MACHINERY SAFEBOOK 5

Allen-Bradley

Guardmaster®

Sistemi di controllo di sicurezza per le macchine

Principi, standard e implementazione

(versione 5 della serie Safebook)

LISTEN. THINK. SOLVE.℠

Rockwell Automation

Sistemi di controllo legati alla sicurezza delle macchine

Contenuto

Capitolo 1 **Regolamenti** **2**
Legislazione e direttive UE, Direttiva Macchine, Direttiva sull'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 per la sicurezza** **22**
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 **Implementazione di misure di protezione** **34**
Prevenzione dell'avviamento imprevisto, lockout/tagout, sistemi di isolamento di sicurezza, prevenzione accessi, protezioni fisse, rilevamento accessi, tecnologie e sistemi di sicurezza

Capitolo 5 **Calcolo delle distanze di sicurezza** **56**
Formule, consigli ed applicazione delle soluzioni di sicurezza mediante il calcolo delle distanze di sicurezza per il controllo sicuro delle parti mobili potenzialmente pericolose.

Capitolo 6 **Sistemi di controllo di sicurezza e sicurezza funzionale** **60**
Introduzione, Che cos'è la sicurezza funzionale? IEC/EN 62061 e (EN) ISO 13849-1:2008, SIL e IEC/EN 62061, PL e (EN) ISO 13849-1:2008, confronto tra PL e SIL

Capitolo 7 **Progettazione del sistema secondo (EN) ISO 13849** **66**
SISTEMA, 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, validazione, messa in servizio delle macchine, esclusione dei guasti

Capitolo 8 **Progettazione del sistema secondo IEC/EN 62061** **87**
Progettazione di sottosistemi – IEC/EN 62061, influenza dell'intervallo delle prove funzionali, influenza dell'analisi dei guasti per causa comune, metodologia di transizione per le categorie, vincoli hardware, B10 e B10d, guasti per causa comune (CCF), copertura diagnostica (DC), tolleranza ai guasti hardware, gestione della sicurezza funzionale, PFH_D (probabilità di guasti pericolosi all'ora), intervallo delle prove funzionali, SFF (percentuale di guasti non pericolosi), guasti sistematici

Capitolo 9 **Sistemi di controllo di sicurezza, considerazioni aggiuntive** **98**
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 10 **Esempi applicativi** **110**
Esempio applicativo di come si potrebbe usare il calcolatore dei livelli prestazionali SISTEMA con la libreria di prodotti SISTEMA di Rockwell Automation.

Capitolo 11 **Prodotti, strumenti e servizi** **138**
Prodotti, tecnologie, strumenti e servizi disponibili presso Rockwell Automation.

Capitolo 1: regolamenti

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. I destinatari sono sia i progettisti che gli utilizzatori di apparecchiature industriali.

Per promuovere il concetto di mercato aperto nello Spazio Economica Europea (SEE) (comprendente gli stati membri UE ed altri tre paesi), tutti gli stati membri sono tenuti ad adottare una legislazione che definisca i requisiti di sicurezza fondamentali per le macchine ed 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 **Direttiva Macchine**

2 **Direttiva sull'uso delle attrezzature di lavoro da parte degli addetti durante il lavoro**

Queste due direttive sono direttamente correlate ed 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 rispettano 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 sulla Compatibilità Elettromagnetica 2014/30/CE e Direttiva ATEX 2014/34/UE.

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 ed 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 ad essere equipaggiato con un sistema di azionamento 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.
Informazioni ed istruzioni dettagliate sulla definizione e su tutti gli altri aspetti della Direttiva Macchine sono riportate nel sito web ufficiale UE:

http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery/index_en.htm

Le disposizioni principali della direttiva originaria (98/37/CE) sono entrate in vigore il 1° gennaio 1995 e, per 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 costruttore o di un suo rappresentante autorizzato assicurare la conformità alla direttiva delle macchine fornite. 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 essere conforme 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 le macchine siano sicure, progettate e realizzate 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. Il testo che segue presenta brevemente alcuni requisiti tipici, ma è importante considerare tutti i requisiti EHSR riportati nell'Allegato 1. È necessario procedere ad una valutazione dei rischi per determinare quali requisiti EHSR sono applicabili alle macchine prese in considerazione.

Gli EHSR riportati nell'Allegato 1 prevedono inoltre una gerarchia di misure atte ad 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 ed all'utilizzo. Devono inoltre essere fornite illuminazione e strumenti adeguati. I comandi ed i sistemi di controllo devono essere sicuri ed 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 ed in grado di resistere alle sollecitazioni prevedibili. Non devono presentare spigoli o superfici che possano causare ferite.

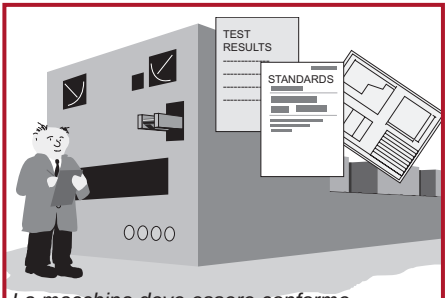
È necessario utilizzare protezioni o dispositivi di protezione che evitino l'insorgenza di rischi dovuti ad esempio a parti in movimento. Tali dispositivi devono essere

robusti e difficili da escludere. Le protezioni fisse devono essere montate in modo che possano essere rimosse solo con attrezzi e gli elementi di fissaggio dovrebbero essere imperdibili. Le protezioni mobili devono essere interbloccate. Le protezioni regolabili non devono richiedere l'uso di attrezzi.

I pericoli legati all'alimentazione elettrica e ad altri tipi di energia, tra cui l'energia accumulata, devono essere prevenuti. Il rischio di lesioni dovute a temperatura, esplosione, rumore, vibrazioni, polvere, gas o radiazioni deve essere minimo. Devono essere previste disposizioni appropriate per la manutenzione e la riparazione. Devono inoltre essere forniti dispositivi di segnalazione ed allarme sufficienti. Le macchine devono essere fornite complete delle istruzioni per l'installazione, l'uso, la regolazione ecc. in sicurezza.

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 essere conforme 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 macchine sono conformi alle attuali norme armonizzate europee, il compito di dimostrare la conformità con gli EHSR è molto semplificato ed il costruttore 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 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 costruttore assicurare il rispetto di tutti i requisiti EHSR, anche di quelli non trattati dalle norme armonizzate EN.

Dossier tecnico

Il costruttore 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 ma 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. Disegni generali della macchina, compresi i disegni del circuito di controllo.

2. Disegni dettagliati, note di calcolo ecc. richiesti per la verifica della conformità della macchina con i requisiti essenziali di salute e sicurezza.

3. Documentazione della valutazione dei rischi, compreso un elenco dei requisiti essenziali di salute e sicurezza applicabili alla macchina ed una descrizione delle misure di protezione implementate.

4. Elenco degli standard o norme e di altre specifiche tecniche utilizzate, in cui siano indicati i requisiti fondamentali di salute e sicurezza considerati.

5. 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. 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. Copia della dichiarazione CE di conformità.

Per la produzione in serie, i dettagli sulle misure interne (ad esempio, sistemi di qualità) usate per garantire che tutte le macchine prodotte siano conformi.

- I costruttori 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 salute e sicurezza.

Valutazione di conformità per le macchine dell'Allegato IV

Valutazioni di conformità

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

L'Allegato IV comprende anche alcuni componenti di sicurezza, come i dispositivi di protezione, destinati a rilevare la presenza delle persone (ad es. barriere fotoelettriche) ed 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 costruttore o il 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 ad 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 ed il costruttore deve applicare un sistema di qualità approvato per la progettazione, la produzione, l'ispezione finale ed il collaudo. 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

Per le macchine non incluse nell'Allegato IV o per quelle incluse ma in piena conformità con le pertinenti Norme Europee Armonizzate, il costruttore o il suo rappresentante autorizzato ha anche la possibilità di preparare la documentazione tecnica, oltre che di autovalutare e dichiarare la conformità della macchina. Devono essere previsti controlli interni per assicurare che la macchina prodotta rimanga conforme.

Organismi notificati

In tutta la 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/growth/tools-databases/nando/

Procedura per la dichiarazione di conformità 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 salute e sicurezza.

La dichiarazione di conformità CE deve contenere le seguenti informazioni:

- Ragione sociale, indirizzo completo del costruttore e, dove applicabile, del rappresentante autorizzato;
- Nome ed indirizzo della persona autorizzata a redigere il dossier tecnico, che deve essere residente nella Comunità (nel caso di un costruttore con sede al di fuori dell'UE può essere il "Rappresentante autorizzato");
- Descrizione ed identificazione della macchina, comprendente denominazione generica, funzione, modello, tipo, numero di serie e nome commerciale;
- Un'espressa dichiarazione che la macchina è conforme a tutte le disposizioni applicabili di questa direttiva e, dove pertinente, una dichiarazione simile che attesti la conformità della macchina ad altre direttive e/o disposizioni applicabili;
- Se pertinente, un riferimento alle norme armonizzate utilizzate;
- Se pertinente, un riferimento alle altre norme armonizzate e specifiche utilizzate;
- (Per le macchine dell'Allegato IV) se pertinente, il nome, l'indirizzo ed il numero di identificazione dell'organismo notificato che ha eseguito l'esame di tipo CE indicato nell'Allegato IX ed il numero del certificato dell'esame di tipo CE;
- (Per le macchine dell'Allegato IV) se pertinente, il nome, l'indirizzo ed 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 costruttore o del rappresentante autorizzato

Dichiarazione CE di incorporazione di macchine parzialmente completate

Se la macchina fornita è destinata ad 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 la macchina non deve essere messa in servizio finché quella 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 macchine che funzionano indipendentemente o che modificano la funzione di una macchina.

La dichiarazione di incorporazione deve contenere le seguenti informazioni:

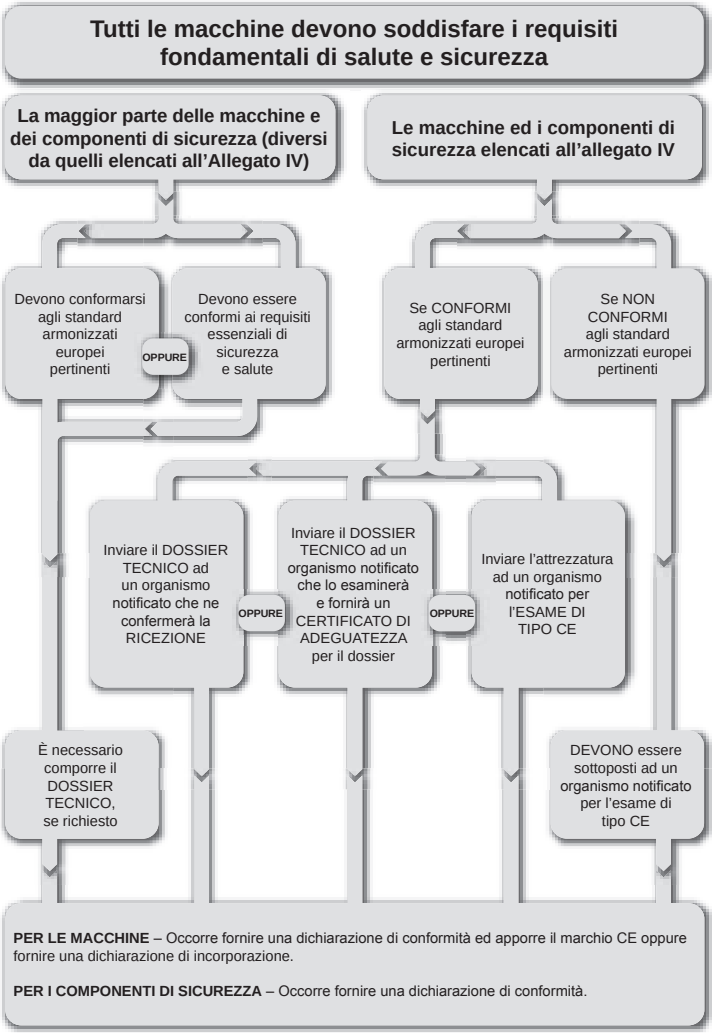
- Ragione sociale ed indirizzo completo del costruttore della macchina parzialmente completata e, se appropriato, del rappresentante autorizzato;
- Nome ed indirizzo della persona autorizzata a redigere la documentazione tecnica applicabile, che deve essere residente nella Comunità (nel caso di un costruttore con sede al di fuori dell'UE può essere il "Rappresentante autorizzato");
- Descrizione ed 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 e soddisfatti ed 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 ad 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 costruttore della macchina parzialmente completata;
- Una frase in cui si dichiari che la macchina parzialmente completata non dovrà essere messa in servizio fino a quando quella 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 costruttore o del rappresentante autorizzato.

