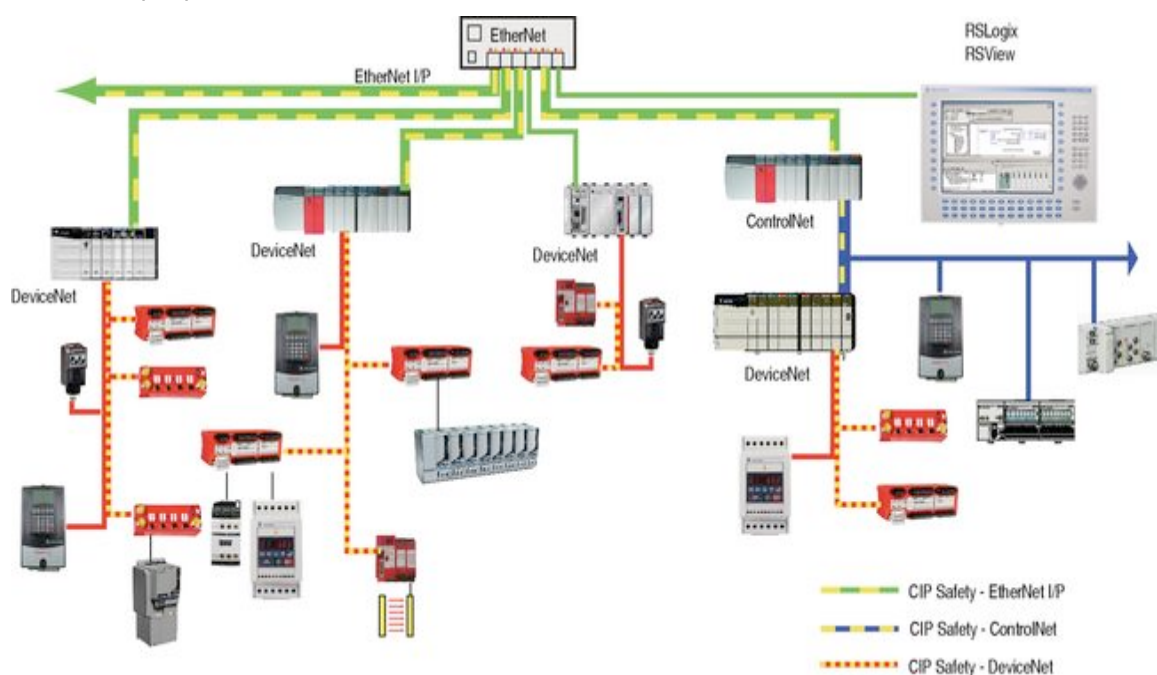


Figura 26 - Esempio di una complessa rete distribuita di sicurezza

PROFIsafe

PROFIsafe è un protocollo di comunicazione certificato per le reti Profibus e PROFINET. Con SIL 3 (Safety Integrity Level) PROFIsafe soddisfa i più elevati requisiti di sicurezza per l'industria di processo e produzione. Sono possibili sia la comunicazione orientata alla sicurezza che quella standard mediante uno stesso cavo.

Il sistema PROFIsafe è un'espansione del sistema Profibus e PROFINET. Con questo sistema è possibile realizzare funzioni di sicurezza liberamente programmabili e trasferire i dati I/O sicuri necessari dai dispositivi I/O sicuri e viceversa.

La comunicazione tra il controllore sicuro e gli utenti bus sicuri avviene attraverso il protocollo PROFIsafe, che viene collegato al protocollo Profibus standard o PROFINET e contiene i dati I/O sicuri e le informazioni sulla sicurezza dei dati.

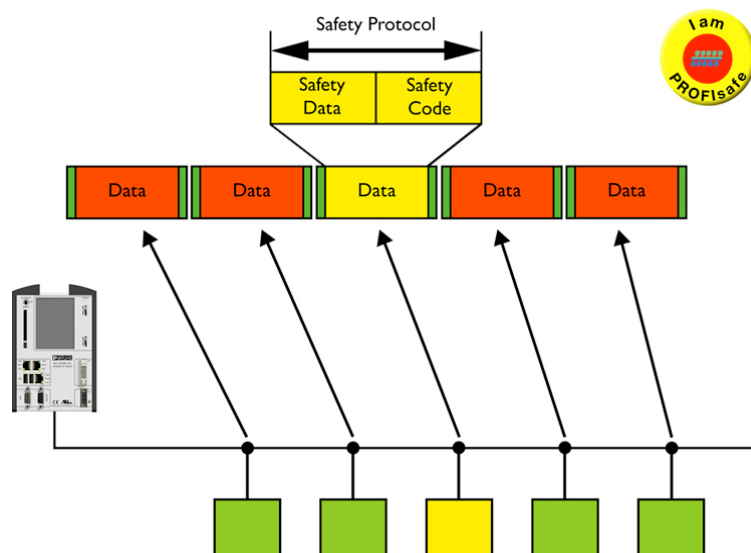


Figura 27 – Sistema PROFIsafe, comunicazione ordinaria e di sicurezza sullo stesso cavo (Phoenix Contact)

