SAFEBOOK 4

Allen-Bradley

Guardmaster®

Sistemi di controllo legati alla sicurezza delle macchine

Principi, standard e implementazione

LISTEN. THINK. SOLVE.℠

Rockwell Automation

Sommario

Capitolo 1 **Regolamenti..... 2**
Legislazione e direttive UE, Direttiva Macchine,Direttiva “Uso delle attrezzature di lavoro”, regolamenti USA, OSHA (Occupational Safety and Health Administration), regolamenti canadesi

Capitolo 2 **Standard..... 18**
ISO (International Organisation for Standardisation), IEC (International Electrotechnical Commission), norme europee armonizzate EN, standard USA, standard OSHA, standard ANSI, standard canadesi, standard australiani

Capitolo 3 **Strategia della sicurezza..... 23**
Valutazione dei rischi, determinazione dei limiti delle macchine, identificazione di attività e pericoli, stima e riduzione dei rischi, progetti a sicurezza intrinseca, misure e sistemi di protezione, valutazione, formazione, dispositivi di protezione personale, standard

Capitolo 4 **Misure di protezione e dispositivi complementari..... 36**
Prevenzione accessi, protezioni fisse, rilevamento accessi, sistemi e prodotti di sicurezza

Capitolo 5 **Calcolo delle distanze di sicurezza..... 59**
Formule, consigli e applicazione delle soluzioni di sicurezza per il controllo delle parti mobili, potenzialmente pericolose, mediante il calcolo delle distanze di sicurezza.

Capitolo 6 **Prevenzione dell’accensione non intenzionale 63**
Lockout/Tagout, sistemi di isolamento di sicurezza, sezionatori di carico, sistemi a chiave bloccata, misure alternative al lockout

Capitolo 7 **Sistemi di controllo legati alla sicurezza e sicurezza funzionale..... 65**
Introduzione, Che cos’è la sicurezza funzionale? IEC/EN 62061 ed EN ISO 13849-1:2008, SIL e IEC/EN 62061, PL ed EN ISO 13849-1:2008, confronto tra PL e SIL

Capitolo 8 **Progettazione del sistema secondo EN ISO 13849-1:2008..... 71**
Architetture dei sistemi di sicurezza (strutture), ciclo di vita, tempo medio prima di un guasto pericoloso ($MTTF_d$), copertura diagnostica (DC), guasti per causa comune (CCF), guasti sistematici, livelli prestazionali (PL), progettazione di sottosistemi e loro combinazioni, convalida, messa in servizio delle macchine, esclusione dei guasti

Capitolo 9 **Progettazione del sistema secondo IEC/EN 62061..... 94**
Progettazione di sottosistemi – IEC/EN 62061, influenza dell’intervallo dei test diagnostici, influenza dell’analisi dei guasti per causa comune, metodologia di classificazione per categorie, vincoli hardware, B10 e $B10_d$, guasti per causa comune (CCF), copertura diagnostica (DC), tolleranza ai guasti hardware, gestione della sicurezza funzionale, PFH_D (Probabilità di guasti pericolosi per ora), intervallo dei test diagnostici, SFF (percentuale di guasti sicuri), guasti sistematici

Capitolo 10 **Sistemi di controllo legati alla sicurezza, considerazioni strutturali..... 106**
Cenni generali, categorie dei sistemi di controllo, guasti non rilevati, classificazione di sistemi e componenti, considerazioni sui guasti, esclusione dei guasti, categorie di arresti secondo IEC/EN 60204-1 e NFPA 79, requisiti dei sistemi di controllo di sicurezza USA, standard per i robot: Stati Uniti/Canada

Capitolo 11 **Esempio applicativo con SISTEMA..... 130**
Esempio applicativo relativo all’uso del tool di calcolo dei livelli prestazionali SISTEMA con la libreria dei prodotti per SISTEMA di Rockwell Automation

Allen-Bradley

Legislazione e direttive UE

Obiettivo di questa sezione è fornire una guida per tutti coloro che si occupano di sicurezza delle macchine e, in particolare, dei sistemi di protezione all'interno dell'Unione Europea. Ed è rivolta sia ai progettisti che agli utilizzatori di apparecchiature industriali.

Per promuovere il concetto di mercato aperto nell'Area Economica Europea (EEA) (comprendente gli stati membri UE e altri tre paesi), tutti gli stati membri sono tenuti ad adottare una legislazione che definisca i requisiti di sicurezza fondamentali per le macchine e il loro uso.

Le macchine che non soddisfano tali requisiti non possono essere commercializzate all'interno dei paesi EEA.

Esistono diverse direttive europee applicabili alla sicurezza delle apparecchiature e delle macchine industriali ma le due più importanti sono le seguenti:

1 La Direttiva Macchine

2 La Direttiva sull'uso delle attrezzature di lavoro da parte dei lavoratori durante il lavoro

Queste due direttive sono direttamente correlate e i requisiti essenziali per la salute e la sicurezza (EHSR) previsti dalla Direttiva Macchine possono essere utilizzati per confermare la sicurezza delle attrezzature descritta nella direttiva sull'uso delle attrezzature di lavoro.

Questa sezione descrive alcuni aspetti di entrambe le direttive. Chi si occupa di progettazione, fornitura, acquisto o utilizzo delle attrezzature industriali all'interno dei paesi SEE e di alcuni altri paesi europei dovrebbe prendere conoscenza dei requisiti previsti da tali testi. I fornitori e gli utilizzatori di macchine che non agiscono conformemente a tali direttive non potranno fornire o operare in questi paesi.

Vi sono altre Direttive europee che potrebbero essere applicabili alle macchine. La maggior parte di queste è piuttosto specialistica nell'applicazione e, per questo motivo, tali testi non saranno trattati nella presente sezione; tuttavia, è importante notare che, laddove pertinente, i loro requisiti devono comunque essere rispettati, come nel caso della Direttiva 2004/108/CE e della Direttiva ATEX 94/9/CE.

La Direttiva Macchine

La Direttiva macchine riguarda la fornitura di macchinari nuovi e di altre attrezzature, compresi i componenti di sicurezza. La fornitura nei Paesi dell'Unione Europea di macchine non conformi alle disposizioni e ai requisiti di questa direttiva costituisce un reato.

La definizione di "macchina" nell'accezione più ampia riportata nella Direttiva è la seguente: insieme equipaggiato o destinato a essere equipaggiato con un sistema di azionamenti diverso dalla forza umana o animale diretta, composto di parti o componenti, di cui almeno uno mobile, collegati tra loro solidamente per un'applicazione ben determinata

Marcatura CE apposta sulla macchina

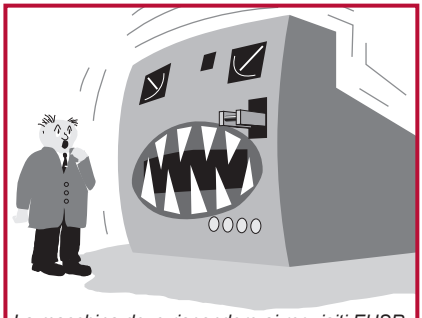
L'attuale Direttiva Macchine (2006/42/CE) ha sostituito la versione precedente (98/37/CE) alla fine del 2009. Essa comprende chiarimenti ed emendamenti, ma non introduce modifiche sostanziali ai requisiti essenziali per la salute e la sicurezza (EHSR) previsti. Invece, comprende delle modifiche da tenere presente a livello di tecnologie e metodi. Inoltre, il suo campo di applicazione è stato ampliato per coprire alcuni tipi di macchine in più (ad es. montacarichi per cantieri edili). Ora inoltre, è richiesta esplicitamente una valutazione dei rischi per la determinazione degli EHSR applicabili e sono state apportate delle modifiche relative alle procedure di valutazione della conformità per le macchine indicate nell'Allegato IV.

Le disposizioni principali della direttiva originaria (98/37/CE) sono entrate in vigore il 1° gennaio 1995 e i componenti di sicurezza il 1° gennaio 1997.

Le disposizioni della direttiva attuale (2006/42/CE) sono entrate in vigore il 29 dicembre 2009. È compito del produttore o di un suo rappresentante autorizzato assicurare la conformità alla direttiva dei macchinari forniti. Ciò comporta le seguenti attività:

- verifica del rispetto degli EHSR indicati nell'Allegato I della direttiva
- redazione di un dossier tecnico
- esecuzione delle opportune valutazioni di conformità
- fornitura di una "Dichiarazione di conformità CE"
- apposizione del marchio CE laddove applicabile
- fornitura di istruzioni per un uso corretto.

Requisiti fondamentali di salute e sicurezza



La macchina deve rispondere ai requisiti EHSR

Nell'Allegato 1 della direttiva è riportato un elenco dei requisiti fondamentali di salute e sicurezza (EHSR) a cui le macchine, ove pertinente, devono conformarsi. Scopo di questo elenco è quello di garantire che i macchinari siano sicuri, progettati e realizzati in modo che le operazioni di uso, regolazione e manutenzione non costituiscano un rischio per le persone, in tutte le fasi della loro vita operativa. Nel testo seguente sono riportati dei cenni generali relativi ad alcuni requisiti tipici, tuttavia è importante considerare tutti gli EHSR indicati nell'Allegato 1.

È necessario eseguire la valutazione dei rischi per determinare gli EHSR applicabili alla macchina in questione.

Gli EHSR riportati nell'Allegato 1 prevedono inoltre una gerarchia di misure atte a eliminare il rischio:

(1) Progettazione a sicurezza intrinseca. Nei casi in cui è possibile, il progetto stesso deve evitare l'insorgere di qualsiasi pericolo.

Laddove non sia possibile, occorre usare **(2) Dispositivi di protezione aggiuntivi** come, ad esempio, protezioni con punti di accesso interbloccati, protezioni non fisiche quali barriere fotoelettriche, pedane sensibili, ecc.

Qualsiasi rischio residuo che non possa essere evitato con i metodi sopra elencati deve essere evitato tramite l'uso di **(3) Dispositivi di protezione e/o formazione del personale**. Il fornitore della macchina deve specificare quanto appropriato.

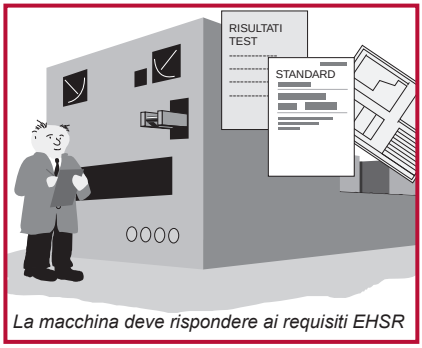
La macchina deve essere realizzata con materiali adatti alla costruzione e all'utilizzo. Devono inoltre essere fornite illuminazione e strumenti adeguati. I comandi e i sistemi di controllo devono essere sicuri e affidabili. Le macchine non devono essere in grado di avviarsi inaspettatamente e devono essere fornite di almeno un dispositivo di arresto di emergenza. Occorre prestare particolare attenzione alle installazioni complesse in cui i processi a monte o a valle possano influire sulla sicurezza della macchina. Un eventuale guasto all'alimentazione o ad un circuito di controllo non deve provocare situazioni pericolose. Le macchine devono essere stabili e in grado di resistere alle sollecitazioni prevedibili. Non devono presentare spigoli o superfici che possano causare ferite.

È necessario utilizzare protezioni o dispositivi di protezione che evitino l'insorgenza di rischi dovuti ad esempio a parti in movimento. Tali dispositivi devono essere robusti e difficili da escludere. Le protezioni fisse devono essere montate in modo che possano essere rimosse solo con l'ausilio di utensili. Le protezioni mobili devono essere interbloccate. Le protezioni regolabili non devono richiedere l'uso di utensili.

Occorre evitare l'insorgenza di rischi di natura elettrica o legati all'alimentazione. Il rischio di lesioni dovute a temperatura, esplosione, rumore, vibrazione, polvere, gas o radiazioni deve essere minimo. Devono essere previste disposizioni appropriate per la manutenzione e la riparazione. Devono inoltre essere forniti dispositivi di indicazione e allarme sufficienti. I macchinari devono esser forniti completi delle istruzioni per l'installazione, l'uso, la regolazione ecc. sicuri.

Valutazione di conformità

Il progettista o qualsiasi altro organismo responsabile deve essere in grado di attestare la conformità ai requisiti EHSR. Questo dossier dovrebbe includere tutte le informazioni pertinenti, come risultati di test, schemi, specifiche ecc.



La macchina deve rispondere ai requisiti EHSR

Una norma armonizzata europea (EN) pubblicata sulla Gazzetta Ufficiale dell'Unione Europea (OJ) sotto la Direttiva Macchine – la cui data di cessazione di presunzione di conformità non sia scaduta – conferisce presunzione di conformità a determinati requisiti EHSR (molte norme recenti pubblicate sulla Gazzetta includono un riferimento incrociato che identifica i requisiti EHSR coperti dalla norma).

Di conseguenza, quando le apparecchiature sono conformi alle attuali norme armonizzate europee, il compito di dimostrare la conformità con gli EHSR è molto semplificato e il produttore beneficia anche della maggiore sicurezza legale. Tali standard non sono richiesti per legge ma il loro utilizzo è fortemente consigliato, poiché dimostrare la conformità tramite metodi alternativi può essere molto complesso. Tali norme supportano la Direttiva Macchine e sono prodotte dal CEN (European Committee for Standardization) in collaborazione con ISO e da CENELEC (European Committee for Electrotechnical Standardization) in collaborazione con l'IEC.

È necessario condurre una valutazione dei rischi approfondita e documentata per garantire che siano stati analizzati tutti i potenziali rischi della macchina. Inoltre, è responsabilità del produttore assicurare il rispetto di tutti i requisiti EHSR, anche di quelli non trattati dalle norme armonizzate EN.

Dossier tecnico

Il produttore o un suo rappresentante autorizzato deve redigere un dossier tecnico per dimostrare la conformità ai requisiti EHSR. Questo dossier dovrebbe includere tutte le informazioni pertinenti, come risultati di test, schemi, specifiche ecc.

Non è fondamentale che tutte le informazioni siano costantemente disponibili in formato cartaceo, tuttavia, deve essere possibile mettere a disposizione l'intero dossier tecnico su richiesta in caso di ispezione da parte di un'autorità competente (organismo incaricato da un paese UE di monitorare la conformità delle macchine).

Come minimo, il dossier tecnico deve comprendere la seguente documentazione:

1. I disegni generali dell'attrezzatura, compresi i disegni del circuito di controllo.
2. I disegni dettagliati, le note di calcolo ecc. richiesti per la verifica della conformità della macchina con i requisiti essenziali di sicurezza e salute.
3. Documentazione relativa alla valutazione dei rischi, ivi compreso un elenco dei requisiti fondamentali di salute e sicurezza applicabili alla macchina e una descrizione delle misure di protezione adottate.
4. Un elenco degli standard o norme e di altre specifiche tecniche utilizzate, in cui siano indicati i requisiti fondamentali di salute e sicurezza considerati.
5. Una descrizione dei metodi adottati per eliminare i rischi presentati dalla macchina.
6. Se pertinenti, eventuali relazioni tecniche o certificati emessi da un laboratorio di prova o altro organismo.
7. Se viene dichiarata la conformità con una norma armonizzata europea, le relazioni tecniche contenenti i risultati dei relativi test.
8. Una copia delle istruzioni relative alla macchina.
9. Se appropriato, la dichiarazione di incorporazione delle macchine parzialmente completate incluse e le istruzioni di assemblaggio relative a tali macchine.
10. Se appropriato, copie della dichiarazione di conformità CE della macchina o di altri prodotti incorporati nella macchina.
11. Una copia della dichiarazione di conformità CE.

Per la produzione in serie, i dettagli sulle misure interne (ad esempio, sistemi di qualità) usate per garantire che tutti i macchinari prodotti siano conformi.

- I produttori devono eseguire tutte le ricerche o i test necessari su componenti, accessori o macchine complete per determinare se la progettazione e la costruzione ne consentono l'installazione e la messa in servizio sicura.
- Il dossier tecnico non deve essere necessariamente costituito da un solo documento, ma deve essere comunque possibile ricostruirlo e renderlo disponibile in tempi ragionevoli. Deve essere disponibile per dieci anni dopo la produzione dell'ultima unità.

Il dossier tecnico non deve necessariamente comprendere piani dettagliati o altre informazioni specifiche sui sottogruppi usati per la produzione della macchina, a meno che non siano essenziali per verificare la conformità con i requisiti essenziali di sicurezza e salute.

Valutazione di conformità per le macchine dell'Allegato IV

Valutazioni di conformità

Alcuni tipi di attrezzature sono soggette a misure speciali. Queste attrezzature sono elencate nell'Allegato IV della direttiva e comprendono le macchine pericolose quali alcuni macchinari per la lavorazione del legno, presse, macchine di stampaggio a iniezione, macchine per lavori sotterranei, ponti elevatori di veicoli, ecc.

L'Allegato IV comprende anche alcuni componenti di sicurezza come dispositivi di protezione destinati a rilevare la presenza delle persone (ad es. barriere fotoelettriche) e unità logiche per garantire le funzioni di sicurezza.

Nel caso di macchine comprese nell'Allegato IV non perfettamente conformi alle norme europee armonizzate applicabili, il produttore o suo rappresentante autorizzato deve adottare una delle seguenti procedure:

1. Esame di tipo CE. Occorre redigere un dossier tecnico e presentare un esempio della macchina a un organismo notificato (laboratorio di prova) per l'esame di tipo CE. Se l'esame viene superato, alla macchina sarà fornito il certificato di esame di tipo CE. La validità del certificato deve essere verificata ogni cinque anni da parte dell'organismo notificato.

2. Garanzia di qualità totale. Occorre redigere un dossier tecnico e il produttore deve applicare un sistema di qualità approvato per la progettazione, la produzione, l'ispezione finale e le prove. Il sistema di qualità deve garantire la conformità della macchina alle disposizioni di questa direttiva. Il sistema di qualità deve essere sottoposto a verifica ispettiva periodica da parte di un organismo notificato.

Valutazioni degli organismi notificati

Nel caso di macchine non incluse nell'Allegato IV o di macchine incluse nell'Allegato IV ma perfettamente conformi alle norme europee armonizzate applicabili, il produttore o suo rappresentante autorizzato in alternativa ha anche la possibilità di redigere autonomamente il dossier tecnico e di autocertificare la conformità della macchina. Devono essere previsti controlli interni per assicurare che la macchina prodotta rimanga conforme.

Organismi notificati

In tutta l'UE esiste una rete di organismi notificati che comunicano tra di loro e lavorano con criteri comuni. Gli organismi notificati sono nominati dai governi (non dall'industria) e tutte le informazioni relative a queste organizzazioni sono rintracciabili su:

http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_ en.htm

Procedura per la dichiarazione di conformità CE

CE

Su tutte le macchine fornite deve essere affisso il marchio CE. Inoltre, insieme alle macchine deve essere fornita una Dichiarazione di Conformità CE.

Il marchio CE attesta che la macchina è conforme a tutte le Direttive Europee applicabili e che è stata sottoposta a tutte le corrispondenti procedure di valutazione della conformità. Apporre il marchio CE per la Direttiva Macchine è un reato se la macchina non soddisfa i requisiti essenziali di sicurezza e salute.

La Dichiarazione di conformità CE deve contenere le seguenti informazioni:

- Ragione sociale e indirizzo completo del produttore e, se appropriato, del rappresentante autorizzato;
- Nome e indirizzo della persona autorizzata a redigere il dossier tecnico, che deve essere residente nella Comunità (nel caso di un produttore con sede al di fuori dell'UE può essere il "Rappresentante autorizzato");
- Descrizione e identificazione della macchina, comprendente denominazione generica, funzione, modello, tipo, numero di serie e nome commerciale;
- Una frase in cui si dichiari espressamente che la macchina è conforme a tutte le disposizioni pertinenti di questa direttiva e, se appropriato, una frase simile in cui si dichiari la conformità ad altre direttive e/o disposizioni pertinenti a cui la macchina è conforme;
- Se appropriato, un riferimento alle norme armonizzate utilizzate;
- Se appropriato, un riferimento alle altre norme armonizzate e specifiche utilizzate;
- (Per le macchine dell'Allegato IV) se appropriato, il nome, l'indirizzo e il numero di identificazione dell'organismo notificato che ha eseguito l'esame di tipo CE indicato nell'Allegato IX e il numero del certificato dell'esame di tipo CE;
- (Per le macchine dell'Allegato IV) se appropriato, il nome, l'indirizzo e il numero di identificazione dell'organismo notificato che ha approvato il sistema di garanzia qualità totale a cui si fa riferimento nell'Allegato X;
- Luogo e data della dichiarazione;
- Identità e firma della persona autorizzata a redigere la dichiarazione per conto del produttore o del rappresentante autorizzato.

Dichiarazione CE di incorporazione di macchine parzialmente completate

Se la macchina fornita è destinata a essere assemblata con altri elementi con cui andrà a costituire una macchina completa in una data successiva, dovrà essere accompagnata da una DICHIARAZIONE DI INCORPORAZIONE. Il marchio CE NON deve essere apposto. La dichiarazione dovrebbe affermare che l'attrezzatura non deve essere messa in servizio finché la macchina in cui sarà incorporata non sarà stata dichiarata conforme. È necessario redigere un dossier tecnico, e insieme alla macchina parzialmente completata devono essere fornite informazioni comprendenti una descrizione delle condizioni che devono essere soddisfatte per una corretta incorporazione nella macchina finale, in modo tale da non compromettere la sicurezza.

Questa opzione non è disponibile per le attrezzature che funzionano indipendentemente o che modificano la funzione della macchina.

La Dichiarazione di incorporazione deve contenere le seguenti informazioni:

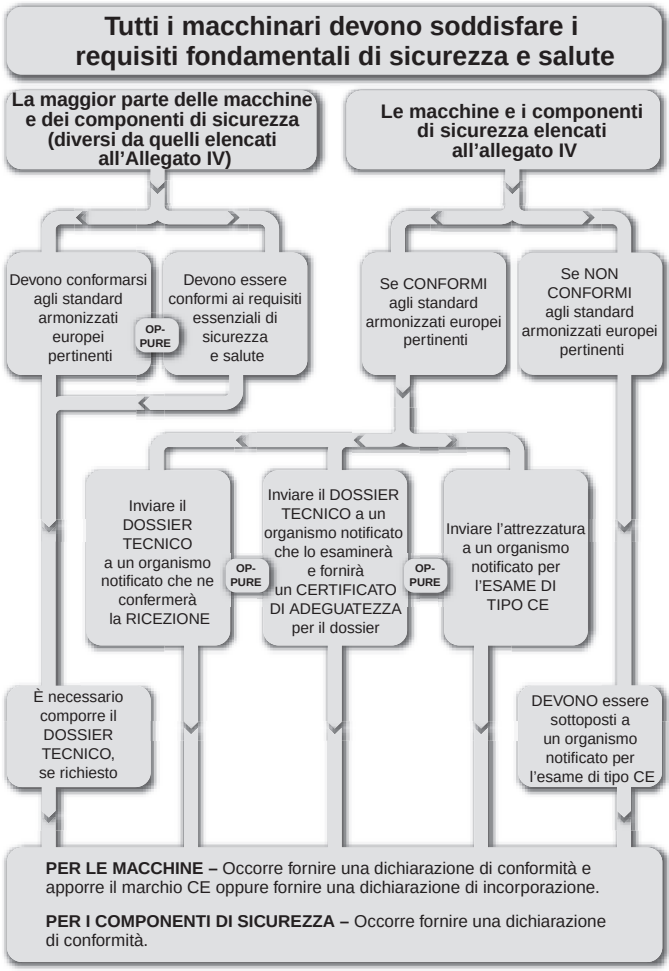
- Ragione sociale e indirizzo completo del produttore della macchina parzialmente completata e, se appropriato, del rappresentante autorizzato
- Nome e indirizzo della persona autorizzata a redigere la documentazione tecnica applicabile, che deve essere residente nella Comunità (nel caso di un produttore con sede al di fuori dell'UE può essere il "Rappresentante autorizzato");
- Descrizione e identificazione della macchina parzialmente completata, comprendente denominazione generica, funzione, modello, tipo, numero di serie e nome commerciale;
- Una frase in cui si indichino i requisiti essenziali di questa direttiva applicati soddisfatti e in cui si dichiari che la documentazione tecnica applicabile è stata compilata in conformità con la parte B dell'Allegato VII, e, se appropriato, una frase in cui si dichiari la conformità della macchina parzialmente completata ad altre direttive applicabili;
- Un impegno a trasmettere, in risposta a una richiesta circostanziata da parte delle autorità nazionali, informazioni rilevanti in merito alla macchina parzialmente completata. Si dovrà indicare il metodo di trasmissione, che non dovrà compromettere i diritti di proprietà intellettuale del produttore della macchina parzialmente completata;
- Una frase in cui si dichiari che la macchina parzialmente completata non dovrà essere messa in servizio fino a quando la macchina finale in cui dovrà essere incorporata non sarà stata dichiarata conforme alle disposizioni di questa direttiva, se appropriato;
- Luogo e data della dichiarazione;
- Identità e firma della persona autorizzata a redigere la dichiarazione per conto del produttore o del rappresentante autorizzato.

Macchine fornite da Paesi non appartenenti all'UE – Rappresentanti autorizzati

Se un produttore con sede in un Paese non appartenente all'UE (o SEE) esporta delle macchine nell'UE, dovrà incaricare un rappresentante autorizzato.

Per "rappresentante autorizzato" si intende una persona fisica o giuridica residente nella Comunità europea che ha ricevuto dal produttore un mandato scritto che la autorizza ad agire per suo conto in relazione agli obblighi e alle formalità connesse alla Direttiva Macchine.

La Direttiva europea “Uso delle attrezzature di lavoro” (Direttiva U.W.E.)



Procedura schematica per la Direttiva Macchine

Mentre la Direttiva Macchine è indirizzata ai fornitori, questa Direttiva (89/655/CEE modificata dalle direttive 95/63/CE, 2001/45/CE e 2007/30/CE) è rivolta agli utilizzatori delle macchine. Riguarda tutti i settori industriali e prevede sia obblighi generali per i datori di lavoro che requisiti minimi di sicurezza delle attrezzature di lavoro. Tutti i paesi UE hanno recepito tale direttiva nelle proprie leggi nazionali per poterla applicare.

Ad esempio, nel Regno Unito, è stata recepita con il nome di “The Provision and Use of Work Equipment Regulations” (spesso indicata con la sigla P.U.W.E.R.). Il tipo di implementazione può variare tra i diversi paesi, ma l’effetto della direttiva rimane invariato.

Gli articoli della direttiva forniscono informazioni dettagliate sui tipi di attrezzature e luoghi di lavoro oggetto della direttiva.

Inoltre, prevedono doveri generali per i datori di lavoro, quali l’istituzione di sistemi sicuri di lavoro e la fornitura di attrezzature adeguate e sicure sottoposte a una corretta manutenzione. Gli operatori delle macchine devono ricevere informazioni e addestramento adeguati per un uso sicuro della macchina.

Le macchine nuove (e le macchine di seconda mano provenienti da paesi esterni all’UE) fornite dopo il 1° gennaio 1993 devono soddisfare le direttive relative al prodotto pertinenti, ad esempio la Direttiva Macchine (questo è soggetto ad accordi transitori). Le macchine di seconda mano provenienti dall’UE fornite per la prima volta nel luogo di lavoro devono soddisfare immediatamente i requisiti minimi indicati nell’allegato della Direttiva U.W.E.

Nota: le macchine esistenti o di seconda mano revisionate o modificate in modo significativo saranno classificate quali attrezzature nuove, pertanto gli interventi apportati devono garantire la conformità con la Direttiva Macchine (anche se si tratta di macchine per uso proprio della società).

L’adeguatezza delle attrezzature di lavoro è un requisito importante della direttiva e sottolinea la responsabilità del datore di lavoro nella realizzazione di una corretta procedura di valutazione dei rischi.

È richiesta una manutenzione corretta della macchina. Normalmente, questo significa che deve esistere un piano di manutenzione ordinaria e preventiva pianificato. Si consiglia di compilare un registro e tenerlo aggiornato. Ciò è particolarmente importante quando la manutenzione e l’ispezione delle attrezzature contribuiscono alla costante integrità della sicurezza di un dispositivo o di un sistema di protezione.

Nell’Allegato della Direttiva U.W.E. sono riportati i requisiti minimi generali applicabili all’attrezzatura di lavoro.

Se le attrezzature sono conformi alle direttive sul prodotto pertinenti, ad esempio la Direttiva Macchine, risulteranno automaticamente conformi ai requisiti di progettazione delle macchine riportati tra i requisiti minimi dell’Allegato.

Agli Stati membri è consentito emanare leggi riguardanti l’uso di attrezzature di lavoro con requisiti più restrittivi rispetto ai requisiti minimi della Direttiva U.W.E.

Per informazioni dettagliate sulla Direttiva “Uso delle attrezzature di lavoro” è possibile consultare il sito Internet ufficiale dell’UE:

http://europa.eu/legislation_summaries/employment_and_social_policy/health_hygiene_safety_at_work/c11116_en.htm

Regolamenti USA

Questa sezione presenta alcuni dei regolamenti di sicurezza relativi alla protezione delle macchine industriali negli Stati Uniti. Si tratta solo di un punto di partenza; gli interessati dovranno approfondire ulteriormente i requisiti relativi alle proprie applicazioni e adottare le misure necessarie a garantire che progetti, procedure e metodi di uso e manutenzione rispondano alle proprie esigenze così come ai regolamenti e ai codici nazionali e locali.

Esistono numerose organizzazioni che promuovono la sicurezza industriale negli Stati Uniti. Queste includono:

1. società, che usano i requisiti stabiliti oltre a stabilire i propri requisiti interni;
2. la Occupational Safety and Health Administration (OSHA);
3. organizzazioni industriali quali National Fire Protection Association (NFPA), Robotics Industries Association (RIA) e Association of Manufacturing Technology (AMT), oltre ai fornitori di soluzioni e prodotti di sicurezza quali Rockwell Automation.

OSHA (Occupational Safety and Health Administration)

Negli Stati Uniti, uno dei promotori principali della sicurezza industriale è la Occupational Safety and Health Administration (OSHA). L’OSHA è stata fondata nel 1970 da una legge del Congresso degli USA. Lo scopo di tale legge è garantire condizioni di lavoro salutari e sicure e preservare le risorse umane. La legge autorizza il Secretary of Labor a definire standard obbligatori, relativi a sicurezza e salute sul lavoro, applicabili alle aziende che commerciano all’interno degli Stati Uniti. Questa legge si applica a tutti i posti di lavoro in uno Stato, nel Distretto di Columbia, nel Commonwealth di Porto Rico, nelle Isole Vergini, nelle Samoa Americane, a Guam, nel Territorio fiduciario delle Isole del Pacifico, nell’Isola di Wake, nelle Outer Continental Shelf Lands definite nell’Outer Continental Shelf Lands Act, nell’Isola Johnston e nella Zona del Canale di Panama.

L’articolo 5 della legge stabilisce i requisiti di base. Ogni datore di lavoro deve fornire, a ognuno dei suoi dipendenti, un lavoro e un posto di lavoro non soggetti a rischi conosciuti che provochino o possano provocare morte o gravi lesioni fisiche. Deve inoltre conformarsi agli standard relativi a salute e sicurezza sul lavoro promulgati da questa legge.

L'articolo 5, inoltre, stabilisce che ogni dipendente deve conformarsi agli standard relativi a salute e sicurezza sul lavoro e a tutte le regole e i regolamenti emessi in base a questa legge e applicabili alle proprie azioni e alla propria condotta.

La legge OSHA prevede responsabilità sia per il datore di lavoro sia per il dipendente. Decisamente diversa la Direttiva Macchine, che impone ai fornitori di immettere sul mercato macchine che non presentino pericoli. Negli Stati Uniti, un fornitore può vendere una macchina senza alcuna protezione. Spetta all'utente il compito di dotare la macchina delle protezioni necessarie a renderla sicura. Sebbene questa fosse una pratica comune quando la legge è stata approvata, la tendenza attuale è quella di fornire macchine dotate di protezioni, poiché concepire una macchina completa di tutti i dispositivi di sicurezza necessari è molto più economico che aggiungere le protezioni dopo la progettazione e la costruzione. Al fine di conformarsi agli standard, fornitori e utilizzatori dovranno comunicare in modo efficace in relazione ai requisiti di protezione, in modo da consentire la costruzione di macchine non solo sicure ma anche più produttive.

Il Secretary of Labor ha l'autorità di promulgare, come standard di salute e sicurezza sul lavoro, qualunque standard che goda di consenso nazionale e qualunque standard federale stabilito, a meno che la promulgazione di tale standard non risulti in un miglioramento delle condizioni di sicurezza e salute solo di certe categorie.

L'OSHA svolge questo ruolo pubblicando regolamenti al Titolo 29 del Code of Federal Regulation (29 CFR). Gli standard che riguardano le macchine industriali sono pubblicati dall'OSHA nella Parte 1910 del 29 CFR. Questi standard sono disponibili sul sito web OSHA – www.osha.gov. Diversamente da molti standard, la cui applicazione è volontaria, gli standard OSHA sono obbligatori di legge.

Alcune delle parti più importanti relative alla sicurezza delle macchine sono le seguenti:

- A – Dati generali
- B – Adozione ed estensione degli Established Federal Standards
- C – Disposizioni generali su salute e sicurezza
- H – Materiali pericolosi
- I – Dispositivi di protezione personale
- J – Controlli ambientali generali – tra cui Lockout/Tagout
- O – Protezione delle macchine e dei macchinari
- R – Settori speciali
- S – Impianti elettrici

Alcuni standard OSHA incorporano, per riferimento, una serie di standard volontari. L'effetto legale dell'incorporazione per riferimento è che il materiale viene trattato come se fosse stato pubblicato per intero nel Federal Register. Quando uno standard che gode di consenso nazionale viene incorporato per riferimento in una delle sottoparti, è considerato obbligatorio. Ad esempio, l'NFPA 70, uno standard volontario conosciuto come US National Electric Code, è riportato nella Sottoparte S. Ciò rende obbligatori i requisiti contenuti nello standard NFPA 70.

Il 29 CFR 1910.147, nella Sottoparte J, è dedicato al controllo delle fonti di energia pericolosa. Si tratta di ciò che è più generalmente conosciuto come lo standard "Lockout/Tagout". Lo standard volontario corrispondente è ANSI Z244.1. Fondamentalmente, questo standard richiede che, prima degli interventi di assistenza e manutenzione, l'alimentazione della macchina venga scollegata e bloccata. Lo scopo è prevenire la messa in tensione o l'avviamento non previsti della macchina e i conseguenti infortuni ai danni dei lavoratori.

I datori di lavoro devono stabilire un programma e utilizzare precise procedure per la sistemazione di adeguati dispositivi di lockout o tagout sui dispositivi di isolamento dell'alimentazione e per disabilitare altrimenti le macchine o le apparecchiature in modo da impedirne la messa in tensione, l'avviamento o il rilascio di energia accumulata, involontari o imprevisti, ed evitare infortuni ai danni dei lavoratori.

Questo standard non copre modifiche e regolazioni di minore importanza e altre operazioni ordinarie che devono avvenire durante il normale funzionamento delle macchine se si tratta di interventi ripetitivi e integranti nell'utilizzo delle apparecchiature di produzione, ammesso che il lavoro sia svolto usando misure alternative che forniscano un'adeguata protezione. Come misure alternative si intendono dispositivi di protezione quali barriere fotoelettriche, pedane di sicurezza, interblocchi porte e altri simili dispositivi collegati a un sistema di sicurezza. La difficoltà, per il progettista di macchine e per l'utilizzatore, sta nel determinare gli aspetti di "minore importanza" e quelli di "routine, ripetitivi e integranti nell'utilizzo".

La Sottoparte O è relativa alla protezione di macchine e macchinari ("Machinery and Machine Guarding"). Questa sottoparte elenca i requisiti generali per tutte le macchine e quelli di alcune particolari macchine. Dal 1970, anno in cui è stato costituito, l'OSHA ha adottato molti standard ANSI esistenti. Ad esempio B11.1 per le presse meccaniche è stato adottato come 1910.217.

Il 1910.212 è lo standard generale OSHA per le macchine. Stabilisce che, per proteggere l'operatore e il personale vicino alla macchina da pericoli come quelli creati dal punto di lavoro, punti di intrappolamento, parti rotanti, schegge e scintille, occorre prevedere uno o più metodi di protezione della macchina. Le protezioni devono essere, quando possibile, installate sulla macchina o fissate in qualunque

altro posto se, per qualche ragione, fosse impossibile farlo sulla macchina. La protezione deve essere tale da non costituire essa stessa un pericolo.

Il “punto di lavoro” è la zona della macchina in cui viene effettivamente lavorato il materiale. Il punto di lavoro di una macchina, il cui funzionamento espone il personale a rischio di lesioni, deve essere protetto. Il dispositivo di protezione deve essere conforme ai corrispondenti standard o, in assenza di specifici standard applicabili, deve essere concepito e costruito in modo tale da impedire che l’operatore introduca una qualunque parte del suo corpo nella zona di pericolo durante il ciclo operativo.

La Sottoparte S (1910.399) stabilisce i requisiti elettrici OSHA. Un’installazione o un’apparecchiatura è accettabile per l’Assistant Secretary of Labor e approvata, secondo i criteri di questa Sottoparte S, se è accettata, certificata, omologata, etichettata o altrimenti dichiarata sicura da un laboratorio di prova riconosciuto a livello nazionale (NRTL).

Che cos’è un’apparecchiatura? Un termine generale che include materiali, accessori, dispositivi, apparecchi, attrezzi di fissaggio, apparati e altri componenti simili usati come parte integrante di un’installazione elettrica o in collegamento ad essa.

Che cosa significa “omologata” (“listed”)? L’apparecchiatura è “omologata” se corrisponde al tipo menzionato in una lista che, (a) sia pubblicata da un laboratorio riconosciuto a livello nazionale che effettua periodiche ispezioni della produzione di tale apparecchiatura, e (b) attesti che tale apparecchiatura risponde agli standard riconosciuti a livello nazionale o è stata testata e riconosciuta sicura per l’uso designato.

Nell’agosto 2009, i laboratori di prova riconosciuti a livello nazionale (NRTL) dall’OSHA erano i seguenti:

- Canadian Standards Association (CSA)
- Communication Certification Laboratory, Inc. (CCL)
- Curtis-Straus LLC (CSL)
- FM Approvals LLC (FM)
- Intertek Testing Services NA, Inc. (ITSNA)
- MET Laboratories, Inc. (MET)
- NSF International (NSF)
- National Technical Systems, Inc. (NTS)
- SGS U.S. Testing Company, Inc. (SGSUS)
- Southwest Research Institute (SWRI)
- TUV America, Inc. (TUVAM)
- TUV Product Services GmbH (TUVPSG)
- TUV Rheinland of North America, Inc. (TUV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

Alcuni stati hanno adottato i propri OSHA locali. Ventiquattro stati, Porto Rico e le Isole Vergini hanno piani nazionali approvati dall'OSHA e hanno adottato propri standard e proprie politiche di applicazione. Nella maggior parte dei casi, questi stati adottano standard identici agli OSHA federali. Tuttavia, alcuni stati hanno adottato standard differenti o diverse politiche di applicazione. I datori di lavoro devono riferire all'OSHA la storia degli incidenti. L'OSHA compila i tassi di incidenti, trasmette le informazioni agli uffici locali e utilizza queste informazioni per pianificare le ispezioni. I principali criteri di controllo sono:

- pericolo imminente
- catastrofi e fatalità
- reclami dei dipendenti
- industrie ad alto rischio
- ispezioni locali pianificate
- ispezioni di monitoraggio
- programmi a livello nazionale e locale

La violazione degli standard OSHA può comportare delle sanzioni. Violazioni e sanzioni sono classificate come segue:

- Grave fino a 7.000 USD per violazione
- Non grave: a discrezione ma non oltre 7.000 USD
- Recidiva: fino a 70.000 USD per violazione
- Intenzionale: fino a 70.000 USD per violazione
- Violazioni causa di decessi: ulteriori penali
- Mancato intervento: 7.000 USD/giorno

La tabella che segue mostra le prime 14 citazioni OSHA, da ottobre 2004 a settembre 2005.

Standard	Descrizione
1910.147	Il controllo delle fonti di energia pericolose (Lockout/Tagout)
1910.1200	Comunicazione dei pericoli
1910.212	Requisiti generali per tutte le macchine
1910.134	Protezione respiratoria
1910.305	Metodi di cablaggio, componenti e apparecchiature di uso generale
1910.178	Veicoli industriali a motore
1910.219	Trasmissione meccanica
1910.303	Requisiti generali
1910.213	Macchinari di lavorazione del legno
19102.215	Mole abrasive
19102.132	Requisiti generali
1910.217	Presse meccaniche
1910.095	Esposizione al rumore sul luogo di lavoro
1910.023	Protezione di fori e aperture a muro e a pavimento

Regolamenti canadesi

In Canada, la sicurezza industriale è governata a livello provinciale. Ogni provincia mantiene e applica i propri regolamenti. L'Ontario, ad esempio, ha promulgato l'Occupational Health and Safety Act che stabilisce i diritti e i doveri di tutti i soggetti sul luogo di lavoro. Il suo scopo principale è quello di proteggere i lavoratori contro i pericoli per la salute e la sicurezza sul lavoro. La legge definisce una serie di procedure atte a gestire i rischi sul posto di lavoro e ne impone l'implementazione per legge nei casi in cui ciò non avvenga volontariamente.

La legge include il regolamento 851, sezione 7, che definisce l'analisi delle condizioni di preavviamento relative a salute e sicurezza. Questa analisi è un requisito dell'Ontario per qualunque componente di macchinari nuovo, ricostruito o modificato, per cui un tecnico professionista deve redigere un rapporto.

Standard e norme

Questa sezione fornisce una lista di alcuni tipici standard e norme, internazionali e nazionali, relativi alla sicurezza delle macchine. Non vuole essere un elenco esaustivo ma dare piuttosto una visione d'insieme sulle problematiche di sicurezza delle macchine che sono oggetto di standardizzazione.