Macchine fornite da paesi non appartenenti alla UE – Rappresentanti autorizzati

Se un costruttore con sede in un paese non appartenente alla UE (o SEE) esporta delle macchine nella UE, dovrà incaricare un rappresentante autorizzato.

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

Direttiva europea sull'uso delle attrezzature di lavoro (Direttiva U.W.E.)



Mentre la Direttiva Macchine si rivolge ai fornitori, questa direttiva (2009/104/CE) è destinata 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.

Nel Regno Unito, ad esempio, è implementata con il nome di “The Provision and Use of Work Equipment Regulations” (spesso abbreviato in P.U.W.E.R.). Il tipo di implementazione può variare tra i diversi paesi ma l’effetto della direttiva rimane lo stesso.

Gli articoli della direttiva forniscono informazioni dettagliate sui tipi di macchine e sui 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 ad una corretta manutenzione. Gli operatori delle macchine devono ricevere informazioni ed addestramento adeguati per un uso sicuro della macchina.

Le macchine nuove (e le macchine di seconda mano provenienti da paesi esterni alla 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’interno della UE e fornite per la prima volta nel luogo di lavoro devono conformarsi immediatamente ai requisiti minimi previsti nell’Allegato della Direttiva U.W.E.

Nota: le macchine esistenti o di seconda mano revisionate o modificate in modo significativo saranno classificate quali macchine 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.

L’Allegato della Direttiva Uso delle Attrezzature dil Lavoro. fornisce i requisiti minimi generali applicabili alle attrezzature di lavoro.

Se le macchine 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 promulgare leggi relative all’uso delle attrezzature di lavoro che vanno oltre i requisiti minimi della Direttiva sull’Uso delle Attrezzature dil Lavoro.

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

https://osha.europa.eu/en/legislation/directives/3

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 ed adottare le misure necessarie a garantire che progetti, procedure e metodi di uso e manutenzione rispondano alle proprie esigenze così come ai regolamenti ed 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 la National Fire Protection Association (NFPA), la Robotics Industries Association (RIA) e la Association of Manufacturing Technology (AMT); ANSI che pubblica un elenco di standard che godono di consenso riconosciuto, i 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 1971 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 salute e sicurezza 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, ad ognuno dei suoi dipendenti, un lavoro ed 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 ed a tutte le regole ed i regolamenti emessi in base a questa legge ed applicabili alle proprie azioni ed 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'utilizzatore 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 ed 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 salute e sicurezza 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 e sono disponibili gratuitamente sul sito web OSHA all'indirizzo 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 una norma

che gode di consenso nazionale viene incorporata per riferimento in una delle sottoparti, tale norma assume “forza di legge”.
Ad esempio, l’NFPA 70, uno standard volontario conosciuto come US National Electric Code, è riportato nella Sottoparte S. Questo 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 ed i conseguenti infortuni ai danni dei lavoratori.

I datori di lavoro devono stabilire un programma di lockout/tagout ed utilizzare procedure per la sistemazione di adeguati dispositivi di lockout o tagout sui dispositivi di sezionamento dell’energia e per disabilitare altrimenti le macchine o le apparecchiature in modo da prevenire eventi imprevisti di messa in tensione, avviamento o rilascio dell’energia accumulata ed evitare infortuni ai danni dei lavoratori.

Lo standard ANSI Z244 “Misure alternative” tratta le piccole operazioni di modifica e regolazione degli utensili e gli interventi di manutenzione di minore importanza da effettuare durante le normali attività di produzione se si tratta di interventi ordinari, ripetitivi ed inerenti all’uso delle macchine per la produzione, a condizione che il lavoro venga svolto usando misure alternative che forniscano un’adeguata protezione. Questo è direttamente supportato da OSHA in “OSHA Minor Servicing Exception”. Come misure alternative si intendono dispositivi di protezione quali barriere fotoelettriche, pedane di sicurezza, interblocchi gate ed altri simili dispositivi collegati ad 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 ed inerenti all’utilizzo”. Questi aspetti possono essere affrontati durante la valutazione dei rischi.

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 1971, 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 ed 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. Per la sua eventuale rimozione deve essere necessario un attrezzo.

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 una macchina è accettabile per l’Assistant Secretary of Labor ed approvata ai sensi 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 ed altri componenti simili usati come parte integrante di un’installazione elettrica o in collegamento ad essa.

Che cosa significa “omologata” (“listed”)? La macchina è “omologata” se corrisponde al tipo menzionato in una lista, (a) pubblicata da un laboratorio di prova riconosciuto a livello nazionale (NTRL) che effettua periodiche ispezioni della produzione di tale macchina, e (b) attesti che tale macchina soddisfa gli 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)

È compito dell'autorità competente (AHJ – Authority Having Jurisdiction) determinare i requisiti necessari. Alcuni stati come NY, CA e IL hanno, ad esempio, requisiti aggiuntivi.

Alcuni stati hanno adottato i propri OSHA locali e possono avere requisiti aggiuntivi rispetto ai requisiti OSHA previsti a livello federale. 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 ed 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

Regolamenti canadesi

In Canada, la sicurezza industriale è governata a livello provinciale. Ogni provincia mantiene ed applica i propri regolamenti. L'Ontario, ad esempio, ha promulgato l'Occupational Health and Safety Act che stabilisce i diritti ed 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 report.

Capitolo 2: standard

Questa sezione tratta una serie di standard 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. Anche gli Stati Uniti fanno ora spesso riferimento agli standard IEC e ISO.

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.

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 ed 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 ed 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 salute e sicurezza coperti da quello standard. 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 ed 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/growth/single-market/european-standards/

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.
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 ed 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 apparecchiature e sistemi elettrici/elettronici delle macchine industriali. 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 ed utilizzatori – tra cui costruttori, consumatori, rivenditori, associazioni, organizzazioni professionali ed 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 ed 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.

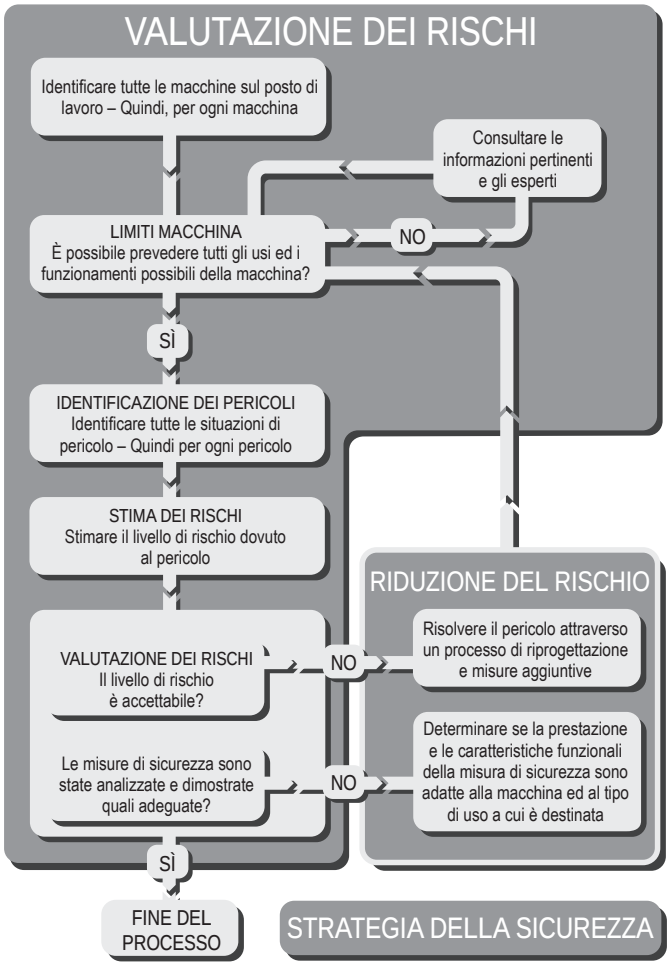
Lo Standards Council of Canada è l'organo di coordinamento del sistema National Standards, una federazione di organizzazioni indipendenti ed autonome che lavorano per l'ulteriore sviluppo e miglioramento della standardizzazione volontaria, nell'interesse nazionale.

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*

Capitolo 3: 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 dei rischi. Il modo in cui questo viene fatto rappresenta la base della STRATEGIA DELLA SICUREZZA per la macchina.

Questo approccio sistematico assicura che siano presi in considerazione tutti gli aspetti 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 costruttori sia agli utilizzatori di macchine.
Il costruttore 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 costruttore, l'utilizzatore dovrebbe comunque procedere ad 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 costruttore 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. È anche possibile che macchine considerate sicure singolarmente vengano assemblate in modo da creare un sistema non sicuro.

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 ad 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'utilizzatore o al progettista di prendere decisioni ragionate sui metodi per garantire la sicurezza.

Esistono vari standard che trattano questo argomento. (EN) ISO 12100: Sicurezza del Macchinario – Principi generali di progettazione – Valutazione del rischio e riduzione del rischio contiene le istruzioni più utilizzate a livello globale. È disponibile anche un Report Tecnico ISO: ISO/TR 14121-2. Questo documento fornisce istruzioni pratiche ed esempi dei metodi per la valutazione dei rischi.

Qualunque sia la tecnica usata per la valutazione dei rischi, un team interfunzionale di persone arriverà ad 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 delle 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 ed il funzionamento, oltre alle conseguenze di malfunzionamenti ed 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 dei task dovrebbero essere confrontati con quelli dell'identificazione dei rischi. Ciò servirà a evidenziare l'eventuale compresenza di un pericolo e di una persona ovvero una situazione pericolosa. Tutte le situazioni pericolose dovrebbero essere riportate in un elenco. A seconda della natura della persona o dell'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 ed 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 ed affrontati separatamente, bisognerebbe fare riferimento al caso di rischio più grave e, di conseguenza, tecnico di manutenzione ed 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 ed 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 report tecnico ISO TR 14121-2: “Risk assessment – Practical guidance and examples of methods” fornisce diversi metodi per la quantificazione dei rischi. Vi sono differenze nella terminologia e nei sistemi di punteggio, ma tutti i metodi fanno riferimento ai principi DEFINITI in (EN) ISO 12100. Il testo che segue delinea i principi di base della quantificazione dei rischi, a prescindere dalla metodologia utilizzata. In linea generale, segue i parametri forniti in Hybrid Tool nell’articolo 6.5 di ISO TR 14121-2.

Vengono presi in considerazione i seguenti fattori:
- LA GRAVITÀ DELLE LESIONI POTENZIALI.
- LA PROBABILITÀ CHE SI VERIFICHINO.

La probabilità di occorrenza comprende almeno due fattori:
- FREQUENZA DELL’ESPOSIZIONE.
- PROBABILITÀ DI LESIONI.

Lo stesso fattore di probabilità è spesso suddiviso in altri fattori, ad esempio:
- PROBABILITÀ DI OCCORRENZA.
- POSSIBILITÀ DI EVITARE IL PERICOLO.

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.

In questa fase, 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).

Gravità delle lesioni potenziali

Per procedere a queste considerazioni, si presume che l’infortunio o l’incidente si sia verificato. 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 dovrebbe essere valutata in base ai fattori forniti nella metodologia scelta.

Ad esempio, come segue:
- Morte, perdita di un occhio o di un braccio
- Effetto permanente, ad es. perdita di dita.
- Effetto reversibile che richiede intervento medico
- Effetto reversibile che richiede intervento di primo soccorso

Frequenza di 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 in base ai fattori forniti nella metodologia scelta.