I tempi di ritardo dei sensori e degli attuatori sono indipendenti dal protocollo Safety utilizzato e devono essere considerati in modo separato. In base a singoli processi liberi non sincronizzati viene determinato il tempo di reazione come somma dei seguenti valori:

- tempo watchdog del modulo d'ingresso
- tempo watchdog impostato della rete dal modulo di ingresso al controllore
- tempo watchdog impostato del controllore sicuro
- tempo watchdog impostato della rete dal controllore al modulo di uscita
- tempo watchdog del modulo di uscita

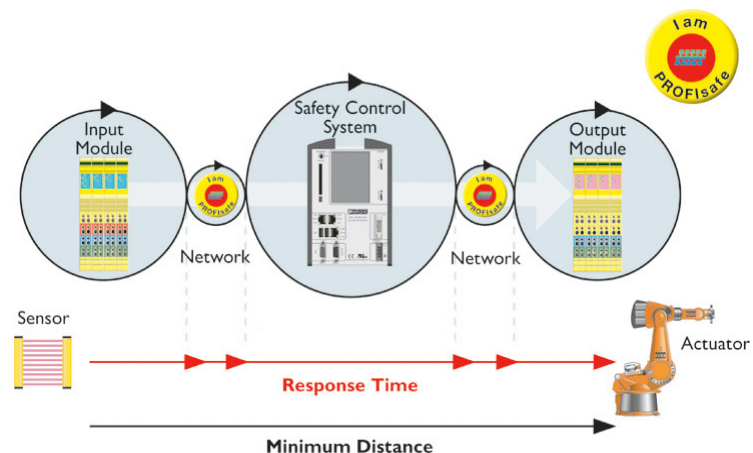


Figura 28 – Tempi di reazione con il sistema PROFIsafe (Phoenix Contact)

Nelle figure seguenti esempi di sicurezza con rete PROFIsafe.

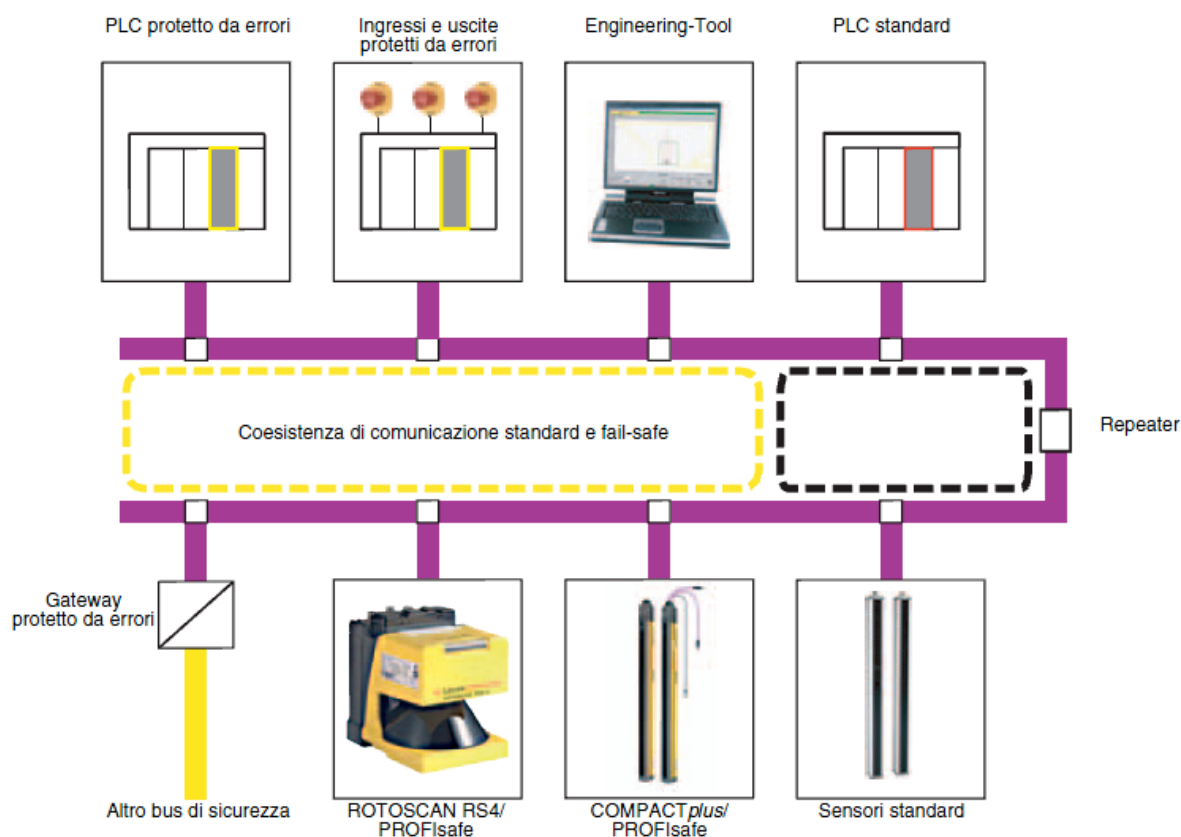


Figura 29 – Collegamento in rete di componenti standard e sensori di sicurezza (giallo) tramite collegamento diretto a rete PROFIBUS con protocollo PROFIsafe (Leuze)