Questa sezione deve essere letta congiuntamente alla sezione dedicata ai regolamenti.

Tutti i paesi stanno lavorando per l'armonizzazione globale degli standard. Ciò è particolarmente evidente nel campo della sicurezza delle macchine. Gli standard di sicurezza globali per le macchine sono governati da due organizzazioni: ISO e IEC. Le norme regionali e nazionali sono ancora in vigore e continuano a supportare i requisiti locali ma, in molti paesi, si è affermata una tendenza all'uso di standard internazionali redatti da ISO e IEC.

Le norme EN (European Norm), ad esempio, vengono utilizzate in tutti i paesi EEA. Tutte le nuove norme EN sono allineate con le norme ISO e IEC e, in molti casi, presentano un testo identico.

L'IEC tratta le problematiche elettrotecniche e l'ISO si occupa di tutte le altre questioni. Molti paesi industrializzati sono membri di IEC e ISO. Gli standard di sicurezza per le macchine sono redatti da gruppi di lavoro costituiti da esperti dei vari paesi industrializzati del mondo.

In molti paesi, gli standard possono essere considerati volontari mentre i regolamenti sono legalmente obbligatori. Tuttavia, gli standard vengono solitamente utilizzati come interpretazione pratica dei regolamenti. Quindi, l'ambito degli standard e quello dei regolamenti sono strettamente interrelati.

Per un elenco completo degli standard, consultare il catalogo sulla sicurezza disponibile sul sito: www.ab.com/safety for a comprehensive list of standards.

ISO (International Organization for Standardization)

L'ISO è una organizzazione non governativa costituita da organismi di normazione nazionali di molti paesi (157 attualmente). Una Segreteria Centrale situata a Ginevra, in Svizzera, coordina il sistema. L'ISO elabora standard atti a progettare, costruire e utilizzare le macchine in modo più efficiente, più sicuro e più pulito. Gli standard, inoltre, facilitano e rendono più trasparente il commercio tra i diversi paesi. Gli standard ISO possono essere identificati dalle tre lettere ISO.

Gli standard ISO per le macchine sono organizzati come gli standard EN, in tre livelli: Tipo A, B e C (v. l'ultima sezione sulle Norme Armonizzate Europee EN).

Per ulteriori informazioni, visitare il sito web ISO: *www.iso.org*.

IEC (International Electrotechnical Commission)

L'IEC redige e pubblica standard internazionali per impianti elettrici, elettronici e relative tecnologie. Attraverso i suoi membri, l'IEC promuove la collaborazione internazionale su tutte le questioni di standardizzazione elettrotecnica e temi collegati, come la valutazione della conformità agli standard elettrotecnici.

Per ulteriori informazioni, visitare il sito web IEC: www.iec/ch

Norme europee armonizzate EN

Questi standard sono condivisi da tutti i paesi SEE e sono redatti dagli enti di normazione europei CEN e CENELEC. Il loro uso è volontario, ma progettare e produrre le apparecchiature in base a questi standard è il modo più semplice e diretto per dimostrare la conformità ai requisiti fondamentali di sicurezza e salute della Direttiva Macchine.

Sono suddivisi in 3 tipi: standard A, B e C.

STANDARD di tipo A: trattano aspetti relativi a tutti i tipi di macchina.

STANDARD di tipo B: sono suddivisi in 2 gruppi.
STANDARD di Tipo B1: trattano aspetti di sicurezza ed ergonomicità specifici dei macchinari.
STANDARD di Tipo B2: riguardano i componenti di sicurezza e i dispositivi di protezione.

STANDARD di tipo C: riguardano tipi o gruppi specifici di macchine.

È importante notare che la conformità con uno standard C implica automaticamente la presunzione di conformità con i requisiti essenziali di sicurezza e salute. In assenza di uno standard C pertinente, è possibile usare gli standard A e B come prova totale o parziale della conformità ai requisiti EHSR evidenziando il rispetto delle sezioni pertinenti.

Per la collaborazione tra CEN/CENELEC e organismi come ISO e IEC, è stata stipulata una serie di accordi miranti alla definizione di standard comuni a livello mondiale. In molti casi, uno standard EN ha uno standard analogo in IEC o ISO. In generale, i due testi sono uguali ed eventuali differenze locali vengono presentate nella premessa dello standard.

Per una lista completa degli standard EN sulla sicurezza delle macchine, accedere a:

http://ec.europa.eu/enterprise/sectors/mechanical/machinery/index_ en.htm.

Standard USA

Standard OSHA

Quando possibile, l'OSHA promulga standard a consenso nazionale o standard federali stabiliti come standard di sicurezza. Le disposizioni obbligatorie (ad es. la parola "deve" implica il carattere obbligatorio) degli standard incorporati per riferimento hanno la stessa forza e lo stesso effetto degli standard elencati nella Parte 1910. Ad esempio, lo standard a consenso nazionale NFPA 70 è riportato come documento di riferimento nell'Appendice A della Sottoparte S-Impianti elettrici della Parte 1910 del 29 CFR. NFPA 70 è uno standard volontario sviluppato dalla National Fire Protection Association (NFPA). Lo standard NFPA 70 è conosciuto anche come National Electric Code (NEC). Per incorporazione, tutti i requisiti obbligatori del NEC sono obbligatori anche per l'OSHA.

Standard ANSI

L'American National Standards Institute (ANSI) funge da amministratore e coordinatore del sistema di standardizzazione volontario del settore privato degli Stati Uniti. Si tratta di un'organizzazione di membri privata e senza scopo di lucro sostenuta da numerose organizzazioni del settore pubblico e privato.

ANSI non si occupa propriamente della creazione degli standard ma ne facilita lo sviluppo promuovendone il consenso tra gruppi qualificati. ANSI, inoltre, garantisce che tutti i gruppi qualificati rispettino i principi di consenso, correttezza dei processi

e trasparenza. Di seguito è riportato un elenco parziale degli standard di sicurezza industriale che si possono ricevere contattando l'ANSI.

Questi standard si distinguono tra standard applicativi e standard costruttivi. Gli standard applicativi determinano il modo in cui applicare una protezione di sicurezza alla macchina. Alcuni esempi sono l'ANSI B11.1, che fornisce informazioni su come usare le protezioni sulle presse e l'ANSI/RIA R15.06, che descrive l'uso dei dispositivi di sicurezza per la protezione dei robot.

NFPA (National Fire Protection Association)

La National Fire Protection Association (NFPA) è stata costituita nel 1896. La sua missione è ridurre i danni causati dagli incendi migliorando la qualità della vita tramite l'uso di codici e standard basati su dati scientifici, la ricerca e l'addestramento in merito alle problematiche riguardati il fuoco e la sicurezza. La NFPA promuove l'uso di numerosi standard che aiutino a realizzare tale missione. Due standard molto importanti correlati alla sicurezza industriale e alla salvaguardia sono il National Electric Code (NEC) e l'Electrical Standard for Industrial Machinery.

L'NFPA agisce in qualità di sostenitore del NEC fin dal 1911. Il documento del codice originale è stato sviluppato nel 1897 in seguito allo sforzo congiunto di vari interessi legati a diversi settori, tra cui quello elettrico, edilizio e delle assicurazioni. Da allora, il NEC è stato aggiornato diverse volte e viene revisionato ogni tre anni circa. L'articolo 670 del NEC contiene alcuni dettagli relativi ai macchinari industriali e fa riferimento all'Electrical Standard for Industrial Machinery, NFPA 79.

NFPA 79 si applica ad attrezzature, apparati o sistemi di macchine industriali elettrici/elettronici che operano a una tensione pari a un massimo di 600 Volt. Lo scopo dell'NFPA 79 è fornire informazioni dettagliate per l'applicazione di attrezzature, apparati o sistemi elettrici/elettronici che fanno parte di macchinari industriali in modo tale da promuovere la sicurezza di beni e persone. L'NFPA 79, adottato ufficialmente da ANSI nel 1962, è molto simile nel contenuto allo standard IEC 60204-1.

Le macchine che non sono coperte da standard specifici OSHA devono essere prive dei rischi riconosciuti e che possono provocare il decesso o danni personali gravi. Tali macchine devono essere progettate e sottoposte a manutenzione almeno conformemente agli standard industriali applicabili. NFPA 79 è uno standard che si applica alle macchine non specificamente coperte dagli standard OSHA.

Standard canadesi

Gli standard CSA riflettono il consenso nazionale di produttori e utilizzatori – tra cui produttori, consumatori, rivenditori, associazioni, organizzazioni professionali e agenzie governative. Gli standard sono ampiamente usati dall'industria e dal commercio e, spesso, adottati nei regolamenti di governi municipali, provinciali e federali, soprattutto nei campi della salute, della sicurezza, dell'edilizia e dell'ambiente.

Privati, società e associazioni di tutto il Canada sostengono attivamente lo sviluppo degli standard CSA, dedicando, in qualità di volontari, tempo e capacità al lavoro del Comitato CSA e supportando gli obiettivi dell'associazione attraverso la loro attiva partecipazione. Il CSA può contare, in totale, su più di 7.000 volontari dei comitati e 2.000 soci sostenitori.

Lo Standards Council of Canada è l'organo di coordinamento del sistema National Standards, una federazione di organizzazioni indipendenti e autonome che lavorano per l'ulteriore sviluppo e miglioramento della standardizzazione volontaria, nell'interesse nazionale.

Standard australiani

Molti di questi standard sono strettamente allineati con gli equivalenti standard ISO/IEC/EN

Standards Australia Limited
286 Sussex Street, Sydney, NSW 2001
Telefono: +61 2 8206 6000
E-mail: mail@standards.org.au
Sito web: www.standards.org.au

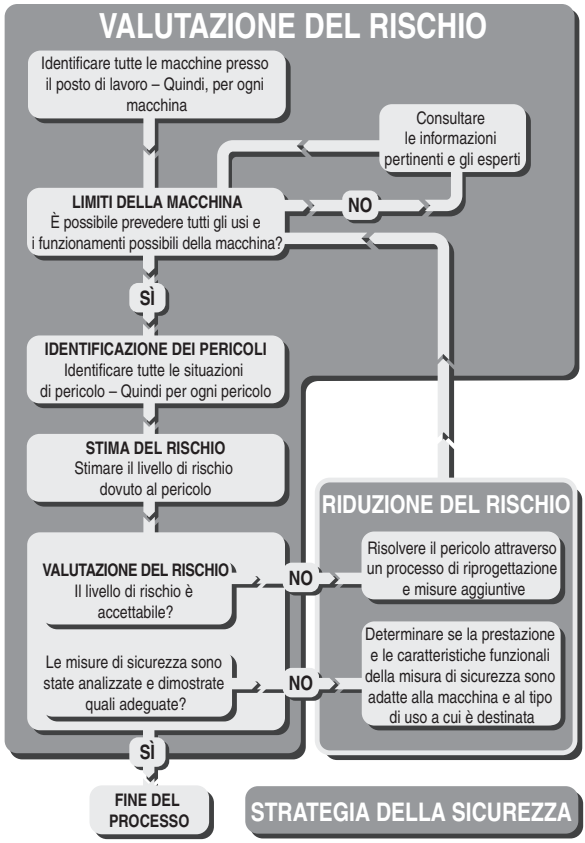
Per acquistare copie degli standard:
SAI Global Limited
286 Sussex Street, Sydney, NSW 2001
Telefono: +61 2 8206 6000
Fax: +61 2 8206 6001
E-mail: mail@sai-global.com
Sito web: www.saiglobal.com/shop

Per un elenco completo degli standard, consultare il catalogo sulla sicurezza disponibile sul sito: www.ab.com/safety.

Strategia della sicurezza

Da un punto di vista puramente funzionale, maggiore è l'efficienza di una macchina nello svolgere la propria attività di lavorazione dei materiali, migliore essa è. Tuttavia, affinché una macchina sia utilizzabile deve anche essere sicura. La sicurezza deve certamente essere considerata di primaria importanza.

Per individuare la corretta strategia di sicurezza, è necessaria l'interazione di due fasi chiave, come mostrato di seguito.



La **VALUTAZIONE DEI RISCHI**, basata su una chiara comprensione dei limiti e delle funzioni della macchina e delle attività che la macchina può dover svolgere durante la sua vita operativa.

La **RIDUZIONE DEI RISCHI** viene eseguita se necessario e le misure di sicurezza vengono selezionate in base alle informazioni ricavate dalla fase di valutazione del rischio. Il modo in cui questo viene fatto rappresenta la base della STRATEGIA DELLA SICUREZZA per la macchina.

È necessario un elenco di controllo da seguire per garantire che tutti gli aspetti siano presi in considerazione e che il principio fondamentale non venga perso di vista nei dettagli. Innanzitutto l'intero processo dovrebbe essere documentato. Questo non solo assicura l'esecuzione di un lavoro più accurato, ma consente anche di rendere disponibili i risultati affinché siano controllati da terzi.

Questa sezione è rivolta sia ai produttori sia agli utilizzatori di macchine. Il produttore deve garantire che la macchina possa essere utilizzata in sicurezza. La valutazione dei rischi dovrebbe essere iniziata in fase di progettazione e dovrebbe considerare tutte le attività previste per la macchina. Questo approccio basato sulle attività, nella fase preliminare di valutazione dei rischi, è molto importante. Ad esempio, può esserci l'esigenza di regolare le parti mobili della macchina. In fase progettuale, dovrebbe essere possibile prevedere misure che consentano di realizzare in sicurezza queste operazioni. Se ciò non avviene in una fase preliminare, può essere difficile o impossibile farlo in una fase successiva. Il risultato potrebbe essere che la regolazione delle parti mobili deve comunque essere realizzata ma in mancanza di sicurezza o in modo inefficiente (o entrambi). Una macchina per la quale siano state considerate tutte le attività durante la valutazione dei rischi sarà più sicura ed efficiente.

L'utilizzatore (o il datore di lavoro) deve garantire che le macchine, nell'ambiente di lavoro, siano sicure. Anche se una macchina è stata dichiarata sicura dal produttore, l'utilizzatore dovrebbe comunque procedere a una valutazione dei rischi per determinare se l'apparecchiatura è sicura nel proprio ambiente di installazione. Le macchine vengono spesso usate in circostanze che il produttore non può prevedere. Ad esempio, una fresatrice usata in un laboratorio scolastico richiederà che vengano fatte ulteriori considerazioni rispetto al caso di una fresa usata in un'officina industriale.

Occorre inoltre ricordare che se una società utilizzatrice acquista due o più macchine indipendenti e le integra all'interno di un processo, diventa a sua volta produttrice della macchina combinata risultante.

Vediamo ora i passaggi principali verso la definizione di una adeguata strategia di sicurezza. Quanto segue può essere applicato alle installazioni già esistenti in fabbrica o a una macchina nuova singola.

Valutazione dei rischi

È errato considerarla come un onere. È invece una procedura utile che fornisce informazioni essenziali e consente all'utente o al progettista di prendere decisioni ragionate sui metodi per garantire la sicurezza.

Esistono vari standard che trattano questo argomento. ISO 14121: "Principi per la valutazione dei rischi" e ISO 12100: "Sicurezza delle macchine – Principi di base" contiene le istruzioni più utilizzate a livello globale.

Qualunque sia la tecnica usata per la valutazione dei rischi, un team interfunzionale di persone arriverà a un risultato più esaustivo ed equilibrato rispetto a un singolo.

La valutazione dei rischi è un processo iterativo che deve essere realizzato in diverse fasi del ciclo di vita della macchina. Le informazioni disponibili varieranno in base alla fase del ciclo di vita. Ad esempio, una valutazione dei rischi condotta da un costruttore potrà avvalersi di ogni dettaglio sui meccanismi della macchina e sui materiali di costruzione ma, probabilmente, potrà soltanto ipotizzare l'ambiente di lavoro finale della macchina. D'altra parte, una valutazione dei rischi effettuata dall'utilizzatore della macchina non entrerà nel merito di tutti i dettagli tecnici ma potrà considerare con precisione l'ambiente di lavoro della macchina. Idealmente, il risultato di una iterazione è l'input per l'iterazione successiva.

Determinazione dei limiti della macchina

Ciò comporta la raccolta e l'analisi di informazioni sulle parti, sui meccanismi e sulle funzioni di una macchina. Inoltre, sarà necessario considerare tutti i tipi di interazione umana con la macchina e l'ambiente in cui questa opererà. L'obiettivo è una chiara comprensione della macchina e delle sue modalità d'uso.

Le macchine singole che vengono collegate, meccanicamente o mediante sistemi di controllo, dovrebbero essere considerate come un'unica macchina, a meno che non siano "separate a zone" da adeguate misure di protezione.

È importante tener conto di tutti i limiti e di tutte le fasi della vita di una macchina, compresa l'installazione, la messa in servizio, la manutenzione, la messa fuori servizio, l'uso corretto e il funzionamento, oltre alle conseguenze di malfunzionamenti e usi errati prevedibili.

Identificazione delle attività e dei pericoli

Tutti i pericoli inerenti alla macchina devono essere identificati ed elencati in base alla loro natura e posizione. I tipi di pericolo includono schiacciamento, taglio, intrappolamento, espulsione di pezzi, emissione di fumi, radiazioni, sostanze tossiche, calore, rumore ecc.

I risultati dell'analisi delle attività dovrebbero essere confrontati con quelli dell'identificazione dei pericoli. Ciò servirà a evidenziare l'eventuale compresenza di un pericolo e di una persona, ossia una situazione pericolosa. Tutte le situazioni pericolose dovrebbero essere riportate in un elenco. A seconda dell'esperienza della persona o del tipo di attività, è possibile che lo stesso pericolo possa produrre diversi tipi di situazioni pericolose. La presenza di un tecnico di manutenzione altamente esperto e qualificato, ad esempio, può avere implicazioni diverse rispetto alla presenza di un addetto alle pulizie senza esperienza, che non conosce la macchina. In queste situazioni, se ogni caso viene elencato e affrontato separatamente, è possibile giustificare misure di protezione diverse per il tecnico di manutenzione e l'addetto alle pulizie. Se i casi non vengono elencati e affrontati separatamente, bisognerebbe fare riferimento al caso di rischio più grave e, di conseguenza, tecnico di manutenzione e addetto alle pulizie sarebbero coperti dalla stessa misura di protezione.

A volte sarà necessario effettuare una valutazione generale dei rischi su macchine già esistenti, già dotate di misure di protezione (ad es. una macchina con parti mobili pericolose protette da una porta interbloccata). Le parti mobili sono un rischio potenziale che può diventare un pericolo effettivo in caso di rottura del sistema di interblocco. A meno che il sistema di interblocco non sia già stato convalidato (attraverso la valutazione dei rischi o una progettazione rispondente a determinati standard), la sua presenza non dovrebbe essere presa in considerazione.

Stima del rischio

Questo è uno degli aspetti più importanti della valutazione dei rischi. Ci sono molti modi di affrontare questo aspetto e, nelle pagine che seguono, se ne illustrano i principi di base.

Qualunque macchina che possa creare situazioni pericolose presenta un rischio di evento pericoloso (ad es. lesioni). Maggiore è il rischio, maggiore è l'importanza di un adeguato intervento. Per un determinato pericolo, il rischio potrebbe essere così ridotto da poter essere tollerato e accettato ma, per un altro pericolo, il rischio potrebbe essere così elevato da rendere indispensabile l'adozione di misure estreme di protezione. Quindi, per prendere una decisione sulla necessità e sul tipo di intervento, occorre essere in grado di quantificare il rischio.

Il rischio viene spesso inteso esclusivamente in termini di gravità delle lesioni in caso di incidente. SIA la gravità del danno potenziale SIA la probabilità che si verifichi devono essere prese in considerazione per stimare la gravità del rischio presente.

Il metodo proposto nelle pagine successive per la valutazione del rischio non è l'unico metodo possibile poiché circostanze diverse potrebbero richiedere approcci diversi. È PRESENTATO SOLO COME LINEA GUIDA GENERALE VOLTA A INCORAGGIARE L'USO DI UNA STRUTTURA METODICA E DOCUMENTATA.

Il sistema a punti utilizzato non è stato calibrato per particolari tipi di applicazione e quindi, potrebbe non essere necessariamente adatto per un'applicazione specifica. Il Rapporto tecnico ISO TR 14121-2 "Risk assessment – Practical guidance and examples of methods" fornisce istruzioni pratiche, alcune delle quali sono dedicate ai vari metodi di quantificazione dei rischi.

Vengono presi in considerazione i seguenti fattori:

- LA GRAVITÀ DELLE LESIONI POTENZIALI.
- LA PROBABILITÀ CHE SI VERIFICHINO.

La probabilità di occorrenza comprende due fattori:

- FREQUENZA DELL'ESPOSIZIONE.
- PROBABILITÀ DI LESIONI.

Assegneremo dei valori a ognuno di questi fattori analizzandoli separatamente.

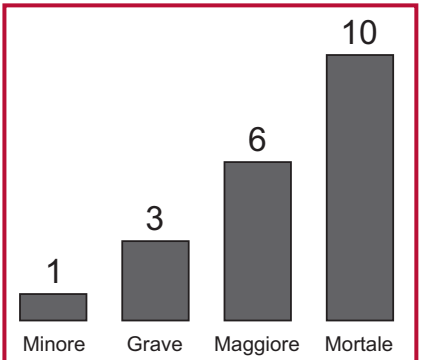
Occorre sfruttare tutti i dati e le esperienze a disposizione. Poiché vengono considerate tutte le fasi di vita della macchina, per evitare troppa complessità, è necessario basare le decisioni sul caso più grave per ogni fattore.

È inoltre importante usare il buon senso. Le decisioni devono basarsi su azioni fattibili, realistiche e plausibili. Questo è il motivo per cui è utile l'approccio da parte di un team interfunzionale.

Ai fini di questo esercizio, non bisognerebbe considerare eventuali sistemi di protezione esistenti. Se la stima dei rischi rivela l'esigenza di un sistema di protezione, attraverso una serie di metodologie, è possibile determinarne le caratteristiche (v. più avanti in questo capitolo).

1. Gravità delle lesioni potenziali

In questo caso si presume che l'incidente o il danno si sia verificato, forse come conseguenza del pericolo. Lo studio accurato del pericolo rivelerà qual è il maggior danno possibile. Ricordare: in questo caso si presume che il danno sia inevitabile e ci si concentra solo sulla sua gravità. Occorre presumere che l'operatore sia esposto al movimento o al processo pericoloso. La gravità del danno deve essere valutata quale:



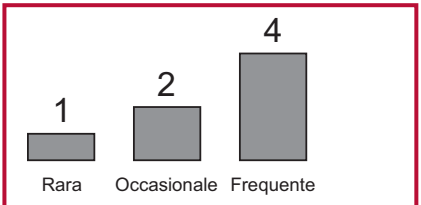
Punti assegnati alla gravità

- FATALE: Morte
- IMPORTANTE: (generalmente irreversibile) disabilità permanente, perdita della vista, amputazione di arti, danni respiratori, ecc.
- GRAVE: (generalmente reversibile) perdita di conoscenza, ustioni, fratture, ecc.
- MINORE: ematomi, tagli, lievi abrasioni, ecc.

A ogni descrizione viene assegnato un valore, come illustrato.

2. Frequenza dell'esposizione

La frequenza di esposizione risponde alla domanda "Quanto spesso l'operatore o il tecnico di manutenzione è esposto al pericolo?". La frequenza di esposizione al pericolo può essere classificata come:



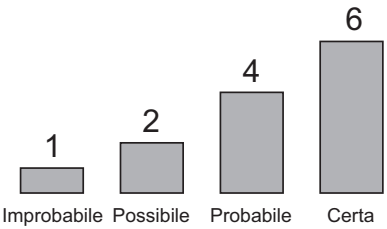
Punti assegnati alla frequenza di esposizione

- FREQUENTE: più volte al giorno.
- OCCASIONALE: una volta al giorno.
- RARA: una volta a settimana o meno

A ogni descrizione viene assegnato un valore, come illustrato.

3. Probabilità di lesioni

Occorre presumere che l'operatore sia esposto al movimento o al processo pericoloso. Se si considera il modo in cui l'operatore interagisce con la macchina e altri fattori (velocità di avviamento, ad esempio) è possibile classificare la probabilità di danno come:



Punti assegnati alla frequenza di esposizione

- IMPROBABILE
- PROBABILE
- POSSIBILE
- CERTA

A ogni descrizione viene assegnato un valore, come illustrato.

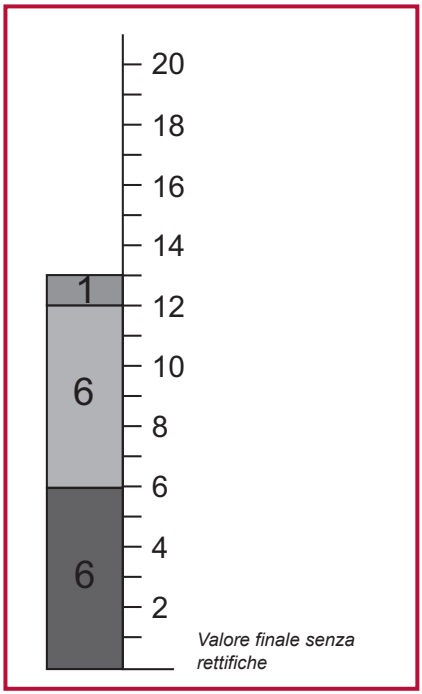
A tutte le descrizioni viene assegnato un valore; tali valori sono quindi sommati per ottenere una stima iniziale. La somma dei tre componenti ammonta a un valore di 13. Ma dobbiamo considerare altri fattori. (Nota: questo non è necessariamente basato sulle illustrazioni degli esempi precedenti).

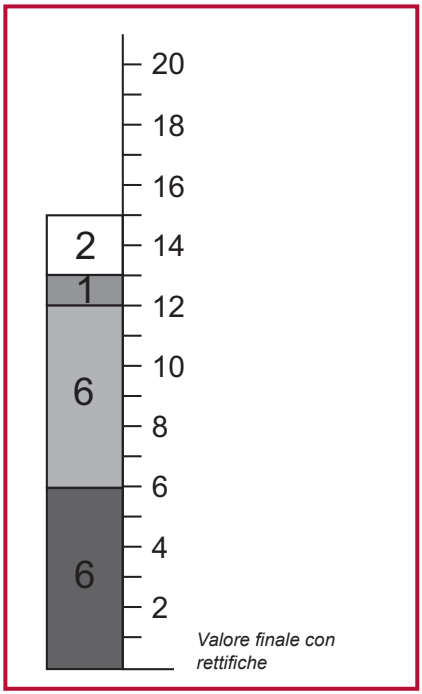
Il prossimo passaggio prevede l'affinamento della stima iniziale prendendo in considerazione fattori aggiuntivi quali quelli illustrati nella seguente tabella. Spesso possono essere analizzati correttamente solo quando la macchina è installata nella sua postazione permanente.

Fattore tipico	**Azione proposta**
Più di una persona esposta al pericolo.	Moltiplicare il fattore di gravità per il numero di persone.
Periodo protratto nella zona pericolosa senza isolamento completo dell'alimentazione.	Se il tempo per ogni accesso è superiore a 15 minuti, aggiungere 1 punto al fattore di frequenza.
L'operatore non è esperto o addestrato.	Aggiungere 2 punti al totale.
Intervalli molto lunghi (ad esempio 1 anno) tra gli accessi. (Potrebbero verificarsi avarie progressive e non rilevate, soprattutto nei sistemi di monitoraggio).	Aggiungere i punti equivalenti al massimo fattore di frequenza.

Considerazioni aggiuntive per la stima dei rischi

I risultati di ogni fattore aggiuntivo devono essere sommati al totale precedente, come illustrato.





Riduzione dei rischi

Ora occorre prendere in considerazione ogni macchina e i rispettivi rischi e attuare le misure necessarie per risolverne tutti i rischi.

La tabella che segue è un esempio di una parte di un processo documentato per tenere conto di tutti gli aspetti legati alla sicurezza della macchina utilizzata. Serve da guida agli utilizzatori della macchina, ma anche i produttori o i fornitori possono usare lo stesso principio per verificare che tutte le apparecchiature siano state convalidate. Inoltre, servirà da indice a rapporti più dettagliati sulla valutazione dei rischi.

Mostra che, nel caso in cui a una macchina sia stato apposto il marchio CE, il processo è più semplice poiché i rischi per la macchina sono già stati valutati dal produttore e tutte le misure necessarie sono già state attuate. Anche nel caso di attrezzature marchiate CE è possibile che siano presenti ulteriori rischi dovuti alla natura della sua applicazione o ai materiali lavorati non previsti dal produttore.

Società – MAYKIT WRIGHT LTD
Stabilimento – Attrezzeria – East Factory.
Data – 8/29/95
Profilo operatore – esperto.

Descrizione apparecchiature e data	Conformità alle Direttive	N. report di valutazione del rischio	Storico incidenti	Note	Descrizione pericolo	Tipo di pericolo	Azione richiesta	Implementata e ispezionata – Riferimento
Tornio parallelo Bloggs. N. di serie 8390726 Installato 1978	Nessuna dichiarata	RA302	Nessuno	L'apparecchiatura elettrica è conforme a BS EN 60204 Pulsanti di emergenza montati (sostituiti 1989)	Rotazione mandrino con protezione aperta	Intrappola-mento Taglio	Montaggio interruttore di interblocco di protezione	11/25/94 J Kershaw Report n. 9567
					Fluido di taglio	Tossicità	Sostituire con tipo non tossico	11/30/94 J Kershaw Report n. 9714
					Pulizia sfridi	Taglio	Fornire guanti	11/30/94 J Kershaw Report n. 9715
Fresatrice a torretta Bloggs N. di serie 17304294 Fabbricata 1995 Installata Maggio 95	Dir. Macchine Dir. EMC	RA416	Nessuno		Movimento slitta (verso la parete)	Schiaccia-mento	Spostare la macchina per assicurare spazio sufficiente	4/13/95 J Kershaw Report n. 10064

Gerarchia delle misure per la riduzione dei rischi

Esistono tre metodi di base, da considerare e usare nel seguente ordine:

1. eliminare o ridurre i rischi nella maggiore misura possibile (progettazione e costruzione di macchine intrinsecamente sicure)
2. installare i sistemi e le misure di protezione necessari (ad es. protezioni interbloccate, barriere fotoelettriche, ecc.) in relazione ai rischi che non possono essere eliminati in fase progettuale.
3. informare gli utenti dei rischi residui dovuti a eventuali lacune delle misure protettive adottate, indicare l'addestramento necessario e specificare l'eventuale necessità di fornire al personale equipaggiamento protettivo aggiuntivo.

Ogni misura di questa gerarchia deve essere presa in considerazione partendo dall'inizio dell'elenco e usata laddove possibile. Questo approccio conduce, di solito, all'uso contemporaneo di più misure.

Progettazione a sicurezza intrinseca

Nella fase di progettazione della macchina, è possibile evitare molti dei possibili rischi semplicemente mediante l'attenta considerazione di fattori come i materiali, i requisiti di accesso, le superfici calde, i metodi di trasmissione, i punti di intrappolamento, i livelli di tensione, ecc.

Ad esempio, se non è necessario accedere a una zona pericolosa, la soluzione è proteggerla all'interno della macchina o con qualche tipo di protezione fissa.

Misure e sistemi di protezione

Se accedere alla zona pericolosa è necessario, la soluzione sarà un po' più complessa. Sarà necessario garantire che l'accesso sia possibile solo con la macchina in condizioni di sicurezza. Saranno necessarie misure protettive quali porte di protezione interbloccate e/o sistemi di sgancio. La scelta del dispositivo o sistema protettivo deve essere fortemente determinata dalle caratteristiche operative della macchina. Questo è estremamente importante, poiché un sistema che peggiora l'efficienza della macchina sarà soggetto a essere rimosso senza autorizzazione o ignorato.

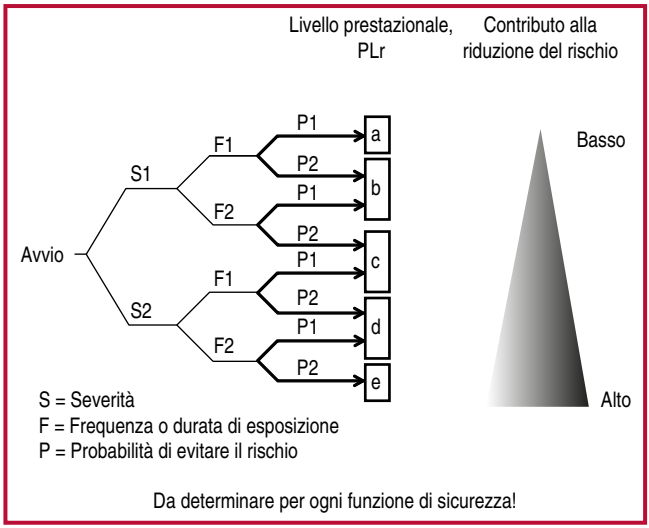
In questo caso, la sicurezza della macchina dipende dalla corretta applicazione e dal funzionamento corretto del sistema protettivo anche in condizioni di guasto.

Adesso occorre esaminare il funzionamento corretto di tale sistema. Per ogni tipo di sistema esistono numerose tecnologie con diversi gradi di prestazione per il monitoraggio, il rilevamento e la prevenzione dei guasti.

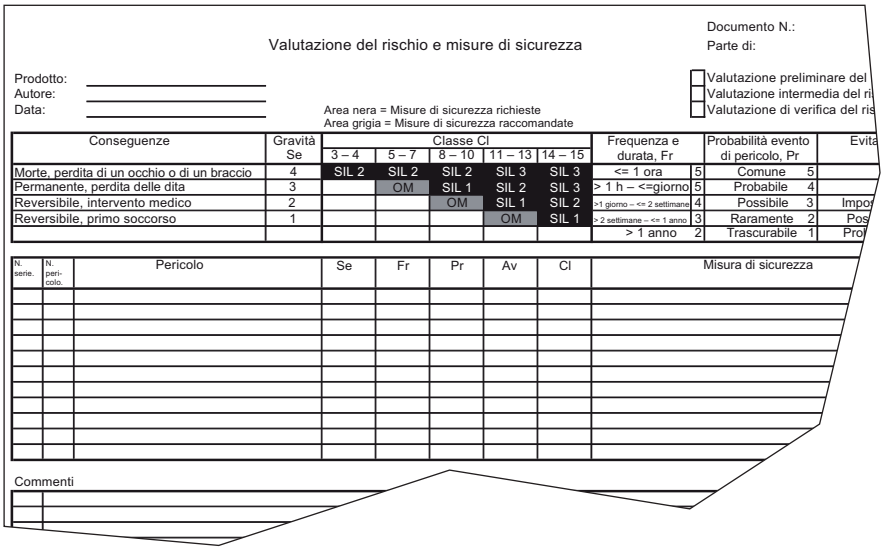
In un mondo ideale tutti i sistemi protettivi sarebbero perfetti e non consentirebbero alcuna possibilità di guasto in condizioni pericolose. Nel mondo reale, tuttavia, siamo limitati dalla nostra conoscenza imperfetta e dai materiali adoperati. Un altro vincolo rilevante è il costo. In base a questi fattori, è chiaro che occorre utilizzare un certo senso delle proporzioni. Sarebbe ridicolo insistere che l'integrità di un sistema di protezione di una macchina che, nel peggiore dei casi, può provocare un ematoma, sia la stessa richiesta per un jumbo jet che vola a chilometri di distanza da terra. Le conseguenze di un eventuale guasto del sistema sono drasticamente diverse e dunque è necessario poter in qualche modo correlare la portata delle misure protettive al livello di rischio calcolato durante la fase di stima dei rischi.

Qualunque sia il dispositivo di protezione prescelto, occorre ricordare che un "sistema legato alla sicurezza" può comprendere numerosi elementi, tra cui il dispositivo di protezione, il cablaggio, un dispositivo di commutazione e a volte componenti del sistema di controllo operativo della macchina. Tutti questi elementi del sistema (comprese protezioni, montaggio, cablaggio, ecc.) devono presentare prestazioni e caratteristiche adatte alla propria progettazione e tecnologia. Gli standard IEC/EN 62061 ed EN ISO 13849-1 comprendono una classificazione gerarchica dei livelli prestazionali dei componenti legati alla sicurezza dei sistemi di controllo, e nei relativi allegati sono descritti dei metodi di valutazione dei rischi che permettono di determinare i requisiti di integrità dei sistemi di protezione.

EN ISO 13849-1:2008, nell'Allegato A, fornisce un grafico migliore del rischio.



IEC 62061, nell'Allegato A, propone il metodo di seguito illustrato.



Valutazione del rischio e misure di sicurezza

Documento N.:
Parte di:

Prodotto:
Autore:
Data:

☐ Valutazione preliminare del
☐ Valutazione intermedia del ri
☐ Valutazione di verifica del ris

Area nera = Misure di sicurezza richieste
Area grigia = Misure di sicurezza raccomandate

Conseguenze	Gravità Se	Classe CI 3 – 4	5 – 7	8 – 10	11 – 13	14 – 15	Frequenza e durata, Fr		Probabilità evento di pericolo, Pr		Evita
Morte, perdita di un occhio o di un braccio	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 ora	5	Comune	5	
Permanente, perdita delle dita	3		OM	SIL 1	SIL 2	SIL 3	> 1 h – <=giorno	5	Probabile	4	
Reversibile, intervento medico	2			OM	SIL 1	SIL 2	>1 giorno – <= 2 settimane	4	Possibile	3	Impo
Reversibile, primo soccorso	1				OM	SIL 1	> 2 settimane – <= 1 anno	3	Raramente	2	Pos
							> 1 anno	2	Trascurabile	1	Pro

N. serie.	N. peri-colo.	Pericolo	Se	Fr	Pr	Av	Cl	Misura di sicurezza

Commenti

L'uso di ognuno dei due metodi sopra menzionati dovrebbe fornire risultati equivalenti. Ogni metodo traduce dettagliatamente il contenuto dello standard a cui appartiene.

In entrambi i casi, è estremamente importante attenersi alle linee guida contenute nel testo dello standard. Il grafico e la tabella dei rischi non devono essere usati prescindendo dal loro contesto o in modo troppo semplicistico.

Valutazione

Dopo aver scelto la misura di protezione e prima che questa sia implementata, è importante ripetere la stima dei rischi. Questa procedura viene spesso trascurata. È possibile che, installando una misura di protezione, l'operatore alla macchina si senta totalmente e completamente protetto contro il rischio originale previsto. Non avendo più la consapevolezza del pericolo originale, può interagire con la macchina in modo diverso, esponendosi più frequentemente al rischio, o ad esempio introducendosi ulteriormente nella macchina. Ciò significa che, se la misura di protezione non funziona, l'operatore sarà esposto a un rischio superiore rispetto a quello inizialmente calcolato. Questo è il rischio effettivo che deve essere stimato. Pertanto, la stima del rischio deve essere ripetuta considerando ogni prevedibile modifica delle modalità di interazione tra l'uomo e la macchina. Il risultato di questa attività serve a controllare che le misure di protezione proposte siano, di fatto, adeguate. Per ulteriori informazioni, si rimanda all'Allegato A dello standard IEC/EN 62061.

Formazione, dispositivi di protezione personale, ecc.

È importante che gli operatori ricevano l'addestramento necessario relativo ai metodi di lavoro sicuri per una specifica macchina. Questo non significa che le altre misure possano esser omesse. Non è accettabile limitarsi a dire all'operatore che non deve avvicinarsi alle aree pericolose invece di installare le adeguate protezioni.

Può anche essere necessario che l'operatore usi dispositivi quali guanti speciali, occhiali, respiratori, ecc. Il progettista della macchina dovrebbe specificare i tipi di dispositivi necessari. L'uso di dispositivi di protezione personale non rappresenta il metodo di sicurezza primario, ma completa le misure di cui sopra.

Standard e norme

Sono diversi gli standard e i rapporti tecnici che forniscono consigli sulla valutazione dei rischi. Alcuni sono di ampia applicabilità mentre altri riguardano applicazioni specifiche. Quella che segue è una lista di standard che includono informazioni sulla valutazione dei rischi.

ANSI B11.TR3: Risk assessment and risk reduction – A guide to estimate, evaluate and reduce risks associated with machine tools.

ANSI PMMI B155.1: Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery.

ANSI RIA R15.06: Safety Requirements for Industrial Robots and Robot Systems.

AS 4024.1301-2006: Principles of risk assessment CSA Z432-04: Safeguarding of Machinery.

CSA Z432-03: Industrial Robots and Robot Systems – General Safety Requirements.

IEC/EN 61508: Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza.

IEC/EN 62061: Sicurezza del macchinario – Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza.

EN ISO 13849-1: Safety of machinery – Safety related parts of control systems

EN ISO 14121-1: Principles for risk assessment

ISO TR 14121-2: Risk assessment – Practical guidance and examples of methods.

Misure di protezione e dispositivi complementari

Quando la valutazione del rischio evidenzia che una macchina o un processo implicano un rischio di lesione personale, tale rischio deve essere eliminato o contenuto. Il modo in cui questo obiettivo viene raggiunto dipende dalla natura della macchina e del pericolo. Le misure di protezione abbinate alle protezioni fisse (ripari) servono a impedire l'accesso a un pericolo o a prevenire movimenti pericolosi in corrispondenza di un pericolo qualora sia possibile l'accesso. Esempi tipici di misure di protezione sono le protezioni interbloccate, le barriere fotoelettriche, le pedane di sicurezza, i comandi a due mani e gli interruttori di abilitazione.

I dispositivi e sistemi di arresto di emergenza sono associati a sistemi di controllo legati alla sicurezza ma non sono sistemi di protezione diretti, devono essere esclusivamente considerati come misure di protezione complementari.

Protezioni fisse che impediscono l'accesso

Se il pericolo riguarda una parte della macchina a cui non è necessario accedere, questa dovrebbe essere protetta mediante una protezione fissa. Per rimuovere questo tipo di protezioni, dovrebbe essere necessario utilizzare degli utensili. Le protezioni fisse devono essere in grado di 1) far fronte all'ambiente operativo, 2) contenere eventuali pezzi scagliati con violenza e 3) non creare pericoli evitando, ad esempio, la presenza di bordi taglienti. Le protezioni fisse possono essere dotate di aperture in corrispondenza del punto di unione con la macchina o per l'utilizzo di recinzioni a rete metallica.