Ad esempio, come segue:
- Più volte all’ora
- Tra una volta all’ora e una volta al giorno
- Tra una volta al giorno e una volta ogni due settimane
- Tra una volta ogni due settimane e una volta all’anno
- Meno di una volta all’anno

Probabilità di lesioni

Occorre presumere che l’operatore sia esposto al movimento o al processo pericoloso. La probabilità di occorrenza di un evento pericoloso può essere classificata in base ai fattori forniti nella metodologia scelta. La probabilità di occorrenza può essere classificata considerando le caratteristiche della macchina, i comportamenti previsti degli operatori e una serie di altri fattori.

Ad esempio, come segue:
- Trascurabile
- Rara
- Possibile
- Probabile
- Molto alta

Possibilità di evitare il pericolo

Considerando le modalità di interazione tra persone e macchina e una serie di altre caratteristiche – ad esempio, la velocità di avviamento – è possibile classificare la possibilità di evitare infortuni in base ai fattori forniti nella metodologia scelta.

Ad esempio, come segue:
- Probabile
- Possibile
- Impossibile

Dopo aver considerato tutti i fattori, i risultati possono essere inseriti nel grafico o nella tabella di quantificazione dei rischi, qualunque sia il metodo utilizzato. In questo modo si ottiene una sorta di stima quantificata dei rischi correlati ai diversi pericoli associati a una macchina. Queste informazioni possono quindi essere utilizzate per decidere quali rischi devono essere ridotti per ottenere un livello di sicurezza accettabile.

Riduzione dei rischi

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

Gerarchia delle misure per la riduzione dei rischi
Esistono tre metodi di base, da considerare ed 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 in relazione ai rischi che non possono essere eliminati in fase progettuale.
3. Fornire informazioni per l'uso in sicurezza della macchina, tra cui cartelli e segnali di avvertenza. Informare su eventuali rischi residui e sulla necessità di corsi di formazione o dispositivi di protezione individuali.

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

Eliminazione del rischio (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 ad 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 fattore è estremamente importante, poiché un sistema che compromette l'efficienza della macchina sarà probabilmente rimosso senza autorizzazione o escluso.

Una delle interazioni più impegnative e complete tra persone e macchine avviene durante le operazioni di manutenzione, ricerca guasti e riparazione. Per garantire la sicurezza durante gli interventi ordinari e secondari, è possibile usare misure di protezione basate su sistemi di sicurezza (vedere la descrizione riportata più avanti). Per tutti i regolamenti è comunque assolutamente chiaro che, per qualunque intervento significativo di manutenzione, riparazione, smontaggio o lavoro sui circuiti di potenza, devono essere previsti sia la fornitura che l'utilizzo di apparecchiature che assicurino l'isolamento e la dissipazione dell'energia (talvolta anche della forza gravitazionale) in corrispondenza della macchina. In questo modo, è possibili eliminare il rischio di avviamento imprevisto ed esposizione alle fonti di energia. Questo argomento è trattato in tutta una serie di regolamenti e standard. Il testo precedente è riportato, ad esempio, negli "U S Regulations" e descrive i regolamenti e gli standard di "Lockout/Tagout". Anche gli standard europei e ISO EN 1037 e ISO 14118 "Prevenzione degli avviamenti involontari" forniscono dei requisiti. In termini di tecnologia elettrica, forniscono istruzioni e requisiti anche IEC/EN 60204-1 e NFPA 79.
Naturalmente è indispensabile che un corretto sistema di lavoro assicuri che vengano seguite tutte le procedure corrette.

La sezione che segue descrive alcune implementazioni tipiche.

Prevenzione dell'accensione non intenzionale

La prevenzione dell'accensione non intenzionale è trattata in molti standard, tra cui ISO 14118, EN 1037, 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 accedere in sicurezza alle zone pericolose della macchina.

Lockout/Tagout

Le macchine nuove devono essere costruite con dispositivi di isolamento dell'energia 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 ad 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 da misure come, ad esempio, i sistemi di interblocco delle porte di protezione. La differenza tra le operazioni di assistenza/manutenzione e quelle di normale funzionamento non è sempre chiara.

Alcune regolazioni ed interventi di assistenza di minore importanza che avvengono durante le normali operazioni di produzione non richiedono necessariamente il lock-out 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 ed inerenti all'utilizzo dell'apparecchiatura di produzione ed 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. Utilizzandole 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 manutenzione.

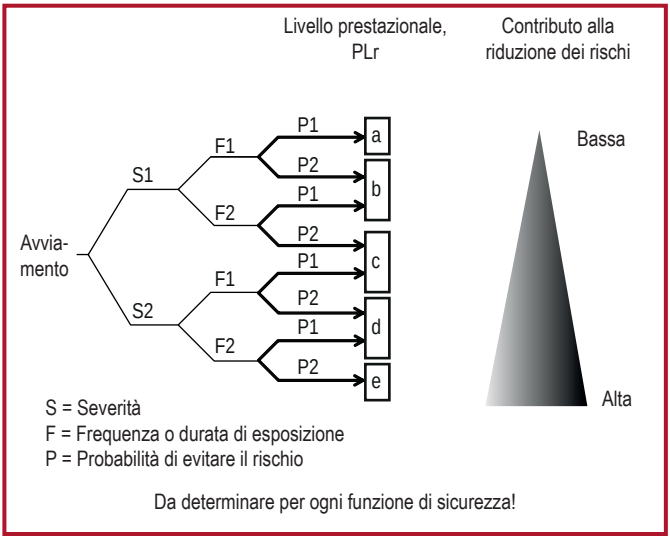
In questo caso, la sicurezza della macchina dipende dalla corretta applicazione e dal funzionamento corretto del sistema protettivo anche in condizioni di guasto. Adesso occorre esaminare il funzionamento corretto di tale sistema. Per ogni tipo di sistema esistono numerose tecnologie con diversi gradi 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 mettere in qualche modo in relazione la portata delle misure di protezione al livello di rischio risultante dalla valutazione dei rischi.

Qualunque sia il dispositivo di protezione prescelto, occorre ricordare che un "sistema di sicurezza" può comprendere numerosi elementi, tra cui il dispositivo di protezione, il cablaggio, un dispositivo di commutazione ed 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. IEC/EN 62061 e (EN) ISO 13849-1 prevedono livelli gerarchici di prestazioni per le parti di sicurezza dei sistemi di controllo e, nei loro allegati, forniscono metodi per la valutazione dei rischi utili a determinare i requisiti di integrità di un sistema di protezione.

Sistemi di controllo legati alla sicurezza delle macchine

Nel suo Allegato A, (EN) ISO 13849-1:2015 fornisce un grafico dei rischi di livello avanzato.



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

Valutazione dei rischi e misure di sicurezza

Documento N.:
Parte di:

Prodotto: _____
Rilasciato da: _____
Data: _____

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

☐ Valutazione preliminare del rischio
☐ Valutazione intermedia del rischio
☐ Valutazione di verifica del rischio

Conseguenza	Gravità SE	Classe CI					Frequenza e durata, Fr		Probabilità di evento pericoloso, Pr		Evitabilità Av	
		3–4	5–7	8–10	11–13	14–15						
Morte, perdita di un occhio o di un braccio		SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 ora	5	Normale	5		
Permanente, perdita della dita			OM	SIL 1	SIL 2	SIL 3	> 1 h – <= giorno	5	Probabile	4		
Reversibile, intervento medico				OM	SIL 1	SIL 2	> 1 giorno – <= 2 settimane	4	Possibile	3	Impossibile	5
Reversibile, primo soccorso					OM	SIL 1	> 2 settimane – <= 1 anno	3	Raramente	2	Possibile	3
							> 1 anno	2	Trascurabile	1	Probabile	1

N. serie	N.	Pericolo	Se	Fr	Pr	Av	Ci	Misura di sicurezza	Sicuro

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, se la misura di protezione non funziona, l'operatore sarà esposto ad 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. Generalmente, sarà comunque necessario adottare cartelli e marcature per facilitare la consapevolezza di eventuali rischi residui.

Capitolo 4: implementazione delle misure di protezione

Quando la valutazione dei rischi 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 di un sistema di controllo di sicurezza, associate alle protezioni fisiche, prevengono l'accesso a un pericolo o il movimento pericoloso verso un pericolo quando l'accesso è disponibile. Gli esempi tipici delle misure di protezione di un sistema di controllo di sicurezza sono riportati più avanti e includono protezioni interbloccate, barriere fotoelettriche, pedane di sicurezza, comandi a due mani e interruttori di abilitazione.

I dispositivi e sistemi di arresto di emergenza sono associati a sistemi di controllo di 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 comodo modo di monitorare le prestazioni della macchina. Occorre prestare attenzione alla selezione dei materiali usati, poiché le interazioni chimiche con fluidi da taglio e 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 ad 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 ed 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.

- Fattori ambientali che possono incidere sull'affidabilità del dispositivo di rilevamento
- 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 ed altri tipi di pericolo; questo tipo di protezione viene spesso utilizzata quando l'accesso al pericolo non è frequente. Le protezioni interbloccate possono essere utilizzate anche per impedire l'accesso alla macchina fino a quando non ha raggiunto uno stato di arresto completo o quando l'arresto durante un ciclo è indesiderabile.

I dispositivi di rilevamento accesso – come barriere fotoelettriche, pedane e laser 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.

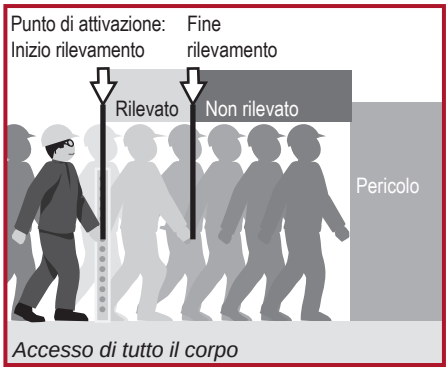
La scelta migliore di misura protettiva è un dispositivo o un sistema che garantisca la massima protezione con la minima interferenza nel normale funzionamento della macchina. Tutti gli aspetti della macchina devono essere considerati poiché l'esperienza insegna che, quando un sistema è difficile da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

Dispositivi di rilevamento accesso

IEC 62046 fornisce utili istruzioni sull'applicazione dei dispositivi di rilevamento accesso, se ne raccomanda l'uso. 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 apparecchiatura, si tratta di due funzioni di sicurezza 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 ed invii un segnale per disinserire l'alimentazione. Se la persona riesce ad 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 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 ad 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 ed 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 raggio singolo, laser scanner di sicurezza e pedane di sicurezza. Per tutti i dispositivi di rilevamento accesso, le dimensioni della zona di rilevamento e il posizionamento del dispositivo devono essere decisi considerando la necessaria distanza 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 (Active Opto-electronic Protective Devices) o ESPE (Electro Sensitive Protective Equipment), le barriere fotoelettriche garantiscono un livello di sicurezza ottimale, pur consentendo un'elevata produttività. Sono perfette per le applicazioni in cui il personale necessita di accedere frequentemente e facilmente ad un punto di lavoro pericoloso.
Le barriere fotoelettriche sono concepite e testate per rispondere a IEC 61496-1 e -2.

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 utilizzate nell'ambito di un'area recintata contenente diverse macchine, nei sistemi di produzione flessibili o nelle celle robotiche. 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. È importante prevenire qualsiasi movimento delle pedane con un fissaggio corretto e sicuro.

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.

Barriere fotoelettriche, scanner, pedane e bordi sensibili sono classificati anche 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 o esiste la possibilità di espulsione violenta di pezzi, si preferisce spesso 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 ed interruttore di interblocco con o senza blocco della protezione è la soluzione più affidabile ed efficiente. (EN) ISO 14119 fornisce utili istruzioni sulla selezione dei dispositivi di interblocco di protezione, se ne raccomanda l'uso.

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

- **Interruttori interbloccati 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 ed 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 ad 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 ed 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 ISO 13849-1. Per ulteriori dettagli, vedere 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 (freni), 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.