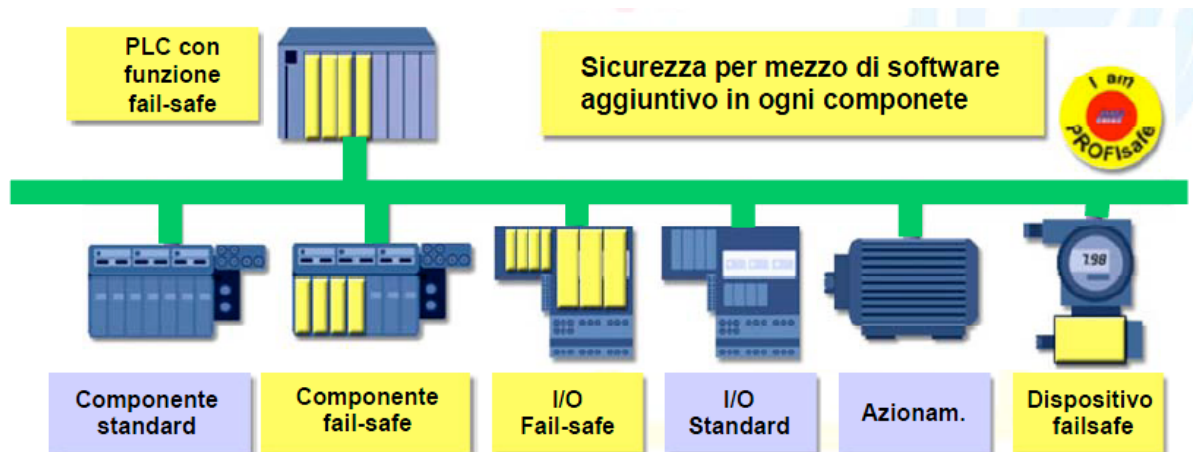


Figura 30 – Collegamento in rete di componenti standard e di sicurezza (giallo) tramite PROFIsafe

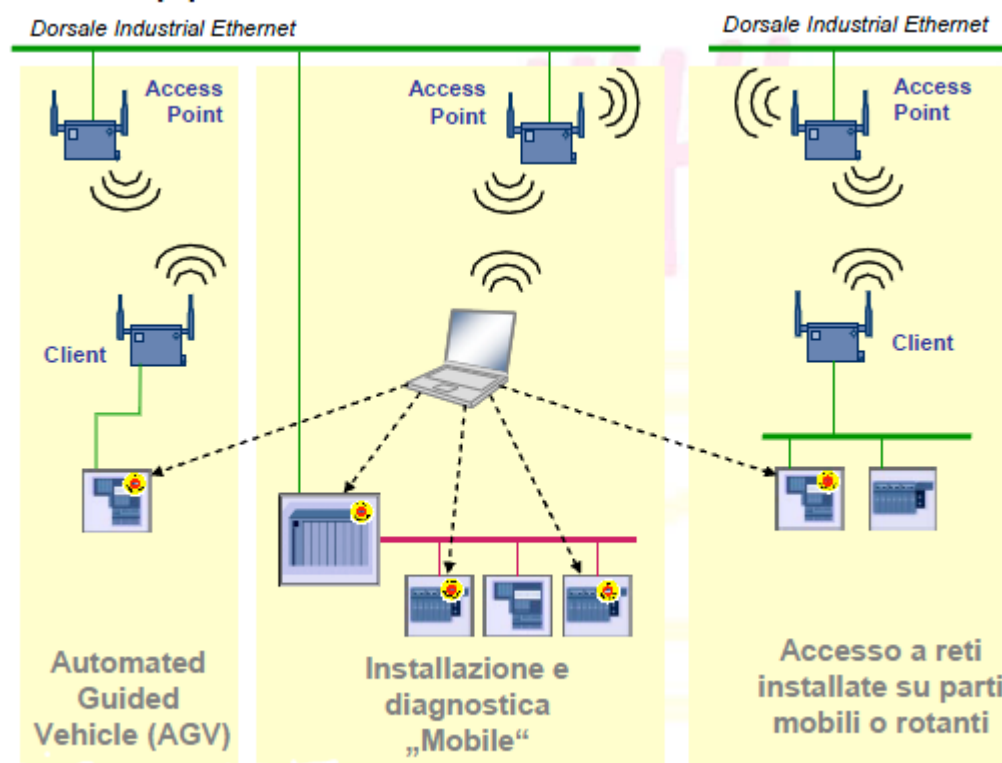


Figura 31 – Applicazioni PROFIsafe Wireless



Fonti

Schneider Electric
Pilz
Omron
Mitsubishi
Phoenix Contact
Allen-Bradley
Rockwell Automation
Siemens
Sick