Le finestre rappresentano un efficiente mezzo per monitorare le prestazioni delle macchine per l'accesso alla parte specifica della macchina. Occorre prestare attenzione alla selezione dei materiali usati per le finestre, poiché le interazioni chimiche con fluidi di taglio e i raggi ultravioletti o il semplice invecchiamento ne provocano l'usura nel tempo.

La dimensione delle aperture deve impedire che l'operatore possa essere esposto al pericolo. La tabella O-10 di OSHA 1910.217 (f) (4), ISO 13854, la tabella D-1 di ANSI B11.19, la tabella 3 di CSA Z432 e AS4024.1 forniscono istruzioni sulla distanza necessaria tra l'apertura e la fonte di pericolo.

Rilevamento degli accessi

Le misure di protezione possono essere utilizzate per rilevare l'accesso a un pericolo. Quando si sceglie il rilevamento come metodo di riduzione dei rischi, il progettista deve essere consapevole della necessità di un completo sistema di sicurezza; il dispositivo di sicurezza, da solo, non fornisce la necessaria riduzione dei rischi.

Questo sistema di sicurezza, generalmente, è costituito da tre blocchi: 1) un dispositivo di ingresso che rileva l'accesso al pericolo, 2) un dispositivo logico che

elabora i segnali provenienti dal dispositivo di rilevamento, controlla lo stato del sistema di sicurezza e attiva o disattiva i dispositivi di uscita, 3) un dispositivo di uscita che controlla l'attuatore (ad es. un motore).

Dispositivi di rilevamento

Per rilevare la presenza di una persona che entra o si trova all'interno di una zona pericolosa, sono disponibili molti dispositivi alternativi. La scelta migliore per una particolare applicazione dipende da una serie di fattori.

- Frequenza di accesso,
- Tempo di arresto del pericolo,
- Importanza del completamento del ciclo della macchina, e
- Contenimento di pezzi scagliati con violenza, fluidi, nebbie, vapori, ecc.

Protezioni mobili, adeguatamente selezionate, possono essere interbloccate per offrire protezione contro pezzi scagliati con violenza, fluidi, nebbie e altri tipi di pericolo; questo tipo di protezione viene spesso utilizzata quando l'accesso al pericolo non è frequente. Le protezioni interbloccate possono anche essere bloccate per impedire l'accesso alla macchina durante il ciclo e quando la macchina impiega molto tempo per fermarsi.

I dispositivi di rilevamento accesso – come barriere fotoelettriche, pedane e scanner – forniscono un rapido e facile accesso alla zona di pericolo e vengono spesso selezionati quando gli operatori devono accedere frequentemente a tale zona. Questo tipo di dispositivi non fornisce protezione contro pezzi scagliati in aria, nebbie, fluidi o altri tipi di pericoli.

La scelta migliore di misura protettiva è un dispositivo o un sistema che garantisca la massima protezione con la minima interferenza nel normale funzionamento della macchina. Tutti gli aspetti della macchina devono essere considerati poiché l'esperienza insegna che si tende a non utilizzare o "aggirare" un sistema difficile da usare.

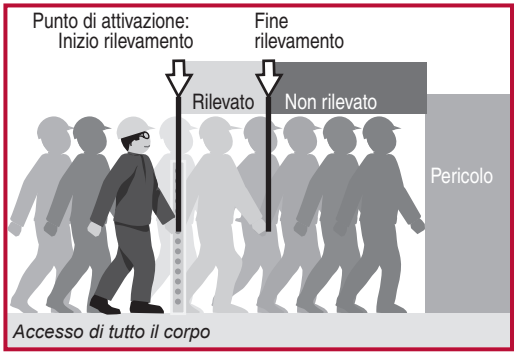
Dispositivi di rilevamento accesso

Quando occorre decidere come proteggere un'area, è importante comprendere a fondo quali funzioni di sicurezza sono necessarie. Di norma, vi saranno almeno due funzioni.

- Disattivare o disabilitare l'alimentazione quando un persona entra nell'area pericolosa.
- Evitare l'attivazione o l'abilitazione dell'alimentazione quando una persona si trova nell'area pericolosa.

A prima vista, potrebbero sembrare una sola funzione, ma sebbene siano strettamente legate e spesso attuate dalla stessa attrezzatura, si tratta di due

funzioni separate. Per realizzare la prima funzione occorre disporre di un dispositivo di protezione, ossia un dispositivo che rilevi che una parte del corpo della persona si trova oltre un determinato punto e invii un segnale per disinserire l'alimentazione. Se la persona riesce a oltrepassare il punto di intervento e la sua presenza non è più rilevata, la seconda funzione (evitare il reinserimento dell'alimentazione) non è stata realizzata.



Lo schema che segue mostra un esempio di accesso di un corpo con una barriera fotoelettrica montata verticalmente che funge da dispositivo di protezione. Anche le porte di protezione interbloccate possono essere considerate come dispositivi di solo intervento quando non c'è niente a impedire che la porta si richiuda dopo l'ingresso.

Se l'accesso dell'intera persona non è possibile, così che una persona non possa proseguire dopo il punto di intervento, la presenza è sempre rilevata e anche la seconda funzione (impedire il reinserimento dell'alimentazione) è attivata.

Per le applicazioni con accesso parziale del corpo, gli stessi tipi di dispositivi svolgono la funzione di intervento e di rilevamento accesso. L'unica differenza sta nel tipo di applicazione.

I dispositivi di rilevamento accesso servono a rilevare la presenza di persone. La famiglia di dispositivi include barriere fotoelettriche di sicurezza, barriere di sicurezza a fascio singolo, scanner della zona di sicurezza, pedane e bordi di sicurezza.

Barriere fotoelettriche di sicurezza

Le barriere fotoelettriche di sicurezza possono essere descritte semplicemente come sensori di presenza fotoelettrici concepiti specificatamente per proteggere il personale dai movimenti pericolosi delle macchine. Note anche come AOPD (dispositivi di protezione optoelettrici attivi) o ESPE (dispositivi elettrosensibili di protezione), le barriere fotoelettriche garantiscono un livello di sicurezza ottimale, pur consentendo un'elevata produttività. Sono inoltre soluzioni più ergonomiche rispetto alle protezioni meccaniche. Sono perfette per le applicazioni in cui il personale necessita di accedere frequentemente e facilmente a un punto di lavoro pericoloso.

Le barriere fotoelettriche sono concepite e testate per rispondere a IEC 61496-1 e -2. Non esiste una versione EN armonizzata della parte 2, pertanto l'Allegato IV della Direttiva Macchine europea richiede la certificazione delle barriere fotoelettriche da parte di organismi terzi, prima della commercializzazione nella Comunità Europea. Gli organismi terzi testano le barriere fotoelettriche per verificarne la conformità a questo standard internazionale. Underwriter's Laboratory ha adottato IEC 61496-1 come standard nazionale USA.

Laser scanner di sicurezza

I laser scanner di sicurezza sono dotati di uno specchio rotante che deflette gli impulsi luminosi su un arco, creando un piano di rilevamento. La posizione dell'oggetto è determinata dall'angolo di rotazione dello specchio. Usando la tecnica "time-of-flight" (tempo di volo) di un raggio riflesso di luce invisibile, lo scanner può rilevare anche la distanza dell'oggetto dallo scanner stesso. Considerando la distanza misurata e la posizione dell'oggetto, il laser scanner ne determina la posizione esatta.

Pedane di sicurezza sensibili alla pressione

Questi dispositivi servono a proteggere un'area a pavimento intorno alla macchina. Una matrice di pedane interconnesse viene disposta intorno all'area pericolosa e qualsiasi pressione esercitata sulla pedana (ad esempio il passo di un operatore) farà sì che l'unità di controllo della pedana tolga alimentazione alla fonte di pericolo. Le pedane sensibili alla pressione sono spesso usate nell'ambito di un'area recintata contenente diverse macchine, ad esempio nelle celle automatizzate flessibili di produzione o a robot. Quando è necessario accedere alla cella (ad es. per operazioni di regolazione o per "istruire" un robot), le pedane impediscono movimenti pericolosi se l'operatore si allontana dalla zona sicura o deve recarsi dietro a una parte dell'apparecchiatura.

Le dimensioni e il posizionamento della pedana devono considerare la distanza di sicurezza.

Bordi sensibili alla pressione

Questi dispositivi sono strisce di bordatura flessibili che possono essere montate sui bordi di una parte in movimento, ad esempio un piano macchina o una porta automatica, che potrebbero schiacciare o ferire gli operatori.

Se la parte in movimento urta l'operatore (o viceversa), il bordo sensibile flessibile viene premuto, comandando l'interruzione dell'alimentazione del componente pericoloso. I bordi sensibili possono inoltre essere usati per proteggere le macchine che potrebbero intrappolare l'operatore. Se un operatore resta intrappolato nella macchina, il contatto con il bordo sensibile provocherà lo spegnimento dell'alimentazione.

Per la realizzazione dei bordi di sicurezza, sono disponibili diverse tecnologie. Una tecnologia molto diffusa è l'inserimento di un lungo interruttore all'interno del bordo. Questo approccio consente di avere bordi dritti e, generalmente, usa la tecnica di collegamento a 4 fili.

Barriere fotoelettriche, scanner, pedane e bordi sensibili sono classificati come "dispositivi di protezione". In effetti non impediscono l'accesso, semplicemente si attivano quando lo rilevano, segnalandolo. La capacità di garantire la sicurezza dipende interamente dalla loro capacità di rilevamento e di interruzione. In generale, sono adatti solo a macchine che si arrestano in tempi ragionevolmente rapidi dopo l'interruzione dell'alimentazione. Poiché un operatore può camminare o raggiungere direttamente l'area pericolosa, è ovviamente necessario che il tempo richiesto per l'interruzione del movimento sia minore di quello necessario affinché l'operatore raggiunga l'area pericolosa dopo aver azionato il dispositivo di protezione.

Interruttori di sicurezza

Quando l'accesso alla macchina non è frequente, è preferibile ricorrere a protezioni mobili (apribili). La protezione è interbloccata con l'alimentazione della fonte di pericolo in modo che, quando la porta di protezione non è chiusa, l'alimentazione sia disinserita. Questo metodo implica l'uso di un interruttore di interblocco fissato alla porta di protezione. Il controllo dell'alimentazione della fonte di pericolo è collegato alla sezione dell'interruttore dell'unità. L'alimentazione è generalmente elettrica, ma può anche essere pneumatica o idraulica. Quando il movimento della porta di protezione (apertura) è rilevato, l'interruttore di interblocco comanda l'isolamento dell'alimentazione direttamente o tramite un contattore (o valvola).

Alcuni interruttori di interblocco comprendono anche un dispositivo di blocco che blocca in posizione chiusa la porta della protezione e non viene rilasciato finché la macchina non si trova in una condizione sicura. Per la maggior parte delle applicazioni, la combinazione di protezione mobile e interruttore di interblocco con o senza blocco della protezione è la soluzione più affidabile ed efficiente.

È disponibile un'ampia serie di interruttori di sicurezza, tra cui i seguenti.

- **Interruttori di interblocco con attuatore** – il funzionamento di questi dispositivi richiede l'inserimento e la rimozione dell'attuatore nell'interruttore.
- **Interruttori di interblocco a cerniera** – questi dispositivi sono situati sulle cerniere delle porte di protezione e funzionano utilizzando l'azione di apertura della porta.
- **Interruttori con blocco della protezione** – in alcune applicazioni, è necessario bloccare la porta in chiusura o temporizzarne l'apertura. I dispositivi adatti a questa funzione sono gli interruttori con blocco della protezione. Sono adatti a macchine con caratteristiche di arresto progressivo, ma possono fornire un importante potenziamento della sicurezza per la maggior parte delle macchine.

- **Interruttori di interblocco senza contatto** – questi dispositivi non richiedono alcun contatto fisico per l'attivazione e alcune versioni integrano una funzione di codifica che incrementa il livello di protezione dalle manomissioni.
- **Interblocchi di posizione (interruttori di finecorsa)** – i commutatori a camme sono, di solito, interruttori di finecorsa (o di posizione) a modalità positiva con camma lineare o rotante. Si utilizzano, generalmente, sulle protezioni scorrevoli.
- **Interblocchi a chiave bloccata** – Le chiavi bloccate codificate possono servire all'interblocco del comando o dell'alimentazione. Nel caso di "interblocco del comando", un dispositivo di interblocco invia un comando di arresto a un dispositivo intermedio che, a sua volta, disattiva un successivo dispositivo per scollegare l'alimentazione dall'attuatore. Nel caso di "interblocco dell'alimentazione", il comando di arresto interrompe direttamente l'alimentazione agli attuatori della macchina.

Dispositivi di interfaccia operatore

Funzione di arresto – Negli Stati Uniti, in Canada, in Europa e a livello internazionale, esiste l'armonizzazione degli standard per quanto riguarda le descrizioni delle categorie di arresto delle macchine o degli impianti di produzione.

Nota: tali categorie sono diverse da quelle previste da EN 954-1 (ISO 13849-1). Per ulteriori informazioni consultare gli standard NFPA 79 e IEC/EN 60204-1. Gli arresti sono suddivisi in tre categorie.

Categoria 0 arresto dovuto all'immediato scollegamento dell'alimentazione degli attuatori della macchina. Sono considerati arresti non controllati. Con l'alimentazione disinserita, l'azione frenante, che richiede energia, non sarà attiva. Questo consente ai motori di girare liberamente e rallentare fino a fermarsi dopo un certo periodo di tempo. In altri casi, è possibile che i sistemi di fissaggio della macchina depositino del materiale e che l'alimentazione sia necessaria per tenere fermo tale materiale. I sistemi di arresto meccanici, poiché non richiedono alimentazione, possono essere usati anche con un arresto di categoria 0. L'arresto di categoria 0 ha la priorità sugli arresti di categoria 1 o 2.

Categoria 1 arresto comandato in cui l'alimentazione è disponibile affinché gli attuatori della macchina eseguano l'arresto. Quindi, l'alimentazione viene rimossa dagli attuatori dopo l'arresto. Questa categoria di arresti consente una frenata con alimentazione che provoca l'arresto rapido del movimento pericoloso, successivamente l'alimentazione può essere rimossa dagli attuatori.

Categoria 2 arresto comandato con alimentazione disponibile per gli attuatori della macchina. Un normale arresto di produzione è considerato un arresto di categoria 2.

Queste categorie di arresti devono essere applicate a ciascuna funzione di arresto; nel caso in cui per funzione di arresto si intende l'azione intrapresa dalle

componenti relative alla sicurezza del sistema di controllo come reazione a un ingresso, deve essere usata la categoria 0 o 1. Le funzioni di arresto devono avere la precedenza sulle funzioni di avviamento. La scelta della categoria di arresto per ogni funzione di arresto deve essere determinata mediante valutazione dei rischi.

Funzione di arresto d'emergenza

La funzione di arresto d'emergenza deve operare come un arresto di categoria 0 o 1, a seconda di quanto determinato dalla valutazione del rischio. Deve essere avviata da un'unica azione umana. Quando viene eseguita, deve avere la precedenza su tutte le altre funzioni e modalità di funzionamento della macchina. L'obiettivo è quello di togliere alimentazione il più rapidamente possibile senza creare rischi aggiuntivi.

Fino a poco tempo fa erano necessari componenti elettromeccanici cablati per i circuiti di arresto di emergenza. Grazie alle recenti modifiche apportate a standard come IEC 60204-1 e NFPA 79, nei circuiti di arresto di emergenza possono essere utilizzati PLC di sicurezza e altre forme di logica elettronica rispondenti ai requisiti di standard come IEC 61508.

Dispositivi di arresto di emergenza

Laddove sussiste il pericolo che un operatore sia messo a rischio da una macchina, occorre che l'accesso al dispositivo di arresto d'emergenza sia facile. Il dispositivo di arresto di emergenza deve essere costantemente in funzione e facilmente disponibile. I pannelli operatore dovrebbero contenere almeno un dispositivo di arresto d'emergenza. È possibile utilizzare ulteriori dispositivi di arresto d'emergenza in altre posizioni, se necessario. I dispositivi di arresto d'emergenza hanno varie forme. Gli interruttori con pulsante e gli interruttori a fune sono esempi dei dispositivi più comunemente diffusi. Quando viene azionato, il dispositivo di arresto di emergenza dev'essere a ritenuta e non deve essere possibile generare il comando di arresto senza tale condizione. Il reset del dispositivo di arresto di emergenza non deve creare una situazione pericolosa. Deve inoltre essere eseguita un'azione separata e deliberata per riavviare la macchina.

Per ulteriori informazioni sui dispositivi di arresto d'emergenza, vedere ISO/EN 13850, IEC 60947-5-5, NFPA 79 e IEC 60204-1, AS4024.1, Z432-94.

Pulsanti di arresto d'emergenza

I dispositivi di arresto di emergenza sono considerati apparecchiature di protezione complementari. Poiché non impediscono e non rilevano l'accesso a un pericolo, non sono considerati dispositivi di protezione primari.

La forma più comune di questo tipo di dispositivi è rappresentata dai pulsanti rossi a fungo su sfondo giallo che l'operatore preme in caso di emergenza. Devono essere distribuiti strategicamente e in quantità sufficiente intorno alla macchina per garantire che ve ne sia sempre uno a portata di mano nell'area pericolosa.

I pulsanti di arresto di emergenza devono essere immediatamente accessibili e disponibili in tutte le modalità di funzionamento della macchina. I pulsanti utilizzati come dispositivi di arresto di emergenza devono essere a fungo (o azionabili con il palmo della mano) e di colore rosso su sfondo giallo. Quando il pulsante viene premuto, i contatti devono cambiare stato non appena il pulsante si blocca in posizione premuta.

Una delle tecnologie più recenti per gli arresti di emergenza è una tecnica di automonitoraggio. Sulla parte posteriore dell'arresto di emergenza viene aggiunto un contatto addizionale che monitora se i componenti del pannello sono presenti. Questo sistema è il cosiddetto blocco di contatti ad autosorveglianza. Consiste in un contatto, azionato a molla, che si chiude quando il blocco di contatti viene inserito in posizione sul pannello. La Figura 80 mostra il contatto di autosorveglianza collegato in serie a uno dei contatti di sicurezza ad apertura diretta.

Interruttori a fune

Per le macchine quali i nastri trasportatori, spesso è più comodo ed efficace usare un dispositivo a fune posto lungo l'area di pericolo come dispositivo di arresto d'emergenza. Questi dispositivi usano un cavo d'acciaio collegato agli interruttori a ritenuta a fune in modo tale che tirando il cavo in qualsiasi direzione e in qualsiasi punto lungo la sua lunghezza l'interruttore venga attivato e interrompa l'alimentazione della macchina.

Gli interruttori a fune devono rilevare sia il tensionamento sul cavo che l'eventuale mancanza di tensionamento. Quest'ultima funzione assicura che il cavo non sia tagliato e, quindi, pronto all'uso.

La distanza del cavo incide sulle prestazioni dell'interruttore. Per brevi distanze, a una estremità è installato l'interruttore di sicurezza e, all'altra estremità, una molla di tensione. Per lunghe distanze, l'interruttore di sicurezza deve essere installato a entrambe le estremità del cavo, in modo da garantire che una singola azione dell'operatore generi un comando di arresto. La forza di trazione necessaria per il cavo non dovrebbe superare i 200 N o uno spostamento di 400 mm nel punto centrale tra i due supporti del cavo.

Comandi a due mani

L'uso dei comandi a due mani (chiamati anche comandi bimanuali) è un metodo molto diffuso per evitare l'accesso a una macchina mentre questa si trova in una condizione pericolosa. Per avviare la macchina, occorre azionare contemporaneamente due comandi (entro 0,5 s uno dall'altro). In questo modo, entrambe le mani dell'operatore sono impegnate in una posizione sicura (ossia sui comandi) e non possono quindi essere spostate nell'area pericolosa. I comandi devono essere azionati continuamente finché permane una situazione di pericolo. Quando uno dei comandi viene rilasciato, il funzionamento della macchina deve cessare e, prima che la macchina possa essere riavviata, devono essere rilasciati entrambi i comandi.

Un sistema di controllo a due mani dipende fortemente dalla capacità del sistema di monitoraggio e di controllo di rilevare eventuali guasti, dunque è importante che questo aspetto sia progettato con le specifiche corrette. La prestazione del sistema di sicurezza a due mani è classificata in Tipi da ISO 13851 (EN 574), correlati alle Categorie ISO 13849-1. I tipi più comunemente usati per la sicurezza delle macchine sono IIIB e IIIC. La tabella che segue mostra la relazione tra i tipi e le categorie di prestazioni di sicurezza.

Requisiti	Tipi				
	I	II	III		
			A	B	C
Attivazione sincrona			X	X	X
Uso della Categoria 1 (da ISO 13849-1)	X		X		
Uso della Categoria 3 (da ISO 13849-1)		X		X	
Uso della Categoria 4 (da ISO 13849-1)					X

La progettazione fisica degli spazi deve impedire l'uso improprio (ad es. utilizzando una mano e un gomito). Ciò è possibile mediante un calcolo delle distanze o l'installazione di schermi. La macchina non deve passare da un ciclo a un altro senza il rilascio e la pressione di entrambi i pulsanti. Questo evita la possibilità che entrambi i pulsanti siano bloccati, lasciando così la macchina in continuo funzionamento. Il rilascio di uno qualsiasi dei pulsanti deve provocare l'arresto della macchina.

L'uso del controllo a due mani deve essere analizzato con attenzione poiché in genere lascia comunque un certo margine di rischio. Il comando a due mani protegge solo la persona che lo usa. L'operatore protetto deve essere in grado di osservare tutta l'area di accesso al pericolo, poiché le altre persone potrebbero non essere protette.

ISO 13851 (EN 574) fornisce ulteriori informazioni sul comando a due mani.

Dispositivi di abilitazione

I dispositivi di abilitazione sono controlli che permettono a un operatore di entrare in una zona pericolosa solo tenendo premuto l'interruttore di abilitazione. I dispositivi di abilitazione sono dotati di interruttori a due o tre posizioni. I tipi a due posizioni sono disattivati quando l'attuatore non è premuto e attivati in caso contrario. Gli interruttori a tre posizioni sono disattivati quando non premuti (posizione 1), attivati quando tenuti in posizione centrale (posizione 2) e disattivati quando premuti oltre la

posizione centrale (posizione 3). Inoltre, nel ritorno dalla posizione 3 alla posizione 1, il circuito di uscita non deve chiudersi passando attraverso la posizione 2.

I dispositivi di abilitazione devono essere usati in combinazione con altre funzioni legate alla sicurezza. Un tipico esempio è il controllo del movimento in modalità lenta. Dopo aver attivato la modalità lenta, l'operatore può entrare nella zona di pericolo con il dispositivo di abilitazione.

Quando si usa un dispositivo di abilitazione, un segnale deve indicare che il dispositivo di abilitazione è attivo.

Dispositivi logici

I dispositivi logici svolgono un ruolo centrale tra i componenti legati alla sicurezza del sistema di controllo. I dispositivi logici effettuano il controllo e il monitoraggio del sistema di sicurezza e consentono l'avviamento della macchina o eseguono i comandi per il suo arresto.

Per creare un'architettura di sicurezza rispondente alla complessità e alla funzionalità di ogni macchina, è disponibile un'ampia serie di dispositivi logici. I piccoli relè di monitoraggio di sicurezza cablati sono più economici e quindi adatti alle macchine più piccole in cui, per completare la funzione di sicurezza, è necessario un dispositivo logico dedicato. I relè di sicurezza di monitoraggio modulari e configurabili sono preferibili dove è necessario un maggior numero di dispositivi di protezione e un controllo di zona minimo. Le macchine medio/grandi e più complesse devono invece considerare sistemi programmabili con I/O distribuiti.

Relè di monitoraggio di sicurezza

I moduli relè di monitoraggio di sicurezza (MSR) svolgono un ruolo centrale in molti sistemi di sicurezza. Questi moduli sono generalmente costituiti da due o più relè a guida forzata con circuiteria addizionale per garantire le prestazioni della funzione di sicurezza.

I relè a guida forzata sono relè specializzati "ice-cube". I relè a guida forzata devono rispondere ai requisiti prestazionali dello standard EN 50025. Fondamentalmente, sono concepiti per evitare che contatti normalmente chiusi e normalmente aperti si chiudano simultaneamente. Concezioni più recenti sostituiscono le uscite elettromeccaniche con uscite di sicurezza allo stato solido.

I relè di monitoraggio 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 MSR 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 adatto dipende da una serie di fattori: il tipo di dispositivo che deve monitorare, il tipo di reset, il numero e il tipo di uscite.

Tipi di ingressi

I dispositivi di protezione hanno diversi modi di indicare il verificarsi di un evento:

Interblocchi a contatto e pulsanti di emergenza: contatti meccanici, a singolo canale con un contatto normalmente chiuso o a doppio canale con entrambi i contatti normalmente chiusi. L'MSR 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.

Interblocchi senza contatto e pulsanti di emergenza: contatti meccanici a doppio canale, uno normalmente aperto e uno normalmente chiuso. L'MSR deve essere in grado di elaborare diversi ingressi.

Dispositivi di commutazione di uscita allo stato solido: barriere fotoelettriche, laser scanner, dispositivi senza contatto allo stato solido hanno due uscite sourcing ed effettuano il rilevamento dei propri guasti incrociati. L'MSR 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. L'MSR 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. L'MSR 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. L'MSR deve essere in grado di tollerare alte tensioni e di rilevare basse tensioni quando il motore rallenta.

Arresto del movimento: l'MSR deve rilevare i treni di impulsi da diversi sensori ridondanti.

Dispositivo di comando a due mani: l'MSR deve rilevare ingressi diversi, normalmente aperti e normalmente chiusi, oltre a fornire la temporizzazione di 0,5 s e la logica sequenziale.

I relè di monitoraggio di sicurezza devono essere concepiti specificamente per interfacciare ognuno di questi dispositivi, poiché hanno diverse caratteristiche elettriche. Alcuni MSR possono collegarsi a diversi tipi di ingressi ma, una volta scelto il dispositivo, l'MSR si può interfacciare solo con quel dispositivo. Il progettista deve selezionare un MSR che sia compatibile con il dispositivo di ingresso.

Impedenza d'ingresso

L'impedenza d'ingresso dei relè di sicurezza di monitoraggio 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 di ingresso consentita massima di 500 Ohm (~). Quando l'impedenza di ingresso è superiore a ~ 500 Ohm, le uscite non vengono attivate. L'utente deve prestare particolare attenzione per garantire che l'impedenza d'ingresso rimanga al di sotto del valore massimo a specifica. La lunghezza, la dimensione e il tipo di cavo usato incidono sull'impedenza d'ingresso.

Numero di dispositivi di ingresso

Il processo di valutazione del rischio deve essere usato per determinare il numero di dispositivi di ingresso da collegare a un relè di monitoraggio di sicurezza (MSR) e la frequenza con cui tali dispositivi devono essere controllati. Per garantire che gli arresti d'emergenza e gli interblocchi della porta siano funzionanti, devono essere controllati a intervalli regolari, in base a quanto determinato dalla valutazione del rischio. Ad esempio, un MSR di ingresso 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 controllato. Questo accade perché l'apertura della protezione fa sì che l'MSR 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.

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 diagnostico" e il tempo tra un test e l'altro è detto "intervallo dei test diagnostici". Un terzo esempio potrebbero essere 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 l'integrità richiesta al processo di verifica. Minore è la frequenza del controllo "automatico", 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 canali dei dispositivi di ingresso, chiamati anche guasti incrociati. Questo avviene tramite il dispositivo di rilevamento o il relè di monitoraggio di sicurezza.

I relè di monitoraggio di sicurezza a microprocessore – come barriere fotoelettriche, laser scanner e sensori avanzati senza contatto – rilevano questi cortocircuiti in molti modi. Un modo comune di rilevare i guasti incrociati è il test con impulsi diversi. 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 sono simultanei e vengono rilevati dal dispositivo.

I relè di monitoraggio di sicurezza elettromeccanici usano un'altra tecnica di differenziazione: un ingresso pull-up e un ingresso pull-down. Un corto dal canale 1 al canale 2 attiva il dispositivo di protezione dalle sovracorrenti e il sistema di sicurezza procede allo spegnimento.

Uscite

Gli MSR sono disponibili con più uscite. I tipi di uscite aiutano a determinare quale MSR usare in determinate applicazioni.

Molti MSR hanno almeno 2 uscite di sicurezza immediatamente operative. Le uscite di sicurezza MSR sono normalmente aperte. Sono considerate di sicurezza grazie alla ridondanza e al controllo interno. Un secondo tipo di uscita sono le uscite temporizzate. Le uscite temporizzate vengono generalmente usate negli arresti di Categoria 1, in cui la macchina ha bisogno di tempo per l'arresto prima di permettere l'accesso alla zona pericolosa. Gli MSR hanno anche uscite ausiliarie. Generalmente, si tratta di uscite normalmente chiuse.

Caratteristiche delle uscite

Le caratteristiche delle uscite descrivono la capacità del dispositivo di protezione di commutare carichi. Generalmente, le caratteristiche dei dispositivi industriali sono descritte come resistive o elettromagnetiche. Un carico resistivo può essere un elemento riscaldatore. I carichi elettromagnetici sono generalmente relè, contattori o elettromagneti che hanno una forte caratteristica induttiva del carico. L'allegato A dello standard IEC 60947-5-1 descrive le categorie dei carichi. Le categorie sono riportate anche nella sezione "Principi" del catalogo di sicurezza.

Lettera di designazione: è una lettera seguita da un numero, ad esempio A300. La lettera fa riferimento alla corrente termica convenzionale in custodia e se la corrente è continua o alternata. Ad esempio, A rappresenta 10 amp di corrente alternata. Il numero indica 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. Gli utilizzi pertinenti allo standard IEC 60947-5 sono riportati nella tabella che segue.

Utilizzo	Descrizione del carico
AC-12	Controllo di carichi resistivi e carichi a stato solido con optoaccoppiatori di isolamento
AC-13	Controllo di carichi a stato solido con trasformatore d'isolamento
AC-14	Controllo di piccoli carichi elettromagnetici (meno di 72 VA)
AC-15	Carichi elettromagnetici superiori a 72 VA
DC-12	Controllo di carichi resistivi e carichi a stato solido con optoaccoppiatori di isolamento
DC-13	Controllo di elettromagneti
DC-14	Controllo di carichi elettromagnetici con resistori nel circuito

Corrente termica, Ith: la corrente termica convenzionale in custodia è il valore della corrente usata per i test di aumento della temperatura dell'apparecchiatura, quando è montata in una custodia specificata.

Tensione operativa Ue e corrente Ie nominali: i valori nominali di corrente e tensione di funzionamento indicano la capacità di chiusura e apertura degli elementi di commutazione in condizioni operative normali. I prodotti Allen-Bradley Guardmaster hanno valori nominali specifici di 125 V CA, 250 V CA e 24 V CC. Consultare il produttore per informazioni sull'uso a tensioni diverse da quelle specificate.

VA: i valori VA (Tensione x Amperaggio) indicano i valori nominali degli elementi di commutazione quando si chiude o si apre il circuito.

Esempio 1: un valore di A150, AC-15 indica che i contatti possono chiudere un circuito di 7.200 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 elettromagnetico, i 60 amp avranno solo una durata limitata, la corrente di spunto del carico elettromagnetico. L'apertura del circuito è a soli 720 VA poiché la corrente a regime del carico elettromagnetico è pari a 6 A, ossia la corrente nominale di funzionamento.

Esempio 2: un valore nominale di N150, DC-13 indica che i contatti possono chiudere un circuito di 275 VA. A 125 V CA, i contatti possono chiudere un circuito con una corrente di 2,2 A. I carichi elettromagnetici in CC non hanno correnti di spunto come quelli in CA. L'apertura del circuito è dunque a 275 VA perché la corrente a regime del carico elettromagnetico è pari a 2,2, la corrente nominale di funzionamento.

Riavvio della macchina

Se, ad esempio, una protezione interbloccata viene aperta 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 chiusura della protezione. Uno dei modi più comuni per ottenere questo risultato è affidarsi a un contattore di avviamento a ritenuta.

La pressione e il rilascio del pulsante di avvio eccita momentaneamente la bobina di controllo del contattore che chiude i contatti di alimentazione. Finché la corrente 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 della protezione è cablato nel circuito di controllo del contattore. Questo significa che il riavvio può essere effettuato solo chiudendo la protezione e quindi impostando su "ON" il normale pulsante di avviamento, resettando così il contattore e avviando la macchina.

I requisiti per le normali situazioni di interblocco sono definiti dallo standard ISO 12100-1 Paragrafo 3.22.4 (estratto)

"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 monta 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 monitoraggio di sicurezza Allen Bradley Guardmaster sono dotati di reset manuale monitorato o reset automatico/manuale.

Reset manuale monitorato

Un reset manuale monitorato richiede un cambiamento di stato del circuito di reset dopo che la porta è stata chiusa o l'arresto di emergenza resettato. I contatti ausiliari normalmente chiusi ad accoppiamento meccanico dei contattori di commutazione di potenza sono connessi in serie con un pulsante instabile. Una volta che la protezione è stata aperta e chiusa nuovamente, il relè di sicurezza non consente alla macchina di essere riavviata finché non si verifica un cambiamento di stato del pulsante di reset. Ciò è in linea con l'intento dei requisiti relativi al reset manuale aggiuntivo previsto da EN ISO 13849-1; vale a dire che la funzione di reset assicura che entrambi i contattori siano su OFF, che entrambi i circuiti di interblocco (e quindi le protezioni) siano chiusi e anche (dal momento che è richiesto un cambiamento di stato) che l'attuatore di reset non sia stato escluso o bloccato in alcun modo. Se questi controlli sono soddisfacenti, la macchina può essere riavviata con i normali comandi. Lo standard EN ISO 13849-1 prevede un cambiamento dallo stato di eccitazione allo stato di diseccitazione, ma lo stesso effetto di protezione può anche essere ottenuto dal principio opposto.

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 presenti più rischi prima di utilizzare la macchina.

Reset automatico/manuale

Alcuni relè di sicurezza sono dotati di 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 sarà rilevato. Con questo approccio potrebbe non essere possibile soddisfare il requisito di un reset manuale supplementare previsto da EN ISO 13849-1, a meno che non siano utilizzati mezzi supplementari.

In alternativa, la linea di reset può essere collegata con un ponticello, 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 condurrà 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.

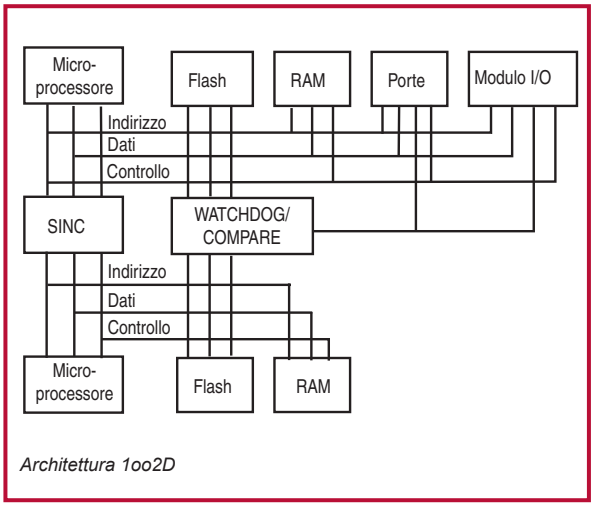
L'interruttore di reset deve essere posizionato in un luogo che consenta di vedere bene il pericolo, in modo che l'operatore possa controllare che l'area non presenti più rischi prima di utilizzare la macchina.

Protezioni di controllo

Una protezione di controllo arresta una macchina quando la protezione è aperta e l'avvia direttamente quando è chiusa. L'uso di questo tipo di protezioni è consentito solo in determinate condizioni molto precise, poiché qualsiasi avviamento imprevisto o il mancato arresto sarebbero estremamente pericolosi. Il sistema di interblocco deve avere la maggiore affidabilità possibile (spesso è consigliabile usare il blocco della protezione). L'uso delle protezioni di controllo può essere preso in considerazione SOLO per le macchine in cui non esiste ALCUNA POSSIBILITÀ che un operatore o parte del suo corpo si trovino all'interno o raggiungano la zona pericolosa mentre la protezione è chiusa. Inoltre, la protezione di controllo deve costituire l'unico accesso all'area pericolosa.

Controlli a logica programmabile di sicurezza

L'esigenza di applicazioni di sicurezza flessibili e scalabili 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 standard e di sicurezza sono molte. I PLC di sicurezza sono disponibili in varie piattaforme, per rispondere ai requisiti di scalabilità, funzionalità e integrazione dei più complessi sistemi di sicurezza.

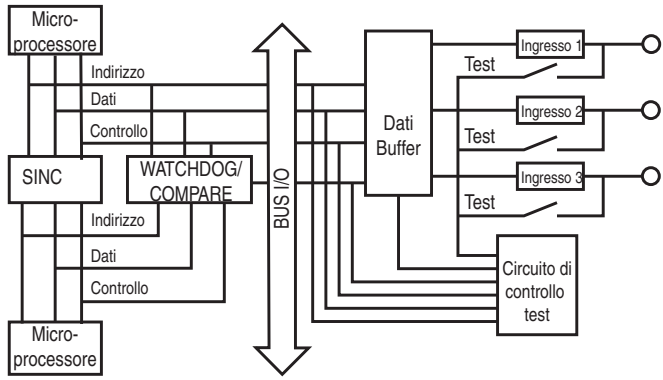


Architettura 1oo2D

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.

Inoltre, ogni circuito di ingresso è testato internamente diverse volte al secondo, per verificarne il corretto funzionamento. 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.



Schema a blocchi del modulo di ingressi di sicurezza

Le uscite del PLC di sicurezza sono elettromeccaniche o di sicurezza allo stato solido. 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 che non dovesse rispondere correttamente viene disattivata dalle altre due e il guasto è riportato dal circuito di monitoraggio interno.

Quando si usano dispositivi di sicurezza con contatti meccanici (pulsanti di emergenza, interblocchi, 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.

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 funziona in modo molto simile a un MSR 127. 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.

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. Questo esempio 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. Un'eccezione è data dal bordo di sicurezza a tecnologia resistiva.

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.

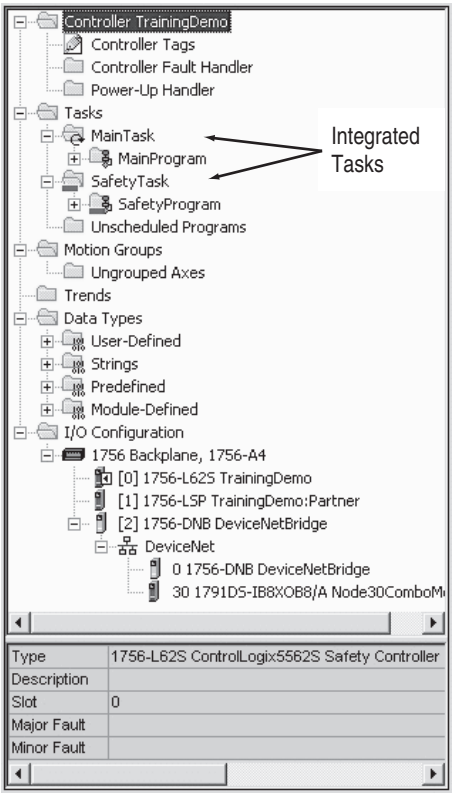
Il cablaggio dei sistemi a logica programmabile è semplificato rispetto a quello dei relè di monitoraggio di sicurezza. Anziché essere cablati a terminali specifici dei relè di monitoraggio di sicurezza, i dispositivi di ingresso sono collegati a qualunque terminale di ingresso e i dispositivi di uscita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

Controllori di sicurezza integrati

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 SIL3 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 che segue 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.

Tutte le funzioni standard e legate alla sicurezza sono isolate una dall'altra. Ad esempio, i tag di sicurezza possono essere letti direttamente dalla logica standard. I tag di sicurezza possono essere scambiati tra i controllori GuardLogix 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.



1. Logica e tag standard si comportano come ControlLogix.

2. Dati tag standard, analizzati dal programma o dal controllore e dispositivi esterni, interfacce operatore, PC, altri controllori, ecc.

3. Come controllore integrato, GuardLogix permette di trasferire (mappare) dati tag standard nei tag di sicurezza da usare per task di sicurezza. Per gli utilizzatori, ciò significa poter leggere informazioni di stato sul lato standard di GuardLogix. I dati non devono essere usati per controllare direttamente una uscita 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 GuardLogix su EtherNet.

7. I dati 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.

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 noto, 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 legato alla 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/controllori di sicurezza, 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.

Dispositivi di uscita

Contattori e relè di controllo di sicurezza

Contattori e relè di controllo servono a togliere alimentazione all'attuatore. In base al livello di sicurezza, contattori e relè di controllo sono dotati di funzioni speciali.

Per il feedback sullo stato dei contattori e dei relè di controllo al dispositivo logico, si utilizzano contatti normalmente chiusi ad accoppiamento meccanico. L'uso di contatti ad accoppiamento meccanico aiuta a garantire la funzione di sicurezza. Per rispondere ai requisiti dei contatti ad accoppiamento meccanico, i contatti normalmente chiusi e quelli normalmente aperti non possono essere, contemporaneamente, in stato di chiusura. IEC 60947-5-1 definisce i requisiti per i contatti ad accoppiamento meccanico. Se i contatti normalmente aperti si saldano, i contatti normalmente chiusi rimangono aperti di almeno 0,5 mm. Viceversa, se i contatti normalmente chiusi si saldano, i contatti normalmente aperti rimangono aperti.

I sistemi di sicurezza devono essere avviati solo in posizioni specifiche. I contattori e i relè di controllo standard permettono di attirare l'indotto per chiudere i contatti normalmente aperti. Sui dispositivi di sicurezza, l'indotto è protetto dall'override manuale per ridurre il rischio di avviamento non intenzionale.