L'arresto di **Categoria 1** è un arresto controllato in cui gli attuatori della macchina vengono alimentati in modo da poter eseguire 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. Questo tipo di arresto può risultare più veloce e controllato e favorire un riavviamento rapido. NOTA: L'edizione 2016 di IEC/EN 60204-1 espanderà i tipi di arresto di Categoria 1.

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 di sicurezza del sistema di controllo come risposta ad 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 dei rischi. 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. 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 utilizzabile e subito disponibile. I pannelli operatore devono contenere almeno un dispositivo di arresto di emergenza. Se necessario, è possibile utilizzare ulteriori dispositivi di arresto di emergenza in altre posizioni. I dispositivi di arresto di emergenza sono disponibili in varie forme. Gli interruttori a pulsante e quelli a fune sono alcuni dei dispositivi più diffusi.

Fino a tempi relativamente recenti, per i circuiti di arresto di emergenza erano necessari componenti elettromeccanici cablati. Una serie di recenti modifiche secondo norme come IEC 60204-1 e NFPA 79 permettono attualmente di usare, nei circuiti di arresto di emergenza, PLC di sicurezza e altre forme di logica elettronica rispondenti ai requisiti di standard come IEC 61508.

I dispositivi di arresto di emergenza sono considerati apparecchiature di protezione complementari. Poiché non impediscono e non rilevano l'accesso ad un pericolo, non sono considerati dispositivi di protezione primari. Si basano sull'interazione umana.

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

Pulsanti di arresto di emergenza

Quando il dispositivo di arresto di emergenza è un pulsante, questo deve essere a forma di fungo e di colore rosso con sfondo giallo. Quando viene azionato, il dispositivo di arresto di emergenza deve rimanere inserito e non deve essere possibile generare il comando di arresto senza tale condizione di ritenuta. Il ripristino 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.

Una delle tecnologie più recenti da applicare agli arresti di emergenza è la 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.

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 ed in qualsiasi punto lungo la sua lunghezza l'interruttore venga attivato ed 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 che sia, quindi, pronto all'uso.

La distanza del cavo incide sulle prestazioni dell'interruttore. Per brevi distanze, ad 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 ad entrambe le estremità del cavo, in modo da garantire che una singola azione

dell'operatore generi un comando di arresto. L'utilizzo di bulloni a occhiello adeguatamente posizionati per sostenere e guidare il cavo è fondamentale. La forza di trazione necessaria del cavo non deve superare 200 N o una distanza di 400 mm in corrispondenza del punto centrale tra due bulloni a occhiello. Per ottenere le prestazioni operative corrette, è importante seguire le istruzioni del costruttore.

Comandi a due mani

L'uso dei comandi a due mani (chiamati anche comandi bimanuali) è un metodo molto diffuso per evitare l'accesso ad 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. Ciò assicura una funzione "antiblocco" e impedisce che l'azione a due mani possa essere eseguita con una sola mano.

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

Tabella dei requisiti ISO 13851

La progettazione fisica degli spazi deve impedire l'uso improprio (ad es. utilizzando una mano ed un gomito). Ciò è possibile mediante un calcolo delle distanze o l'installazione di schermi. La macchina non deve passare da un ciclo ad un altro senza il rilascio e la pressione di entrambi i pulsanti. Ciò assicura una funzione di "antiripetizione" e previene la possibilità che entrambi i pulsanti siano bloccati, lasciando così la macchina in funzionamento continuo. 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 talvolta rientrano in una strategia di autorizzazione e che permettono a un operatore di entrare in una zona pericolosa, con il motore in funzione a velocità di sicurezza, 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 ed 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 di sicurezza. Un tipico esempio è il controllo del movimento in modalità lenta, sicura e controllata. 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 di sicurezza del sistema di controllo. I dispositivi logici effettuano il controllo ed 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 ed 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. Per macchine di dimensioni medio-grandi o particolarmente complesse può essere preferibile adottare sistemi di sicurezza programmabili con I/O distribuiti.

Relè di monitoraggio di sicurezza (MSR)

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 concepiti per evitare che contatti normalmente chiusi e normalmente aperti si chiudano simultaneamente. Alcuni relè di monitoraggio di sicurezza hanno uscite di sicurezza a 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, il relè MSR controlla gli attuatori esterni collegati alle sue uscite. Se il risultato è positivo, l'MSR attende un segnale di reset per eccitare le sue uscite. Quindi un MSR correttamente selezionato e configurato può assicurare il rilevamento dei guasti del sistema controllando i dispositivi collegati di ingresso e di uscita. Può anche servire a implementare un interblocco di avviamento/riavviamento.

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, ecc.

Tipi di ingresso per i relè di monitoraggio di sicurezza (MSR)

I tipi di ingresso per un relè di monitoraggio di sicurezza cambiano in base al dispositivo di protezione; quindi è importante controllare la compatibilità. Quello che segue è un breve sommario dei tipi di ingresso che possono essere previsti e delle caratteristiche richieste di rilevamento dei guasti incrociati.

Interblocchi elettromeccanici, alcuni interblocchi senza contatto e pulsanti di emergenza: contatti meccanici, a canale singolo con un contatto normalmente chiuso o a canale doppio con entrambi i contatti normalmente chiusi. Il relè 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.

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

Dispositivi con uscite a stato solido: barriere fotoelettriche, laser scanner e alcuni interblocchi di protezione senza contatto hanno due uscite sourcing ed effettuano il rilevamento dei propri guasti incrociati. Il relè 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 concepito specificatamente o configurabile per questa applicazione.

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.

Rilevamento del movimento del motore: 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 specificatamente o configurabili per interfacciare ognuno di questi dispositivi, poiché hanno diverse caratteristiche elettriche. Alcuni MSR sono completamente configurabili in tipi differenti. 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 o configurare 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, la massima impedenza di ingresso ammissibile di un relè di sicurezza è di 500 Ohm. Quando l'impedenza di ingresso è superiore a 500 Ohm, le uscite non vengono attivate. L'utilizzatore deve prestare particolare attenzione per garantire che l'impedenza d'ingresso rimanga al di sotto del valore massimo a specifica. La lunghezza, la dimensione ed il tipo di cavo usato incidono sull'impedenza d'ingresso.

Numero di dispositivi di ingresso

Il processo di valutazione dei rischi 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 siano funzionanti, gli arresti di emergenza e gli interblocchi dei ripari devono essere controllati a intervalli regolari, in base a quanto determinato dalla valutazione dei rischi. Ad esempio, un MSR di ingresso a canale doppio collegato ad un riparo interbloccato che deve essere aperto ad 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 ed 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 vengono generalmente utilizzati 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 programmati. Questo modo di verificare il sistema di sicurezza è conosciuto come "test funzionale". Un terzo esempio potrebbe essere rappresentato dalle 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 dei rischi 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, denominati 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 diversi modi. Uno dei modi più comuni per rilevare i guasti incrociati è il test ad impulsi. Gli impulsi dei segnali di ingresso all'MSR 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 ed un ingresso pull-down. Un corto dal canale 1 al canale 2 attiva il dispositivo di protezione dalle sovracorrenti ed 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 ed 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.

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.

Valori nominali di tensione (Ue) e corrente (Ie) di funzionamento: i valori nominali di corrente e tensione di funzionamento indicano la capacità di chiusura e apertura degli elementi di commutazione in condizioni operative normali. Generalmente, i prodotti Allen-Bradley Guardmaster hanno valori nominali di 125 V CA, 250 V CA e 24 V CC.

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 7200 VA. A 120 V CA, i contatti possono chiudere un circuito con una corrente di spunto di 60 A. Poiché l'AC-15 è un carico 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

da 2,2 A. I carichi elettromagnetici in CC non hanno correnti di spunto come quelli in CA. Anche l'apertura del circuito è a 275 VA perché la corrente a regime del carico elettromagnetico è pari a 2,2 A, che è 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 ad un contattore di avviamento a ritenuta.

La pressione ed 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 ed 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 ed avviando la macchina.

I requisiti per le normali situazioni di interblocco sono definiti dallo standard ISO 12100 (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 la chiusura del riparo o il ripristino dell'arresto di emergenza. 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. Questo comportamento è conforme ai requisiti per il reset manuale aggiuntivo riportati in (EN) ISO 13849-1. In altre parole, la funzione di reset assicura che entrambi i contattori siano OFF, che entrambi i circuiti di interblocco (e quindi le protezioni) siano chiusi e anche (dato che è necessario un cambiamento di stato) che l'attuatore di reset non sia stato bypassato o bloccato in alcun modo. Se questi controlli sono soddisfacenti, la macchina può essere riavviata con i normali comandi. (EN) ISO 13849-1 parla di cambiamento di stato da eccitato a diseccitato ("fronte di discesa").

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.

Reset automatico/manuale

Alcuni relè di sicurezza sono dotati di reset automatico/manuale. La modalità di reset manuale non è monitorata ed il reset avviene quando il pulsante è premuto. Un cortocircuito o un blocco nel pulsante di reset non sarà rilevato. Con questo approccio può non essere possibile soddisfare i requisiti per il reset manuale aggiuntivo riportati in (EN) ISO 13849-1, a meno che non vengano utilizzati mezzi aggiuntivi.

In alternativa, la linea di reset può essere collegata con un ponticello, consentendo un reset automatico. L'utilizzatore deve quindi fornire un altro meccanismo per evitare l'avviamento della macchina quando il gate 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

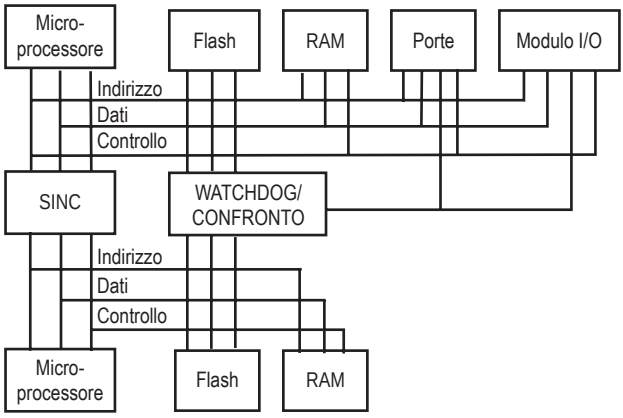
Una protezione di controllo arresta una macchina quando la protezione è aperta e l'avvia direttamente quando è chiusa. L'uso di questo tipo di protezioni è consentito solo in determinate condizioni molto precise, poiché qualsiasi avviamento imprevisto o il mancato arresto sarebbero estremamente pericolosi.

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

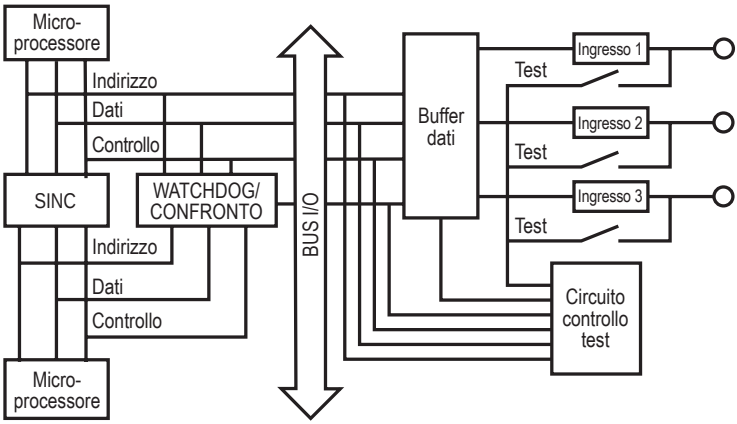
L'esigenza di applicazioni di sicurezza flessibili e scalabili è alla base dello sviluppo dei controllori/PLC di sicurezza. I controllori programmabili di sicurezza offrono agli utilizzatori in un'applicazione di sicurezza lo stesso livello di flessibilità del controllo che avrebbero con controllori 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 ed integrazione dei più complessi sistemi di sicurezza.

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.