Sui relè di controllo di sicurezza, il contatto normalmente chiuso è azionato dal comando principale. I contattori di sicurezza usano un blocco per contatti supplementare per posizionare i contatti ad accoppiamento meccanico. Se il blocco di contatti fuoriesce dalla base, i contatti ad accoppiamento meccanico rimangono chiusi. I contatti ad accoppiamento meccanico sono fissati permanentemente al relè di controllo o al contattore di sicurezza. Sui contattori più grandi, un blocco per contatti supplementare è insufficiente a riflettere accuratamente lo stato dell'azionamento più grande. Su entrambi i lati del contattore, sono situati dei contatti speculari (Figura 4.81).

Il tempo di diseccitazione dei relè di controllo o dei contattori influisce sul calcolo della distanza di sicurezza. Spesso, nella bobina, è installato un soppressore di picchi di tensione che aumenta la vita dei contatti che azionano la bobina. Per le bobine CA, il tempo di diseccitazione rimane invariato. Per le bobine CC, il tempo di diseccitazione aumenta. L'aumento dipende dal tipo di soppressione selezionato.

Contattori e relè di controllo sono concepiti per commutare grandi carichi, da 0,5 a oltre 100 A. Il sistema di sicurezza funziona a basse correnti. Il segnale di feedback generato dal dispositivo logico del sistema di sicurezza può andare da pochi milliampere a decine di milliampere, di solito a 24 V CC. Per commutare in modo affidabile una corrente così bassa, contattori e relè di controllo di sicurezza sono dotati di contatti biforcati, placcati in oro.

Protezione dai sovraccarichi

Gli standard elettrici impongono la protezione dei motori dai sovraccarichi. La diagnostica fornita dal dispositivo di protezione dai sovraccarichi aumenta non solo la sicurezza dell'apparecchiatura ma anche quella dell'operatore. Le tecnologie attualmente disponibili possono rilevare condizioni di guasto come sovraccarico, mancanza di fase, guasto verso terra, stallo, blocco, sottocarico, squilibrio di corrente e sovratemperatura. Il rilevamento e la comunicazione delle condizioni anomale prima dell'intervento aiutano a ridurre i tempi di fermo della produzione e a proteggere operatori e personale di manutenzione da condizioni di pericolo impreviste.

Azionamenti e asservimenti

Azionamenti e asservimenti di sicurezza possono essere usati per impedire la trasmissione dell'energia rotazionale e permettere un arresto di sicurezza o un arresto di emergenza.

Gli inverter ottengono il livello di sicurezza con canali ridondanti per togliere alimentazione dalla circuiteria del controllo di gate. Un canale è il segnale di abilitazione, un segnale hardware che rimuove il segnale di ingresso alla circuiteria del controllo di gate. Il secondo canale è un relè a guida forzata che scollega l'alimentazione elettrica dalla circuiteria del controllo di gate. Il relè a guida forzata, inoltre, ritrasmette un segnale di stato al sistema logico. Questo approccio ridondante consente di applicare l'azionamento di sicurezza ai circuiti di arresto di emergenza, senza bisogno di un contattore.

L'asservimento funziona in modo simile agli inverter, mediante segnali di sicurezza ridondanti per ottenere la funzione di sicurezza. Un segnale interrompe il comando alla circuiteria del controllo di gate. Un secondo segnale scollega l'alimentazione elettrica dalla circuiteria del controllo di gate. Due relè a guida forzata sono utilizzati per rimuovere i segnali e fornire feedback al dispositivo logico di sicurezza.

Sistemi di collegamento

I sistemi di collegamento aggiungono valore riducendo i costi di installazione e manutenzione dei sistemi di sicurezza. I progetti devono prendere in considerazione sistemi a canale singolo, a doppio canale, a doppio canale con segnalazione e molteplici tipi di dispositivi.

Quando è necessario un collegamento in serie di interblocchi a due canali, un blocco di distribuzione può semplificare l'installazione. Con un grado di protezione IP67, questi dispositivi possono essere installati sulla macchina in posizioni remote. Quando è necessario un diverso gruppo di dispositivi, è possibile utilizzare un

modulo ArmorBlock Guard I/O. Per installare vari tipi di dispositivi, gli ingressi possono essere configurati via software.

Calcolo delle distanze di sicurezza

Le funzioni di sicurezza devono intervenire in tempo per evitare che l'operatore possa raggiungere il punto di pericolo. Per il calcolo delle distanze di sicurezza, esistono due gruppi di standard. In questo capitolo, questi standard sono raggruppati come segue:

ISO EN: (ISO 13855 ed EN 999)

US CAN (ANSI B11.19, ANSI RIA R15.06 e CAN/CSA Z434-03)

Formula

La distanza minima di sicurezza dipende dal tempo necessario a elaborare il comando di arresto e da quanto l'operatore può penetrare la zona di rilevamento prima del rilevamento. In tutto il mondo, la formula utilizzata ha la stessa forma e gli stessi requisiti. Le differenze sono i simboli usati per rappresentare variabili e unità di misura.

Le formule sono:

ISO EN: $S = K \times T + C$

US CAN: $Ds = K \times (Ts + Tc + Tr + Tbm) + Dpf$

Dove: Ds e S sono la distanza di sicurezza minima dalla zona di pericolo al più vicino punto di rilevamento

Direzioni di avvicinamento

Quando si considera il calcolo della distanza di sicurezza per una barriera fotoelettrica o uno scanner, occorre considerare l'avvicinamento al dispositivo di rilevamento. L'avvicinamento può essere di tre tipi:

Normale – avvicinamento perpendicolare al piano di rilevamento

Orizzontale – avvicinamento parallelo al piano di rilevamento

Inclinato – avvicinamento inclinato rispetto alla zona di rilevamento.

Costante di velocità

K è una costante di velocità. Il valore della costante di velocità dipende dai movimenti dell'operatore (velocità delle mani, velocità di camminata e lunghezza del passo). Questo parametro è basato su dati di ricerca secondo cui è ragionevole presumere, per il movimento della mano di un operatore a corpo fermo, una velocità

di 1.600 mm/s. Occorre comunque considerare le circostanze effettive dell'applicazione. In linea generale, la velocità di avvicinamento varierà da 1.600 mm/s a 2.500 m/s. La costante di velocità adeguata deve essere determinata mediante la valutazione dei rischi.

Tempo di arresto

T è il tempo di arresto globale del sistema. Il tempo totale, in secondi, inizia dalla generazione del segnale di arresto alla cessazione del pericolo. Per facilitare l'analisi, questo tempo può essere suddiviso nelle sue parti incrementali (Ts, Tc, Tr e Tbm). Ts è il tempo di arresto peggiore della macchina/apparecchiatura. Tc è il tempo di arresto peggiore del sistema di controllo. Tr è il tempo di risposta del dispositivo di protezione, compresa la sua interfaccia. Tbm è l'ulteriore tempo di arresto consentito dal dispositivo di controllo del freno prima che rilevi il superamento dei limiti predeterminati dall'utente finale per il tempo di arresto. Tbm si usa con presse meccaniche a tavola rotante. Ts + Tc + Tr sono usualmente misurati da un dispositivo di misurazione del tempo di arresto se i valori sono sconosciuti.

Fattori di penetrazione in profondità

I fattori di penetrazione in profondità sono rappresentati dai simboli C e Dpf. Si tratta della corsa massima verso il pericolo prima del rilevamento da parte del dispositivo di protezione. I fattori di penetrazione in profondità cambiano a seconda del tipo di dispositivo e di applicazione. Per determinare il miglior fattore di penetrazione in profondità, occorre far riferimento allo standard corrispondente. Per un avvicinamento normale a una barriera fotoelettrica o a uno scanner, la cui sensibilità agli oggetti è inferiore a 64 mm, gli standard ANSI e canadesi usano:

Dpf = 3,4 x (Sensibilità oggetti – 6,875 mm), ma non meno di zero.

Per un avvicinamento normale a una barriera fotoelettrica o a uno scanner, la cui sensibilità agli oggetti è inferiore a 40 mm, gli standard ISO e EN usano:

C = 8 x (Sensibilità oggetti – 14 mm), ma non meno di 0

Queste due formule hanno un punto di convergenza a 19,3 mm. Per sensibilità agli oggetti inferiori a 19 mm, lo standard US CAN è più restrittivo, dato che la barriera fotoelettrica o lo scanner dell'area devono essere maggiormente allontanate dal pericolo. Per sensibilità agli oggetti superiori a 19,3 mm, è più restrittivo lo standard ISO EN. I costruttori che intendono commercializzare le loro macchine in tutto il mondo devono prevedere le condizioni peggiori di entrambe le equazioni.

Applicazioni “reach-through” (attraversamento)

Quando si utilizzano sensibilità agli oggetti più grandi, gli standard US CAN e ISO EN differiscono leggermente sul fattore di penetrazione in profondità e sulla sensibilità agli oggetti. Il valore ISO EN è di 850 mm mentre il valore US CAN è 900 mm. Gli standard differiscono anche nella sensibilità agli oggetti. Lo standard ISO EN ammette valori compresi tra 40 e 70 mm, mentre lo standard US CAN ammette fino a 600 mm.

Applicazioni “reach-over” (superamento)

Entrambi gli standard stabiliscono che l’altezza minima del raggio più basso dovrebbe essere di 300 mm, ma differiscono per quanto riguarda l’altezza minima del raggio più alto. ISO EN stabilisce 900 mm, mentre US CAN stabilisce 1.200 mm. Il valore per il raggio più alto sembra essere controverso. Quando si considera una applicazione “reach-through”, l’altezza del raggio più alto dovrà essere molto più elevata per un operatore in posizione eretta. Se l’operatore può oltrepassare la parte superiore del piano di rilevamento, allora si applica il criterio “reach-over”.

Raggi singoli o multipli

I raggi separati, singoli o multipli, sono ulteriormente definiti negli standard ISO EN. Le cifre che seguono mostrano le altezze “praticabili” dei raggi multipli rispetto al pavimento. La penetrazione in profondità è di 850 mm per la maggior parte dei casi e di 1.200 mm per il raggio singolo. In confronto, lo standard US CAN considera ciò tra i requisiti “reach-through”. Il passaggio sopra, sotto o attorno ai raggi singoli o multipli deve sempre essere preso in considerazione.

Numero di raggi	Altezza dal pavimento (mm)	C (mm)
1	750 1.200	
2	400, 900	850
3	300, 700, 1.100	850
4	300, 600, 900, 1.200	850

Calcoli della distanza

Per l’avvicinamento normale alla barriera fotoelettrica, il calcolo della distanza di sicurezza, per ISO EN e US CAN, è simile ma esistono delle differenze. Per l’avvicinamento normale a barriere fotoelettriche verticali la cui sensibilità agli oggetti è di 40 m max., lo standard ISO EN richiede due fasi. Innanzitutto, calcolare S usando 2.000 come costante di velocità.

$S = 2.000 \times T + 8 \times (d - 1\ 4)$

La distanza minima per S è di 100 mm.

Una seconda fase può essere usata quando la distanza è superiore a 500 mm. Il valore di K può essere ridotto a 1.600. Quando si usa K = 1.600, il valore minimo di S è 500 mm.

Lo standard US CAN usa l'approccio a una fase: Ds = 1.600 x T * Dpf

Ciò comporta differenze superiori al 5% tra gli standard, quando il tempo di risposta è inferiore a 560 ms.

Avvicinamenti inclinati

La maggior parte delle applicazioni con barriera fotoelettrica e scanner sono installate in verticale (avvicinamento normale) o in orizzontale (avvicinamento parallelo). Queste installazioni non sono considerate inclinate se l'angolazione è compresa tra ±5° rispetto alla progettazione. Se l'angolo è superiore a ±5°, occorre prendere in considerazione i rischi potenziali (ad es. distanza più corta) degli avvicinamenti prevedibili. In generale, gli angoli superiori a 30° rispetto al piano di riferimento (ad es. pavimento) dovrebbero essere considerati normali, mentre quelli inferiori a 30 considerati paralleli.

Pedane di sicurezza

Con le pedane, la distanza di sicurezza deve prendere in considerazione velocità e passo degli operatori. Si presume che l'operatore cammini e che le pedane di sicurezza siano installate a pavimento. Il primo passo dell'operatore sulla pedana ha un fattore di penetrazione in profondità di 1.200 mm o 48 pollici. Se l'operatore deve salire per passare su una piattaforma, il fattore di penetrazione in profondità può essere ridotto di un fattore pari al 40% dell'altezza del passo.

Esempio

Esempio: un operatore si avvicina normalmente a una barriera fotoelettrica di 14 mm, collegata a un relè di monitoraggio di sicurezza che, a sua volta, è collegato a un contattore alimentato in CC con un soppressore a diodi. Il tempo di risposta del sistema di sicurezza, Tr, è 20 + 15 + 95 = 130 ms. Il tempo di arresto della macchina, Ts+Tc, è 170 ms. Il dispositivo di controllo del freno non è utilizzato. Il valore Dpf è 1 pollice e il valore C è zero. Il calcolo sarebbe il seguente:

Dpf = 3,4 (14 – 6,875) = 1 poll. (24,2 mm)

C = 8 (14-14) = 0

Ds = K x (Ts + Tc + Tr + Tbm) + Dpf
Ds = 63 x (0,17 + 0,13 + 0) + 1
Ds = 63 x (0,3) + 1
Ds = 18,9 + 1
Ds = 19,9 poll. (505 mm)

S = K x T + C
S = 1.600 x (0,3) + 0
S = 480 mm (18,9 poll.)

Quindi, per una macchina utilizzabile in qualsiasi parte del mondo, la distanza di sicurezza minima a cui la barriera fotoelettrica di sicurezza deve essere montata rispetto al pericolo è di 20 pollici o 508 mm.

Prevenzione dell'accensione non intenzionale

La prevenzione dell'accensione non intenzionale è trattata in molti standard, tra cui ISO 14118, EN1037, ISO 12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05 e AS 4024.1603. Questi standard hanno un oggetto comune: il metodo primario per impedire accensioni non intenzionali è scollegare l'alimentazione al sistema e bloccare il sistema in stato di disattivazione. Lo scopo è permettere alle persone di entrare in sicurezza nelle zone pericolose della macchina.

Lockout/Tagout

Le macchine nuove devono essere costruite con dispositivi di isolamento dell'alimentazione bloccabili. I dispositivi si applicano a tutti i tipi di energia – elettrica, idraulica, pneumatica, gravitazionale e laser. Per lockout si intende l'applicazione di un blocco a un dispositivo di isolamento dell'alimentazione. Il blocco deve essere rimosso solo dal suo proprietario o da un supervisore, in condizioni controllate. Quando sulla macchina devono lavorare diverse persone, ogni persona deve applicare il proprio blocco ai dispositivi di isolamento dell'alimentazione. Ogni blocco deve essere rapportabile al suo proprietario.

Negli USA, il tagout è una alternativa al lockout per le macchine più vecchie su cui non è mai stato installato un dispositivo lucchettabile. In questo caso, la macchina viene spenta e viene applicato un cartellino per avvisare tutto il personale di non avviare la macchina mentre l'operatore che ha apposto il cartellino sta lavorando sulla macchina. A partire dal 1990, le macchine che sono state modificate devono essere aggiornate in modo da prevedere un dispositivo lucchettabile di isolamento dell'alimentazione.

Un dispositivo di isolamento dell'alimentazione è un dispositivo meccanico che, fisicamente, impedisce la trasmissione o il rilascio di energia. Questi dispositivi possono essere interruttori automatici, sezionatori, interruttori manuali, combinazioni spina/presa o valvole manuali. I dispositivi di isolamento elettrico devono commutare tutti i conduttori di alimentazione non messi a terra e nessun polo può operare in modo indipendente.

Lo scopo del lockout e del tagout è impedire l'avviamento non intenzionale della macchina. L'avviamento non intenzionale può essere il risultato di varie cause: un guasto del sistema di controllo, un'azione inadeguata su un comando di avviamento, un sensore, un contattore o una valvola, il ripristino dell'alimentazione dopo un'interruzione o una serie di altre influenze interne o esterne. Al termine del processo di lockout/tagout, deve essere verificata la dissipazione dell'energia.

Sistemi di isolamento di sicurezza

I sistemi di isolamento di sicurezza eseguono lo spegnimento ordinario di una macchina consentendo, nel contempo, di scollegare l'alimentazione in modo semplice. Questo approccio funziona bene con macchine e sistemi di fabbricazione più grandi, soprattutto quando diverse fonti di alimentazione sono situate a livello intermedio o in posizioni distanti.

Sezionatori di carico

Per l'isolamento locale dei dispositivi elettrici, subito prima del dispositivo da isolare e bloccare possono essere installati degli interruttori. Gli interruttori di carico serie 194E sono un esempio di prodotto in grado sia di isolare sia di bloccare.

Sistemi a chiave bloccata

I sistemi a chiave bloccata sono un altro metodo per implementare un sistema di lockout. Molti sistemi a chiave bloccata sono inizializzati da un dispositivo di isolamento dell'alimentazione. Quando l'interruttore è spento dalla chiave "primaria", l'alimentazione alla macchina viene rimossa, simultaneamente, da tutti i conduttori di alimentazione non messi a terra. La chiave primaria può quindi essere rimossa e portata nel posto in cui è necessario accedere alla macchina. Per configurazioni di lockout più complesse, possono essere aggiunti vari componenti.

Misure alternative al lockout

Lockout e tagout devono essere usati durante le operazioni di manutenzione o assistenza sulle macchine. Gli interventi sulla macchina durante le normali operazioni di produzione sono protetti. La differenza tra le operazioni di assistenza/manutenzione e quelle di normale funzionamento non è sempre chiara.

Alcune regolazioni e interventi di assistenza di minore importanza che avvengono durante le normali operazioni di produzione non richiedono necessariamente il lockout della macchina. Si tratta, ad esempio, di carico e scarico dei materiali, modifiche e regolazioni ordinarie degli utensili, controllo dei livelli di lubrificazione e rimozione del materiale di scarto. Queste attività devono essere di routine, ripetitive e integranti nell'utilizzo dell'apparecchiatura di produzione e il lavoro è realizzato usando misure di protezione alternative che forniscono effettiva protezione. Tra queste misure, ci sono le protezioni interbloccate, le barriere fotoelettriche e le pedane di sicurezza. Usate con adeguati dispositivi di uscita e logici di sicurezza, gli operatori possono accedere in sicurezza alle zone di pericolo della macchina per le normali attività di produzione o di assistenza.

Sistemi di controllo legati alla sicurezza

Introduzione

Che cos'è un sistema di controllo legato alla sicurezza (spesso abbreviato SRCS)? Si tratta della parte di un sistema di controllo di una macchina atta a impedire che si verifichi una condizione pericolosa. Può essere un sistema dedicato separato o essere integrato all'interno del normale sistema di controllo della macchina.

La sua complessità va da un sistema semplice, come l'interruttore di interblocco di una porta e l'interruttore per un arresto di emergenza collegati in serie fino alla bobina di controllo di un contattore di potenza o a un sistema composto che comprende sia dispositivi semplici sia complessi, comunicanti attraverso software e hardware.

I sistemi di controllo legati alla sicurezza sono concepiti per realizzare funzioni di sicurezza. Il sistema SRCS deve continuare a funzionare correttamente in tutte le condizioni prevedibili. Quindi che cos'è una funzione di sicurezza, come possiamo progettare un sistema per realizzarla e una volta messa a punto, come dimostrare la sua efficacia?

Funzione di sicurezza

Una funzione di sicurezza è implementata dai componenti legati alla sicurezza del sistema di controllo della macchina per ottenere o mantenere l'apparecchiatura in uno stato di sicurezza rispetto a uno specifico pericolo. Un guasto della funzione di sicurezza può comportare un immediato aumento dei rischi legati all'uso dell'apparecchiatura; ovvero una condizione pericolosa.

Una macchina deve presentare almeno un "pericolo", altrimenti non è una macchina. Una "condizione pericolosa" si verifica quando una persona è esposta a un pericolo. Una condizione pericolosa non implica che la persona sia ferita. La persona esposta può essere in grado di riconoscere il pericolo e di evitare lesioni. La persona esposta può non essere in grado di riconoscere il pericolo o il pericolo può essere originato da un avviamento non intenzionale. Il compito principale del progettista di sistemi di sicurezza è prevenire le condizioni pericolose e gli avviamenti non intenzionali.

La funzione di sicurezza può spesso essere descritta con requisiti multicomponente. Ad esempio, la funzione di sicurezza originata da una protezione di interblocco si basa su tre aspetti:

1. i pericoli coperti dalla protezione non possono agire fino a che la protezione è chiusa;
2. l'apertura della protezione provoca l'arresto del pericolo, se attivo al momento dell'apertura;
3. la chiusura della protezione non riavvia il pericolo coperto dalla protezione.

Quando si definisce la funzione di sicurezza per una specifica applicazione, la parola “pericolo” deve essere sostituita dal pericolo specifico. Il pericolo non deve essere confuso con le sue conseguenze. Schiacciamento, taglio e ustioni sono le conseguenze di un pericolo. Esempi di pericolo sono motori, stantuffi, coltelli, torce, pompe, laser, robot, organi terminali di robot, solenoidi, valvole, altri tipi di attuatore o pericoli meccanici con effetti gravitazionali.

Nella discussione sui sistemi di sicurezza, è stata utilizzata la frase “in concomitanza o prima della richiesta di intervento della funzione di sicurezza”. Che cos’è una richiesta di intervento della funzione di sicurezza? Esempi di richiesta di intervento della funzione di sicurezza sono l’apertura di una protezione interbloccata, l’interruzione di una barriera fotoelettrica, il passo su una pedana di sicurezza o la pressione di un arresto di emergenza. Un operatore chiede che il pericolo sia bloccato o, se questa condizione già sussiste, che non sia trasmessa energia.

I componenti legati alla sicurezza del sistema di controllo della macchina eseguono la funzione di sicurezza. La funzione di sicurezza non è eseguita da un singolo dispositivo, ad esempio, solo dalla protezione. L’interblocco sulla protezione invia un comando a un dispositivo logico che, a sua volta, disabilita un attuatore. La funzione di sicurezza inizia con il comando e finisce con l’implementazione.

Il sistema di sicurezza deve essere progettato con un livello di integrità commisurato ai rischi della macchina. Rischi maggiori richiedono maggiori livelli di integrità per garantire l’operatività della funzione di sicurezza. I sistemi di sicurezza della macchina possono essere classificati in base al tipo di progettazione e alla capacità di garantire l’operatività della funzione di sicurezza o, in altre parole, in base al livello di integrità della sicurezza funzionale.

Sicurezza funzionale dei sistemi di controllo

Importante: *gli standard e i requisiti considerati in questa sezione sono relativamente nuovi. I gruppi di redazione stanno ancora lavorando ad alcuni aspetti, soprattutto per quanto riguarda il chiarimento e la combinazione di alcuni di questi standard. Quindi, è possibile che ci siano ancora delle variazioni rispetto ad alcuni dei dettagli forniti in queste pagine. Per le ultime informazioni, consultare: http://www.ab.com/safety.*

Che cos’è la sicurezza funzionale?

Per sicurezza funzionale si intende quella parte della sicurezza complessiva che dipende dal corretto funzionamento del processo o delle apparecchiature in risposta ai relativi ingressi. Lo standard IEC TR 61508-0, per contribuire a chiarire il significato di sicurezza funzionale, fornisce il seguente esempio. “Per esempio, un dispositivo di protezione da sovratemperature che utilizza un sensore termico negli avvolgimenti di un motore elettrico per diseccitare il motore prima che possa surriscaldarsi è un esempio di sicurezza funzionale. Ma l’isolamento di un componente

contro le alte temperature non è un esempio di sicurezza funzionale (anche se è sempre un esempio di sicurezza e potrebbe proteggere esattamente dallo stesso pericolo).” Come ulteriore esempio, confrontiamo una protezione fisica e una protezione interbloccata. La protezione fisica non è considerata “sicurezza funzionale” anche se può proteggere contro l’accesso allo stesso pericolo, come una porta interbloccata. La porta interbloccata, invece, è un esempio di sicurezza funzionale. Quando la protezione è aperta, l’interblocco funge da ingresso per il sistema che garantisce lo stato di sicurezza. Anche i dispositivi di protezione personale (DPP) vengono utilizzati come misura protettiva per contribuire ad aumentare la sicurezza del personale. Ma i DPP non sono considerati sistemi di sicurezza funzionale.

Il termine “sicurezza funzionale” è stato introdotto nello standard IEC 61508:1998. Da allora, è stato talvolta associato solo ai sistemi di sicurezza programmabili. Ma si tratta di una idea sbagliata. La sicurezza funzionale copre un’ampia gamma di dispositivi che vengono usati per creare sistemi di sicurezza. Dispositivi come interblocchi, barriere fotoelettriche, relè di sicurezza, PLC di sicurezza, contattori di sicurezza e azionamenti di sicurezza sono interconnessi per formare un sistema di sicurezza che realizza una specifica funzione di sicurezza. Questa è sicurezza funzionale. Quindi, la sicurezza funzionale di un sistema di controllo elettrico è altamente inerente al controllo dei pericoli proveniente dalle parti mobili di una macchina.

Per la sicurezza funzionale, sono necessari due tipi di requisiti:

- la funzione di sicurezza e
- l’integrità della sicurezza.

La valutazione dei rischi svolge un ruolo chiave nello sviluppo dei requisiti di sicurezza funzionale. L’analisi delle attività e dei pericoli consente di definire i requisiti funzionali per la sicurezza (ossia, la funzione di sicurezza). Dalla quantificazione dei rischi si ottengono invece i requisiti di integrità della sicurezza (ossia, il livello di integrità della sicurezza o livello prestazionale).

Di seguito sono riportati quattro dei più significativi standard di sicurezza funzionale dei sistemi di controllo per i macchinari:

1. **IEC/EN 61508** “Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza”

   Questo standard contiene i requisiti e le disposizioni applicabili alla progettazione di sistemi e sottosistemi, elettronici e programmabili, complessi. Lo standard è generico e quindi non è limitato al settore delle macchine.

2. **IEC/EN 62061** “Sicurezza del macchinario – Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza”

   Questo standard costituisce il recepimento specifico per le macchine di IEC/EN 61508. Indica i requisiti applicabili alla progettazione, a livello di

sistema, di tutti i tipi di sistemi di controllo elettrici legati alla sicurezza dei macchinari, oltre che alla progettazione di dispositivi o sottosistemi non complessi. I sottosistemi programmabili o complessi dovrebbero soddisfare IEC/EN 61508

3. **EN ISO 13849-1:2008** "Sicurezza delle macchine – Componenti legati alla sicurezza dei sistemi di controllo"

   Questo standard nasce per indicare un percorso di transizione diretta dalle categorie del precedente EN 954-1.

4. **IEC 61511** "Sicurezza funzionale – Sistemi strumentali di sicurezza per il settore dell'industria di processo"

   Questo standard rappresenta il recepimento di IEC/EN 61508 specifico per il settore dell'industria di processo.

Gli standard di sicurezza funzionale rappresentano un significativo passo avanti rispetto a requisiti esistenti, quali il controllo affidabile e il sistema di categorie della precedente ISO 13849-1:1999 (EN 954-1:1996).

Le categorie non scompariranno completamente; sono anche presenti nell'attuale EN ISO 13849-1 che utilizza il concetto di sicurezza funzionale e ha introdotto una nuova terminologia e nuovi requisiti. Vi sono importanti aggiunte e differenze rispetto al vecchio EN 954-1 (ISO 13849-1:1999). In questa sezione, ci riferiremo all'attuale versione come EN ISO 13849-1. (EN ISO 13849-1:2008 ha lo stesso testo di ISO 13849-1:2006).

IEC/EN 62061 e EN ISO 13849-1:2008

Sia IEC/EN 62061 che EN ISO 13849-1 riguardano i sistemi di controllo elettrici correlati alla sicurezza. L'intento è quello di farli confluire in un unico standard con terminologia comune. Entrambi gli standard producono lo stesso risultato utilizzando, tuttavia, metodi diversi. Sono concepiti per offrire all'utente la possibilità di scegliere quello più adatto alla propria situazione. L'utente può scegliere indifferentemente l'uno o l'altro standard, dal momento che sono entrambi armonizzati in base alla Direttiva Macchine europea.

I risultati di entrambi gli standard sono livelli comparabili di integrità o prestazioni di sicurezza. Le metodologie di ogni standard presentano differenze a seconda degli utenti a cui sono destinate.

La metodologia IEC/EN 62061 mira a permettere l'uso di complesse funzionalità di sicurezza da implementare attraverso precedenti architetture di sistema non convenzionali. La metodologia EN ISO 13849-1 ha come scopo la definizione di un percorso più diretto e meno complicato per garantire funzionalità di sicurezza più convenzionali implementate da architetture di sistema convenzionali.

Ancora una volta, la differenza fondamentale tra questi due standard è l'applicabilità alle varie tecnologie. IEC/EN 62061 è limitato ai sistemi elettrici. Lo standard EN ISO 13849-1 può essere invece applicato ai sistemi pneumatici, idraulici, meccanici ed elettrici.

Relazione tecnica congiunta su IEC/EN 62061 e EN ISO 13849-1

Le commissioni IEC e ISO hanno redatto una relazione tecnica congiunta a supporto degli gli utenti dei due standard.

Questa relazione illustra il rapporto tra i due standard e i principi di equivalenza tra i PL (Livelli prestazionali) di EN ISO 13849-1 e i SIL (Livelli di integrità della sicurezza) di IEC/EN 62061, sia a livello di sistemi che di sottosistemi.

Per dimostrare che i due standard danno risultati equivalenti, nella relazione viene illustrato un sistema di sicurezza di esempio, calcolato in base alle metodologie dei due standard. La relazione inoltre fornisce chiarimenti in merito a varie questioni che sono state interpretate in modi diversi. Forse una delle problematiche più significative è l'aspetto dell'esclusione dei guasti.

In generale, quando si richiede il livello PLe per l'implementazione di una funzione di sicurezza da parte di un sistema di controllo legato alla sicurezza, di norma le esclusioni dei guasti non sono considerate sufficienti per raggiungere tale livello prestazionale. Ciò dipende dalla tecnologia impiegata e dall'ambiente operativo previsto. Pertanto il progettista deve prestare molta attenzione all'uso delle esclusioni dei guasti all'aumentare dei livelli PL richiesti.

In generale, l'uso delle esclusioni dei guasti non è applicabile agli aspetti meccanici degli interruttori di posizione elettromeccanici e degli interruttori ad azionamento manuale (ad es. un dispositivo di arresto di emergenza) per conseguire il livello PLe nella progettazione di un sistema di controllo legato alla sicurezza. Le esclusioni dei guasti applicabili a specifiche condizioni di guasto meccaniche (es. usura/corrosione, rottura) sono descritte nella Tabella A.4 di ISO 13849-2.

Ad esempio, nel caso di un sistema di interblocco di uno sportello che deve raggiungere il livello PLe si dovrà prevedere una tolleranza ai guasti minima pari a 1 (ad es. con due interruttori di posizione meccanici di tipo tradizionale) per ottenere tale livello prestazionale, dal momento che normalmente non è possibile giustificare l'esclusione di guasti come la rottura degli attuatori degli interruttori. Tuttavia, in un pannello di controllo progettato in conformità con standard pertinenti, potrebbe anche essere accettabile escludere i guasti come i cortocircuiti dei cablaggi.

SIL e IEC/EN 62061

IEC/EN 62061 descrive sia l'entità del rischio da ridurre che la capacità di un sistema di controllo di ridurre quel rischio in termini di SIL (Safety Integrity Level – Livello di integrità della sicurezza). Sono tre i SIL usati nel settore delle macchine, SIL1 è il più basso e SIL3 il più alto.

Dal momento che il termine SIL è utilizzato nella stessa accezione anche in altri settori industriali, come quello petrolchimico, della generazione dell'energia e ferroviario, lo standard IEC/EN 62061 si rivela molto utile quando le macchine vengono utilizzate in tali settori. Maggiori rischi possono verificarsi in altri settori come l'industria di processo e, per questo motivo, IEC 61508 e lo standard specifico per il settore dell'industria di processo IEC 61511 includono SIL4.

Un SIL si applica a una funzione di sicurezza. I sottosistemi che costituiscono il sistema che implementa la funzione di sicurezza devono avere una adeguata capacità SIL. Questo, talvolta, è riferito come SIL Claim Limit (SIL CL). Prima che possa essere correttamente applicato, è necessario un completo e dettagliato studio di IEC/EN 62061.

PL e EN ISO 13849-1:2008

EN ISO 13849-1:2008 non userà il termine SIL; userà il termine PL (Performance Level). Per molti aspetti, PL può essere collegato a SIL. I livelli prestazionali sono cinque, PLa è il più basso e PLe il più alto.

Confronto tra PL e SIL

Questa tabella mostra la relazione approssimativa tra PL e SIL applicata a strutture di circuito tipiche.

PL (livello prestazionale)	PFH_D (Probabilità di guasti pericolosi all'ora)	SIL (Livello di integrità della sicurezza)
a	da $\geq 10^{-5}$ a $<10^{-4}$	Nessuno
b	da $\geq 3 \times 10^{-6}$ a $<10^{-5}$	1
c	da $\geq 10^{-6}$ a $<3 \times 10^{-6}$	1
d	da $\geq 10^{-7}$ a $<10^{-6}$	2
e	da $\geq 10^{-8}$ a $<10^{-7}$	3

Corrispondenza approssimata tra PL e SIL

***IMPORTANTE:** la tabella sopra riportata è soltanto indicativa e NON deve essere usata a scopi di conversione. È necessario indicare i requisiti completi degli standard.*

Progettazione del sistema secondo EN ISO 13849 e SISTEMA

Prima che possa essere correttamente applicato, è necessario un completo e dettagliato studio di EN ISO 13849-1:2008. Quanto segue è una breve presentazione:

Questo standard fornisce i requisiti per la progettazione e l'integrazione dei componenti di sicurezza dei sistemi di controllo, compresi alcuni elementi software. Lo standard si applica a un sistema di sicurezza ma può anche applicarsi ai componenti del sistema.

Tool software per il calcolo dei livelli prestazionali SISTEMA

SISTEMA è un tool software per l'implementazione di EN ISO 13849-1, che semplifica notevolmente l'applicazione dello standard.

SISTEMA sta per "Safety Integrity Software Tool for the Evaluation of Machine Applications". È stato sviluppato in Germania dalla BGIA ed è utilizzabile gratuitamente. Come si vedrà più avanti in questa sezione, richiede l'inserimento di vari tipi di dati relativi alla sicurezza funzionale.

I dati possono essere inseriti manualmente o automaticamente utilizzando una libreria SISTEMA del produttore.

La libreria SISTEMA di Rockwell Automation è a disposizione degli utenti, e può essere scaricata utilizzando un link al sito di download di SISTEMA accessibile da: *www.discoverrockwellautomation.com/safety*

Cenni generali su EN ISO 13849-1

Questo standard ha un campo di applicazione molto ampio, dato che vale per tutte le tecnologie (elettrica, idraulica, pneumatica, meccanica, ecc.). Sebbene ISO 13849-1 sia applicabile ai sistemi complessi, per i sistemi complessi con software integrato rimanda anche il lettore a IEC 62061 e IEC 61508.

Di seguito verranno esaminate le differenze principali tra il vecchio standard EN 954-1 e il nuovo EN ISO 13849-1. Nel vecchio standard si parlava di categorie [B, 1, 2, 3 e 4]. Nel nuovo standard invece si parla di Livelli prestazionali [PL a, b, c, d ed e]. Il concetto di categoria è stato mantenuto, tuttavia affinché sia possibile affermare che un sistema è conforme al PL richiesto, occorre soddisfare dei requisiti aggiuntivi.

Tali requisiti possono essere essenzialmente riassunti come segue:

- Architettura del sistema. Essenzialmente riprende i concetti che in passato ci eravamo abituati a chiamare con il termine “categorie”
- Sono necessari dei dati sull’affidabilità delle parti costituenti del sistema
- È necessario specificare la copertura diagnostica [Diagnostic Coverage – DC] del sistema, che rappresenta effettivamente la quantità di errori monitorati nel sistema
- Protezione contro guasti per causa comune
- Protezione contro guasti sistematici
- Ove pertinente, requisiti specifici per il software

Questi fattori verranno analizzati successivamente in maniera più approfondita, ma prima di tutto è utile esaminare la finalità e il principio di base dell’intero standard. È chiaro che in questa fase ci sono cose nuove da apprendere, ma i dettagli avranno più senso una volta capito cosa si sta cercando di ottenere e perché.

La prima domanda è perché abbiamo bisogno di un nuovo standard. È ovvio che la tecnologia utilizzata nei sistemi di sicurezza delle macchine è progredita e cambiata notevolmente nel corso degli ultimi dieci anni. Fino a poco tempo fa i sistemi di sicurezza dipendevano da apparecchiature “semplici” con modalità di guasto molto prevedibili. Di recente abbiamo assistito a un crescente utilizzo di dispositivi elettronici programmabili più complessi nei sistemi di sicurezza. Questo ha portato a dei vantaggi in termini di costi, flessibilità e compatibilità, ma anche fatto sì che gli standard preesistenti non fossero più adeguati. Per sapere se un sistema di sicurezza è sufficientemente valido, dobbiamo saperne di più. Questo è il motivo per cui il nuovo standard richiede più informazioni. Dato che i sistemi di sicurezza hanno iniziato a utilizzare un approccio a “scatola nera”, si è cominciato a contare molto di più sulla loro conformità agli standard. Di conseguenza tali standard devono essere in grado di interrogare correttamente la tecnologia, e per fare ciò devono attestare i fattori base di affidabilità, rilevamento guasti, integrità dell’architettura e del sistema. Questo è il compito dello standard EN ISO 13849-1.

Per individuare la logica della normativa è importante osservare che essa si rivolge fondamentalmente a due tipi di utenti: il progettista di sottosistemi legati alla sicurezza e il progettista di sistemi legati alla sicurezza. In generale, il progettista di sottosistemi [tipicamente il produttore di un componente di sicurezza] è sottoposto a un livello di complessità più elevato. Deve fornire i dati richiesti in modo che il progettista di sistemi possa garantire un’integrità adeguata al sottosistema, e ciò

richiede di solito test, analisi e calcoli. I risultati sono espressi in forma di dati richiesti dallo standard.

Il progettista di sistemi [tipicamente un progettista di macchine o un integratore] userà i dati del sottosistema per eseguire alcuni calcoli relativamente semplici al fine di determinare il livello prestazionale [PL] generale del sistema.

Per indicare il livello prestazionale richiesto dalla funzione di sicurezza si usa la sigla PLr. Per determinare il PLr richiesto la norma prevede un grafico di analisi del rischio in cui sono inseriti i fattori di applicazione di gravità del danno, frequenza di esposizione e possibilità di evitabilità.

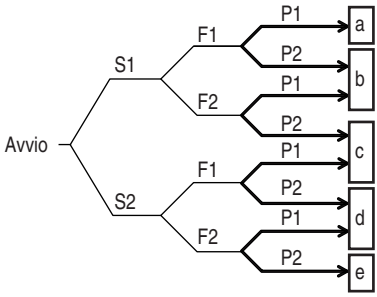


Grafico dei rischi ricavato dall'Allegato A dello standard EN ISO 13849-1

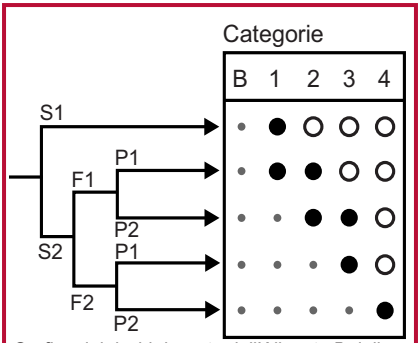


Grafico dei rischi ricavato dall'Allegato B dello standard EN 945-1

Il risultato è il PLr. Chi usava la vecchia norma EN 954-1 ha familiarità con questo tipo di approccio ma di fatto ora la linea S1 si suddivide, al contrario del vecchio grafico del rischio. Ne consegue un possibile riesame dell'integrità delle misure di sicurezza richieste a livelli di rischio più bassi.

Tuttavia, vi è ancora una parte molto importante da esaminare. Lo standard ci serve a quantificare la qualità del sistema e anche come determinarla, ma non sappiamo cosa si deve fare. Dobbiamo definire la funzione di sicurezza. Indubbiamente, la funzione di sicurezza deve essere appropriata all'applicazione, quindi come stabilirlo? In che modo ci aiuta lo standard?

La funzionalità richiesta può essere determinata solo considerando le caratteristiche prevalenti a livello dell'applicazione effettiva. Questo riguarda il concetto di sicurezza in fase di progettazione. Questo aspetto non può essere interamente trattato dallo standard poiché la norma non conosce tutte le caratteristiche di una specifica applicazione, e ciò spesso vale anche per il costruttore che produce la macchina ma non conosce necessariamente le esatte condizioni per le quali verrà utilizzata.

La norma fornisce un aiuto elencando molte delle funzioni di sicurezza più comunemente usate (ad es. funzione di arresto correlata alla sicurezza attivata da una protezione, funzione di muting, funzione di avviamento/riavviamento) e indicando alcuni requisiti normalmente associati a esse. Altri standard quali EN ISO 12100: Principi generali di progettazione e EN ISO 14121: Valutazione del rischio, sono altamente raccomandati in questa fase. Esiste inoltre una vasta gamma di standard specifici per le macchine in grado di fornire soluzioni per particolari gruppi di macchine. Nell'ambito degli standard EN europei sono detti standard di tipo C, la maggior parte dei quali ha un equivalente ISO.

Si può constatare che il concetto di sicurezza in fase di progettazione dipende dal tipo di macchina e dalle caratteristiche dell'applicazione e dell'ambiente in cui essa viene impiegata. Il costruttore di macchine deve anticipare questi fattori per poter progettare il concetto di sicurezza. Le condizioni d'impiego concepite [ovvero previste] dovrebbero essere indicate nel manuale dell'utente. L'utente della macchina deve verificare che esse corrispondano alle reali condizioni di utilizzo.