Architettura 1oo2D

Inoltre, ogni circuito di ingresso è testato internamente diverse volte al secondo, per verificarne il corretto funzionamento. Il pulsante di emergenza viene magari premuto una sola volta al mese, ma il circuito interno è stato testato continuamente.



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 ed il guasto è riportato dal circuito di monitoraggio interno.
Quando si usano dispositivi di sicurezza con contatti meccanici (pulsanti di emergenza, interruttori di sicurezza, ecc.), l'utilizzatore può applicare segnali di prova a impulsi per rilevare i guasti incrociati.

Software

La programmazione dei PLC di sicurezza è molto simile a quella dei PLC standard. Il sistema operativo gestisce la diagnostica aggiuntiva ed 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 l'arresto di emergenza funziona in modo molto simile a un MSR. Anche se la logica alla base di ognuna di queste istruzioni è complessa, i programmi di sicurezza sembrano relativamente semplici perché il programmatore non fa altro che collegare tra 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 ed alla logica ladder, i PLC di sicurezza forniscono anche istruzioni applicative di sicurezza certificate. Le istruzioni di sicurezza certificate servono a gestire il comportamento specifico dell'applicazione.

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'utilizzatore dovrebbe registrare questa firma tra i risultati di validazione, per futuro riferimento. Se il programma ha bisogno di modifiche, è richiesta una nuova validazione e la registrazione di una nuova firma. Per impedire modifiche non autorizzate, il programma può anche essere bloccato con una password.

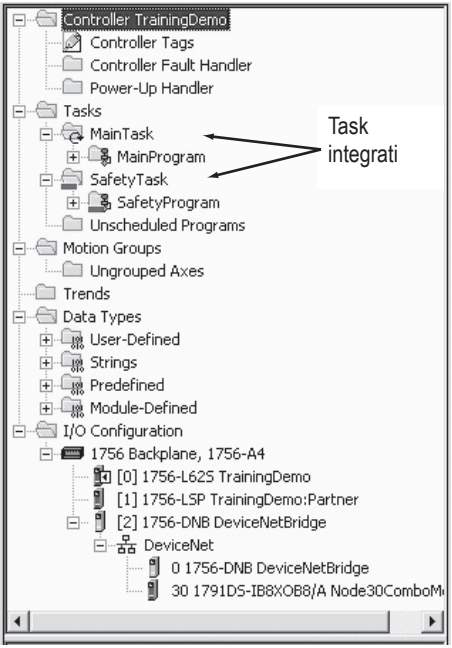
Il cablaggio dei sistemi a logica programmabile è semplificato rispetto a quello dei relè di monitoraggio di sicurezza. Anziché essere cablati a morsetti specifici dei relè di monitoraggio di sicurezza, i dispositivi di ingresso sono collegati a qualunque morsetto di ingresso di sicurezza e i dispositivi di uscita a qualunque morsetto di uscita di sicurezza. I morsetti 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 possibilità di realizzare task di movimento, azionamento, processo, batch, controllo sequenziale ad alta velocità e sicurezza SIL 3 in un solo 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 di sicurezza sono isolate una dall'altra. Ad esempio, i tag di sicurezza possono essere letti direttamente dalla logica standard. I tag di sicurezza tra i controllori GuardLogix possono essere scambiati su EtherNet/IP, 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 in ambito programma o 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/IP.

7. I dati tag di sicurezza, in ambito programma o controllore, possono essere letti da dispositivi esterni, interfacce operatore, PC, altri controllori, ecc. Dopo essere stati utilizzati per task standard, questi dati sono considerati 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 anche dell'implementazione delle reti di sicurezza industriali. Queste reti di sicurezza consentono ai costruttori di distribuire I/O e dispositivi di sicurezza sulle macchine mediante un unico cavo di rete, sia per le comunicazioni I/O di sicurezza che per quelle standard, riducendo i costi di installazione, migliorando la diagnostica e permettendo l'installazione di 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 sono concepite per rilevare gli errori di trasmissione e attivare un'adeguata funzione di risposta agli errori. 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 generalmente chiamato "stato di sicurezza". Il modulo di comunicazione I/O di sicurezza deve rilevare questi errori di comunicazione e poi entrare, se necessario, in stato di sicurezza.

Le prime reti di sicurezza erano legate ad 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 ed un'altra per il controllo di sicurezza), con l'aumento dei costi di installazione, formazione e dei pezzi di ricambio.

Le moderne reti di sicurezza consentono di comunicare con dispositivi di controllo standard e di sicurezza mediante un unico cavo di rete. CIP (Common Industrial Protocol) Safety è un protocollo standard aperto, pubblicato da ODVA (Open DeviceNet Vendors Association), che permette la comunicazione di sicurezza tra i dispositivi di sicurezza su reti DeviceNet, ControlNet e EtherNet/IP. Dato che CIP Safety è una estensione del protocollo CIP standard, i dispositivi di sicurezza e quelli standard possono risiedere tutti sulla stessa rete. Gli utilizzatori possono anche collegare tra loro a ponte reti contenenti dispositivi di sicurezza, con la possibilità di suddividere i dispositivi di sicurezza per regolare con precisione i tempi di risposta o, semplicemente, per facilitare la distribuzione dei dispositivi

di sicurezza. Dato che il protocollo di sicurezza è di esclusiva responsabilità dei dispositivi finali (PLC/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 ausiliari servono a interrompere l'alimentazione elettrica dell'attuatore. Per consentirne l'uso in applicazioni di sicurezza, contattori e relè ausiliari sono dotati di funzioni speciali.

Per il feedback sullo stato dei contattori e dei relè ausiliari al dispositivo logico di monitoraggio si utilizzano contatti ausiliari a guida forzata. 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 60947-4-1 definisce i requisiti per i contatti a guida forzata. 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 ed 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. Si utilizzano dei contatti a specchio sui lati del contattore.

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 ausiliari sono concepiti per commutare grandi carichi, da 0,5 A 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, tipicamente 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 ed asservimenti

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

I convertitori di frequenza ottengono il livello di sicurezza con canali ridondanti per togliere alimentazione dalla circuiteria del controllo gate. I canali ridondanti, a seconda del tipo di azionamento, vengono monitorati dalla logica esterna o da quella integrata. 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 ai convertitori di frequenza, utilizzando segnali di sicurezza ridondanti per ottenere la funzione di sicurezza Safe Torque-off.

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 canale doppio, a canale doppio 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.

Capitolo 5: 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: (EN ISO 13855)

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

Formula

La distanza minima di sicurezza dipende dal tempo necessario ad 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 ed 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'angolo di 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 mm/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'utilizzatore 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, consultare lo standard corrispondente. Per un avvicinamento normale ad una barriera fotoelettrica o ad 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 ad una barriera fotoelettrica o ad 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.

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 (29,5)	1.200 (47,2)
2	400 (5,7), 900 (35,4)	850 (33,4)
3	300 (11,8), 700 (27,5), 1.100 (43,3)	850 (33,4)
4	300 (11,8), 600 (23,6), 900 (35,4), 1.200 (47,2)	850 (33,4)

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 perpendicolare a barriere fotoelettriche verticali la cui sensibilità agli oggetti è di 40 mm max, lo standard ISO EN richiede due fasi. Innanzitutto, calcolare S usando 2.000 come costante di velocità.

S = 2.000 x T + 8 x (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 ad 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 perpendicolari, mentre quelli inferiori a 30° dovrebbero essere 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. Se l'operatore deve salire su una piattaforma, il fattore di penetrazione in profondità può essere ridotto del 40% per l'altezza del passo. È importante fissare la pedana saldamente, per evitare che si muova.

Esempio

Esempio: un operatore si avvicina perpendicolarmente 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 diodo soppressore. 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 ed il valore C è zero. Il calcolo sarebbe il seguente:

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

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)

C = 8 (14-14) = 0

S = K x T + C
S = 1600 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 millimetri.

Capitolo 6: sistemi di controllo di sicurezza

Introduzione

Che cos'è un sistema di controllo di sicurezza (spesso abbreviato in SRCS)? Si tratta della parte di un sistema di controllo di una macchina atta ad 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 ad un sistema composto che comprende sia dispositivi semplici sia complessi, comunicanti attraverso software e hardware.

I sistemi di controllo di 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 ed una volta messa a punto, come dimostrare la sua efficacia?

Funzione di sicurezza

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

Una "condizione pericolosa" si verifica quando una persona potrebbe essere 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 protetto dal riparo.

Quando si definisce la funzione di sicurezza per una specifica applicazione, la parola “pericolo” deve essere sostituita dal pericolo specifico. La fonte del pericolo non deve essere confusa con le sue conseguenze. Schiacciamento, taglio ed ustioni sono le conseguenze di un pericolo. Esempi di fonti 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 pulsante di arresto di emergenza. Un operatore chiede che il pericolo sia bloccato o, se questa condizione già sussiste, che non sia trasmessa energia.

I componenti di 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 ad 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 livelli di prestazione relativamente alla loro 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

Che cos’è la sicurezza funzionale?

La sicurezza funzionale fa parte del requisito di sicurezza complessivo e 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. “Un esempio di sicurezza funzionale è un dispositivo di protezione da sovratemperatura che utilizza un sensore termico negli avvolgimenti di un motore elettrico per diseccitare il motore prima che possa surriscaldarsi. 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 ed 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 ed 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 dei task 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 “Sicurezza delle macchine – Parti dei sistemi di comando legate alla sicurezza”

   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 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 ed il sistema di categorie della precedente ISO 13849-1:1999 (EN 954-1:1996).

Le categorie non sono scomparse del tutto e vengono ancora utilizzate nell’attuale (EN) ISO 13849-1.

IEC/EN 62061 e (EN) ISO 13849-1

Sia IEC/EN 62061 che (EN) ISO 13849-1 riguardano i sistemi di controllo elettrici di sicurezza. È possibile che vengano fatti confluire in un unico standard con terminologia comune. Entrambi gli standard producono lo stesso risultato utilizzando, tuttavia, metodi diversi. Sono concepiti per offrire all’utilizzatore la possibilità di scegliere quello più adatto alla propria situazione. L’utilizzatore 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 forniscono livelli comparabili di integrità o prestazioni di sicurezza. Le metodologie di ogni standard presentano differenze a seconda degli utilizzatori 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 più adatto ai sistemi elettrici. Lo standard

(EN) ISO 13849-1 può essere invece applicato ai sistemi pneumatici, idraulici, meccanici ed elettrici.

Report tecnico congiunto su IEC/EN 62061 e (EN) ISO 13849-1

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

Questo report illustra la relazione 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 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 richiesti.

In generale, il ricorso alle esclusioni dei guasti non è applicabile agli aspetti meccanici degli interruttori di posizione elettromeccanici per ottenere PLe nella progettazione di un sistema di controllo di sicurezza. Le esclusioni dei guasti applicabili a specifiche condizioni di guasto meccaniche (ad es. usura/corrosione, rottura) sono indicate nella Tabella A.4 di ISO 13849-2.

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 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, SIL 1 è il più basso e SIL 3 è 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 SIL 4.

Un SIL si applica ad 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

(EN) ISO 13849-1 non usa il termine SIL; usa il termine PL (livello prestazionale). 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	$\geq 10^{-5}$ a $<10^{-4}$	Nessuno
b	$\geq 3 \times 10^{-6}$ a $<10^{-5}$	1
c	$\geq 10^{-6}$ a $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ a $<10^{-6}$	2
e	$\geq 10^{-8}$ 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. Le tabelle nell'Allegato K forniscono informazioni più dettagliate.

Capitolo 7: progettazione dei sistemi secondo (EN) ISO 13849

Prima di poter applicare correttamente (EN) ISO 13849-1, è necessario uno studio completo e dettagliato dello standard. 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 ad un sistema di sicurezza ma può anche applicarsi ai componenti del sistema.

Strumento software per il calcolo dei livelli prestazionali SISTEMA

SISTEMA è uno strumento software per l'implementazione di (EN) ISO 13849-1 che semplifica notevolmente gli aspetti di quantificazione e calcolo dell'implementazione dello standard.

SISTEMA sta per "Safety Integrity Software Tool for the Evaluation of Machine Applications" e viene regolarmente rivisto e aggiornato da IFA. 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 la libreria di dati SISTEMA del costruttore.

La libreria SISTEMA di Rockwell Automation è a disposizione degli utilizzatori, e può essere scaricata utilizzando un link al sito di download di SISTEMA accessibile da: *www.rockwellautomation.com, in Solutions & Services > Safety Solutions.*

Cenni generali su (EN) ISO 13849-1

La descrizione generale che segue serve a presentare le disposizioni di base di (EN) ISO 13849-1. Contiene anche dei riferimenti alla revisione pubblicata all'inizio del 2016. È indispensabile che lo standard venga studiato in tutti i suoi dettagli. 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 componenti complessi con software integrato rimanda il lettore anche a IEC 61508.

In ISO 13849-1 si parla di livelli prestazionali [PL a, b, c, d, e]. Il concetto originale di Categoria è stato mantenuto ma, perché 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 l'efficacia del monitoraggio dei guasti 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 considerazioni aggiuntive di cui tener conto, ma i dettagli saranno più chiari una volta compreso che cosa lo standard cerca di ottenere e perché.

La prima domanda è perché abbiamo bisogno di questo 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. Attualmente, assistiamo a un crescente utilizzo di dispositivi elettronici e programmabili sempre 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 gli standard sulla sicurezza funzionale richiedono più informazioni. Dato che i sistemi di sicurezza utilizzano attualmente un approccio a "scatola nera", integrando sottosistemi prequalificati, 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 utilizzatori: il progettista di sottosistemi di sicurezza ed il progettista di sistemi di sicurezza. In generale, al progettista di sottosistemi [generalmente il costruttore di un componente di sicurezza] si richiede un livello di rigore 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 [generalmente un progettista di macchine o un integratore] userà i dati del sottosistema per eseguire alcuni calcoli relativamente semplici nell'ambito della determinazione del livello prestazionale [PL] generale raggiunto dal sistema.

Determinazione della funzione di sicurezza

Dobbiamo definire la funzione di sicurezza. Indubbiamente, la funzione di sicurezza deve essere appropriata al task richiesto. 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 aiuto elencando molte delle funzioni di sicurezza più comunemente usate (ad es. funzione di arresto di sicurezza attivata da una protezione, funzione di muting, funzione di avviamento/riavviamento) e indicando alcuni requisiti normalmente associati a esse. In questa fase, è consigliabile lo studio di (EN) ISO 12100: "Principi generali di progettazione e valutazione dei rischi". ISO TR 22100-2 fornisce utili istruzioni sulla relazione tra il processo di valutazione dei rischi della macchina previsto in ISO 12100 e il processo di assegnazione dei PL di (EN) ISO 13849-1. Esiste inoltre una vasta gamma di standard specifici per le macchine in grado di fornire i requisiti delle funzioni di sicurezza per determinate macchine. Nell'ambito degli standard EN europei sono detti standard di tipo C, la maggior parte dei quali ha un equivalente ISO. ISO TR 22100-1 fornisce ulteriori informazioni sulle relazioni tra ISO 12100 e gli standard C.

È evidente 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'utilizzatore. L'utilizzatore della macchina deve verificare che esse corrispondano alle reali condizioni di utilizzo.

Per indicare il livello prestazionale richiesto dalla funzione di sicurezza si usa la sigla PLr. Il livello Plr è determinato durante la valutazione dei rischi. 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.

Il risultato è il PLr. Chi usava la vecchia norma EN 954-1 ha familiarità con questo tipo di approccio ma va sottolineato che, nell'ambito di (EN) ISO 13849-1, la linea S1 si suddivide, contrariamente a quanto avveniva nel vecchio grafico del rischio. La versione 2015 offre la possibilità di ridurre il PLr di un livello in alcune circostanze, a seconda della probabilità di occorrenza prevedibile.

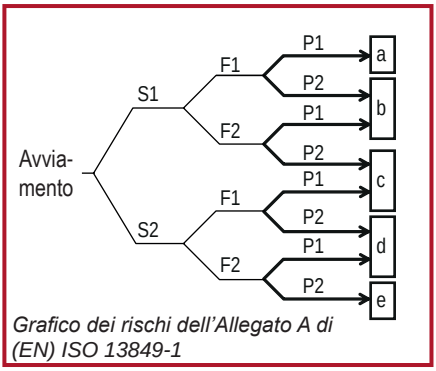


Grafico dei rischi dell'Allegato A di (EN) ISO 13849-1

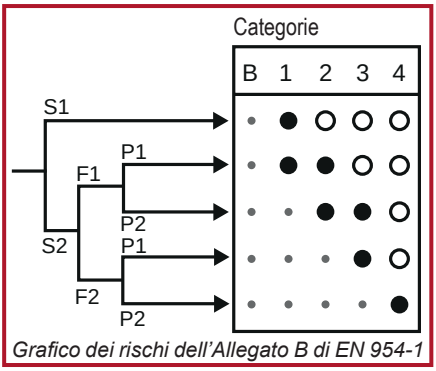


Grafico dei rischi dell'Allegato B di EN 954-1

Così, ora abbiamo una descrizione della funzionalità di sicurezza e del livello prestazionale richiesto [PLr] per le parti del sistema di controllo di sicurezza [SRP/CS] 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 uno strumento software, chiamato SISTEMA, che supporta l'utilizzatore per quanto riguarda gli aspetti della documentazione e del calcolo, consentendo anche di produrre un dossier tecnico.

SISTEMA è disponibile in diverse lingue, tra cui tedesco e inglese. IFA, l'azienda sviluppatrice di SISTEMA, è un istituto tedesco di ricerca e test 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.

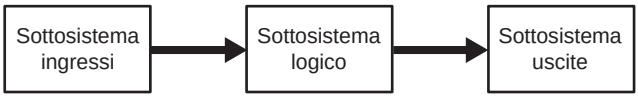
I tecnici IFA e i loro colleghi della BG hanno dato un grande contributo alla stesura di entrambe le norme (EN) ISO 13849-1 e IEC/EN 62061.

Rockwell Automation mette a disposizione una “libreria” dei propri dispositivi di sicurezza da utilizzare con SISTEMA, disponibile sul seguente sito: *www.rockwellautomation.com, in Solutions & Services > Safety Solutions.*

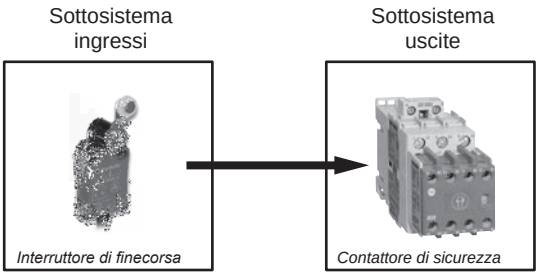
A prescindere da come viene effettuato il calcolo del PL, è importante partire dalla giusta base. Dobbiamo vedere il nostro sistema con gli stessi occhi dello standard, quindi cominciamo da qui.

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 ed attuazione [alcuni sistemi semplici non hanno logica].

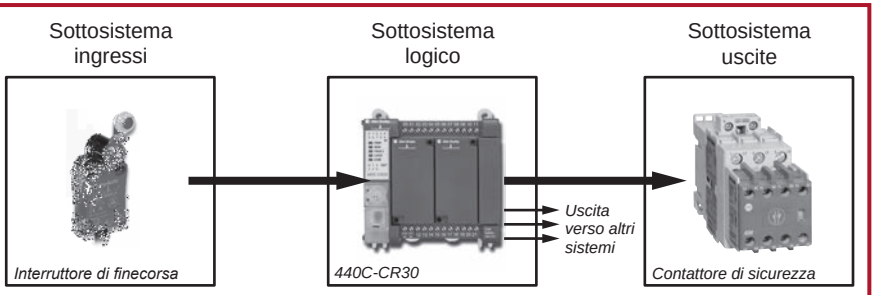


I gruppi di componenti che attuano queste funzioni sono detti sottosistemi.



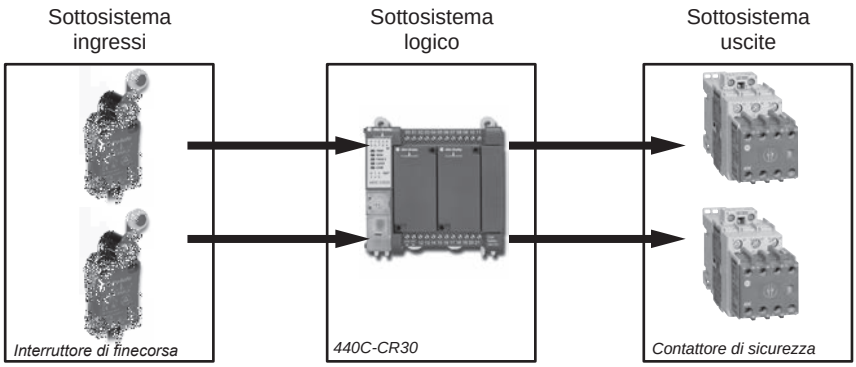
Interruttore di interblocco e contattore di sicurezza

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



Interruttore di interblocco, controllore di sicurezza e contattore di sicurezza

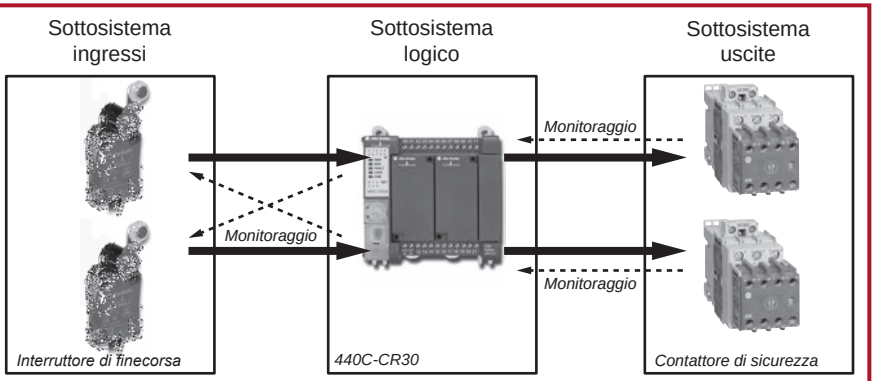
Il sistema sopra illustrato è leggermente più complesso perché è richiesta anche della logica. Il controllore di sicurezza di per sé è internamente tollerante ai guasti (ad es. a canale doppio), ma il sistema nel suo complesso è ancora limitato allo stato di canale singolo perché singoli sono i sottosistemi ovvero l'interruttore di finecorsa e il contattore. Se uno dei suoi sottosistemi a canale singolo si guasta, un sistema a canale singolo va in guasto; non è "tollerante ai guasti".



Sistema di sicurezza a canale doppio

Sopra è illustrato un sistema a canale doppio [detto anche ridondante o "tollerante a guasti"]. Ogni sottosistema ha due canali ed è quindi in grado di tollerare un guasto singolo continuando a fornire la funzione di sicurezza. Questa funzione di sicurezza deve subire due guasti, uno in ogni canale, prima che il sottosistema e il sistema vadano in guasto. Chiaramente un sistema a canale doppio ha meno probabilità di fallire in una condizione pericolosa rispetto ad 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

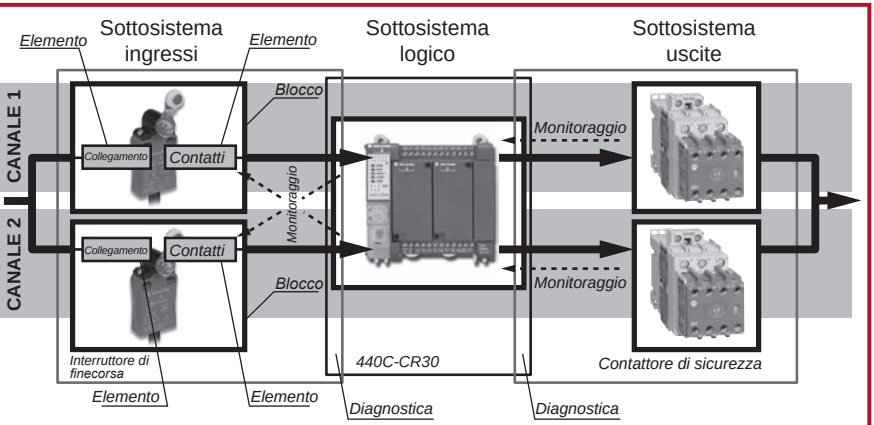
e mettere il sistema in uno stato sicuro. Il seguente schema mostra l'inserimento di misure diagnostiche ottenute con tecniche di monitoraggio.