Siamo arrivati così a una descrizione della funzionalità di sicurezza. L'allegato A dello standard ci indica il livello prestazionale richiesto [PLr] per le parti del sistema di controllo [SRP/CS] correlate alla sicurezza che saranno utilizzate per attuare tale funzionalità. Non resta che progettare il sistema assicurandoci che sia conforme al PLr.

Uno dei fattori più significativi da valutare nel decidere quale standard adottare [EN ISO 13849-1 o EN/IEC 62061] è la complessità della funzione di sicurezza. Nella maggior parte dei casi, per le macchine, la funzione di sicurezza è relativamente semplice e lo standard EN ISO 13849-1 rappresenta la strada più indicata. Per valutare il PL si utilizzano i seguenti fattori: dati di affidabilità, copertura diagnostica [DC], architettura del sistema [categoria], guasti per causa comune e, ove opportuno, i requisiti per il software.

Questa è una descrizione semplificata e sommaria. È importante però capire che devono essere applicate tutte le disposizioni indicate nello standard. Tuttavia, abbiamo un aiuto a portata di mano. Esiste un tool software, chiamato SISTEMA, che supporta l'utente per quanto riguarda gli aspetti della documentazione e del calcolo, consentendo anche di produrre un dossier tecnico.

Al momento della stampa della presente pubblicazione, SISTEMA è disponibile in tedesco e in inglese, ma saranno presto rilasciate versioni in altre lingue. BGIA, l'azienda sviluppatrice di SISTEMA, è un istituto tedesco di ricerca e prove molto conosciuto. In particolare, si occupa di trovare soluzioni a problemi tecnici e scientifici riguardanti la sicurezza nel settore delle assicurazioni contro gli infortuni e la prevenzione in Germania. Collabora con agenzie che operano nel campo della sicurezza e salute occupazionale in oltre venti paesi. I tecnici BGIA e i loro colleghi della

BG hanno dato un grande contributo alla stesura di entrambe le norme EN ISO 13849-1 e IEC/EN 62061.

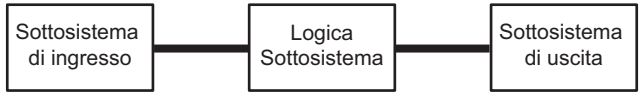
Rockwell Automation mette a disposizione una “libreria” dei propri dispositivi di sicurezza da utilizzare con SISTEMA, disponibile sul seguente sito:

www.discoverrockwellautomation.com/safety

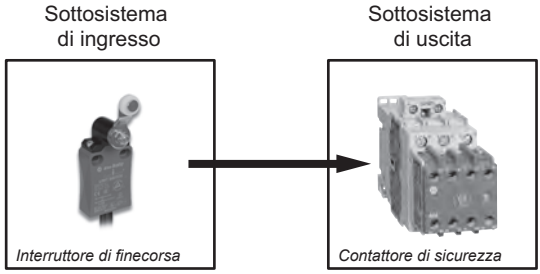
A prescindere da come viene effettuato il calcolo del PL, è importante partire dalla giusta base. Dobbiamo vedere il nostro sistema con gli stessi occhi dello standard, quindi cominciamo da qui.

Struttura del sistema

Ogni sistema può essere scomposto in componenti base o “sottosistemi”. Ciascun sottosistema possiede una propria funzione discreta. La maggior parte dei sistemi può essere suddivisa in tre funzioni base: ingresso, logica e attuazione [alcuni sistemi semplici non hanno logica]. I gruppi di componenti che attuano queste funzioni sono detti sottosistemi.

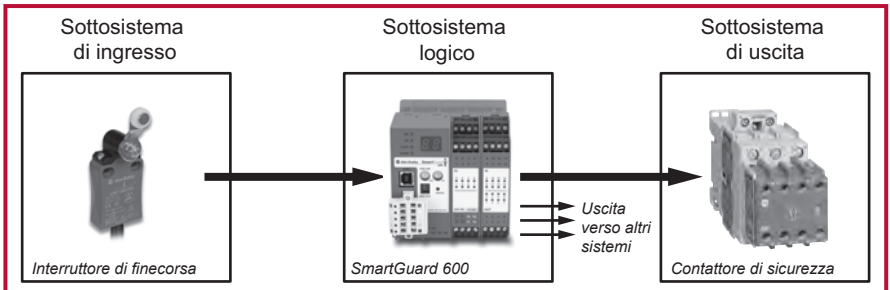


Ogni sistema può essere scomposto in componenti base o “sottosistemi”. Ciascun sottosistema possiede una propria funzione discreta. La maggior parte dei sistemi può essere suddivisa in tre funzioni base: ingresso, logica e attuazione [alcuni sistemi semplici non hanno logica]. I gruppi di componenti che attuano queste funzioni sono detti sottosistemi.



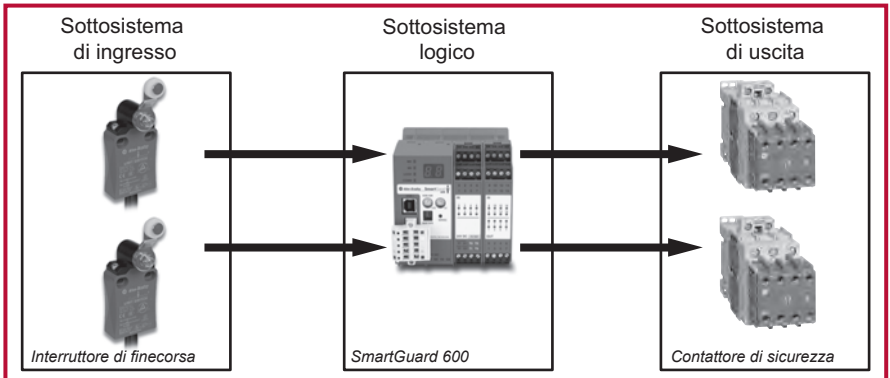
Interruttore di interblocco e contattore di sicurezza

Sopra è riportato un esempio di sistema elettrico semplice a canale singolo, che comprende solo sottosistemi di ingresso e uscita.



Interruttore di interblocco, controllore di sicurezza e contattore di sicurezza

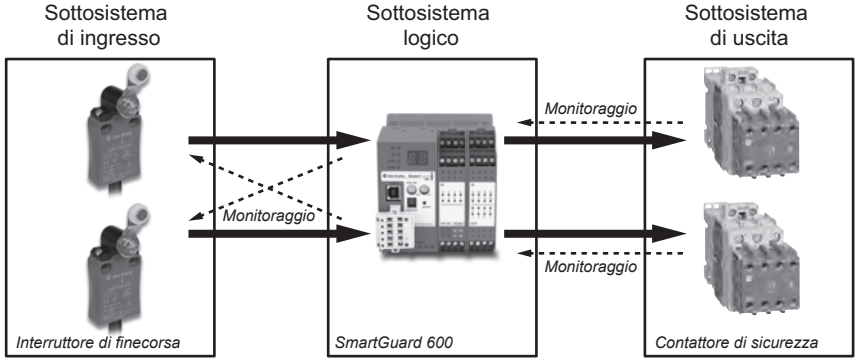
Questo sistema è leggermente più complesso perché è richiesta anche della logica. Il controllore di sicurezza di per sé è tollerante ai guasti (ad es. a canale doppio) internamente, ma l'intero sistema è ancora limitato allo stato di canale singolo a causa dell'interruttore di finecorsa e del contattore singoli.



Sistema di sicurezza a doppio canale

Se si considera l'architettura di base dello schema precedente, ci sono anche altri aspetti da valutare. In primo luogo il numero di "canali" del sistema. Un sistema a canale singolo si guasta se uno dei suoi sottosistemi fallisce. Un sistema a due canali [anche detto ridondante] dovrà avere due guasti, uno per canale, prima che il sistema fallisca. Proprio perché possiede due canali, esso può tollerare un guasto singolo e continuare a lavorare. Nel diagramma sopra è rappresentato un sistema a due canali.

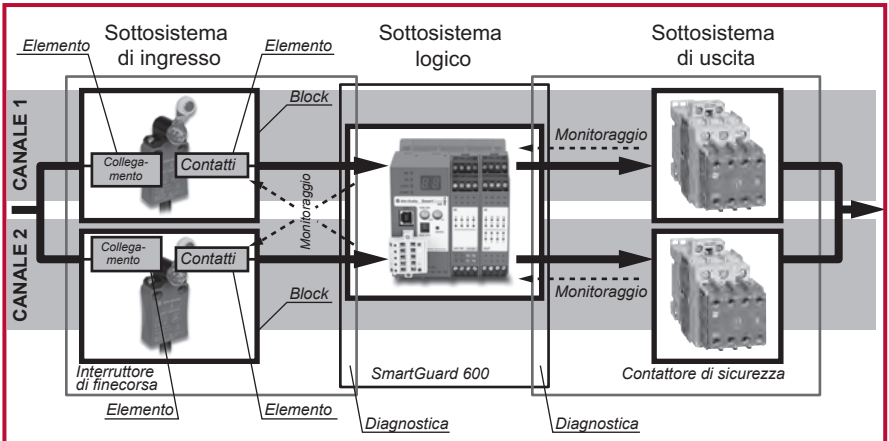
Chiaramente un sistema a doppio canale ha meno probabilità di fallire in una condizione pericolosa rispetto a un sistema a canale singolo. Ma possiamo renderlo più affidabile [in termini della sua funzione di sicurezza] se nel rilevamento del guasto includiamo delle misure diagnostiche. Naturalmente, dopo aver identificato il guasto, dobbiamo essere pronti a reagire e mettere il sistema in uno stato sicuro. Il seguente schema mostra l'inserimento di misure diagnostiche ottenute con tecniche di monitoraggio.



Diagnostica con un sistema di sicurezza a doppio canale

Di solito [ma non sempre] il sistema comprende due canali in tutti i suoi sottosistemi. Pertanto, in questo caso, ogni sottosistema ha due "sottocanali". Lo standard li descrive come "blocchi". Un sottosistema a due canali avrà minimo due blocchi e un sottosistema a canale singolo avrà minimo un blocco. È possibile che alcuni sistemi comprendano una combinazione di blocchi a canale doppio e singolo.

Se vogliamo analizzare il sistema in maniera più approfondita, è necessario considerare i componenti dei blocchi. Il tool SISTEMA usa il termine di "elementi" per questi componenti.



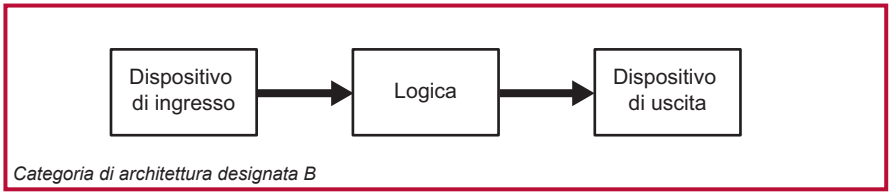
Sistema suddiviso con diagnostica con un sistema di sicurezza a doppio canale

Il sottosistema degli interruttori di finecorsa viene mostrato scomposto fino a livello di elemento. Il sottosistema dei contattori di uscita è suddiviso sino a livello di blocco, mentre il sottosistema logico non è suddiviso affatto. La funzione di monitoraggio sia per gli interruttori di finecorsa che per i contattori viene svolta dal controllore logico. Pertanto le caselle che rappresentano i sottosistemi degli interruttori di finecorsa e dei contattori si sovrappongono leggermente a quella del sottosistema logico.

Questo principio di suddivisione del sistema si ritrova nella metodologia indicata nello standard EN ISO 13849-1 e nel principio della struttura base del sistema adottato dal tool SISTEMA. Tuttavia, è importante notare che vi sono alcune sottili differenze. Lo standard non è restrittivo nella sua metodologia ma, per il metodo semplificato di stima del PL, il primo passo di solito consiste nello scomporre la struttura del sistema in canali e in blocchi all'interno di ciascun canale. Con il tool SISTEMA, il sistema in genere viene dapprima suddiviso in sottosistemi. Lo standard non definisce esplicitamente il concetto di sottosistema ma l'uso indicato da SISTEMA prevede un approccio più comprensibile e intuitivo. Naturalmente non vi è alcun effetto sul calcolo finale. SISTEMA e lo standard utilizzano entrambi gli stessi principi e le stesse formule. È altrettanto interessante osservare che l'approccio del sottosistema si ritrova anche nello standard EN/IEC 62061.

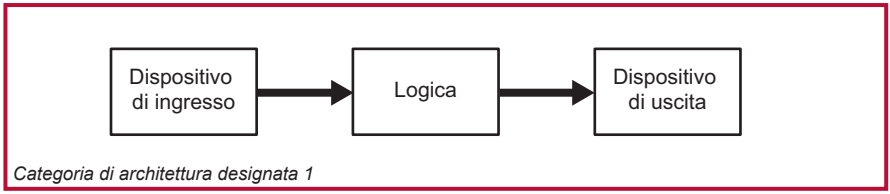
Il sistema che abbiamo illustrato come esempio è solo uno dei cinque tipi base di architetture del sistema previste dallo standard. Chi conosce il sistema delle categorie saprà che questo esempio è rappresentativo sia della categoria 3 che 4.

Lo standard considera le categorie originali della EN 954-1 come i cinque tipi base di architetture di sistema predefinite, dette categorie di architetture designate (Designated Architecture Categories). I requisiti delle categorie sono quasi [ma non del tutto] identici a quelli indicati nell'EN 954-1. Le categorie di architetture designate sono rappresentate nelle seguenti figure. È importante notare che tali categorie possono essere applicate sia a un sistema completo che a un sottosistema. Gli schemi non devono essere visti semplicemente come una struttura fisica, ma piuttosto come una rappresentazione grafica di requisiti concettuali.



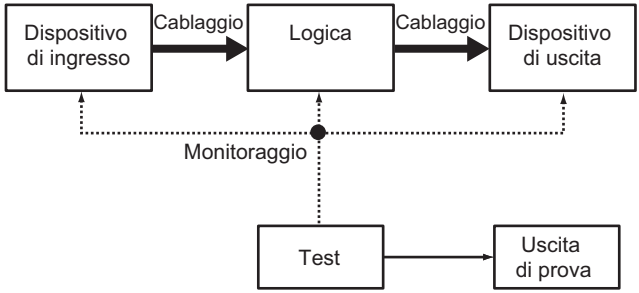
Categoria di architettura designata B

La categoria di architettura designata B deve adottare i principi di sicurezza base [vedere allegato dello standard EN ISO 13849-2]. Il sistema o il sottosistema può fallire in caso di un singolo guasto. Per i requisiti completi consultare lo standard EN ISO 13849-1.



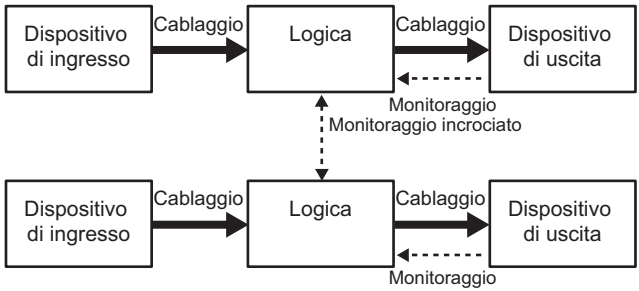
Categoria di architettura designata 1

La categoria di architettura designata 1 ha la stessa struttura della categoria B e può ancora fallire in caso di singolo guasto. Ma poiché si avvale di principi di sicurezza collaudati [vedere allegato dell'EN ISO 13849-2], la probabilità che questo accada è inferiore rispetto alla categoria B. Per i requisiti completi consultare lo standard EN ISO 13849-1.



Categoria di architettura designata 2

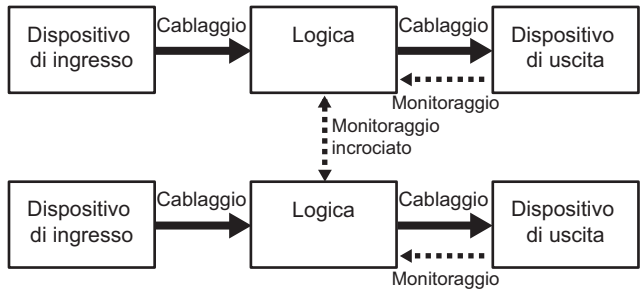
La categoria di architettura designata 2 deve adottare i principi di sicurezza base [vedere allegato dello standard EN ISO 13849-2]. È necessario inoltre un monitoraggio diagnostico tramite un test funzionale del sistema o sottosistema. Ciò deve aver luogo all'avvio e poi periodicamente con una frequenza che equivale ad almeno un centinaio di test per ogni richiesta di intervento della funzione di sicurezza. Il sistema o il sottosistema può ancora fallire se si verifica un singolo guasto tra un test funzionale e l'altro, ma la probabilità è di solito inferiore rispetto alla categoria 1. Per i requisiti completi consultare lo standard EN ISO 13849-1.



Categoria di architettura designata 3

La categoria di architettura designata 3 deve usare i principi di sicurezza base [vedere allegato dello standard EN ISO 13849-2]. Si richiede inoltre che il sistema/sottosistema non possa fallire in caso di singolo guasto. Ciò significa che il sistema deve avere una tolleranza al singolo errore in relazione alla sua funzione di sicurezza. Il modo più comune per soddisfare questo requisito è di usare un'architettura a canale doppio come mostrato sopra. Inoltre, è necessario, per quanto possibile, che il guasto singolo sia rilevato. Questo requisito corrisponde al requisito originale previsto per la categoria 3 dello standard EN 954-1. In tale contesto il significato

dell'espressione "per quanto possibile" era alquanto problematico. Significava che la categoria 3 poteva coprire qualsiasi sistema da un sistema con ridondanza ma senza rilevamento di guasto [spesso definita opportunamente come "ridondanza stupida"] a un sistema ridondante in cui sono rilevati tutti i guasti singoli. Questo problema viene affrontato nello standard EN ISO 13849-1 con la necessità di stimare la qualità della copertura diagnostica (Diagnostic Coverage) [DC]. Maggiore è l'affidabilità [MTTFd] del sistema, minore è la DC necessaria. Tuttavia è altrettanto chiaro che per la categoria di architettura 3, la DC deve essere almeno pari al 60 %.



Categoria di architettura designata 4

La categoria di architettura designata 4 deve usare i principi di sicurezza base [vedere allegato dello standard EN ISO 13849-2]. Lo schema dei requisiti è simile alla categoria 3 ma richiede un monitoraggio più ampio, cioè una maggiore copertura diagnostica. Ciò è indicato dalle linee tratteggiate più marcate che rappresentano le funzioni di monitoraggio. In sostanza, la differenza tra le categorie 3 e 4 è che per la categoria 3 deve essere rilevata la maggior parte dei guasti, mentre per la categoria 4 devono essere rilevati tutti i guasti singoli. La DC deve essere almeno del 99%. Anche le combinazioni di guasti non devono causare un guasto pericoloso.

Dati di affidabilità

Lo standard EN ISO 13849-1 utilizza dati quantitativi di affidabilità dei componenti nel calcolo del PL ottenuto dalle parti di un sistema di controllo legate alla sicurezza. Questa è una importante divergenza rispetto all'EN 954-1. La prima domanda che si pone è: "qual è la fonte di questi dati?" È anche possibile ricorrere a dati di affidabilità attendibili, ma lo standard afferma chiaramente che la fonte preferita è il produttore. A tal fine, Rockwell Automation sta mettendo a disposizione le informazioni più rilevanti sotto forma di libreria per il software SISTEMA. In seguito, i dati verranno anche pubblicati in altre forme. Prima di proseguire però dovremmo esaminare quali tipi di dati sono richiesti e capire come si ottengono.

L'ultimo tipo di dati richiesti nella determinazione del PL secondo lo standard [e

SISTEMA] è il PFH [probabilità di guasti pericolosi/ora]. Sono gli stessi dati indicati dall'abbreviazione PFH_D (probabilità di guasti pericolosi per ora) usata nello standard IEC/EN 62061.

PL (livello prestazionale)	PFH_D (Probabilità di guasti pericolosi all'ora)	SIL (Livello di integrità della sicurezza)
a	da $\geq 10^{-5}$ a $<10^{-4}$	Nessuno
b	da $\geq 3 \times 10^{-6}$ a $<10^{-5}$	1
c	da $\geq 10^{-6}$ a $<3 \times 10^{-6}$	1
d	da $\geq 10^{-7}$ a $<10^{-6}$	2
e	da $\geq 10^{-8}$ a $<10^{-7}$	3

La tabella qui sopra mostra il rapporto tra PFH, PL e SIL. Per alcuni sottosistemi, il PFH può essere indicato direttamente dal produttore. Questo facilita il calcolo. Il produttore di solito deve eseguire calcoli relativamente complessi e/o test sul sottosistema per fornire questo dato. Nel caso non fosse disponibile, lo standard EN ISO 13849-1 ci fornisce un approccio alternativo semplificato, basato sull'MTTFd medio [tempo medio prima di un guasto pericoloso] di un singolo canale. Il PL [e quindi il PFH] di un sistema o sottosistema può essere quindi calcolato utilizzando la metodologia e le formule dello standard, o in maniera ancora più pratica usando SISTEMA.

Nota: è importante comprendere che, nel caso di un sistema a doppio canale (con o senza diagnostica), non è corretto utilizzare $1/PFH_D$ per determinare il MTTFd richiesto dallo standard EN ISO 13849-1, in quanto lo standard richiede il calcolo del MTTFd di un canale singolo. Questo valore è molto diverso dal MTTFd della combinazione dei due canali di un sottosistema a due canali. Se si conosce il PFH_D di un sottosistema a due canali, è possibile inserirlo direttamente nel software SISTEMA.

MTTFd di un canale singolo

Rappresenta il tempo medio prima del verificarsi di un guasto che può portare a un errore della funzione di sicurezza, e si esprime in anni. Si tratta di un valore medio dei MTTFd dei "blocchi" di ciascun canale e può essere applicato a un sistema o a un sottosistema. Lo standard indica la seguente formula che viene usata per calcolare la media di tutti i MTTFd di ciascun elemento utilizzato in un singolo canale o sottosistema.

In questa fase, l'utilità di SISTEMA è evidente. Si risparmia tempo a consultare tabelle e a eseguire calcoli con le formule poiché questo lavoro viene svolto dal software. I risultati finali possono essere stampati sotto forma di una relazione di più pagine.

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{MTTF_{dj}}$$ (Formula D1 dello standard EN ISO 13849-1)

Nella maggior parte dei sistemi a canale doppio i due canali sono identici, perciò il risultato della formula rappresenta indifferentemente l'uno o l'altro canale.

Se i canali del sistema/sottosistema sono differenti, lo standard prevede una formula apposita.

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right]$$

Questa, in effetti, fa una media dei due valori medi. Per semplificare le cose è anche consentito usare il valore più sfavorevole tra quelli dei due canali.

Lo standard raggruppa l'MTTFd in tre campi:

Denotazione MTTFd di ogni canale	**Campo MTTFd di ogni canale**
Basso	3 anni <= MTTFd <10 anni
Medio	10 anni <= MTTFd <30 anni
Alto	30 anni <= MTTFd <100 anni

Livelli di $MTTF_d$

Si noti che lo standard EN ISO 13849-1 limita l'MTTFd utilizzabile di un canale singolo di un sottosistema a un massimo di 100 anni, anche se i valori effettivi derivati possono essere molto superiori

Come vedremo più avanti, il campo ottenuto dalla media degli MTTFd viene combinato con la categoria di architettura designata e la copertura diagnostica [DC] per dare una stima preliminare del PL. Qui si usa il termine preliminare poiché si devono ancora soddisfare altri requisiti, ove rilevanti, come l'integrità sistematica e le misure contro un guasto per causa comune.

Metodi di determinazione dei dati

Ora dobbiamo approfondire l'argomento, illustrando i modi in cui il produttore determina i dati sotto forma di PFH_D o MTTFd. Quando si parla di dati di un produttore, è essenziale capire di cosa si tratta. I componenti possono essere raggruppati in tre tipologie base:

- meccanici (elettromeccanici, meccanici, pneumatici, idraulici ecc.)
- elettronici (ad es. a stato solido)
- software.

Vi è una differenza fondamentale tra i meccanismi di guasto comune di questi tre tipi di tecnologie. Sinteticamente si può riassumere come segue:

Tecnologia meccanica

Il guasto è proporzionale all'affidabilità intrinseca e al tasso di utilizzo. Più è alto il tasso di utilizzo, maggiore è la probabilità che uno dei componenti possa guastarsi e fallire. Questa però non è l'unica causa di guasto ma, a meno che non si limiti il tempo/i cicli di funzionamento, sarà la causa predominante. È evidente che un contattore che ha un ciclo di commutazione di una volta ogni dieci secondi funzionerà in modo affidabile per un tempo molto più breve rispetto a un contattore identico che entra in funzione una volta al giorno. I dispositivi a tecnologia meccanica comprendono componenti progettati individualmente per il loro uso specifico. I componenti sono modellati, stampati, fusi, lavorati ecc. e sono uniti tra loro con collegamenti, molle, magneti, avvolgimenti elettrici ecc. per formare un meccanismo. Dato che in genere non ci sono informazioni storiche sull'utilizzo dei componenti in altre applicazioni, non possiamo trovare informazioni preesistenti sulla loro affidabilità. La stima del PFH_D o MTTFd per il meccanismo si basa di norma su prove. Gli standard EN/IEC 62061 ed EN ISO 13849-1 prevedono entrambi l'esecuzione di una prova chiamata test B10d.

Durante il test B10d un numero di componenti campione [in genere almeno dieci] viene sottoposto a prove in condizioni rappresentative. Il numero medio di cicli operativi eseguiti prima che il 10% dei campioni subisca guasti determinando condizioni pericolose è detto valore B10d. Nella prassi, spesso accade che tutti i campioni si guastino in uno stato sicuro, ma in tal caso lo standard chiarisce che il valore B10d [pericoloso] può essere considerato pari a due volte il valore B10 [sicuro].

Tecnologia elettronica

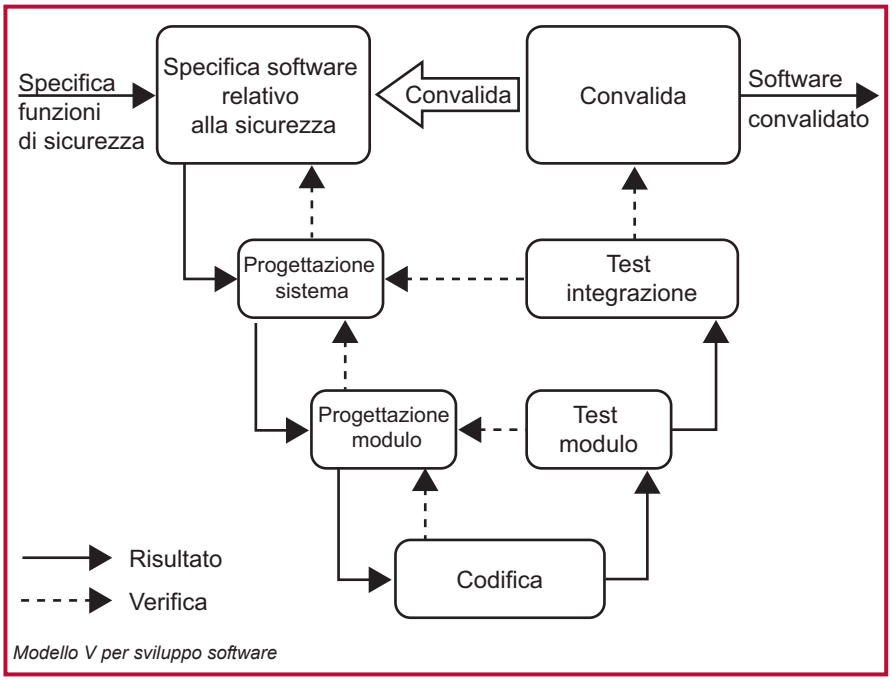
In questo caso non si verifica alcuna usura fisica relativa alle parti mobili. Dato un ambiente operativo commisurato alle specifiche caratteristiche elettriche, di temperatura [ecc.], il guasto predominante di un circuito elettronico è proporzionale all'affidabilità intrinseca dei suoi componenti costitutivi [o alla mancanza di essa]. Un singolo componente può guastarsi per vari motivi: difetti di fabbricazione, picchi di potenza eccessivi, problemi di connessione meccanica ecc. In genere, i guasti ai componenti elettronici sono difficili da prevedere con un'analisi e sembrano essere di natura casuale. Pertanto, eseguendo dei test di laboratorio su un dispositivo elettronico non è necessariamente detto che sia possibile individuare dei modelli di guasto tipici a lungo termine.

Per determinare l'affidabilità dei dispositivi elettronici si è soliti ricorrere all'analisi e al calcolo. Esistono dati di affidabilità, in cui è possibile reperire dati utili relativi ai singoli componenti. Tramite l'analisi si possono individuare le modalità di guasto dei componenti che risultano pericolose. È pratica accettabile e usuale fare una media, valutando le modalità di guasto per il 50% sicure e il 50% pericolose. In questo modo in genere si ottengono dati relativamente conservativi.

Lo standard IEC 61508 fornisce formule per il calcolo della probabilità generale che si verifichi un danno pericoloso [PFH o PFD] del dispositivo, ossia del sottosistema. Le formule sono abbastanza complesse e prendono in considerazione [laddove applicabile] l'affidabilità dei componenti, il grado di propensione a guasti di causa comune [fattore beta], la copertura diagnostica [DC], l'intervallo dei test funzionali e l'intervallo dei test diagnostici. La buona notizia è che questo calcolo complesso viene normalmente eseguito dal produttore del dispositivo. Sia l'EN/IEC 62061 che l'EN ISO 13849-1 accettano un sottosistema calcolato in questo modo in base all'IEC 61508. Il PFH_D che ne risulta può essere utilizzato direttamente nell'Allegato K dell'EN ISO 13849-1 o nel tool di calcolo SISTEMA.

Software

I guasti al software sono di natura intrinsecamente sistematica. I guasti sono causati dal modo in cui il software è concepito, scritto o compilato. Pertanto, tutti i guasti sono causati dal sistema in cui viene eseguito, non dal suo utilizzo. Perciò per controllare gli errori occorre controllare il sistema. Sia l'IEC 61508 che l'EN ISO 13849-1 indicano requisiti e metodologie ideati a questo scopo. Non c'è bisogno di entrare in dettaglio se non per dire che utilizzano il classico modello V. Il software integrato è un problema che riguarda il progettista di dispositivi. In genere si tende a sviluppare software integrati in conformità con i metodi formali stabiliti nello standard IEC 61508 parte 3. Per quanto riguarda il codice applicativo, il software con cui l'utente interfaccia, la maggior parte dei dispositivi di sicurezza programmabili sono dotati di routine o blocchi funzione "certificati". Ciò semplifica il compito di convalida del codice applicativo, ma non bisogna dimenticare che il programma applicativo completo deve essere ancora convalidato. Il modo in cui i blocchi sono collegati e parametrizzati deve essere verificato e convalidato per l'applicazione prevista. Gli standard EN ISO 13849-1 e IEC/EN 62061 forniscono entrambi criteri per questo processo.



Modello V per sviluppo software

Copertura diagnostica

Abbiamo già affrontato questo argomento quando abbiamo parlato delle categorie di architetture designate 2, 3 e 4. Queste categorie richiedono una qualche forma di test autodiagnostici per verificare se la funzione di sicurezza è ancora operativa. Per descrivere l'efficacia di questo test si utilizza il termine "copertura diagnostica" [solitamente abbreviato in DC]. È importante notare che la DC non si basa solo sul numero di componenti che possono causare un guasto pericoloso, ma tiene conto dell'incidenza totale (tasso) dei guasti pericolosi. Il "tasso di guasto" è indicato con il simbolo λ. La DC è il rapporto dei tassi di incidenza dei due seguenti tipi di guasti pericolosi:

Guasti pericolosi rilevabili [λdd]: sono guasti che potrebbero causare o portare a una perdita della funzione di sicurezza, ma sono rilevabili. Dopo il rilevamento, una funzione di reazione del guasto fa sì che il dispositivo o il sistema passi allo stato sicuro.

Guasti pericolosi [λd]: sono tutti i guasti che potenzialmente possono causare o portare a una perdita della funzione di sicurezza. Il dato comprende sia i guasti rilevabili che quelli che non lo sono. Naturalmente i guasti che sono veramente pericolosi sono i guasti pericolosi non rilevabili [indicati con il simbolo λdu]

La DC è data dalla formula

DC = λdd/λd espressa in percentuale.

Questa accezione del termine DC è comune agli standard EN ISO 13849-1 ed EN/IEC 62061, ma il modo in cui viene ricavata è diverso. Quest'ultimo standard propone l'utilizzo di un calcolo basato sull'analisi della modalità di guasto mentre l'EN ISO 13849-1 fornisce un metodo semplificato sotto forma di tabelle di consultazione, in cui sono elencate varie tecniche diagnostiche tipiche con la percentuale DC che si intende ottenere. In alcuni casi si richiede ancora un giudizio razionale, per esempio in alcune tecniche il valore DC ottenuto è proporzionale alla frequenza con cui viene eseguita la prova. C'è chi sostiene che questo approccio è troppo vago. Tuttavia la stima di DC può dipendere da molte variabili diverse e, qualsiasi tecnica si utilizzi, il risultato potrà essere veramente considerato solo approssimativo.

È importante comprendere che le tabelle dello standard EN ISO 13849-1 sono basate su un'ampia attività di ricerca condotta dalla BGIA, con risultati ottenuti tramite tecniche diagnostiche note usate in applicazioni reali. Per semplificare le cose, lo standard suddivide la DC in quattro campi base:

<60% = nessuna

dal 60% a <90% = bassa

dal 90% a <99% = media

≥99% = alta

Questo approccio basato sull'uso dei campi anziché di singoli valori percentuali può essere considerato più realistico in termini di precisione ottenibile. Il tool SISTEMA si avvale delle stesse tabelle di consultazione dello standard. Poiché i dispositivi legati alla sicurezza richiedono un'elettronica sempre più complessa, la DC diventa un fattore molto importante. È probabile che in futuro gli standard cercheranno di fare chiarezza su questo problema. Nel frattempo il giudizio dei tecnici e il buon senso dovrebbero essere sufficienti a determinare una scelta corretta del campo di DC.

Guasto per causa comune

Nella maggior parte dei sistemi o sottosistemi a canale doppio [ovvero a prova di singolo guasto] il principio diagnostico si basa sul presupposto che non vi siano guasti pericolosi in entrambi i canali allo stesso tempo. Il concetto di "allo stesso tempo" è espresso in maniera più accurata come "entro l'intervallo del test diagnostico". Se l'intervallo di test diagnostico è ragionevolmente breve [ad es. meno di otto ore] è ragionevole ipotizzare che sia molto improbabile che due guasti separati e indipendenti si verifichino entro tale termine. Tuttavia, lo standard indica che dobbiamo considerare attentamente se le possibilità di guasto sono davvero separate e indipendenti. Ad esempio, se un guasto in un componente può prevedibilmente portare a guasti di altri componenti, ne consegue che i guasti nel loro insieme vengono considerati come un guasto unico.

È inoltre possibile che un evento che provoca il guasto di un componente possa anche causare il guasto di altri componenti. Questo caso è detto "guasto per causa comune", normalmente abbreviato in CCF. Il grado di propensione per un CCF è in genere indicato come fattore beta (ß). È molto importante che i progettisti di sistemi e sottosistemi siano consapevoli delle possibilità del CCF. Esistono diversi tipi di

CCF e, di conseguenza, diversi modi per evitarlo. Nello standard EN ISO 13849-1 è indicato un approccio razionale, che costituisce una via di mezzo tra la complessità e l'ipersemplificazione. Questo standard adotta un approccio che è essenzialmente qualitativo, come l'EN/IEC 62061, e fornisce un elenco di misure note per essere efficaci nell'evitare un CCF.

N.	Misura contro CCF	Punteggio
1	Separazione/Segregazione	15
2	Diversità	20
3	Progettazione/Applicazione/ Esperienza	20
4	Valutazione/Analisi	5
5	Competenza/Formazione	5
6	Ambiente	35

Punteggio per i guasti per causa comune

Nella progettazione di un sistema o sottosistema occorre applicare un numero sufficiente di tali misure. Si potrebbe sostenere, non senza ragione, che l'uso di questo elenco da solo non sia adeguato a prevenire tutte le possibilità di un CCF. Tuttavia, se si considera correttamente lo scopo dell'elenco, è chiaro che lo spirito dei suoi requisiti è quello di portare il progettista ad analizzare le possibilità di CCF e attuare misure preventive appropriate basate sul tipo di tecnologia e di caratteristiche dell'applicazione. Utilizzando l'elenco si presta maggiore attenzione ad alcune delle metodologie più importanti ed efficaci, come la diversità delle modalità di guasto e le competenze di progettazione. Anche il tool SISTEMA di BGIA richiede l'applicazione delle tabelle di consultazione relative ai CCF dello standard e le rende disponibile in una forma pratica.

Guasti sistematici

Abbiamo già parlato della quantificazione dell'affidabilità sotto forma di MTTFd e della probabilità di guasto pericoloso. Ma non è tutto qui. Abbiamo esaminato questi termini pensando in realtà a guasti che sembrano essere di natura casuale. Infatti lo standard IEC/EN 62061 si riferisce specificatamente all'abbreviazione PFH_D come la probabilità di un guasto hardware casuale. Ma vi sono alcuni tipi di guasti definiti collettivamente come "guasti sistematici" che possono essere attribuiti a errori commessi durante la progettazione o la fabbricazione. Il classico esempio di questo è un errore nel codice software. Lo standard indica nell'Allegato G delle misure atte a prevenire tali errori [e quindi i guasti]. Tra queste misure figurano ad esempio l'utilizzo di materiali e tecniche di produzione idonei, revisioni, analisi e simulazioni al computer. Vi sono poi eventi prevedibili e caratteristiche che possono verificarsi nell'ambiente operativo che potrebbero causare un guasto a meno che il loro effetto non venga controllato. L'allegato G comprende anche misure a questo riguardo. Ad esempio, è facilmente prevedibile che si possano verificare occasionali interruzioni dell'alimentazione. Perciò, in caso di diseccitazione dei componenti, il sistema deve rimanere in uno stato sicuro. Anche se possono sembrare solo dettate dal buon senso, cosa che peraltro è vera, queste misure sono essenziali. Gli altri requisiti dello standard hanno senso solo se viene prestata la dovuta considerazione al controllo e alla prevenzione dei guasti sistematici. Ciò a volte richiede gli stessi tipi di misure utilizzate per il controllo di guasti hardware casuali [per ottenere il PFH_D richiesto] come test di autodiagnosi e hardware ridondante.

Esclusione dei guasti

Uno dei principali strumenti di analisi per i sistemi di sicurezza è l'analisi dei guasti. Il progettista e l'utilizzatore devono capire come funziona il sistema di sicurezza in presenza di guasti. Sono molte le tecniche disponibili per realizzare questa analisi. Per esempio, analisi dell'albero dei guasti; analisi dei modi, degli effetti e della criticità dei guasti; analisi dell'albero degli eventi; analisi "load-strength (prova di carico)".

Durante l'analisi, possono rimanere scoperti alcuni guasti impossibili da rilevare con la diagnostica automatica, se non con alti costi economici. Inoltre, la probabilità che tali guasti si verifichino può essere molto ridotta usando appositi metodi di progettazione, costruzione e verifica. In queste condizioni, i guasti possono essere esclusi da ulteriore considerazione. L'esclusione dei guasti è la mancata considerazione di un guasto vista la scarsa probabilità che si verifichi quel guasto specifico del sistema di controllo legato alla sicurezza.

Lo standard ISO 13849-1:2006 ammette l'esclusione dei guasti in base all'improbabilità tecnica che si verifichino, all'esperienza tecnica comune e ai requisiti tecnici legati all'applicazione. Lo standard ISO 13849-2:2003 fornisce una serie di esempi e giustificazioni per escludere certi guasti per i sistemi elettrici, pneumatici, idraulici e meccanici. L'esclusione dei guasti deve essere dichiarata con giustificazioni dettagliate, fornite nella documentazione tecnica.

Non è sempre possibile valutare un sistema di controllo legato alla sicurezza senza presumere che certi guasti possano essere esclusi. Per informazioni dettagliate sull'esclusione dei guasti, vedere ISO 13849-2.

All'aumentare del livello di rischio, le giustificazioni per l'esclusione dei guasti diventano più rigorose. In generale, quando si richiede il livello PLe per l'implementazione di una funzione di sicurezza da parte di un sistema di controllo legato alla sicurezza, di norma le esclusioni dei guasti non sono considerate sufficienti per raggiungere tale livello prestazionale. Ciò dipende dalla tecnologia impiegata e dall'ambiente operativo previsto. Pertanto è il progettista che deve prestare molta attenzione all'uso delle esclusioni dei guasti man mano che i requisiti a livello di PL aumentano.

Ad esempio, nel caso di un sistema di interblocco porte che deve raggiungere il livello PLe si dovrà prevedere una tolleranza ai guasti minima pari a 1 (ad esempio con due interruttori di posizione meccanici di tipo tradizionale) per ottenere tale livello prestazionale, dal momento che normalmente non è possibile giustificare l'esclusione di guasti come la rottura degli attuatori degli interruttori. Tuttavia, in un pannello di controllo progettato in conformità con standard pertinenti, potrebbe anche essere accettabile escludere i guasti come i cortocircuiti dei cablaggi.

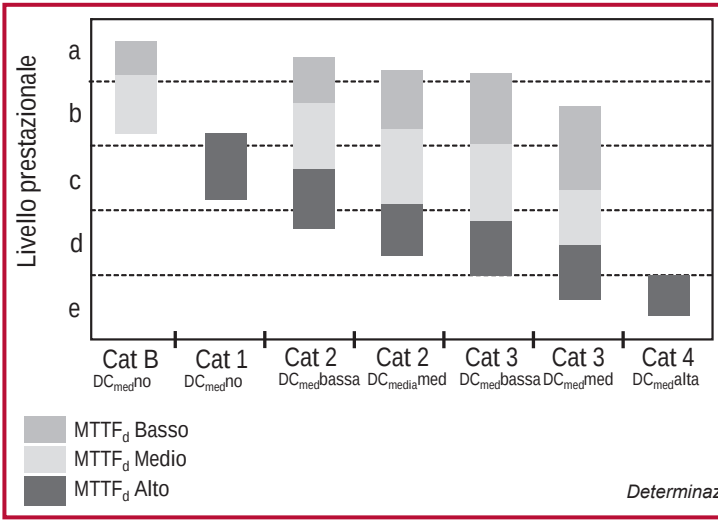
Livelli prestazionali (PL)

Il livello prestazionale è un livello discreto che specifica la capacità dei componenti legati alla sicurezza del sistema di controllo di svolgere una funzione di sicurezza.