Diagnostica con un sistema di sicurezza a canale doppio

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 ed 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. Lo strumento SISTEMA usa il termine di "elementi" per questi componenti.



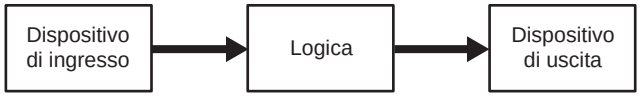
Sistema suddiviso con diagnostica con un sistema di sicurezza a canale doppio

Il sottosistema degli interruttori di finecorsa viene mostrato scomposto fino a livello di elemento. Il sottosistema dei contattori di uscita è suddiviso fino al livello di blocco. Il sottosistema logico non è suddiviso perché già qualificato e validato dal costruttore a un determinato PL. 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 per lo strumento 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 il sistema completo in canali e in blocchi all'interno di ciascun canale. Con SISTEMA, è generalmente più comodo dividere il sistema in sottosistemi e poi ogni sottosistema in blocchi. Lo standard non definisce esplicitamente il concetto di sottosistema ma l'uso indicato da SISTEMA prevede un approccio più comprensibile ed 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.

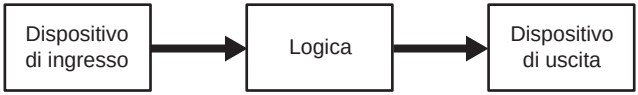
Il sistema che abbiamo illustrato come esempio è solo uno dei cinque tipi base di architetture del sistema previste dallo standard. Chi conosce il sistema delle categorie saprà che questo esempio è rappresentativo della Categoria 3 o 4.

Lo standard utilizza le cinque categorie originali del precedente standard EN 954 definendole "categorie di architettura designata". 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 ad un sistema completo che ad un sottosistema. Gli schemi non devono essere visti necessariamente come una struttura fisica ma piuttosto come una rappresentazione grafica di requisiti concettuali.



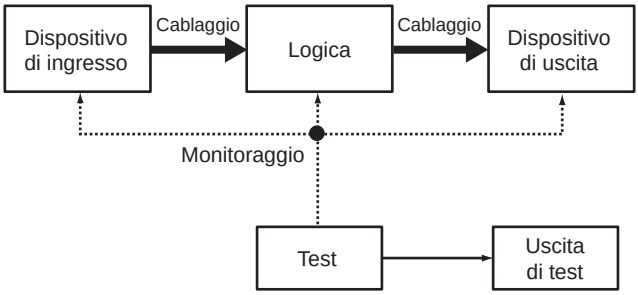
Categoria di architettura designata B

La Categoria di Architettura Designata B deve adottare i principi di sicurezza base [vedere l'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.



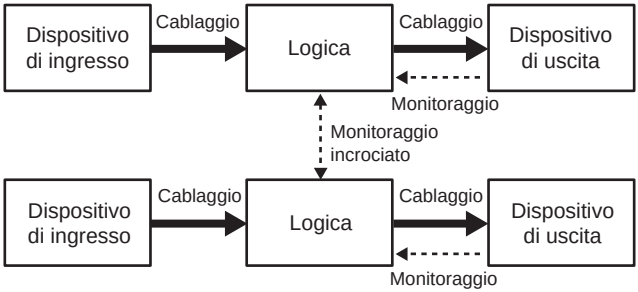
Categoria di architettura designata 1

La categoria di architettura designata 1 ha la stessa struttura della categoria B e può ancora fallire in caso di singolo guasto. Poiché si avvale di principi di sicurezza comprovati [vedere l'allegato di (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.



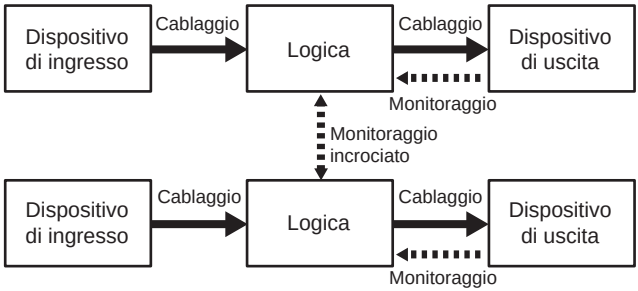
Categoria di architettura designata 2

La Categoria di Architettura Designata 2 deve adottare i principi di sicurezza base [vedere l'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. La revisione del 2015 ammette un requisito alternativo perché la funzione di sicurezza entri in stato di sicurezza prima del tempo di sicurezza del processo. Il sistema o sottosistema può comunque andare in guasto se si verifica un guasto singolo tra i test funzionali, ma questo è generalmente meno probabile che per la Categoria 1. Va sottolineato che, per la Categoria 2 utilizzata per PLd, ci devono essere due dispositivi di uscita del segnale perché, in caso di rilevamento di un guasto, l'uscita di test deve attivare uno stato di sicurezza. Per i requisiti completi, consultare lo standard (EN) ISO 13849-1.



Categoria di architettura designata 3

La Categoria di Architettura Designata 3 deve adottare i principi di sicurezza base [vedere gli allegati 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 guasti [spesso definita come "ridondanza stupida"] a un sistema ridondante in cui vengono 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 [$MTTF_D$] del sistema, minore è la copertura DC necessaria. In ogni caso, tuttavia, per l'architettura di Categoria 3, la DC deve essere almeno pari al 60%.



Categoria di architettura designata 4

La Categoria di Architettura Designata 4 deve adottare i principi di sicurezza base [vedere gli allegati 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 pericolosi e tutte le combinazioni pericolose di guasti. In pratica, questo si ottiene con un livello elevato di diagnostica che assicuri che tutti i guasti rilevanti vengano rilevati prima che si accumulino. La copertura DC deve essere almeno del 99%.

Dati di affidabilità

Lo standard (EN) ISO 13849-1 utilizza dati quantitativi di affidabilità nel calcolo del PL ottenuto dalle parti di sicurezza di un sistema di controllo. 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 costruttore. A tal fine, Rockwell Automation ha reso disponibili le informazioni rilevanti sotto forma di libreria dati per il software SISTEMA.
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 utilizzati in IEC 61508 e 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	$\geq 10^{-5}$ a $<10^{-4}$	Nessuno
b	$\geq 3 \times 10^{-6}$ a $<10^{-5}$	1
c	$\geq 10^{-6}$ a $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ a $<10^{-6}$	2
e	$\geq 10^{-8}$ a $<10^{-7}$	3

La tabella qui sopra mostra il rapporto tra PFH_D, PL e SIL. Per alcuni sottosistemi, il PFH_D può essere disponibile presso il costruttore. Questo facilita il calcolo.
Il costruttore 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’$MTTF_D$ medio [tempo medio prima di un guasto pericoloso] di un canale singolo.

Il PL [e quindi il PFH_D] 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 canale doppio (con o senza diagnostica), non è corretto utilizzare $1/PFH_D$ per determinare l'$MTTF_D$ richiesto dallo standard (EN) ISO 13849-1, in quanto lo standard richiede il calcolo dell'$MTTF_D$ di un canale singolo. Questo valore è molto diverso dall'$MTTF_D$ 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.

$MTTF_D$ di un canale singolo

Rappresenta il tempo medio prima del verificarsi di un guasto che può portare ad un errore della funzione di sicurezza, e si esprime in anni. Si tratta di un valore medio degli $MTTF_D$ dei "blocchi" di ciascun canale e può essere applicato ad un sistema o a un sottosistema. Lo standard indica la seguente formula che viene usata per calcolare la media di tutti gli $MTTF_D$ 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 ad 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'$MTTF_D$ in tre campi:

Denotazione dell'$MTTF_D$ di ogni canale	Campo $MTTF_D$ di ogni canale
Bassa	3 anni <= $MTTF_D$ < 10 anni
Media	10 anni <= $MTTF_D$ < 30 anni
Alta	30 anni <= $MTTF_D$ < 100 anni

Livelli di $MTTF_D$

Si noti che lo standard (EN) ISO 13849-1 limita l'$MTTF_D$ 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 si vedrà più avanti, il campo ottenuto della media degli $MTTF_D$ viene poi combinato con la categoria di architettura designata e la copertura diagnostica [DC], per fornire un valore PL preliminare. 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

Segue un approfondimento sulle modalità con cui il costruttore determina i dati sotto forma di PFH_D o $MTTF_D$. Quando si parla di dati di un costruttore, 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 ed 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 ad 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 vengono modellati, stampati, fusi, lavorati ecc. e 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 $MTTF_D$ per il meccanismo si basa di norma su test. Gli standard EN/IEC 62061 ed (EN) ISO 13849-1 prevedono entrambi l'esecuzione di una prova denominata test $B10_D$.

Durante il test $B10_D$ 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.

Tecnologia elettronica

In questo caso non si verifica alcuna usura fisica relativa alle parti mobili. Dato un ambiente operativo commisurato alle specifiche caratteristiche elettriche e di temperatura, 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 tensione eccessivi, problemi di accoppiamento meccanico ecc. In genere, i guasti ai componenti elettronici possono essere dovuti a condizioni di carico, tempo e temperatura ma 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.

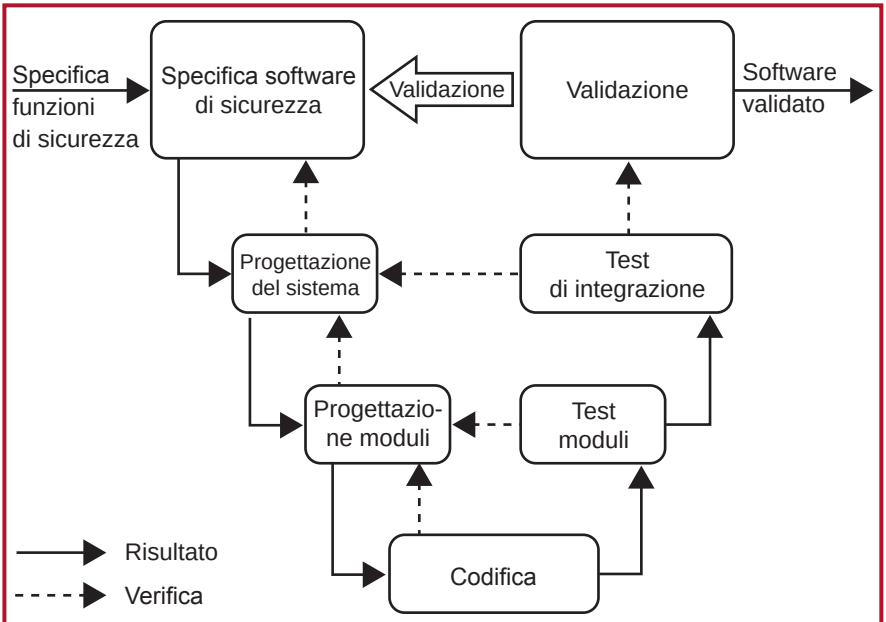
Per determinare l'affidabilità dei dispositivi elettronici si è soliti ricorrere all'analisi ed al calcolo. Esistono dati di affidabilità, in cui è possibile reperire dati utili relativi ai singoli componenti. Tramite l'analisi si possono individuare le modalità di guasto dei componenti che risultano pericolose. È pratica accettabile e usuale fare una media valutando le modalità di guasto come sicure al 50% e pericolose al 50%. 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 costruttore del dispositivo. Sia EN/IEC 62061 che (EN) ISO 13849-1 accettano un sottosistema calcolato in questo modo in base a

IEC 61508. Il PFH_D che ne risulta può essere utilizzato direttamente nell'Allegato K di (EN) ISO 13849-1 o nello strumento 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 IEC 61508 che (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 si interfaccia l'utilizzatore, la maggior parte dei dispositivi di sicurezza programmabili è dotata di routine o blocchi funzione "certificati". Ciò semplifica il compito di validazione 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 ad una perdita della funzione di sicurezza, ma sono rilevabili. Dopo il rilevamento, una funzione di risposta al 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 ad 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 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 ma consente anche l'uso del metodo semplificato sotto forma di tabelle di conversione, come previsto in (EN) ISO 13849-1. Qui sono elencate varie tecniche diagnostiche tipiche con la percentuale DC che si intende ottenere. In alcuni casi si richiede ancora un giudizio razionale, ad 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 si basano su un'ampia attività di ricerca condotta da IFA, 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
da 60% a <90% = bassa
da 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. Lo strumento SISTEMA si avvale delle stesse tabelle di consultazione dello standard. Poiché i dispositivi di 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 ed 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 ed indipendenti si verifichino entro tale termine. Tuttavia, lo standard indica che dobbiamo considerare attentamente se le possibilità di guasto sono davvero separate ed 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 guasto CCF è in genere indicato come fattore beta (β). 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 un compromesso tra complessità e 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 ed 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 lo strumento SISTEMA di IFA richiede l'applicazione delle tabelle di conversione relative ai CCF dello standard e le rende disponibili in una forma pratica.