Per valutare il PL ottenuto mediante l'implementazione di una delle cinque architetture designate, sono necessari i seguenti dati del sistema (o sottosistema):

- $MTTF_d$ (tempo medio prima di un guasto pericoloso di ogni canale)
- DC (copertura diagnostica)
- Architettura (la categoria)

Il seguente diagramma mostra un metodo grafico per determinare il PL dalla combinazione di questi fattori. La tabella riportata alla fine di questo documento mostra i risultati tabulari di differenti modelli Markov che sono alla base di questo diagramma. Quando è necessaria una determinazione più accurata, consultare la tabella.



Determinazione grafica PL

Per ottenere il PL necessario, devono essere realizzati anche altri fattori. Tra questi requisiti figurano le disposizioni per i guasti per causa comune, i guasti sistematici, le condizioni ambientali e il ciclo di vita.

Se il PFH_D del sistema o sottosistema è conosciuto, la Tabella 10.4 (Allegato K dello standard) può essere usata per ricavare il PL.

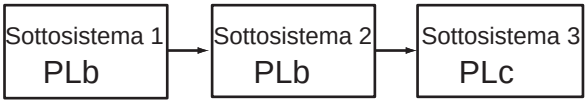
Progettazione dei sottosistemi e combinazioni

I sottosistemi conformi a un PL possono essere combinati semplicemente in un sistema usando la Tabella 10.3. La logica alla base di questa tabella è chiara. Primo, il sistema può essere affidabile solo quanto il più debole dei sottosistemi. Secondo, più sono i sottosistemi, maggiore è la possibilità di guasto.

PL_{basso}	N_{basso}	PL
a	>3	non ammesso
	≤3	a
b	>2	a
	≤2	b
c	>2	b
	≤2	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

Calcolo del PL per sottosistemi combinati in serie

Nel sistema mostrato nel diagramma che segue, i livelli prestazionali più bassi sono quelli dei sottosistemi 1 e 2. Entrambi sono PLb. Quindi, usando questa tabella, possiamo seguire i dati b (nella colonna PL_{basso}) e 2 (nella colonna N_{basso}) per trovare il PL del sistema come b (nella colonna PL). Se tutti e tre i sottosistemi fossero stati PLb, il PL risultante sarebbe stato PLa.



Combinazione di sottosistemi in serie come sistema PLb

Convalida

La convalida svolge un ruolo importante in tutto il processo di sviluppo e di messa in servizio del sistema di sicurezza. Lo standard ISO/EN 13849-2:2003 definisce i requisiti per la convalida, e richiede la definizione di un piano di convalida e la valutazione mediante tecniche di analisi e di prova quali l'analisi dell'albero dei guasti e dei modi, degli effetti e della criticità dei guasti. Molti di questi requisiti si applicheranno al produttore del sottosistema anziché all'utilizzatore.

Messa in servizio delle macchine

In fase di messa in servizio delle macchine o del sistema, deve essere effettuata una convalida delle funzioni di sicurezza, in tutte le modalità operative, che dovrebbe coprire tutte le condizioni anomale prevedibili e normali. Anche le combinazioni di ingressi e sequenze di funzionamento dovrebbero essere considerate. Questa procedura è importante perché è sempre necessario controllare che il sistema sia adatto alle caratteristiche ambientali e operative esistenti. Alcune di queste caratteristiche possono essere diverse da quelle anticipate in fase progettuale.

Progettazione del sistema secondo IEC/EN 62061

Lo standard **IEC/EN 62061**, “Sicurezza del macchinario – Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza”, rappresenta il recepimento specifico per i macchinari dello standard IEC/EN 61508. Indica i requisiti applicabili alla progettazione, a livello di sistema, di tutti i tipi di sistemi di controllo elettrici legati alla sicurezza dei macchinari, oltre che alla progettazione di dispositivi o sottosistemi non complessi.

La valutazione dei rischi sfocia in una strategia di riduzione dei rischi che, a sua volta, identifica le esigenze relative alle funzioni di controllo legate alla sicurezza. Queste funzioni devono essere documentate e devono includere quanto segue:

- specifica dei requisiti funzionali e
- specifica dei requisiti di integrità della sicurezza.

I requisiti funzionali sono dati quali frequenza di funzionamento, tempo di risposta richiesto, modalità operative, cicli di carico, ambiente operativo e funzioni di reazione ai guasti. I requisiti di integrità della sicurezza sono espressi in livelli di integrità della sicurezza (SIL). In base alla complessità del sistema, occorre considerare alcuni o tutti gli elementi nella tabella che segue, per determinare se la progettazione del sistema risponde ai SIL richiesti.

Elemento per la considerazione SIL	**Simbolo**
Probabilità di guasti pericolosi all’ora	PFH_D
Tolleranza ai guasti hardware	Nessun simbolo
Percentuale di guasti sicuri	SFF
Intervallo dei test diagnostici	T_1
Intervallo di test diagnostici	T_2
Suscettibilità ai guasti per causa comune	ß
Copertura diagnostica	DC

Elementi per la considerazione dei SIL

Sottosistemi

Il termine “sottosistema” ha un significato speciale nello standard IEC/EN 62061. Si tratta della suddivisione di primo livello di un sistema in parti che, in caso di guasto, provocano un guasto della funzione di sicurezza. Quindi, se in un sistema vengono

usati due interruttori ridondanti, nessun singolo interruttore è un sottosistema. Il sottosistema sarebbe rappresentato da entrambi gli interruttori e dall'eventuale funzione di diagnostica guasti associata.

Probabilità di guasti pericolosi all'ora (PFH_D)

Lo standard IEC/EN 62061 utilizza gli stessi metodi di base illustrati nella sezione dedicata a EN ISO 13849-1 per determinare i tassi di guasto a livello di componente. Per i componenti "meccanici" ed elettronici valgono le stesse disposizioni e gli stessi metodi. Lo standard IEC/EN 62061 non fa riferimento al MTTFd in anni. Il tasso di guasto all'ora (λ) viene calcolato direttamente oppure ricavato o derivato dal valore B10 applicando la seguente formula:

λ = 0,1 x C/B10 (dove C = numero di cicli operativi all'ora)

Vi è una differenza significativa tra i due standard per quanto riguarda la metodologia di calcolo del PFH_D totale di un sottosistema o sistema. Per determinare la probabilità di guasto dei sottosistemi, occorre analizzare i componenti. Vengono proposte delle formule semplificate per il calcolo delle architetture di sottosistemi comuni (descritti più avanti nel testo). Nei casi in cui tali formule non sono adatte, è necessario utilizzare metodi di calcolo più complessi come i modelli di Markov. Le probabilità di guasti pericolosi (PFH_D) dei singoli sottosistemi vengono quindi sommate per determinare il PFH_D totale del sistema. La tabella 15 (Tabella 3 dello standard) può quindi essere utilizzata per determinare il livello di integrità della sicurezza (Safety Integrity Level – SIL) appropriato per tale intervallo di PFH_D.

$$\lambda_{DssB} = (1-ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2})/2$$

Le formule relative a questa architettura prendono in considerazione la configurazione parallela degli elementi del sottosistema e aggiungono i seguenti due elementi ricavati dalla tabella precedente:

ß (beta) è la suscettibilità a guasti per causa comune

SIL (Livello di integrità della sicurezza)	**PFH_D (Probabilità di guasti pericolosi all'ora)**
3	da $\geq 10^{-8}$ a $<10^{-7}$
2	da $\geq 10^{-7}$ a $<10^{-6}$
1	da $\geq 10^{-6}$ a $<10^{-5}$

Probabilità di guasto pericoloso per SIL

I dati di PFH_D relativi a un sottosistema normalmente vengono forniti dal produttore. I dati relativi ai sistemi e ai componenti di sicurezza di Rockwell Automation sono reperibili in varie forme, per esempio accedendo al sito:

www.discoverrockwellautomation.com/safety

IEC/EN 62061 chiarisce anche che, se e dove applicabile, possono essere utilizzati i Reliability Data Handbook.

Per i dispositivi elettromeccanici a bassa complessità, il meccanismo di guasto è generalmente collegato al numero e alla frequenza delle operazioni anziché solo al tempo. Quindi, per questi componenti, i dati deriveranno da qualche test (ad es. B10, come descritto nel capitolo dedicato allo standard EN ISO 13849-1). Una serie di informazioni legate all'applicazione, come il numero previsto di operazioni all'anno, è poi necessaria per convertire il B10d o dati simili in PFH_D.

Nota: in generale, la seguente relazione è vera (inserendo un fattore per convertire gli anni in ore):

$PFH_D = 1/MTTFd$

Tuttavia, è importante comprendere che, nel caso di un sistema a doppio canale (con o senza diagnostica), non è corretto utilizzare 1/ PFH_D per determinare il MTTFd richiesto dallo standard EN ISO 13849-1, poiché tale standard richiede il calcolo del MTTFd di un canale singolo. Questo valore è molto diverso dal MTTFd della combinazione dei due canali di un sottosistema a due canali.

Vincoli hardware

L'aspetto fondamentale dello standard IEC/EN 62061 è la suddivisione del sistema di sicurezza in sottosistemi. Il livello di integrità della sicurezza hardware che può essere richiesto per un sottosistema è limitato non solo dal PFH_D ma anche dalla tolleranza ai guasti hardware e dalla percentuale di guasti sicuri dei sottosistemi. La tolleranza ai guasti hardware è la capacità del sistema di eseguire la sua funzione in presenza di guasti. Una tolleranza ai guasti di zero significa che la funzione non viene realizzata quando si verifica un singolo guasto. Una tolleranza ai guasti di uno permette al sottosistema di realizzare la sua funzione in presenza di un singolo guasto. La percentuale di guasti sicuri è la porzione del tasso di guasto globale che non comporta un guasto pericoloso. La combinazione di questi due elementi è detta vincolo hardware, a cui è associato il SIL Claim Limit (SIL CL). La tabella che segue mostra la relazione tra vincoli hardware e SIL CL. Un sottosistema (e, di conseguenza, il relativo sistema) deve soddisfare sia i requisiti a livello di PFH_D che i vincoli hardware, oltre alle altre disposizioni pertinenti dello standard.

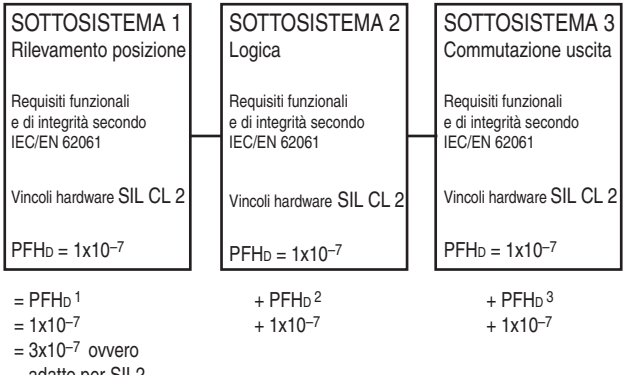
SFF (percentuale di guasti sicuri)	Tolleranza ai guasti hardware		
	0	1	2
<60%	Non ammesso se non per specifiche eccezioni	SIL1	SIL2
60% – <90%	SIL1	SIL2	SIL3
90% – <99%	SIL2	SIL3	SIL3
≥99%	SIL3	SIL3	SIL3

Vincoli hardware su SIL

Per esempio, l'architettura di un sottosistema con tolleranza a un singolo guasto e una percentuale di guasti sicuri del 75% non può andare oltre SIL2, a prescindere dalla probabilità di guasto pericoloso. Quando si combinano i sottosistemi, il SIL ottenuto dall'SRCS deve essere inferiore o uguale al SIL CL più basso tra i sottosistemi coinvolti nella funzione di controllo legata alla sicurezza.

Realizzazione del sistema

Per calcolare la probabilità di guasto pericoloso, ogni funzione di sicurezza deve essere suddivisa in blocchi funzione, che vengono poi realizzati come sottosistemi. L'implementazione del progetto di sistema di una funzione di sicurezza tipica prevede un dispositivo di rilevamento collegato a un dispositivo logico collegato, a sua volta, a un attuatore. Questo crea una configurazione in serie di sottosistemi. Come abbiamo visto, se possiamo determinare la probabilità di guasto pericoloso per ogni sottosistema e conoscere il suo SIL CL, sarà possibile calcolare facilmente la probabilità di guasto del sistema sommando le probabilità di guasto dei sottosistemi. Questo concetto è spiegato di seguito.



Se, per esempio, vogliamo ottenere SIL2, ogni sottosistema deve avere un SIL Claim Limit (SIL CL) di almeno SIL2, e la somma del PFH_D per il sistema non deve superare il limite consentito nella precedente tabella “probabilità di guasto pericoloso per SIL”.

Progettazione del sottosistema – IEC/EN 62061

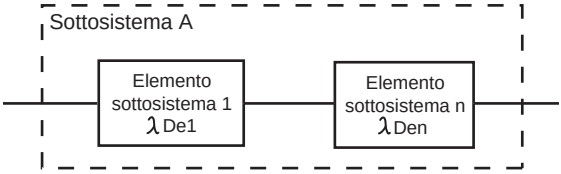
Se un progettista, nei sottosistemi, usa componenti “preconfezionati” conformi a IEC/EN 62061, tutto diventa più facile perché i requisiti specifici per la progettazione dei sottosistemi non si applicano. Questi requisiti saranno coperti, in generale, dal produttore del dispositivo (sottosistema) e sono molto più complessi di quelli richiesti per la progettazione di sistema.

Lo standard IEC/EN 62061 richiede che i sottosistemi complessi, come i PLC di sicurezza, siano conformi a IEC 61508 o ad altri standard appropriati. Ciò significa che, per dispositivi che usano componenti programmabili o elettronici complessi, IEC 61508 si applica in tutto il suo rigore. Questo può essere un processo molto rigoroso. Per esempio, la valutazione del PFH_D ottenuto da un sottosistema complesso può essere un processo molto complicato se si usano tecniche come la modellazione di Markov, gli schemi a blocchi per l’affidabilità o l’analisi dell’albero dei guasti.

IEC/EN 62061 non fornisce requisiti per la progettazione di sottosistemi di complessità inferiore. Generalmente, ciò includerebbe componenti elettrici relativamente semplici come interruttori interbloccati e relè di monitoraggio di sicurezza elettromeccanici. I requisiti non sono complessi come quelli in IEC 61508, ma possono ancora essere piuttosto complicati.

Lo standard IEC/EN 62061 indica quattro architetture logiche dei sottosistemi, con relative formule, che possono essere usate per valutare il PFH_D ottenuto da un sottosistema a bassa complessità. Queste architetture sono rappresentazioni puramente logiche e non dovrebbero essere pensate come architetture fisiche. Le quattro architetture logiche dei sottosistemi e relative formule sono riportate nei seguenti quattro schemi.

Per l’architettura dei sottosistemi di base mostrata di seguito, le probabilità di guasti pericolosi sono semplicemente sommate.

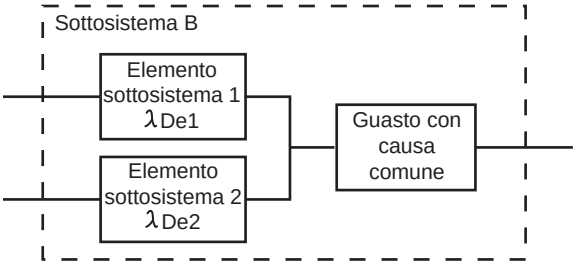


Architettura logica sottosistema A

$\lambda_{DssA} = \lambda_{De1} + \ldots + \lambda_{Den}$
$PFH_{DssA} = \lambda_{DssA} \times 1h$

λ, Lambda designa il tasso di guasto. Il tasso di guasto si esprime in guasti all'ora. λ_D è il tasso di guasto pericoloso. λ_{DssA} è il tasso di guasto pericoloso del sottosistema A. λ_{DssA} è la somma dei tassi di guasto dei singoli elementi, e1, e2, e3, fino a en compreso. La probabilità di guasto pericoloso è moltiplicata per 1 ora, per creare la probabilità di guasto in un'ora.

Il diagramma successivo mostra un sistema tollerante a un singolo guasto, senza una funzione di diagnostica. Quando una architettura include la tolleranza a un singolo guasto, il potenziale dei guasti per causa comune esiste e deve essere considerato. La determinazione dei guasti per causa comune è brevemente descritta più avanti, in questo capitolo.



Architettura logica sottosistema B

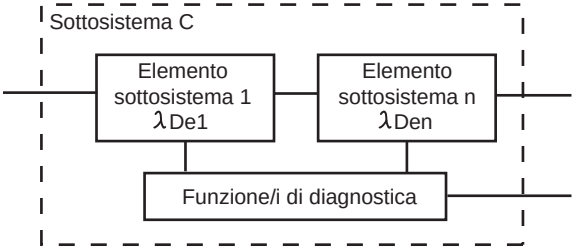
$\lambda_{DssB} = (1-ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2})/2$
$PFH_{DssB} = \lambda_{DssB} \times 1h$

Le formule per questa architettura prendono in considerazione la configurazione parallela degli elementi del sottosistema, a cui si aggiungono i seguenti due elementi ricavati dalla precedente tabella "Elementi per la considerazione dei SIL":

ß – la suscettibilità a guasti per causa comune (Beta)

T1 – l'intervallo dei test diagnostici o ciclo di vita, a seconda di qual è il più breve. Il test diagnostico è concepito per rilevare i guasti e il degrado del sottosistema di sicurezza, in modo che il sottosistema possa essere riportato a una condizione operativa. In termini pratici, in tal caso si rende necessaria una sostituzione (come nel caso del termine equivalente "ciclo di vita" – "mission time" – dello standard EN ISO 13849-1).

Il prossimo schema mostra la rappresentazione funzionale di un sistema con tolleranza zero guasti, con una funzione diagnostica. La copertura diagnostica serve a ridurre la probabilità di guasti hardware pericolosi. I test di autodiagnosi vengono realizzati automaticamente. La definizione di copertura diagnostica è identica a quella riportata nello standard EN ISO 13849-1, ossia il rapporto del tasso dei guasti pericolosi rilevati rispetto al tasso di tutti i guasti pericolosi.



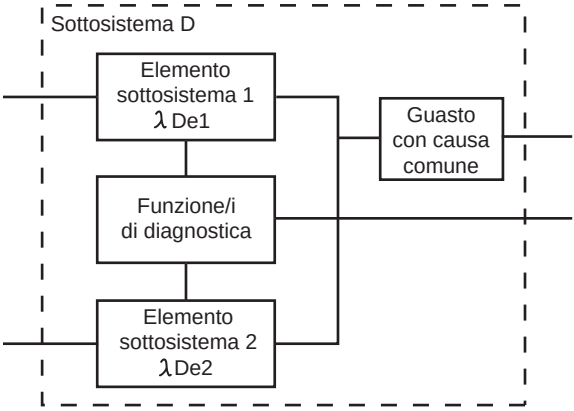
Architettura logica sottosistema C

$\lambda_{DssC} = \lambda_{De1} (1\text{-}DC_1) + \ldots + \lambda_{Den} (1\text{-}DC_n)$

$PFH_{DssC} = \lambda_{DssC} \times 1h$

Queste formule includono la copertura diagnostica (DC) per ogni elemento del sottosistema. I tassi di guasto di ognuno dei sottosistemi sono ridotti dalla copertura diagnostica di ogni sottosistema.

Di seguito, è riportato il quarto esempio di architettura di un sottosistema. Questo sottosistema è a tolleranza di un singolo guasto e include una funzione diagnostica. Con i sistemi a tolleranza di un singolo guasto, deve essere considerato anche il potenziale di guasti per causa comune.



Architettura logica sottosistema D

Se gli elementi del sottosistema sono diversi, si usano le seguenti formule:

$\lambda_{DssD} = (1 - ß)^2 \{ \lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \times T_2/2 + \lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \times T_1/2 \} + ß \times (\lambda_{De1} + \lambda_{De2})/2$

$PFH_{DssD} = \lambda_{DssD} \times 1h$

Se gli elementi del sottosistema sono gli stessi, si usano le seguenti formule:

$\lambda_{DssD} = (1 - ß)^2 \{[\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1-DC)] \times T_1 \} + ß \times \lambda_{De}$
$PFH_{DssD} = \lambda_{DssD} \times 1h$

Si noti che in entrambe le formule è presente un parametro in più, T2 ovvero l'intervallo di diagnostica. Questo è solo un controllo periodico della funzione. Si tratta di un test meno completo del test diagnostico.

A titolo di esempio, consideriamo i seguenti valori nel caso in cui gli elementi del sottosistema siano differenti:

ß = 0,05
$\lambda_{De} = 1 \times 10^{-6}$ guasti/ora
T1 = 87.600 ore (10 anni)
T2 = 2 ore
DC = 90%

PFH_{DssD} = 5.791E-08 guasti pericolosi/ora. Questo risultato rientra nel campo richiesto per il SIL3.

Influenza dell'intervallo dei test diagnostici

Secondo lo standard IEC/EN 62061 è consigliabile (ma non obbligatorio) un intervallo dei test diagnostici (Proof Test Interval – PTI) di 20 anni. Consideriamo ora l'effetto che l'intervallo dei test diagnostici ha sul sistema. Se ricalcoliamo la formula imponendo un T1 pari a 20 anni otteniamo PFH_{DssD} = 6.581E-08. Tale valore rientra ancora nel campo richiesto per il SIL3. Il progettista deve tenere a mente che, per calcolare il tasso di guasto pericoloso globale, questo sottosistema deve essere combinato con gli altri sottosistemi.

Influenza dell'analisi dei guasti per causa comune

Guardiamo l'influenza che i guasti per causa comune hanno sul sistema. Supponiamo di adottare misure supplementari e di portare il nostro valore ß (Beta) all'1% (0,01), mentre l'intervallo dei test diagnostici rimane a 20 anni. Il tasso di guasto pericoloso migliora, passando a 2.71E-08, che significa che il sottosistema ora è più adatto a essere impiegato in un sistema SIL3.

Guasti per causa comune (CCF)

I guasti per causa comune si verificano quando molteplici guasti, risultanti da una singola causa, producono un guasto pericoloso. Le informazioni sui CCF generalmente sono necessarie solo al progettista del sottosistema, di solito il produttore. Nelle formule fornite serve a stimare il PFH_D di un sottosistema. Generalmente, non sarà necessario per la progettazione del sistema.

L'allegato F di IEC/EN 62061 propone un approccio semplice per la stima dei CCF. La tabella che segue mostra un riepilogo del sistema di punteggio.

N.	Misura contro CCF	Punteggio
1	Separazione/Segregazione	25
2	Diversità	38
3	Progettazione/Applicazione/ Esperienza	2
4	Valutazione/Analisi	18
5	Competenza/Formazione	4
6	Ambiente	18

Punteggio delle misure contro i guasti per causa comune

Per adottare misure specifiche contro i CCF, vengono assegnati dei punti. Il punteggio viene poi sommato per determinare il fattore dei guasti per causa comune, mostrato nella seguente tabella. Il fattore beta serve a “regolare” il tasso di guasto nei modelli di sottosistema.

Punteggio totale	Fattore guasti per causa comune (ß)
<35	10% (0,1)
35 – 65	5% (0,05)
65 – 85	2% (0,02)
85 – 100	1% (0,01)

Fattore Beta per i guasti per causa comune

Copertura diagnostica (DC)

Per ridurre la probabilità di pericolosi guasti hardware, si utilizzano test di autodiagnosi. Essere in grado di rilevare tutti i guasti hardware pericolosi sarebbe l’ideale, ma, nella pratica, il valore massimo è impostato al 99% (che si può esprimere come 0,99)

La copertura diagnostica è il rapporto tra la probabilità dei guasti pericolosi rilevati e la probabilità di tutti i guasti pericolosi.

$$DC = \frac{\text{Probabilità di guasti pericolosi rilevati, } \lambda_{DD}}{\text{Probabilità di guasti pericolosi totali, } \lambda_{Dtotale}}$$

Il valore di copertura diagnostica sarà tra zero e uno.

Tolleranza ai guasti hardware

La tolleranza ai guasti hardware rappresenta il numero di guasti che possono essere sostenuti da un sottosistema prima di generare un guasto pericoloso. Per esempio, una tolleranza ai guasti hardware di 1 significa che 2 guasti potrebbero provocare una perdita della funzione di controllo legata alla sicurezza, ma un solo guasto no.

Gestione della sicurezza funzionale

Lo standard fornisce i requisiti per il controllo delle attività tecniche e di gestione necessarie all'ottenimento di un sistema di controllo elettrico legato alla sicurezza.

Intervallo dei test diagnostici

L'intervallo dei test diagnostici rappresenta il tempo dopo cui un sottosistema deve essere totalmente controllato o sostituito per garantire che sia "come nuovo". In pratica, nel settore delle macchine, ciò si ottiene mediante sostituzione. Quindi, l'intervallo dei test diagnostici corrisponde, di solito, al ciclo di vita. EN ISO 13849-1:2008 fa riferimento a questo come ciclo di vita.

Un test diagnostico è un controllo che permette di rilevare i guasti e l'usura di un SRCS in modo da poterlo riportare, per quanto possibile, "come nuovo". Il test diagnostico deve rilevare il 100% di tutti i guasti pericolosi. Canali separati devono essere testati separatamente.

Diversamente dai test delle funzioni di autodiagnosi, che sono automatici, i test diagnostici vengono generalmente realizzati manualmente e offline. Essendo automatici, i test di autodiagnosi sono realizzati più spesso rispetto ai test funzionali che, invece, vengono realizzati raramente. Per esempio, i circuiti collegati all'interruttore di interblocco di una protezione possono essere testati automaticamente, per cortocircuiti o interruzioni, con i test diagnostici (ad es. a impulsi).

L'intervallo dei test diagnostici deve essere dichiarato dal produttore. Talvolta, il produttore fornisce una serie di intervalli dei test diagnostici differenti.

SFF (percentuale di guasti sicuri)

La percentuale di guasti sicuri è simile alla copertura diagnostica ma considera anche qualunque tendenza intrinseca a generare un guasto in stato di sicurezza. Per esempio, un fusibile bruciato è un guasto ma è altamente probabile che si risolva in una interruzione di circuito che, in molti casi, è un guasto "sicuro". SFF (la somma del tasso di guasti "sicuri" più il tasso di guasti pericolosi rilevati) viene diviso per (la somma del tasso di guasti "sicuri" più il tasso di guasti pericolosi rivelati e non rivelati). È importante capire che i soli tipi di guasto da considerare sono quelli che potrebbero avere qualche effetto sulla funzione di sicurezza.

Molti dispositivi meccanici a bassa complessità, come pulsanti di emergenza e interruttori di interblocco, avranno (da soli) un certo valore di SFF specifico. La maggior parte dei dispositivi elettronici relativi alla sicurezza sono caratterizzati da ridondanza e funzioni di monitoraggio interne, pertanto è abbastanza comune avere

un SFF superiore al 90%, anche se ciò di norma è interamente dovuto alla capacità di ottenimento della copertura diagnostica. Il valore SFF viene generalmente fornito dal produttore.

Il valore SFF può essere calcolato con la seguente equazione:

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$$

dove:

λ_S = tasso di guasti sicuri
$\Sigma\lambda_S + \Sigma\lambda_D$ = tasso di guasto complessivo
λ_{DD} = tasso di guasti pericolosi rilevati
λ_D = tasso di guasti pericolosi.

Guasti sistematici

Lo standard ha requisiti per il controllo e l'eliminazione dei guasti sistematici. I guasti sistematici sono diversi dai guasti hardware casuali che si verificano, di solito, per usura dei componenti hardware. Possibili guasti sistematici sono errori di progettazione software, errori di progettazione hardware, errori di specifica dei requisiti e procedure operative. Tra le misure necessarie a evitare i guasti sistematici ci sono le seguenti:

- corretta selezione, combinazione, disposizione, assemblaggio e installazione dei componenti;
- uso di buone pratiche di progettazione;
- rispetto delle specifiche del produttore e delle istruzioni di installazione;
- verifica della compatibilità tra i componenti;
- compatibilità alle condizioni ambientali;
- uso di materiali adatti.

Sistemi di controllo legati alla sicurezza – considerazioni strutturali

Cenni generali

In questo capitolo verranno riportati principi e considerazioni strutturali da tenere presente durante la progettazione di un sistema di controllo legato alla sicurezza in conformità a qualsiasi standard. La terminologia ruoterà principalmente intorno al concetto di categorie dello standard EN 954-1 in via di dismissione, dal momento che le categorie si riferiscono principalmente alla struttura dei sistemi di controllo.

Categorie dei sistemi di controllo

Il concetto di "categorie" dei sistemi di controllo è nato con lo standard EN 954-1:1996 (ISO 13849-1:1999), in via di dismissione. Tuttavia, le categorie vengono tuttora spesso utilizzate per descrivere i sistemi di controllo di sicurezza e rimarranno parte integrante dello standard EN ISO 13849-1, come descritto nella sezione "Introduzione alla sicurezza funzionale dei sistemi di controllo".

Per descrivere le prestazioni di reazione ai guasti di un sistema di controllo legato alla sicurezza si utilizzano cinque categorie, riepilogate nella Tabella 19. Le note si riferiscono alla tabella.

Nota 1: la categoria B non prevede misure speciali per la sicurezza ma rappresenta la base per le altre categorie.

Nota 2: più errori provocati da una causa comune o inevitabili conseguenze del primo guasto devono essere considerati quale un solo guasto.

Nota 3: la revisione dei guasti può essere limitata a una combinazione di due errori se questo può essere giustificato, ma nel caso di circuiti complessi (ad esempio circuiti a microprocessori) è possibile che sia necessario prendere in considerazione più errori contemporaneamente.

La categoria 1 è volta alla PREVENZIONE degli errori. Si ottiene utilizzando principi progettuali, componenti e materiali adeguati. La semplicità del principio di funzionamento e del progetto, e le caratteristiche stabili e prevedibili del materiale, sono i punti essenziali di questa categoria.

Le categorie 2, 3 e 4 richiedono che se il guasto non può essere prevenuto, deve essere RILEVATO e quindi devono essere presi i provvedimenti necessari.

Ridondanza, diversità e monitoraggio sono le chiavi di queste categorie. La ridondanza è la duplicazione della stessa tecnica. La diversità è l'uso di due diverse tecniche. Il monitoraggio è il controllo dello stato dei dispositivi e l'adozione delle misure conseguenti. Il solito (ma non l'unico) metodo di monitoraggio consiste nel duplicare le funzioni essenziali per la sicurezza e confrontare il funzionamento.

Riepilogo dei requisiti	Comportamento del sistema
CATEGORIA B (vedere la nota 1) Le parti correlate alla sicurezza del sistema di controllo della macchina e/o dei dispositivi di protezione, oltre ai relativi componenti, devono essere progettati, costruiti, selezionati, assemblati e combinati in conformità con gli standard pertinenti affinché resistano alle influenze previste. I principi base di sicurezza devono essere applicati.	Quando si verifica un guasto, questo può comportare una perdita della funzione di sicurezza.
CATEGORIA 1 Si applicano i requisiti della categoria B; inoltre occorre usare componenti di sicurezza e principi di sicurezza di comprovata efficienza.	Come per la categoria B ma con una più alta affidabilità della funzione di sicurezza. (Maggiore è l'affidabilità, minore è la probabilità di guasto).
CATEGORIA 2 Si applicano i requisiti della categoria B e principi di sicurezza di comprovata efficienza. Le funzioni di sicurezza devono essere controllate all'avviamento della macchina e periodicamente dal sistema di controllo della macchina. Qualora sia rilevato un guasto deve essere creato uno stato sicuro e, se ciò non fosse possibile, deve essere lanciato un allarme. Lo standard EN ISO 13849-1 presuppone che la frequenza di test sia almeno 100 volte superiore alla frequenza della domanda. Lo standard EN ISO 13849-1 presuppone che l'MTTFd delle apparecchiature di prova esterne sia superiore alla metà dell'MTTFd dei macchinari funzionali in esame.	La perdita della funzione di sicurezza è rilevata dal controllo. Il verificarsi di un guasto può comportare la perdita della funzione di sicurezza tra gli intervalli di controllo.
CATEGORIA 3 (vedere le note 2 e 3) Si applicano i requisiti della categoria B e principi di sicurezza di comprovata efficienza. Il sistema deve essere progettato in modo che un singolo guasto in una sua parte qualsiasi non comporti la perdita della funzione di sicurezza. Dove possibile, un singolo guasto deve essere rilevato.	Quando si verifica un singolo guasto, la funzione di sicurezza viene sempre eseguita. Alcuni ma non tutti gli errori vengono rilevati. Un accumulo di errori non rilevati può comportare la perdita della funzione di sicurezza.
CATEGORIA 4 (vedere le note 2 e 3) Si applicano i requisiti della categoria B e principi di sicurezza di comprovata efficienza. Il sistema deve essere progettato in modo che un singolo guasto, in qualunque sua parte, non comporti la perdita della funzione di sicurezza. Il singolo guasto deve essere rilevato in occasione o prima della successiva richiesta di intervento della funzione di sicurezza. Se tale rilevamento non è possibile, l'accumulo di errori non deve comportare la perdita della funzione di sicurezza.	Quando si verificano i guasti, la funzione di sicurezza viene sempre eseguita. I guasti vengono rilevati in tempo utile per prevenire la perdita della funzione di sicurezza.

Categoria B

La categoria B fornisce i requisiti di base di qualunque sistema di controllo; che si tratti di un sistema di controllo legato alla sicurezza o meno. Un sistema di controllo deve lavorare nell'ambiente previsto. Il concetto di affidabilità rappresenta un fondamento per i sistemi di controllo, dato che l'affidabilità è definita come la probabilità che un dispositivo realizzi la funzione prevista, per un determinato intervallo, nelle condizioni previste.

La Categoria B richiede l'applicazione dei principi di sicurezza di base. ISO 13849-2 contiene i principi di sicurezza di base dei sistemi elettrici, pneumatici, idraulici e meccanici. I principi elettrici sono riepilogati come segue.

- Corretta selezione, combinazione, disposizione, assemblaggio e installazione (in conformità alle istruzioni del produttore)
- Compatibilità dei componenti a tensioni e correnti
- Compatibilità alle condizioni ambientali
- Uso del principio di diseccitazione
- Soppressione dei transitori elettrici
- Riduzione del tempo di risposta
- Protezione contro gli avviamenti non intenzionali
- Fissaggio sicuro dei dispositivi di ingresso (ad es. montaggio di interblocchi)
- Protezione del circuito di controllo (secondo NFPA 79 e IEC 60204-1)
- Corretto collegamento di protezione a massa

Il progettista deve selezionare, installare e assemblare i componenti secondo le istruzioni del fabbricante. Questi dispositivi devono funzionare entro i valori nominali di tensione e corrente previsti. Anche le condizioni ambientali previste devono essere considerate – compatibilità elettromagnetica, vibrazioni, urti, contaminazione, lavaggi. È stato usato il principio di diseccitazione: nelle bobine del contattore, è installata la protezione dai transitori elettrici. Il motore è protetto contro i sovraccarichi. Il cablaggio e la messa a terra rispondono ai corrispondenti standard elettrici.

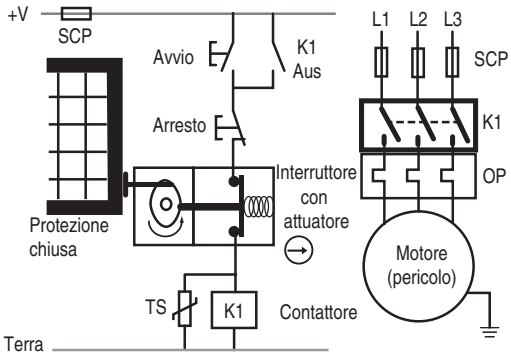
Categoria 1

La Categoria 1 richiede che il sistema sia conforme ai termini della Categoria B e che usi componenti di sicurezza di comprovata efficienza. Che cosa sono esattamente i componenti di sicurezza e come sappiamo se sono di comprovata efficienza? ISO 13849-2 ci aiuta a rispondere a queste domande per i sistemi elettrici, pneumatici, idraulici e meccanici. L'Allegato D tratta i componenti elettrici.

I componenti sono considerati di comprovata efficienza se sono stati usati con successo in molte altre simili applicazioni. I componenti di sicurezza progettati recentemente sono considerati di comprovata efficienza se concepiti e verificati in conformità ai corrispondenti standard.

Componente di comprovata efficienza	**Standard**
Interruttore a modalità di apertura positiva (apertura diretta)	IEC 60947-5-1
Dispositivo di arresto di emergenza	ISO 13850, IEC 60947-5-5
Fusibile	IEC 60269-1
Interruttore automatico	IEC 60947-2
Contattori	IEC 60947-4-1, IEC 60947-5-1
Contatti ad accoppiamento meccanico	IEC 60947-5-1
Contattore ausiliario (ad es. contattore, relè ausiliario, relè a guida forzata)	EN 50205 IEC 60204-1, IEC 60947-5-1
Trasformatore	IEC 60742
Cavo	IEC 60204-1
Dispositivi di interblocco	ISO 14119
Termostato	IEC 60947-5-1
Pressostato	IEC 60947-5-1 + requisiti pneumatici o idraulici
Apparecchiatura o dispositivo di commutazione di protezione e controllo (CPS)	IEC 60947-6-2
Controllore a logica programmabile	IEC 61508, IEC 62061

Applicando componenti di comprovata efficienza al nostro sistema di Categoria B, l'interruttore di finecorsa sarebbe sostituito da un interruttore con attuatore ad azione di apertura diretta e il contattore sarebbe sovradimensionato per una maggiore protezione contro la saldatura dei contatti.



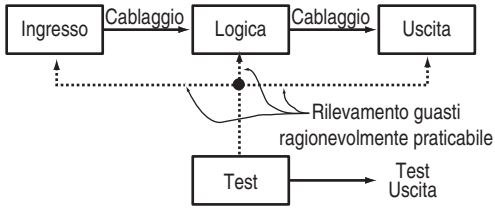
Semplice sistema di sicurezza di Categoria 1

Qui sono riportate le modifiche a un semplice sistema di Categoria B, per ottenere la Categoria 1. Interblocco e contattore svolgono il ruolo chiave di scollegare l'alimentazione all'attuatore, quando è necessario accedere al pericolo. L'interblocco con attuatore risponde ai requisiti IEC 60947-5-1 per i contatti ad azione di apertura diretta (contrassegnati, nel disegno, dalla freccia nel cerchio). Con componenti di comprovata efficienza, la probabilità che l'alimentazione venga scollegata è più alta per la Categoria 1 che per la Categoria B. L'uso di componenti di comprovata efficienza serve a impedire la perdita della funzione di sicurezza. Anche con questi miglioramenti, un singolo guasto può comunque comportare la perdita della funzione di sicurezza.

Le Categorie B e 1 sono basate sulla prevenzione. La concezione è intesa a prevenire le situazioni pericolose. Quando la sola prevenzione non consente una sufficiente riduzione del rischio, bisogna ricorrere al rilevamento dei guasti. Le Categorie 2, 3 e 4 sono basate sul rilevamento dei guasti, con requisiti sempre più severi per ottenere sempre maggiori livelli di riduzione dei rischi.

Categoria 2

Oltre a rispondere ai requisiti della Categoria B e a utilizzare principi di sicurezza di comprovata efficienza, il sistema di sicurezza deve essere sottoposto a test per rispondere ai requisiti della Categoria 2. I test devono essere concepiti per rilevare guasti nei componenti di sicurezza del sistema di controllo. Se non viene rilevato alcun guasto, la macchina può entrare in funzione. In presenza di guasti, il test deve generare un comando. Quando possibile, il comando deve portare la macchina in stato di sicurezza.



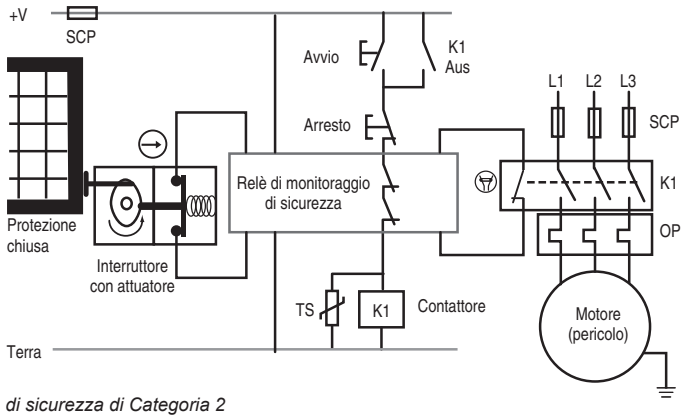
Il test deve permette di rilevare i guasti in modo ragionevolmente praticabile. L'apparecchiatura che effettua il test può essere parte integrante del sistema di sicurezza o uno strumento separato.

Il test deve essere realizzato nelle seguenti condizioni:

- alla prima accensione della macchina,
- prima della generazione di un pericolo, e
- periodicamente, se ritenuto necessario dalla valutazione dei rischi.

Nota: lo standard EN ISO 138491-1 presuppone che il tasso di richiesta della funzione di sicurezza sia 100 volte inferiore al tasso di richiesta della funzione di test. L'esempio riportato qui non soddisferebbe tale requisito.

Le espressioni "quando possibile" e "ragionevolmente praticabile" indicano che non tutti i guasti sono rilevabili. Trattandosi di un sistema a canale singolo (ovvero un unico cavo collega, in sequenza, ingresso-logica-uscita), un singolo guasto può comportare la perdita della funzione di sicurezza. In alcuni casi, la Categoria 2 non può essere completamente applicata a un sistema di sicurezza, perché non tutti i componenti possono essere controllati.

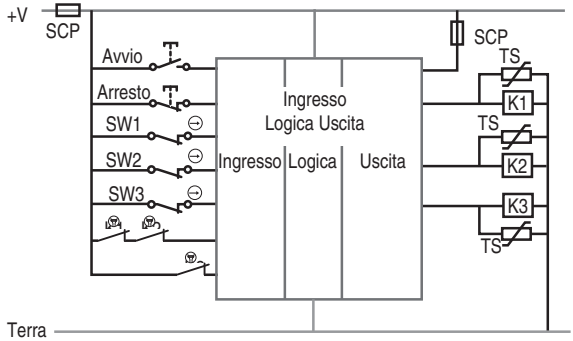


Sistema di sicurezza di Categoria 2

Questo è un semplice sistema di Categoria 1, migliorato per rispondere alla Categoria 2. Un relè di monitoraggio di sicurezza (MSR) realizza il test. All'accensione, l'MSR controlla i suoi componenti interni. Se non viene rilevato alcun guasto, l'MSR controlla l'interruttore con attuatore monitorando la funzionalità dei suoi contatti. Se non viene rilevato alcun guasto e la protezione è chiusa, l'MSR controlla il dispositivo di uscita: i contatti ad accoppiamento meccanico del contattore. Se non viene rilevato alcun guasto e il contattore è disattivato, l'MSR eccita la sua uscita interna e collega la bobina di K1 al pulsante di arresto. A questo punto, i componenti non legati alla sicurezza del sistema di controllo della macchina, il circuito di Avviamento/Arresto/Interblocco, possono accendere e spegnere la macchina.

Aprendo la protezione, si disattivano le uscite dell'MSR. Quando la protezione viene richiusa, l'MSR ripete i controlli sul sistema di sicurezza. Se non viene rilevato alcun guasto, l'MSR attiva la sua uscita interna. L'MSR permette a questo circuito di rispondere alla Categoria 2 testando il dispositivo di ingresso, il dispositivo logico (se stesso) e il dispositivo di uscita. Il test è eseguito alla prima accensione e prima dell'inizio del pericolo.

Con le sue capacità logiche intrinseche, un sistema di sicurezza basato su PLC può essere concepito per rispondere alla Categoria 2. Come stabilito nella precedente trattazione della Categoria 1, il punto diventa la giustificazione di comprovata efficienza del PLC (tra cui le sue capacità di test). Per sistemi di sicurezza complessi che richiedono una classificazione di Categoria 2, un PLC non di sicurezza dovrebbe essere sostituito con un PLC di sicurezza conforme a IEC 61508.



Sistema di sicurezza complesso di Categoria 2

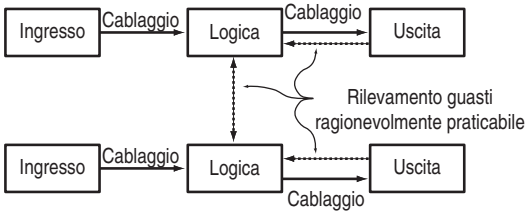
Questo è l'esempio di un sistema complesso che usa un PLC di sicurezza. Un PLC di sicurezza, essendo concepito secondo un determinato standard, risponde ai requisiti di comprovata efficienza. I contatti ad accoppiamento meccanico dei contattori sono portati all'ingresso del PLC a scopo di test. A seconda della logica di programma, questi contatti possono essere collegati in serie a un terminale di ingresso o a singoli terminali di ingresso.

Anche se vengono utilizzati componenti di sicurezza di comprovata efficienza, un singolo guasto tra i controlli può comportare la perdita della funzione di sicurezza. Quindi, i sistemi di Categoria 2 sono utilizzati nelle applicazioni a rischio più basso. Quando sono necessari livelli più alti di tolleranza ai guasti, il sistema di sicurezza deve essere di Categoria 3 o 4.

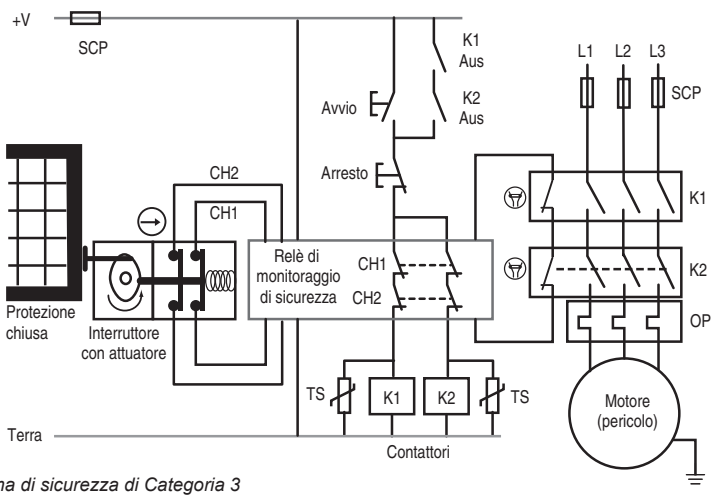
Categoria 3

Oltre a rispondere ai requisiti della Categoria B e ai principi di sicurezza di comprovata efficienza, la Categoria 3 richiede l'operatività della funzione di sicurezza in presenza di un singolo guasto. Il guasto deve essere rilevato in concomitanza o prima della successiva richiesta di intervento della funzione di sicurezza, ogniqualvolta ragionevolmente praticabile.

Di nuovo, abbiamo la frase "ogniqualvolta ragionevolmente praticabile". Ciò considera i guasti che possono non essere rilevati. Fino a che il guasto non rilevabile non comporta la perdita della funzione di sicurezza, la funzione di sicurezza può rispondere alla Categoria 3. Di conseguenza, un accumulo di guasti non rilevabili può comportare la perdita della funzione di sicurezza.



Lo schema a blocchi qui presentato spiega i principi di un sistema di Categoria 3. Per garantire le prestazioni della funzione di sicurezza, si ricorre alla ridondanza e al monitoraggio incrociato e delle uscite, quando ragionevolmente praticabile.



Sistema di sicurezza di Categoria 3

Questo è un esempio di sistema di Categoria 3. Un set ridondante di contatti viene aggiunto all'interruttore di interblocco con attuatore. Internamente, il relè di monitoraggio di sicurezza (MSR) contiene circuiti ridondanti che si monitorano reciprocamente. Un set ridondante di contattori toglie alimentazione al motore. I contattori sono monitorati dall'MSR attraverso i contatti ad accoppiamento meccanico nel modo "ragionevolmente praticabile".

Il rilevamento dei guasti deve essere preso in esame per ogni componente del sistema di sicurezza, oltre che per i collegamenti (ovvero il sistema). Quali sono le modalità di guasto di un interruttore con attuatore a due canali? Quali sono le modalità di guasto dell'MSR? Quali sono le modalità di guasto dei contattori K1 e K2? Quali sono le modalità di guasto del cablaggio?

L'interruttore interbloccato con attuatore è concepito con contatti ad apertura diretta. Quindi sappiamo che l'apertura della protezione è concepita per aprire un contatto saldato. Questo risolve una modalità di guasto. Esistono altre modalità di guasto?

L'interruttore ad azione di apertura diretta è di solito concepito con un ritorno a molla. Se la testa viene rimossa o staccata, i contatti di sicurezza tornano in stato di chiusura (sicuro). Molti interruttori di interblocco sono concepiti con teste rimovibili, per adattarsi ai requisiti di installazione di varie applicazioni. La testa può essere rimossa e ruotata tra due e quattro posizioni.

Se le viti di montaggio della testa non sono correttamente serrate, potrebbe verificarsi un guasto. In questa condizione, le vibrazioni della macchina possono provo-

care l'uscita delle viti di montaggio della testa. La testa, sotto la pressione della molla, rilascia i contatti di sicurezza che, quindi, si chiudono. Di conseguenza, l'apertura della protezione non apre i contatti di sicurezza e si verifica un guasto in grado di generare un pericolo.

In modo simile, anche il meccanismo operativo all'interno dell'interruttore deve essere esaminato. Qual è la probabilità che il guasto di un singolo componente comporti la perdita della funzione di sicurezza? Una pratica comune è l'uso di interblocchi con attuatore con doppi contatti in circuiti di Categoria 3. Ciò deve essere basato sull'esclusione del singolo guasto dell'interruttore per aprire i contatti di sicurezza. Si tratta della cosiddetta "esclusione del guasti", trattata più avanti in questo capitolo.

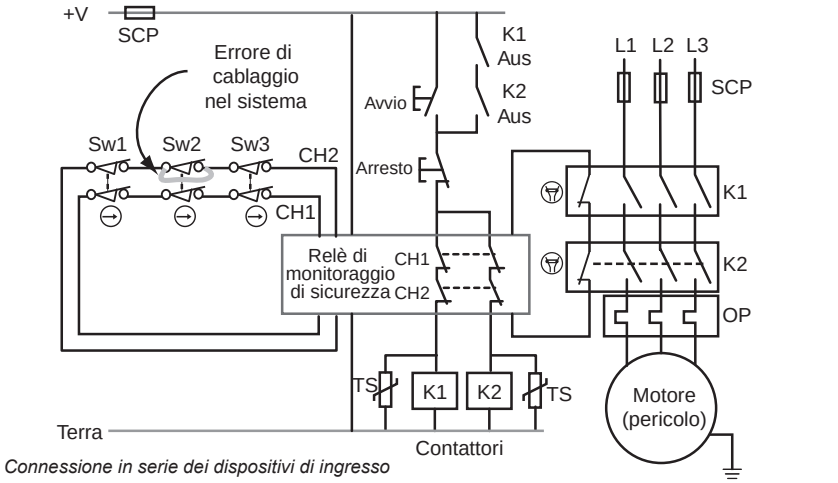
I relè di monitoraggio di sicurezza (MSR) spesso vengono valutati da terzi, dopodiché viene loro assegnata una categoria (e/o un PL e SIL CL). L'MSR prevede spesso capacità a doppio canale, monitoraggio incrociato dei canali e dei dispositivi esterni, protezione dai cortocircuiti. Non esistono standard specifici che forniscano indicazioni sulla progettazione o l'uso dei relè di monitoraggio di sicurezza. Gli MSR sono valutati in base alla loro capacità di svolgere la funzione di sicurezza, secondo ISO 13849-1 o EN 954-1, in via di dismissione. Il livello dell'MSR deve corrispondere a o superare il livello richiesto per il sistema in cui viene utilizzato.

Due contattori aiutano a garantire che i dispositivi di uscita realizzino la funzione di sicurezza. Con una protezione contro i sovraccarichi e i cortocircuiti, la probabilità che il contattore abbia problemi di contatti saldati è scarsa, ma non impossibile. Un contattore può generare un guasto anche a causa di contatti di commutazione che rimangono chiusi a causa del blocco dell'indotto. Se il guasto di un contattore genera uno stato pericoloso, il secondo contattore toglie alimentazione alla fonte del pericolo. L'MSR rileva il contattore in guasto al successivo ciclo della macchina. Quando la protezione è chiusa e il pulsante di avviamento viene premuto, i contatti ad accoppiamento meccanico del contattore guasto rimangono aperti e l'MSR, non essendo in grado di chiudere i contatti di sicurezza, rivela il guasto.

Guasti non rilevati

Nel caso di un sistema con struttura di categoria 3 vi possono essere dei guasti che non possono essere rilevati ma che, di per sé, non devono comportare la perdita della funzione di sicurezza.

Se i guasti possono essere rilevati, dobbiamo sapere se, in determinate circostanze, potrebbero risultare mascherati o azzerati involontariamente con l'intervento di altri dispositivi all'interno della struttura del sistema.



Connessione in serie dei dispositivi di ingresso

L'approccio qui riportato è ampiamente utilizzato per collegare molteplici dispositivi a un relè di monitoraggio di sicurezza. Ogni dispositivo contiene due contatti ad azione di apertura diretta, normalmente chiusi. Questi dispositivi possono essere una combinazione di interblocchi o pulsanti di arresto di emergenza. Dato che i dispositivi di ingresso sono collegati a margherita, questo approccio consente di risparmiare sui costi di cablaggio. Presumiamo che, attraverso uno dei contatti, si verifichi un cortocircuito in corrispondenza di Sw2, come mostrato in figura. Il guasto può essere rilevato?

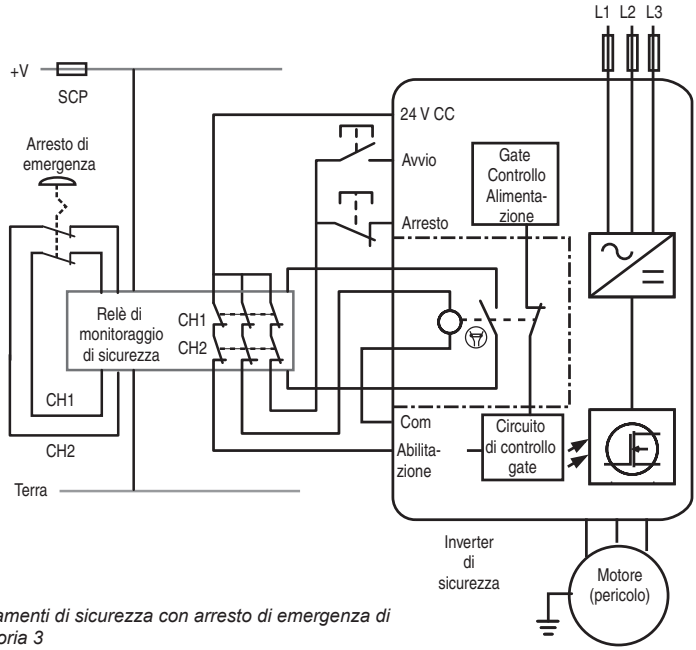
Se l'interruttore Sw1 (o Sw3) viene aperto, sia Ch1 che Ch2 diventano circuiti aperti e l'MSR toglie corrente alla zona di pericolo. Se quindi Sw3 viene aperto e richiuso, il guasto tra i suoi contatti non viene rilevato poiché non si ha un cambiamento di stato in corrispondenza dell'MSR: sia Ch1 che Ch2 rimangono aperti. Se quindi si chiude Sw1 (o Sw3), il pericolo può essere riattivato premendo il pulsante di avviamento. In queste circostanze il guasto non ha determinato una perdita della funzione di sicurezza ma non è stato rilevato, e persiste nel sistema, pertanto un guasto successivo (un cortocircuito attraverso il secondo contatto di Sw2) potrebbe comportare la perdita della funzione di sicurezza.

Se si apre e si chiude solo Sw2, senza intervento degli altri interruttori, Ch1 viene aperto e Ch2 rimane chiuso. L'MSR diseccita il pericolo poiché Ch1 è aperto. Quando Sw2 si chiude, il motore non può essere avviato con il pulsante di avviamento premuto, perché Ch2 non si è aperto. Il guasto viene rilevato. Tuttavia, se per qualsiasi motivo Sw1 (o Sw3) dovesse quindi essere aperto e chiuso, sia Ch1 che Ch2 diverranno prima circuiti aperti e poi circuiti chiusi. Questa sequenza simula l'azzeramento del guasto e determina un reset involontario dell'MSR.

Si pone quindi l'interrogativo di quale DC dichiarare per i singoli interruttori quando si utilizza lo standard EN ISO 13849-1 o IEC 62061. Al momento della pubblicazione di questo testo non esistono indicazioni specifiche e definitive sull'argomento, ma nella prassi si è soliti considerare una DC del 60%, a patto che gli interruttori vengano testati individualmente con cadenza adeguata per individuare i guasti. Se è prevedibile che uno (o più) interruttori non vengano mai testati singolarmente, si può affermare che si dovrebbe indicare una DC pari a zero. Al momento della pubblicazione di questo testo lo standard EN ISO 13849-2 è in fase di revisione. La nuova versione potrebbe contenere indicazioni maggiori su questo argomento.

Il collegamento in serie dei contatti meccanici è limitato alla Categoria 3, dato che può portare alla perdita della funzione di sicurezza a causa dell'accumulo di guasti. In termini pratici la diminuzione della DC (e conseguentemente di SFF) limita i PL e SIL massimi raggiungibili a PLd e SIL2.

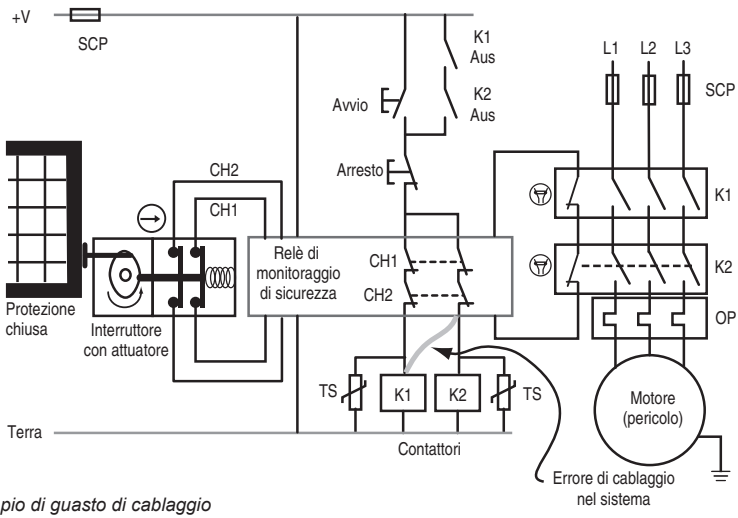
È interessante notare che è sempre stato necessario considerare queste caratteristiche di una struttura di Categoria 3, ma questi aspetti sono diventati particolarmente rilevanti con i nuovi standard sulla sicurezza funzionale.



Azionamenti di sicurezza con arresto di emergenza di Categoria 3

Questo è un circuito di Categoria 3 che usa un inverter di sicurezza. Con i recenti sviluppi delle tecnologie di azionamento, unitamente all'aggiornamento degli standard EN/IEC 60204-1 e NFPA 79, è possibile usare gli inverter di sicurezza nei circuiti di arresto di emergenza, senza bisogno di un sezionatore elettromeccanico dell'attuatore (ad es. il motore).

Premendo il pulsante di emergenza si aprono le uscite dell'MSR. Questo invia un segnale di arresto all'inverter, rimuove il segnale di abilitazione e interrompe l'alimentazione del controllo di gate. L'inverter esegue un arresto di Categoria 0 – immediato scollegamento dell'alimentazione al motore. Questa funzione è conosciuta con il termine di "Safe Torque Off". L'inverter raggiunge la Categoria 3 perché ha segnali ridondanti per togliere alimentazione al motore: il segnale di abilitazione e un relè a guida forzata. Il relè a guida forzata fornisce all'attuatore il feedback ragionevolmente praticabile. Lo stesso inverter viene analizzato per determinare che un singolo guasto non comporti la perdita della funzione di sicurezza.

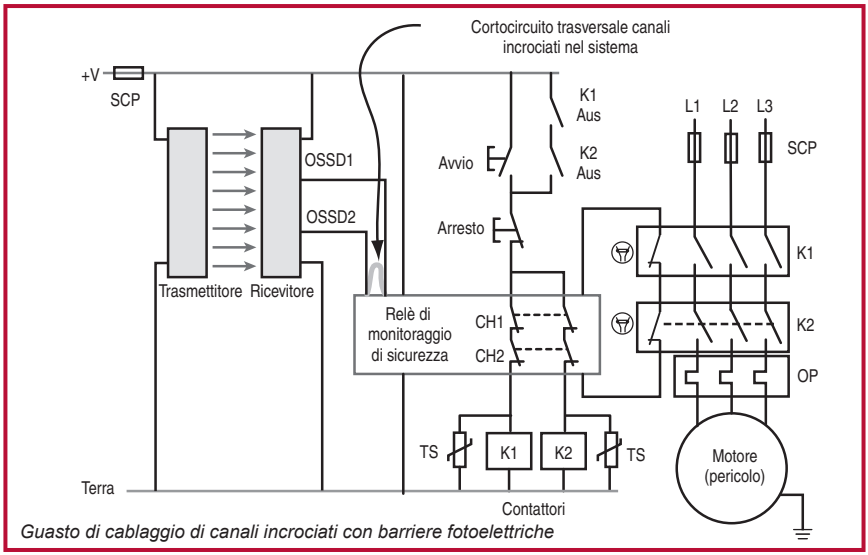


Esempio di guasto di cablaggio

Questo è un esempio di un guasto di cablaggio, un cortocircuito tra l'uscita di sicurezza del Canale 2 MSR e la bobina del contattore K1. Tutti i componenti stanno funzionando correttamente. Questo guasto di cablaggio può verificarsi prima della messa in servizio della macchina o successivamente, durante le operazioni di manutenzione o aggiornamento.

Il guasto può essere rilevato?

Questo guasto non può essere rilevato dal sistema di sicurezza come mostrato. Fortunatamente, di per sé non comporta la perdita della funzione di sicurezza. Questo guasto, come il guasto da Ch1 a K2, deve essere rilevato durante la messa in servizio o controlli successivi agli interventi di manutenzione. L'elenco di possibili esclusioni dei guasti riportato in EN ISO 13849-2 Allegato D Tabella D4 chiarisce che questo tipo di guasti può essere escluso se l'apparecchiatura è contenuta in un armadio elettrico e sia l'armadio che i cablaggi risultano conformi ai requisiti dello standard IEC/EN 60204-1. Nella relazione tecnica congiunta su EN ISO 13849-1 e IEC 62061 viene inoltre chiarito che questa esclusione dei guasti può essere considerata fino a PLe e SIL3 compresi, e può essere utilizzata anche con la Categoria 4.



Guasto di cablaggio di canali incrociati con barriere fotoelettriche

Questo è un esempio di sistema di sicurezza con barriera fotoelettrica (uscite OSSD)

Il sistema di sicurezza può rilevare questo guasto?

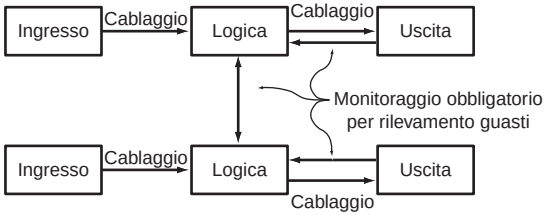
L'MSR non può rilevare questo guasto, perché entrambi gli ingressi sono in "pull up" a +V. In questo esempio, il guasto di cablaggio è rilevato dalla barriera fotoelettrica. Alcune barriere fotoelettriche usano una tecnica di rilevamento dei guasti chiamata "test a impulsi". Con queste barriere fotoelettriche, il rilevamento del guasto è immediato e la barriera fotoelettrica disattiva la sua uscita. In altre, il rilevamento avviene quando la barriera fotoelettrica è liberata. Quando la barriera fotoelettrica tenta di eccitare la sua uscita, il guasto viene rilevato e l'uscita rimane disattivata. In entrambi i casi, il pericolo rimane disattivato in presenza del guasto.

Rilevamento dei guasti mediante test a impulsi

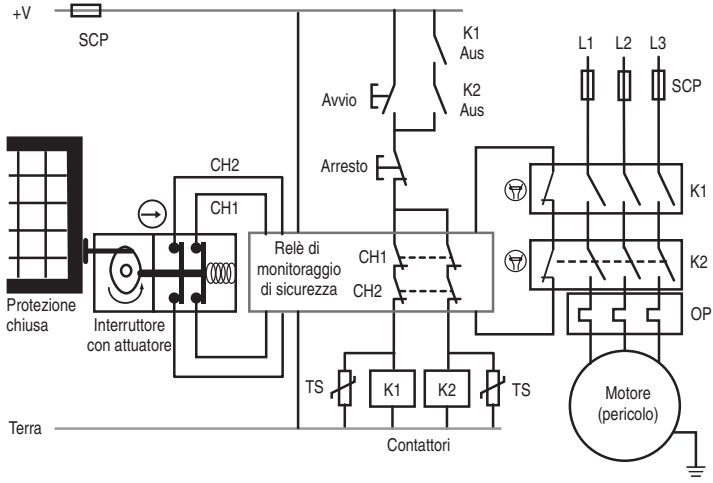
I circuiti di sicurezza sono concepiti per condurre corrente quando il sistema di sicurezza è attivo e il pericolo è protetto. Il test a impulsi è una tecnica per cui la corrente del circuito scende a zero per un periodo molto breve. La durata è troppo breve perché il circuito di sicurezza risponda e disattivi il pericolo, ma è abbastanza lunga per il rilevamento da parte di un sistema a microprocessore. Gli impulsi sui canali sono sfasati uno rispetto all'altro. Se si verifica un cortocircuito incrociato, il microprocessore rileva gli impulsi su entrambi i canali e genera un comando di disattivazione del pericolo.

Categoria 4

Come la Categoria 3, la Categoria 4 impone che il sistema di sicurezza risponda alla Categoria B, usi principi di sicurezza e realizzi la funzione di sicurezza in presenza di un singolo guasto. Diversamente dalla Categoria 3, dove un accumulo di guasti può portare alla perdita della funzione di sicurezza, la Categoria 4 richiede l'operatività della funzione di sicurezza in presenza di un accumulo di guasti. Quando si considera un accumulo di guasti, 2 guasti possono essere sufficienti anche se, per alcune configurazioni, possono essere necessari 3 guasti.



Questo è lo schema a blocchi per la Categoria 4. Il monitoraggio di entrambi i dispositivi di uscita e il monitoraggio incrociato sono requisiti essenziali, non solo quando ragionevolmente praticabile. Questo contribuisce a differenziare la Categoria 4 dalla Categoria 3.

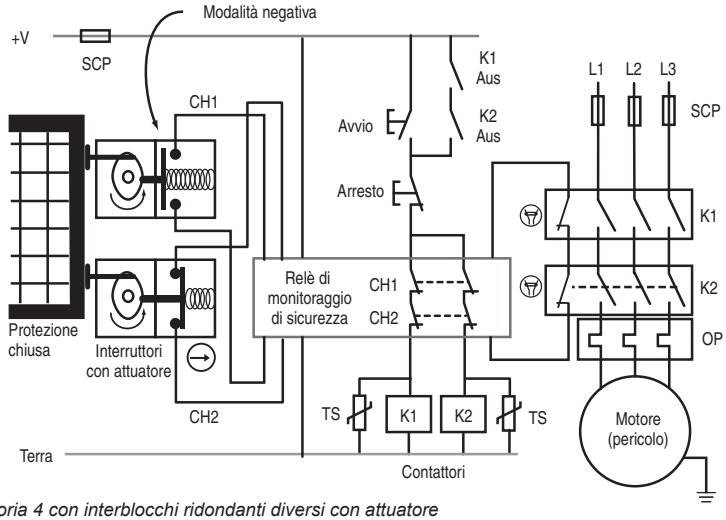


Categoria 4 con esclusione dei guasti sull'interblocco con attuatore

Questo è un esempio di circuito di Categoria 4 con esclusione dei guasti sull'interblocco con attuatore. L'esclusione dei guasti elimina la considerazione del guasto di apertura dei contatti dell'interblocco con attuatore. L'esclusione del guasto deve essere tecnicamente giustificata e documentata. Nella giustificazione, devono essere considerati velocità e allineamento dell'attuatore, arresti meccanici e protezione della testa.

Se il progettista del sistema di sicurezza preferisce usare interblocchi con attuatore e non utilizzare l'esclusione dei guasti sugli interblocchi, per rispondere alla Categoria 4 possono essere usati due interblocchi con attuatore. Lo stesso relè di monitoraggio di sicurezza deve essere classificato adatto alla Categoria 4 ed entrambi i contattori di uscita con contatti ad accoppiamento meccanico devono essere monitorati.

La diversità può essere applicata per ridurre ulteriormente la probabilità di perdita della funzione di sicurezza dovuta a guasti per causa comune o di modo comune; uno degli interruttori interbloccati con attuatore può essere convertito in modalità negativa. Un interruttore che funziona in modalità negativa è accettabile se un secondo interruttore usa contatti ad azione di apertura diretta. Lo schema che segue mostra un esempio di questo approccio di diversità. Con questo approccio, l'MSR deve essere concepito per accettare ingressi normalmente aperti e normalmente chiusi.



Categoria 4 con interblocchi ridondanti diversi con attuatore

Classificazione di sistemi e componenti

Le categorie possono esser utilizzate sia nelle classificazioni dei componenti (dispositivi) di sicurezza che nelle classificazioni dei sistemi. Questo genera un po' di confusione che può essere superata conoscendo i componenti e le loro capacità. Studiando gli esempi precedenti rileviamo che un componente come ad esempio un interruttore di interblocco attribuito alla Categoria 1 può essere utilizzato da solo in un sistema di Categoria 1, e può essere utilizzato in un sistema di Categoria 2 prevedendo un monitoraggio funzionale supplementare. Inoltre, può anche rientrare

in un sistema di Categoria 3 o 4 se due di tali componenti vengono utilizzati insieme facendo svolgere una funzione di diagnostica a un relè di monitoraggio di sicurezza.

Alcuni componenti come i relè di monitoraggio di sicurezza e i controllori di sicurezza programmabili sono dotati di diagnostica interna autonoma e sono in grado di controllarsi autonomamente per garantire prestazioni adeguate. Pertanto, possono essere classificati come componenti di sicurezza conformi ai requisiti previsti per le Categorie 2, 3 e 4 senza adottare altre misure.

Considerazione ed esclusione dei guasti

La valutazione della sicurezza richiede una ampia analisi dei guasti e una perfetta comprensione della funzionalità del sistema di sicurezza in presenza di guasti. ISO 13849-1 e ISO 13849-2 forniscono dettagli sulla considerazione e l'esclusione dei guasti.

Se un guasto comporta il guasto di un componente successivo, esso deve essere considerato, insieme a tutti quelli successivi, come un unico guasto.

Se due o più guasti avvengono come risultato di una singola causa, devono essere considerati come un unico guasto. Questo è ciò che si definisce "guasto per causa comune".

Il verificarsi simultaneo di due o più guasti è considerato altamente improbabile e non è affrontato in questa analisi. Il presupposto di base è che si verifichi un solo un guasto tra le richieste di intervento della funzione di sicurezza, a patto che i periodi tra l'utilizzo della funzione non siano eccessivamente lunghi.

Esclusioni dei guasti

Lo standard EN 954-1 in via di dismissione, e i più recenti EN ISO 13849-1 e IEC 62061 consentono tutti di utilizzare le esclusioni dei guasti nella determinazione della classificazione di un sistema di sicurezza, a patto che possa essere dimostrato che il guasto è altamente improbabile. Se si utilizzano le esclusioni dei guasti, è importante che vengano giustificate correttamente e che siano valide per la durata prevista del sistema di sicurezza. Più è alto il livello di rischio coperto dal sistema di sicurezza, tanto più rigorosa dovrà essere la giustificazione richiesta per l'esclusione del guasto. Ciò ha sempre provocato una certa confusione in merito alle tipologie di esclusioni dei guasti che possono essere utilizzate o meno. Come abbiamo già osservato in questo capitolo, gli standard e i documenti di riferimento più recenti hanno chiarito alcuni aspetti di questo problema.

In generale, quando si richiede il livello PLe o SIL3 per l'implementazione di una funzione di sicurezza da parte di un sistema di sicurezza, di norma le esclusioni dei guasti non sono considerate sufficienti per raggiungere tale livello prestazionale. Ciò dipende dalla tecnologia impiegata e dall'ambiente operativo previsto. Pertanto il progettista deve prestare molta attenzione all'uso delle esclusioni dei guasti all'aumentare dei livelli PL o SIL richiesti. Ad esempio le esclusioni dei guasti non sono applicabili agli aspetti meccanici degli interruttori di posizione elettromeccanici

e degli interruttori ad azionamento manuale (ad es. un dispositivo di arresto di emergenza) per conseguire il livello PLe o SIL3. Le esclusioni dei guasti applicabili a specifiche condizioni di guasto meccaniche (es. usura/corrosione, rottura) sono indicate nella Tabella A.4 di ISO 13849-2. Pertanto, nel caso di un sistema di interblocco di una protezione che deve raggiungere il livello PLe o SIL3 si dovrà prevedere una tolleranza ai guasti minima pari a 1 (ad esempio con due interruttori di posizione meccanici di tipo tradizionale) per ottenere tale livello prestazionale, dal momento che normalmente non è possibile giustificare l'esclusione di guasti come la rottura degli attuatori degli interruttori. Tuttavia, in un pannello di controllo progettato in conformità con standard pertinenti, potrebbe anche essere accettabile escludere i guasti come i cortocircuiti dei cablaggi.

La nuova versione rivista dello standard EN ISO 13849-2 in via di pubblicazione conterrà ulteriori informazioni sull'uso delle esclusioni dei guasti.

Categorie di arresto secondo IEC/EN 60204-1 e NFPA 79

Il fatto che il termine "Categoria" venga utilizzato con due accezioni diverse in relazione ai sistemi di controllo relativi alla sicurezza è fonte di confusione. Finora abbiamo preso in esame le categorie derivanti dallo standard EN 954-1, che sono una classificazione delle prestazioni di un sistema di sicurezza in condizioni di guasto.

Ma esiste anche una classificazione basata sulle cosiddette "Categorie di arresto" che deriva dagli standard IEC/EN 60204-1 e NFPA 79. Esistono tre categorie di arresto.

La **Categoria di arresto 0** richiede lo scollegamento immediato dell'alimentazione agli attuatori. In questo caso talvolta si parla di arresto incontrollato, poiché, in determinate circostanze, l'arresto del movimento può richiedere un po' di tempo, in quanto il motore potrebbe essere lasciato libero di arrestarsi per inerzia.

La **Categoria di arresto 1** impone che l'alimentazione rimanga attiva per poter frenare fino all'arresto, dopodiché si potrà scollegare l'alimentazione agli attuatori.

La **Categoria di arresto 2** ammette che non si debba scollegare l'alimentazione agli attuatori.

Si noti che solo le Categorie di arresto 0 e 1 possono essere utilizzate come arresti di emergenza. La scelta della categoria da utilizzare tra le due deve essere basata su una valutazione dei rischi.

In tutti gli esempi di circuito illustrati finora in questo capitolo è stata utilizzata la Categoria di arresto 0. Per ottenere una Categoria di arresto 1 è necessaria un'uscita temporizzata per la disattivazione finale dell'alimentazione. Un arresto di Categoria 1 è spesso associato a una protezione interbloccata con blocco della protezione. Questo fa sì che la protezione rimanga bloccata in posizione di chiusura fino a quando la macchina raggiunge uno stato di sicurezza (arresto).

Arrestare una macchina senza tener conto del controllore programmabile può influire sul riavviamento e potrebbe essere causa di gravi danni agli utensili e alla macchina. Per l'arresto di sicurezza, non ci si può affidare a un PLC standard (non di sicurezza) e, quindi, devono essere considerati altri approcci.

Di seguito sono riportate due possibili soluzioni:

1. Relè di sicurezza con comando di override temporizzato

Si utilizza un relè di sicurezza sia con uscite ad azione immediata che con uscite ad azione ritardata. Le uscite ad azione immediata sono collegate a ingressi del dispositivo programmabile (ad esempio un PLC) e le uscite ad azione ritardata sono collegate al contattore. Quando l'interruttore di interblocco della protezione è attivato, le uscite immediate del relè di sicurezza commutano. Questo segnala al sistema programmabile di eseguire un arresto secondo la sequenza corretta. Dopo un periodo di tempo breve ma sufficiente per l'esecuzione del processo, l'uscita ad azione ritardata del relè di sicurezza scatta e isola il contattore principale.

Nota: tutti i calcoli che servono a determinare il periodo di arresto totale devono prendere in considerazione il ritardo di uscita del relè di sicurezza. Ciò è particolarmente importante quando questo fattore viene usato per determinare il posizionamento dei dispositivi in conformità con il calcolo della distanza di sicurezza.

2. PLC di sicurezza

Le funzioni logiche e di temporizzazione richieste possono essere implementate in modo pratico utilizzando un PLC (di sicurezza) con livello di integrità della sicurezza appropriato. Nella pratica, ciò si può ottenere con un PLC di sicurezza come SmartGuard o GuardLogix.

Requisiti dei sistemi di controllo di sicurezza USA

Negli USA esiste tutta una serie di standard sui requisiti dei sistemi di controllo legati alla sicurezza, ma due sono i documenti più importanti: ANSI B11.TR3 e ANSI R15.06. Il rapporto tecnico ANSI B11.TR3 stabilisce quattro livelli caratterizzati dal livello previsto di riduzione dei rischi che ognuno può fornire. Ecco i requisiti per ogni livello.

Livello minimo di riduzione dei rischi

In ANSI B11.TR3, tra le protezioni che forniscono il minimo grado di riduzione dei rischi ci sono dispositivi elettrici, elettronici, idraulici o pneumatici e relativi sistemi di controllo con configurazione a canale singolo. Implicita nei requisiti è l'esigenza di usare dispositivi di sicurezza. Questo livello è strettamente allineato con la Categoria 1 di ISO 13849-1.

Livello medio/basso di riduzione dei rischi

In ANSI B11.TR3, le protezioni di sicurezza che offrono una riduzione dei rischi medio/bassa includono i sistemi di controllo ridondanti che possono essere controllati manualmente per verificare la funzionalità del sistema di sicurezza. Facendo esclusivamente riferimento ai requisiti, il sistema prevede una ridondanza semplice. L'uso di una funzione di controllo non è richiesta. Senza controllo, l'eventuale guasto di uno dei componenti di sicurezza ridondanti potrebbe non essere rilevato dal sistema di sicurezza. Ciò risulterebbe in un sistema a singolo canale. Questo livello di riduzione dei rischi si allinea meglio con la Categoria 2 in associazione al controllo.

Livello medio/alto di riduzione dei rischi

Le protezioni di sicurezza che, per ANSI B11.TR3, forniscono una riduzione dei rischi medio/alta includono sistemi di controllo con ridondanza e autodiagnostica all'avviamento, per confermare la funzionalità del sistema di sicurezza. Per le macchine che vengono avviate ogni giorno, l'autodiagnostica rappresenta un significativo miglioramento dell'integrità della sicurezza rispetto a un sistema puramente ridondante. Per le macchine che funzionano 24 ore al giorno, 7 giorni su 7, l'autodiagnostica nella migliore delle ipotesi è un miglioramento marginale. Con il monitoraggio periodico del sistema di sicurezza, si allinea con la Categoria 3.

Livello massimo di riduzione dei rischi

ANSI B11.TR3 identifica la più alta riduzione dei rischi con sistemi di controllo ridondanti e con autodiagnostica continua. L'autodiagnostica deve verificare la funzionalità del sistema di sicurezza. L'obiettivo, per il progettista del sistema di sicurezza, è determinare che cosa si intende per "autodiagnostica continua". Molti sistemi di sicurezza effettuano i loro controlli all'avviamento e in presenza di una richiesta di intervento al sistema di sicurezza.

Alcuni componenti, d'altra parte, effettuano una autodiagnostica continua. Le barriere fotoelettriche, per esempio, accendono e spengono sequenzialmente i loro LED. Se si verifica un guasto, la barriera fotoelettrica disattiva le sue uscite, prima della richiesta di intervento al sistema di sicurezza, dato che esso si controlla continuamente. I PLC di sicurezza e i relè a microprocessore sono altri componenti che effettuano autodiagnostica continua.

Il requisito del sistema di controllo riguardante l'autodiagnostica "continua" non vuole limitare la selezione dei componenti a barriere fotoelettriche e unità logiche a microprocessore. Il controllo dovrebbe essere realizzato all'avviamento e dopo ogni richiesta di intervento al sistema di sicurezza. Questo livello di riduzione dei rischi vuole essere in linea con la Categoria 4 di ISO 13849-1.

Standard per i robot: Stati Uniti/Canada

Gli standard per i robot negli USA (ANSI RIA R15.06) e in Canada (CSA Z434-03) sono piuttosto simili. Entrambi prevedono quattro livelli, simili alle categorie di EN 954-1:1996, descritte di seguito.

Semplice

Al livello più basso, semplici sistemi di controllo di sicurezza devono essere progettati e costruiti con circuiteria approvata a canale singolo e questi sistemi possono essere programmabili. In Canada, questo livello è ulteriormente limitato esclusivamente ad attività di segnalazione e annuncio. Per il progettista del sistema di sicurezza, il punto è determinare che cosa è “approvato”. Che cos’è un circuito a singolo canale approvato? E da chi il sistema è approvato? La categoria semplice è strettamente allineata con la Categoria B di EN 954-1:1996.

Canale singolo

Il livello successivo è il sistema di controllo di sicurezza a canale singolo che:

- è basato su hardware o è un dispositivo software/firmware di sicurezza
- integra componenti di sicurezza; e
- è utilizzato secondo le raccomandazioni dei produttori e
- usa configurazioni di circuito comprovate.

Un esempio di “configurazione di circuito comprovata” è un dispositivo elettromeccanico, ad apertura positiva e a singolo canale, che segnala un arresto in stato di diseccitazione. Trattandosi di un sistema a canale singolo, il guasto di un singolo componente può comportare la perdita della funzione di sicurezza. La categoria Semplice è strettamente allineata con la Categoria 1 di EN 9541:1996.

Dispositivi software/firmware di sicurezza

Sebbene i sistemi hardware siano stati il metodo preferito per la protezione di sicurezza dei robot, i dispositivi software/firmware si stanno affermando sempre maggiormente grazie alla loro capacità di gestire sistemi complessi. I dispositivi software/firmware (PLC o controllori di sicurezza) sono ammessi purché siano di sicurezza. Questa classificazione impone che un singolo guasto del firmware o di un componente di sicurezza non comporti la perdita della funzione di sicurezza. Quando il guasto viene rilevato, il successivo funzionamento automatico del robot viene impedito fino alla cancellazione del guasto.

Per ottenere una classificazione di sicurezza, il dispositivo software/firmware deve essere testato, in base a uno standard approvato, da un laboratorio certificato. Negli USA, l'OSHA mantiene aggiornata una lista dei laboratori di prova riconosciuti a livello nazionale (NRTL). In Canada, lo Standard Council of Canada (SCC) dispone di una lista simile.

Singolo canale con monitoraggio

I sistemi di controllo di sicurezza a singolo canale con monitoraggio devono rispettare tutti i requisiti richiesti per il singolo canale, essere di sicurezza e avere funzionalità di controllo. Il controllo delle funzioni di sicurezza deve essere effettuato all'avviamento della macchina e, periodicamente, durante il funzionamento. Il controllo automatico è preferibile a quello manuale.

L'operazione di controllo permette il funzionamento se non viene rilevato alcun guasto o genera un segnale di arresto se il guasto viene rilevato. Eventuali pericoli persistenti dopo la cessazione del movimento devono essere segnalati. Naturalmente, il controllo stesso non deve provocare una situazione pericolosa. Dopo il rilevamento del guasto, il robot deve rimanere in stato di sicurezza fino alla correzione del guasto. La categoria Singolo canale con monitoraggio è strettamente allineata con la Categoria 2 di EN 954-1:1996.

Controllo affidabile

Il più alto livello di riduzione dei rischi negli standard per i robot statunitensi e canadesi si ottiene attraverso sistemi di controllo di sicurezza conformi ai requisiti della tipologia "a controllo affidabile". I sistemi di controllo di sicurezza a controllo affidabile sono architetture a due canali con monitoraggio. La funzione di arresto del robot non deve essere impedita dal guasto di alcun singolo componente, neanche dalla funzione di monitoraggio.

Al rilevamento di un guasto, il monitoraggio deve generare un comando di arresto. Eventuali pericoli persistenti dopo la cessazione del movimento devono essere segnalati. Il sistema di sicurezza deve rimanere in stato di sicurezza fino alla correzione del guasto. Preferibilmente, il guasto deve essere rilevato immediatamente. Se ciò non è possibile, deve essere rilevato alla successiva richiesta di intervento al sistema di sicurezza. Se c'è una significativa probabilità che possano verificarsi, i guasti per causa comune devono essere considerati.

I requisiti canadesi differiscono dai requisiti USA per l'aggiunta di due ulteriori requisiti. Primo, i sistemi di controllo di sicurezza devono essere indipendenti dai

normali sistemi di controllo di programma. Secondo, il sistema di sicurezza non deve essere facilmente escluso o bypassato senza rilevamento.

I sistemi a controllo affidabile sono in linea con le Categorie 3 e 4 di EN 954-1:1996.

Note sui sistemi a controllo affidabile

L'aspetto fondamentale dei sistemi a controllo affidabile è la tolleranza al singolo guasto. I requisiti stabiliscono come il sistema di sicurezza deve rispondere in presenza di "un singolo guasto", di "qualunque singolo guasto" o di "qualunque guasto di un singolo componente".

Riguardo ai guasti, devono essere considerati tre concetti molto importanti: (1) non tutti i guasti sono rilevati, (2) l'aggiunta della parola "componente" implica problematiche di cablaggio, (3) il cablaggio è parte integrante del sistema di sicurezza. I guasti di cablaggio possono provocare la perdita di una funzione di sicurezza.

L'intento dell'affidabilità del controllo è chiaramente l'operatività della funzione di sicurezza in presenza di un guasto. Se il guasto viene rilevato, il sistema di sicurezza deve eseguire una azione sicura, segnalare il guasto e impedire l'ulteriore funzionamento della macchina fino alla correzione del guasto. Se il guasto non viene rilevato, la funzione di sicurezza deve, su richiesta, poter essere eseguita.

Esempio applicativo con SISTEMA

Questo esempio pratico illustra le procedure di cablaggio, configurazione e programmazione di un controllore di automazione programmabile (PAC) Compact GuardLogix e I/O PointGuard per il monitoraggio di un sistema di sicurezza a due zone. Ogni zona comprende un interruttore di interblocco di sicurezza singolo che, quando viene azionato, segnala la disattivazione dell'alimentazione da una coppia di contattori ridondanti relativi a tale zona. Questa configurazione è replicata nella seconda zona. Le due zone, inoltre, sono protette da un arresto di emergenza globale che, all'attivazione, segnala lo spegnimento sicuro di entrambe le zone.

Nota: questo esempio è riportato esclusivamente a titolo illustrativo. A causa delle molteplici variabili e dei requisiti associati a ogni installazione specifica, Rockwell Automation non può assumersi alcuna responsabilità per un uso basato su questo esempio.

Caratteristiche e vantaggi

- Compact GuardLogix consente di gestire sia applicazioni standard che di sicurezza in un unico controllore.
- È possibile combinare I/O standard e di sicurezza sulla stessa scheda Ethernet.
- Lo stato di sicurezza e la diagnostica possono essere trasferiti facilmente dall'applicazione di sicurezza all'applicazione standard per la visualizzazione sull'interfaccia operatore e trasferiti in remoto ad altri dispositivi collegati attraverso la rete Ethernet.
- L'applicazione qui descritta può essere ampliata e incorporata nell'applicazione specifica del cliente.

Descrizione

Questa applicazione permette di monitorare due zone. Ciascuna zona è protetta da un interruttore di sicurezza SensaGuard. Se uno dei due gate viene aperto, i contattori di uscita vengono diseccitati, determinando lo spegnimento delle macchine associate a tale zona. Il reset è manuale. Le due zone, inoltre, sono protette da un interruttore di arresto di emergenza globale. All'azionamento dell'arresto di emergenza, i due set di contattori vengono diseccitati.

Funzione di sicurezza

Ciascun interruttore di sicurezza SensaGuard è collegato a una coppia di ingressi di sicurezza di un modulo 1734-IB8S (I/O POINTGuard). Il modulo I/O è connesso tramite CIP Safety su una rete EtherNet/IP al controllore di sicurezza Compact GuardLogix (1768-L43S). Il codice di sicurezza del processore di sicurezza monitora lo stato degli ingressi di sicurezza tramite un'istruzione di sicurezza precertificata detta DCS (Dual Channel Input Stop). Il codice di sicurezza è eseguito in parallelo in una configurazione 1oo2. Quando tutte le condizioni sono soddisfatte, il gate

di sicurezza è chiuso, non sono rilevati guasti sui moduli di ingresso, l'arresto di emergenza globale non è azionato e il pulsante di reset è premuto, un secondo blocco funzione certificato detto CROUT (Configurable Redundant Output) verifica lo stato dei dispositivi di controllo finali, una coppia di contattori ridondanti 100S. Il controllore quindi emette un segnale d'uscita verso il modulo 1734-OBS determinando l'attivazione di una coppia di uscite in modo da eccitare i contattori di sicurezza. La funzione di arresto di emergenza globale è anche monitorata da un'istruzione DCS. Se viene azionato, l'arresto di emergenza globale determina lo spegnimento di entrambe le zone.

Distinta dei materiali

In questo esempio applicativo sono utilizzati i componenti elencati di seguito.

Numero di catalogo	Descrizione	Quantità
440N-Z21SS2A	Interruttore SensaGuard RFP in plastica senza contatto	2
800FM-G611MX10	Pulsante di reset 800F – Metallo, con protezione, blu, R, portacontatti in metallo, 1 contatto/i N.A., Standard	4
100S-C09ZJ23C	Serie 100S-C – Contattori di sicurezza	2
1768-ENBT	Modulo ponte EtherNet/IP CompactLogix	1
1768-L43S	Processore CompactLogix L43, memoria standard 2,0 MB, memoria di sicurezza 0,5 MB	1
1768-PA3	Alimentatore, ingresso 120/240 V CA, 3,5 A a 24 V CC	1
1769-ECR	Terminazione destra	1
1734-AENT	Scheda Ethernet 24 V CC	1
1734-TB	Base modulo con morsetti a vite IEC rimovibili	4
1734-IB8S	Modulo di ingresso di sicurezza	2
1734-OB8S	Modulo d'uscita di sicurezza	1
1783-US05T	Switch Ethernet non gestito Stratix 2000	1

Configurazione e cablaggio

Per informazioni dettagliate sull'installazione e il cablaggio, consultare i manuali forniti insieme ai prodotti, oppure scaricarli dal sito http://literature.rockwellautomation.com

Cenni generali sul sistema

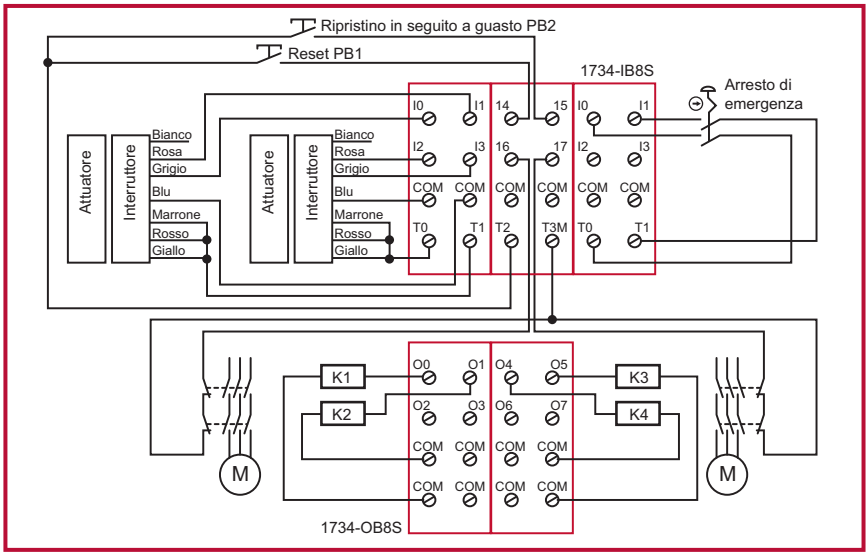
Il modulo d'ingresso 1734-IB8S monitora gli ingressi dei due interruttori SensaGuard.

Sensaguard utilizza le uscite OSSD che eseguono test periodici sulle uscite. In questo modo, sono le uscite OSSD che verificano l'integrità del cablaggio tra l'interruttore SensaGuard e gli ingressi di sicurezza.

Le uscite a impulsi di prova sono configurate come sorgenti a 24 V.

Il dispositivo di controllo finale è costituito da una coppia di contattori di sicurezza 100S, K1 e K2. I contattori sono controllati dal modulo d'uscita di sicurezza 1734-OBS. Questi ultimi sono cablati in una configurazione ridondante e vengono testati all'avviamento per ricercare eventuali guasti. Il test all'avviamento viene eseguito monitorando il circuito di feedback sull'ingresso 2 (I2), prima che i contattori siano eccitati. Ciò avviene tramite un'istruzione CROUT (Configurable Redundant Output). Il sistema viene resettato dal pulsante instabile PB1.

Cablaggio



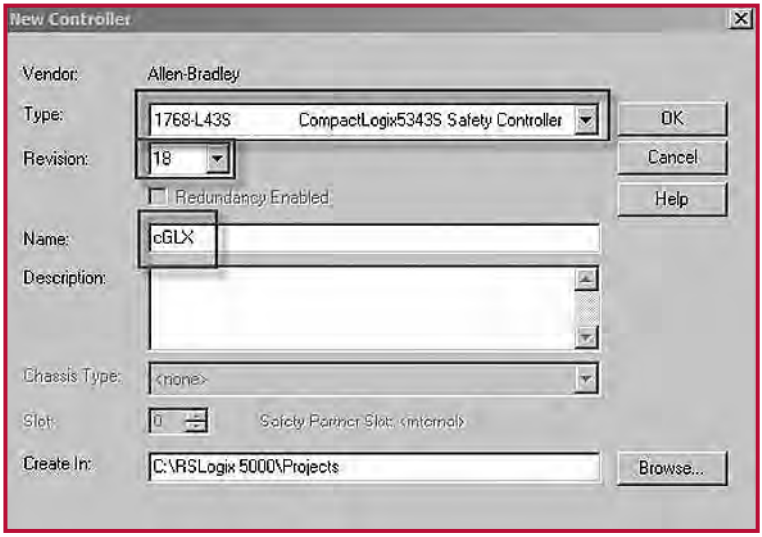
Configurazione

Per la configurazione del controllore Compact GuardLogix si utilizza RSLogix 5000, versione 18 o successive. Occorre creare un nuovo progetto e aggiungere i moduli I/O, dopodiché si configurano i moduli I/O in base ai tipi corretti di ingressi e uscite. In questo documento non è possibile fornire una descrizione dettagliata di tutte le fasi. La descrizione presuppone una conoscenza di base dell'ambiente di programmazione RSLogix.

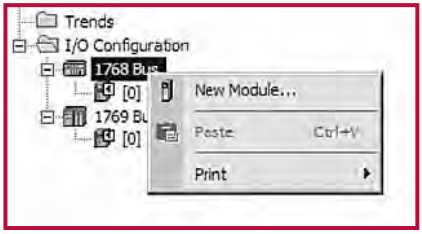
Configurazione del controllore e dei moduli I/O aggiuntivi

Attenersi alla seguente procedura.

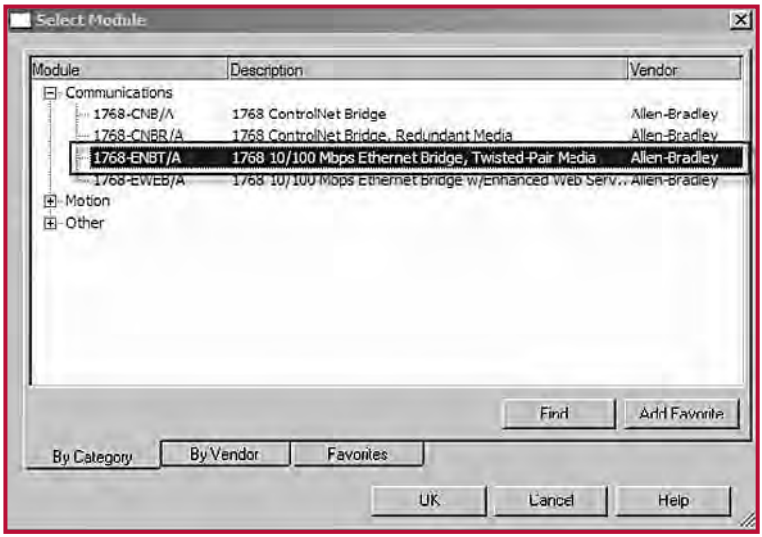
1. Nel software RSLogix 5000, creare un nuovo progetto.



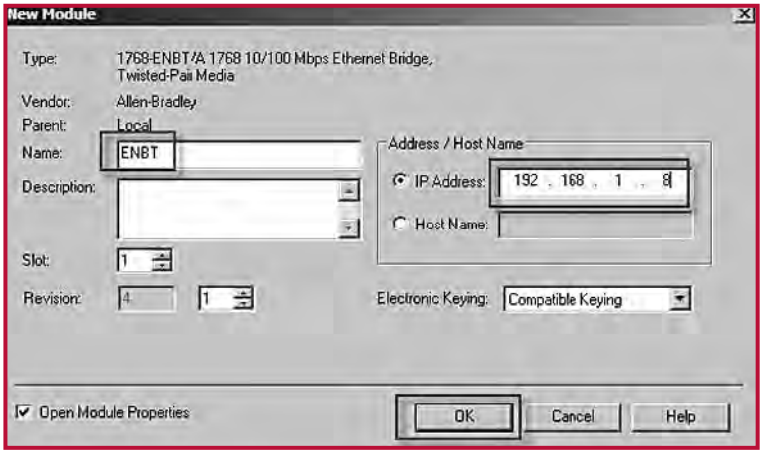
2. Nell'Organizer del controllore, aggiungere il modulo 1768-ENBT alla sbarra 1768.



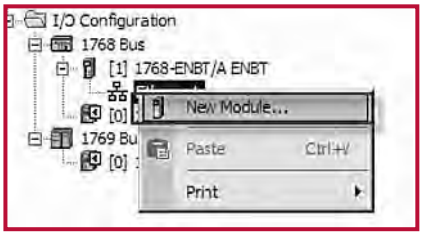
3. Selezionare il modulo 1768-ENBT e fare clic su OK.



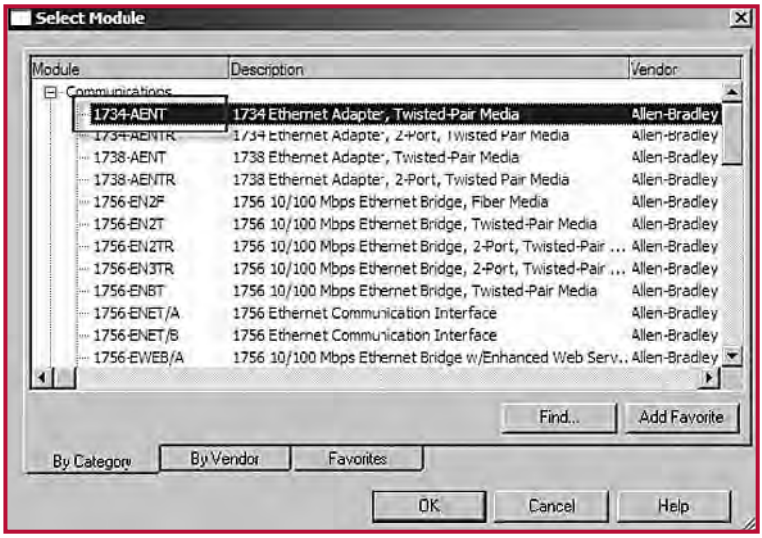
4. Nominare il modulo, digitare il relativo indirizzo IP, quindi fare clic su OK. In questo esempio è stato utilizzato l'indirizzo 192.168.1.8. L'indirizzo dell'utente può essere diverso.



5. Aggiungere la scheda 1734-AENT facendo clic con il pulsante destro del mouse sul modulo 1768-ENBT nell'Organizer del controllore e selezionare New Module.

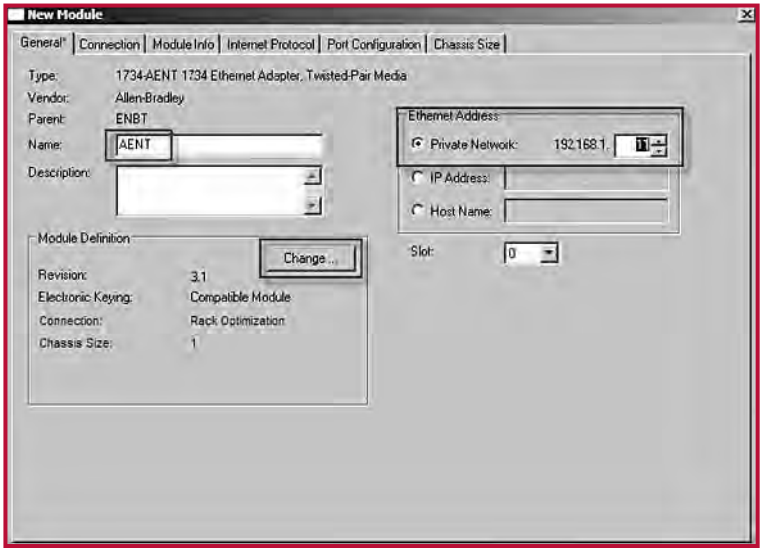


6. Selezionare la scheda 1734-ENBT e fare clic su OK.



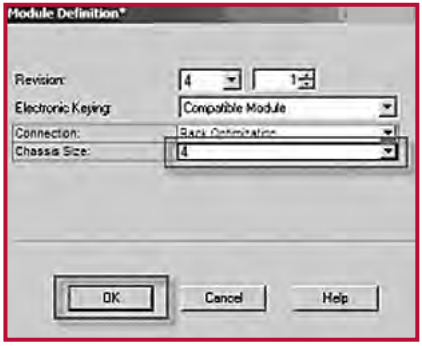
7. Nominare il modulo, digitare il relativo indirizzo IP, quindi fare clic su OK. In questo esempio è stato utilizzato l'indirizzo 192.168.1.11. L'indirizzo dell'utente può essere diverso.

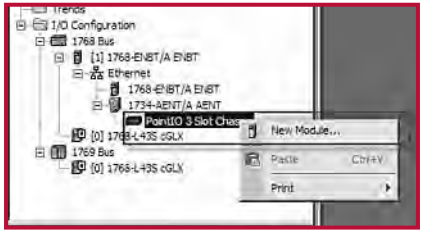
8. Fare clic su Change.



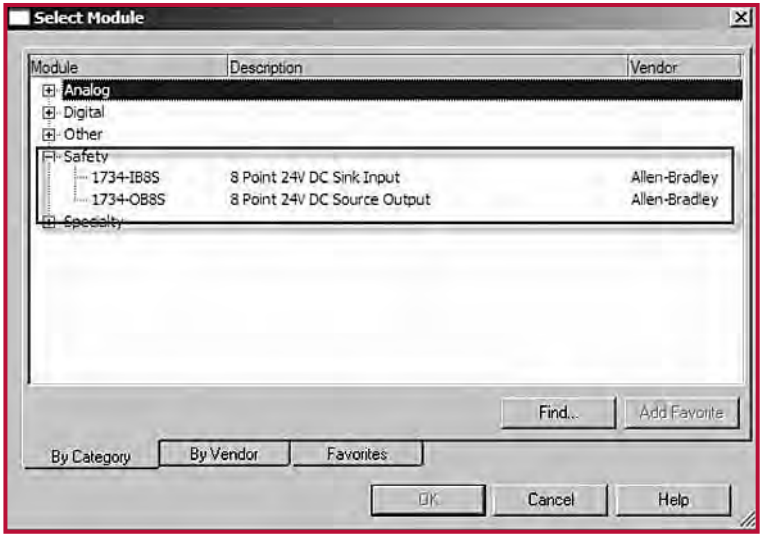
9. Impostare la dimensione dello chassis 4 per la scheda 1734-AENT e fare clic su OK. La dimensione dello chassis è data dal numero di moduli che vi verranno inseriti. Si suppone che la scheda 1734-AENT si trovi nello slot 0, pertanto, nel caso di due moduli di ingresso e un modulo di uscita, lo chassis ha una dimensione pari a 4.

10. Nell'Organizer del controllore, fare clic con il pulsante destro del mouse sulla scheda 1734-AENT e scegliere New Module.

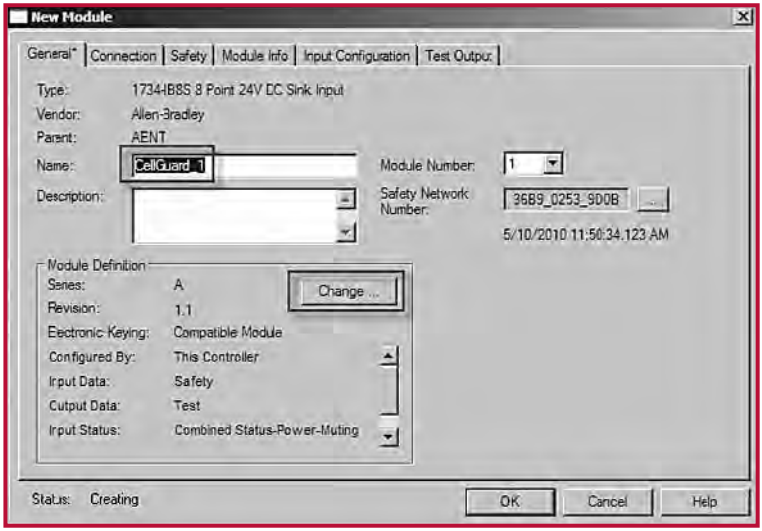




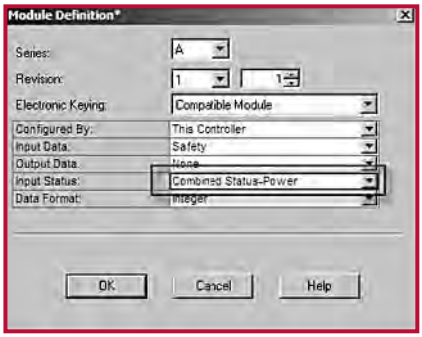
11. Espandere Safety, selezionare il modulo 1734-IB8S, quindi fare clic su OK.



12. Nella finestra di dialogo New Module, nominare il dispositivo “CellGuard_1”, quindi fare clic su Change.



13. Quando si aprirà la finestra di dialogo Module Definition, impostare Input Status su Combined Status-Power, quindi fare clic su OK.



14. Chiudere la finestra di dialogo Module Properties facendo clic su OK.

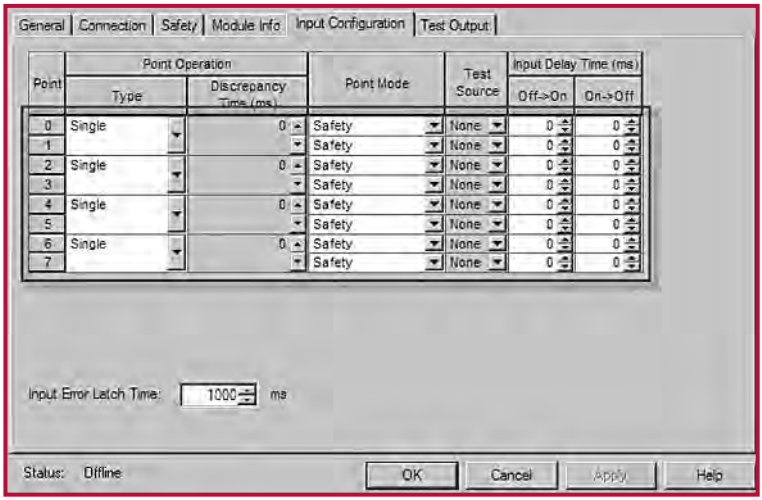
15. Ripetere i passaggi 10 – 14 per aggiungere un secondo modulo d'ingresso di sicurezza 1734-IB8S e un modulo di uscita di sicurezza 1734-OB8S.

Configurazione dei moduli I/O

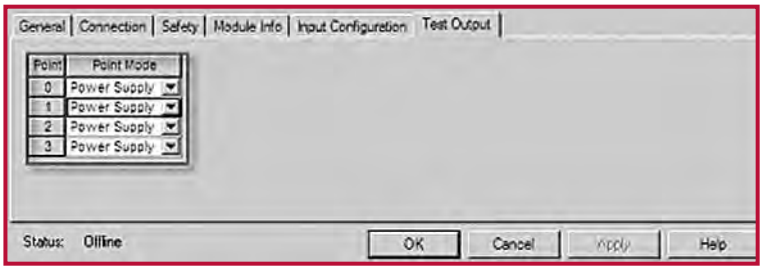
Per configurare i moduli POINT Guard I/O, attenersi alla seguente procedura.

1. Nell'Organizer del controllore, fare clic con il pulsante destro del mouse su un modulo 1734-IB8S e scegliere Properties.

2. Fare clic su Input Configuration e configurare il modulo come indicato in figura.



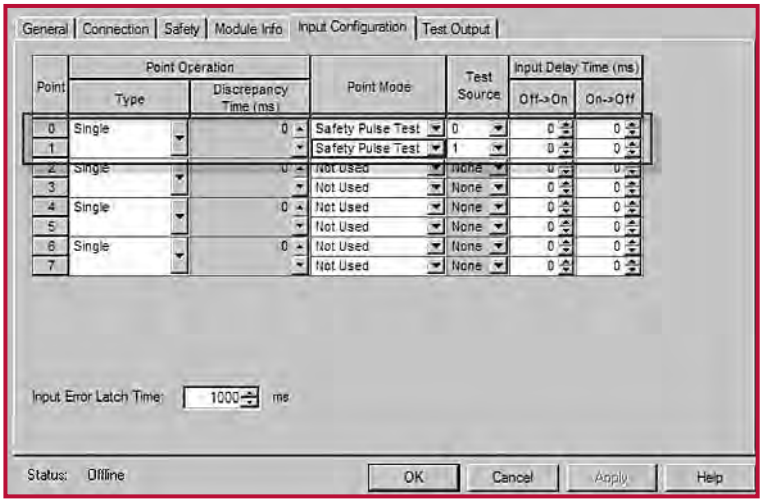
3. Fare clic su Test Output e configurare il modulo come indicato in figura.



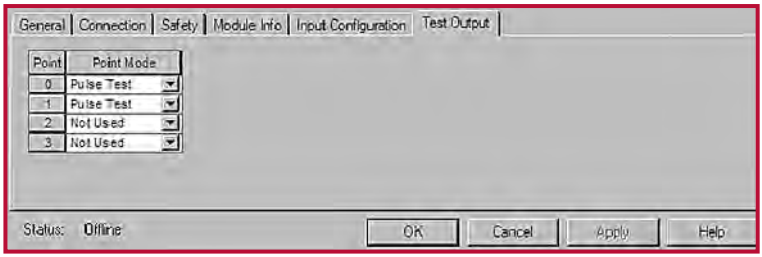
4. Fare clic su OK.

5. Nell'Organizer del controllore, fare clic con il pulsante destro del mouse sul secondo modulo 1734-IB8S e scegliere Properties.

6. Fare clic su Input Configuration e configurare il modulo come indicato in figura.



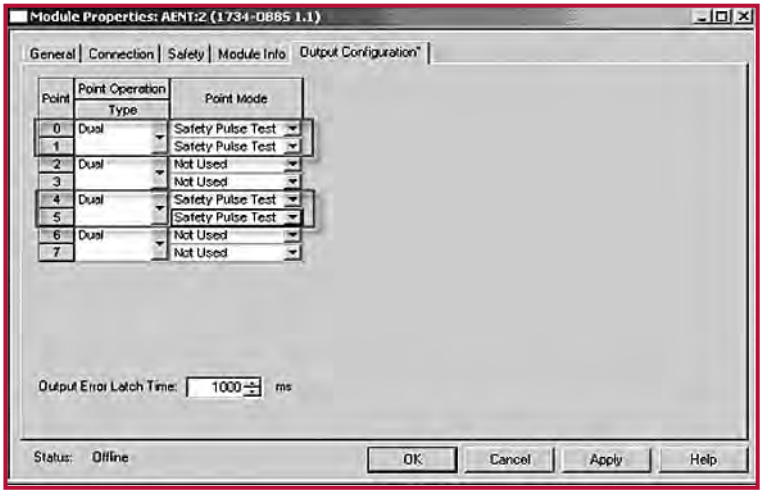
7. Fare clic su Test Output e configurare il modulo come indicato in figura.



8. Fare clic su OK.

9. Nell'Organizer del controllore, fare clic con il pulsante destro del mouse sul modulo 1734-OB8S e scegliere Properties.

10. Fare clic su Output Configuration e configurare il modulo come indicato in figura.

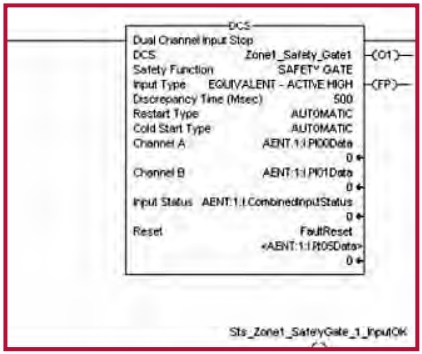


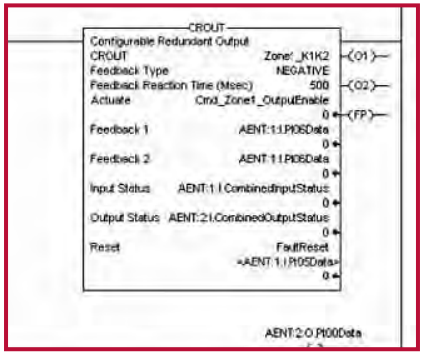
11. Fare clic su OK.

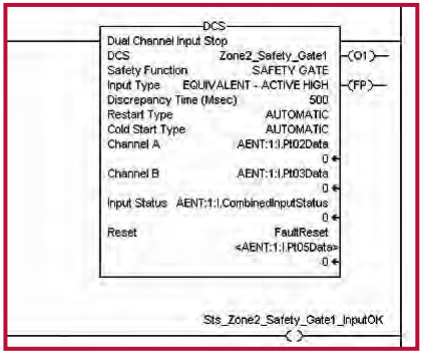
Programmazione

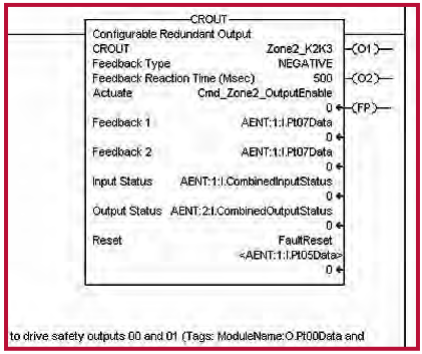
L'istruzione DCS (Dual Channel Input Stop) monitora i dispositivi di sicurezza a doppio ingresso, la cui funzione principale è quella di arrestare una macchina in sicurezza. Ad esempio, rientrano in questa categoria gli arresti di emergenza, le barriere fotoelettriche o i gate di sicurezza. Questa istruzione può solo eccitare l'Uscita 1 quando i due ingressi di sicurezza, Canale A e Canale B, sono in stato attivo, determinato dal parametro Input Type, e se sono state eseguite le azioni di reset corrette. L'istruzione DCS verifica la coerenza dei canali a doppio ingresso (Equivalent – Active High) e rileva i guasti e interviene in caso di rilevamento di un'incoerenza per un tempo superiore al tempo di discrepanza configurato (Discrepancy Time – ms). L'istruzione CROUT (Configurable Redundant Output) controlla e monitora le uscite ridondanti. Il tempo di reazione per il feedback relativo alle uscite è configurabile. L'istruzione supporta segnali di feedback positivi e negativi.

Il codice applicativo di sicurezza della routine di uscita di sicurezza impedisce che le uscite vengano riavviate in caso di reset automatico del canale d'ingresso, svolgendo il ruolo di funzionalità di anti-tiedown del reset del circuito.



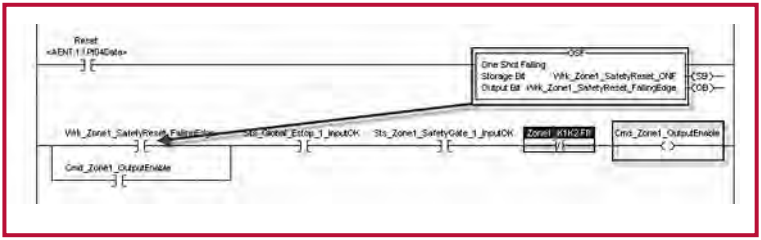






Reset su fronte di discesa

Lo standard EN ISO 13849-1 stabilisce che le funzioni di reset delle istruzioni siano collocate in corrispondenza dei fronti di discesa dei segnali. Per ottemperare a questo requisito, occorre aggiungere un'istruzione one shot sul fronte di discesa nel codice di reset, come mostrato di seguito.



Dati prestazionali

Se la configurazione è eseguita correttamente, ciascuna funzione di sicurezza può raggiungere un livello di sicurezza pari a PLe, CAT 4 secondo EN ISO 13849.1 2008.

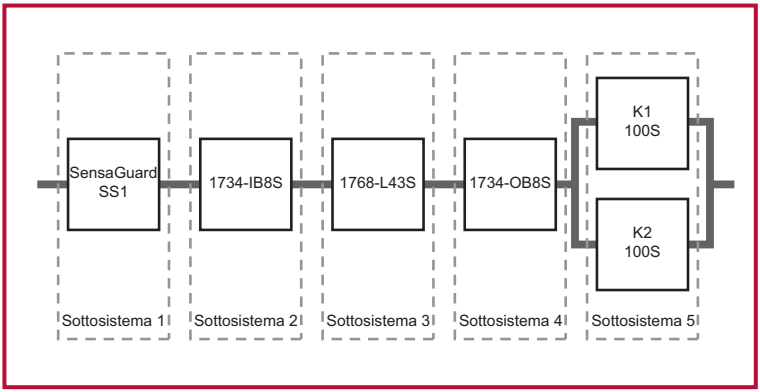
I calcoli vengono eseguiti considerando 360 giorni di funzionamento l'anno per 16 ore al giorno, con un azionamento del gate di sicurezza ogni ora per un totale di 5.760 operazioni l'anno. La funzione di arresto di emergenza globale viene testata una volta al mese.

Safety Gate 1	
PLr	e
PL	e
PFH [1/h]	2.64E-8

Estop 1	
PLr	d
PL	e
PFH [1/h]	5E-8

Safety Gate 2	
PLr	e
PL	e
PFH [1/h]	2.64E-8

Le singole funzioni di gate di sicurezza possono essere rappresentate come segue.



Interlock Switch: SensaGuard	
PL	e
PFH [1/h]	1.12E-9
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

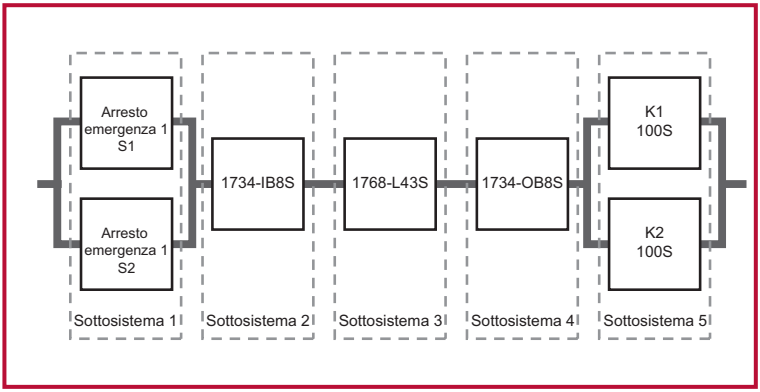
Safety I/O: 1734-IB8S	
PL	e
PFH [1/h]	2.25E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

Safety PLC: Compact GuardLogix 1768	
PL	e
PFH [1/h]	2.1E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

Safety I/O: 1734-OB8S	
PL	e
PFH [1/h]	2.29E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

Contactors	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

La funzione di arresto di emergenza può essere rappresentata come segue.



Estop 1	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

Safety I/O: 1734-IB8S	
PL	e
PFH [1/h]	2.25E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

Safety PLC: Compact GuardLogix 1768	
PL	e
PFH [1/h]	2.1E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

Safety I/O: 1734-OB8S	
PL	e
PFH [1/h]	2.29E-10
Cat.	4
MTTFd [a]	*not relevant*
DCavg [%]	*not relevant*
CCF	*not relevant*

Contactors	
PL	e
PFH [1/h]	2.47E-8
Cat.	4
MTTFd [a]	100 (High)
DCavg [%]	99 (High)
CCF	65 (fulfilled)

Questo esempio, il relativo file di calcolo SISTEMA e il codice applicativo RSLogix 5000 possono essere scaricati dal sito:

www.discoverrockwellautomation.com

Per ulteriori informazioni sui prodotti utilizzati in questo esempio è possibile consultare la relativa documentazione eseguendo una ricerca nella pagina dei riferimenti bibliografici (“Literature library”) di Rockwell Automation, inserendo nel campo di ricerca i numeri delle pubblicazioni sotto riportati. In alternativa, è possibile consultare le panoramiche dei prodotti sul sito www.ab.com.

L’indirizzo Internet della Literature library è: **www.theautomationbookstore.com**

Risorsa	**Descrizione**
Controllori Compact GuardLogix Manuale dell’utente. Pubblicazione: **1768-UM002**	Contiene informazioni sulla configurazione, il funzionamento e la manutenzione dei controllori Compact GuardLogix
Moduli di sicurezza POINT Guard I/O Manuale di installazione e manuale dell’utente. Pubblicazione: **1734-UM013**	Contiene informazioni sull’installazione, la configurazione e l’uso dei moduli POINT Guard I/O
Sistemi di controllori GuardLogix Manuale di riferimento per la sicurezza. Pubblicazione: **1756-RM093**	Contiene informazioni dettagliate sui requisiti per il conseguimento e il mantenimento delle classi di sicurezza con il sistema di controllori GuardLogix
Manuale di riferimento – Set di istruzioni per l’applicazione di sicurezza GuardLogix. Pubblicazione: **1756-RM095**	Contiene informazioni dettagliate sui set di istruzioni per l’applicazione di sicurezza GuardLogix
Safety Accelerator Toolkit for GuardLogix Systems, Quick Start Guide (in inglese). Pubblicazione: **IASIMP-QS005**	Guida passo-passo all’uso degli strumenti di progettazione, programmazione e diagnostica del Safety Accelerator Toolkit
Catalogo dei prodotti di sicurezza Pubblicazione: **S117-CA001A**	Pubblicazione completa dedicata ai prodotti di sicurezza, con esempi applicativi e informazioni utili

Rockwell Automation ha sviluppato una serie di esempi simili, scaricabili dalla Literature library. Per visionarli, accedere alla Literature library ed eseguire una ricerca immettendo la dicitura “SAFETY-AT” nel campo di ricerca e selezionando “Publication Number” nell’elenco a discesa.

Sono inoltre disponibili i calcoli SISTEMA e i codici applicativi RSLogix 5000 per alcune applicazioni. Per scaricarli, visitare il sito:

www.discoverrockwellautomation.com

MTTFd per ogni canale in anni	Probabilità media di guasti pericolosi all'ora (1/h) e corrispondente livello prestazionale (PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{media} = nessuna		DC_{media} = nessuna		DC_{media} = bassa		DC_{media} = media		DC_{media} = bassa		DC_{media} = media		DC_{media} = alta	
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	a	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	a	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-5}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-5}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}31 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		

MTTFd per ogni canale in anni	Probabilità media di guasti pericolosi all'ora (1/h) e corrispondente livello prestazionale (PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{media} = nessuna		DC_{media} = nessuna		DC_{media} = bassa		DC_{media} = media		DC_{media} = bassa		DC_{media} = media		DC_{media} = alta	
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americhe: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496, USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Medio Oriente/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgio, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asia: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: +852 2887 4788, Fax: +852 2508 1846

Italia: Rockwell Automation S.r.l., Via Gallarate 215, 20151 Milano, Tel: +39 02 334471, Fax: +39 02 33447701, www.rockwellautomation.it
Svizzera: Rockwell Automation AG, Buchserstrasse 7, CH-5001 Aarau, Tel.: +41 (62) 889 77 77, Fax: +41 (62) 889 77 11

Pubblicazione: SAFEBK-RM002B-IT-P – Marzo 2011
Sostituisce la pubblicazione: SAFEBK-RM002A-IT-P

© 2011 Rockwell Automation, Inc. Tutti i diritti riservati.