Guasti sistematici

Abbiamo già parlato della quantificazione dei dati di affidabilità sotto forma di $MTTF_D$ 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 alla probabilità di un guasto hardware casuale. Ma vi sono alcuni tipi di guasti definiti collettivamente come "guasti sistematici" che possono essere attribuiti ad 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 ed 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. Ad 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 di sicurezza.

(EN) ISO 13849-1 ammette l'esclusione dei guasti in base all'improbabilità tecnica che si verifichino, all'esperienza tecnica comune e ai requisiti tecnici legati all'applicazione. (EN) ISO 13849-2 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 di 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 di sicurezza, 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.

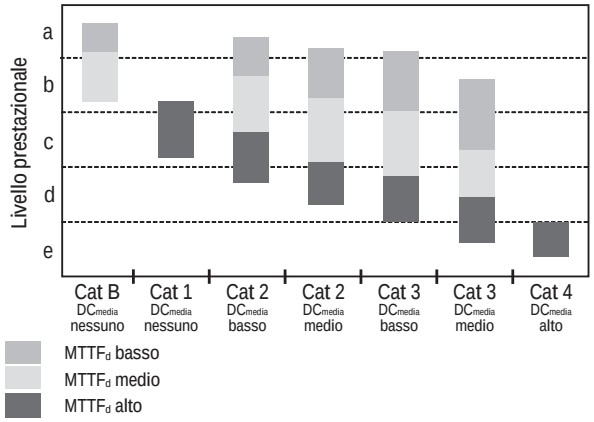
Livelli prestazionali (PL)

Il livello prestazionale è un livello discreto che specifica la capacità dei componenti di 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 nell'Allegato K mostra i risultati tabulari di differenti modelli Markov che sono alla base di questo grafico. 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 ed il ciclo di vita. Se il PFH_D del sistema o sottosistema è conosciuto, le tabelle nell'Allegato K possono essere usate per ricavare il PL.

Progettazione dei sottosistemi e combinazioni

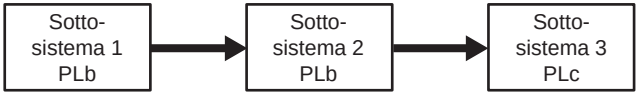
I sottosistemi conformi ad un PL possono essere combinati in un sistema usando la tabella come illustrato.

PLbasso	**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

L'uso di questa tabella dello standard non è obbligatorio, ma fornisce un metodo molto semplice e alternativo a quello del caso peggiore se i valori PFHd non sono conosciuti. Il sistema PL può essere calcolato con altri metodi, tra cui SISTEMA. La logica della 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.

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 PLbasso) e 2 (nella colonna Nbasso) 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

Validazione

La validazione delle funzioni di sicurezza include e va oltre la verifica dei livelli prestazionali ottenuti. L'intento è quello di verificare che la funzione di sicurezza implementata supporti nei fatti i requisiti di sicurezza globale delle macchine. La validazione svolge un ruolo importante in tutto il processo di sviluppo e di messa in servizio del sistema di sicurezza. Lo standard ISO/EN 13849-2:2012 definisce i requisiti per la validazione e richiede la definizione di un piano di validazione 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 costruttore 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 validazione 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 ed operative esistenti. Alcune di queste caratteristiche possono essere diverse da quelle anticipate in fase progettuale.

Capitolo 8: 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 risposta 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	HFT
Percentuale di guasti non pericolosi	SFF
Intervallo dei test diagnostici	T_1
Intervallo di test diagnostici	T_2
Suscettibilità ai guasti per causa comune	β
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 per 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 all'$MTTF_D$ 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 all'ora (PFH_D) dei singoli sottosistemi vengono quindi sommate per determinare il PFH_D totale del sistema. La 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.

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

Probabilità di guasto pericoloso per SIL

I dati di PFH_D relativi ad un sottosistema vengono normalmente forniti dal costruttore. I dati dei componenti e dei sistemi di sicurezza Rockwell Automation sono disponibili all'indirizzo:

www.rockwellautomation.com, in Solutions & Services > Safety Solutions

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 ed 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 B10d o simili dati in PFH_D.
NOTA: in generale, la seguente relazione è vera (inserendo un fattore per convertire gli anni in ore):

$PFH_D = 1/MTTF_D$

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

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 non pericolosi 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 non pericolosi 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 quindi il relativo sistema) deve soddisfare sia i requisiti a livello di $PFHD_D$ che i vincoli hardware, oltre alle altre disposizioni pertinenti dello standard.

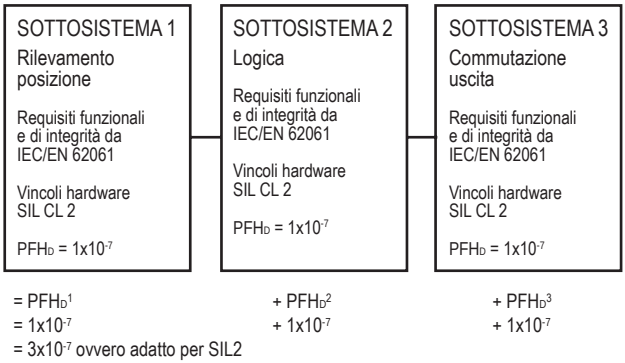
SFF (percentuale di guasti non pericolosi)	Tolleranza ai guasti hardware		
	0	1	2
<60%	Non ammesso se non per specifiche eccezioni	SIL1	SIL2
60% – <90%	SIL1	SIL2	SIL3
90% – <99%	SIL2	SIL3	SIL3
≥99%	SIL3	SIL3	SIL3

Vincoli hardware su SIL

Ad esempio, l'architettura di un sottosistema con tolleranza a un singolo guasto e una percentuale di guasti non pericolosi 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 ad un dispositivo logico collegato, a sua volta, ad 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, ad esempio, vogliamo ottenere SIL 2, ogni sottosistema deve avere un SIL Claim Limit (SIL CL) di almeno SIL 2 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 costruttore del dispositivo (sottosistema) e sono molto più complessi di quelli richiesti per la progettazione di sistema.

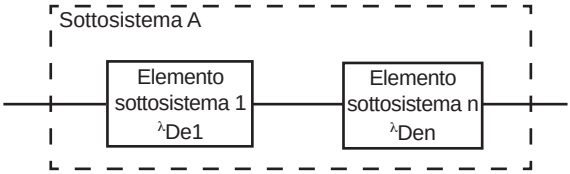
Progettazione del sistema secondo IEC/EN 62061

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. Ad 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.

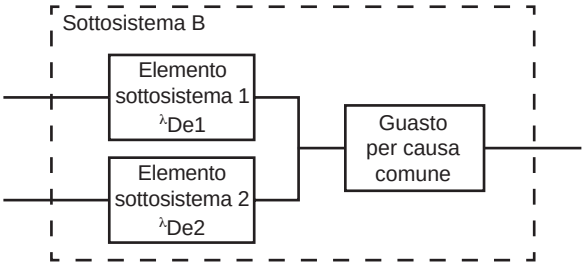


Architettura logica sottosistema A

$\lambda DssA = \lambda De1 + \ldots + \lambda Den$
$PFHDssA = \lambda DssA$

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 λ. λDssA 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 ad un singolo guasto, senza una funzione di diagnostica. Quando una architettura include la tolleranza ad 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

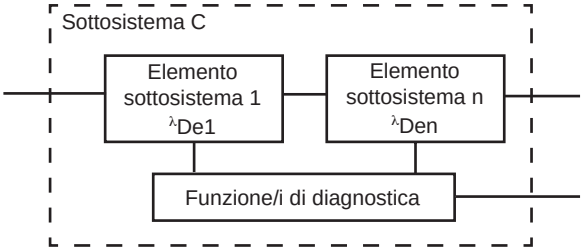
DssB = $(1-\beta)^2$ x *λDe1* x *λDe2* x T1 + β x (*λDe1* + *λDe2*)/2
PFHDssB = λDssB

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”.

β – 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 ed il degrado del sottosistema di sicurezza, in modo che il sottosistema possa essere riportato ad 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.

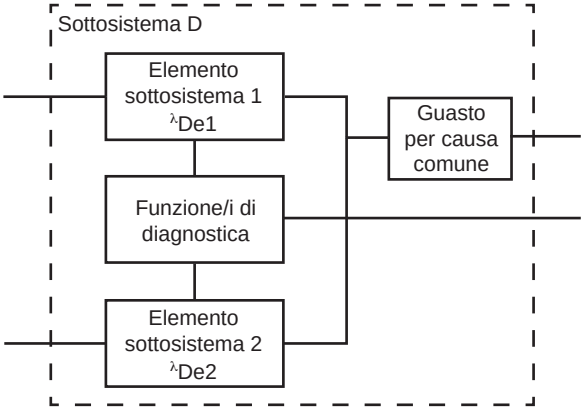


Architettura logica sottosistema C

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

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 ed 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:

λDssD = (1 – β)2 {[λDe1 x λDe2 x (DC1+ DC2)] x T2/2 + [λDe1 x λDe2 x (2- DC1 – DC2)] x T1/2 } + β x (λDe1 + λDe2)/2
PFHDssD = λDssD

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

$A_{DssD} = (1 – \beta)^2 \{[\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1\text{-}DC)] \times T_1 \} + \beta \times \lambda_{De}$
PFHDssD = λDssD

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 identici:

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

PFH_{DssD} = 5,790E-8 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 PFHDssD = 6,58E-8. Rientra ancora nel campo richiesto per SIL 3. 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 β (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-8, che significa che il sottosistema ora è più adatto a essere impiegato in un sistema SIL 3.

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 costruttore. 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.

No	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 (R)
<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 compreso tra zero e 99%.

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. Ad 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 di 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 lo definisce 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 con la funzione di diagnostica (se presente). Canali separati devono essere testati separatamente.

Diversamente dai test delle funzioni di autodiagnosi, che sono automatici, i test diagnostici vengono generalmente realizzati manualmente ed offline. Essendo automatici, i test di autodiagnosi sono realizzati più spesso rispetto ai test funzionali che, invece, vengono realizzati raramente. Ad 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. ad impulsi).

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

preferisce sostituire semplicemente il sottosistema con uno nuovo anziché eseguire effettivamente un test diagnostico.

SFF (percentuale di guasti non pericolosi)

La percentuale di guasti non pericolosi è simile alla copertura diagnostica ma considera anche qualunque tendenza intrinseca a generare un guasto in stato di sicurezza. Ad 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.

Il valore SFF viene generalmente dichiarato dal costruttore, se pertinente.

Il valore SFF può essere calcolato con la seguente equazione:

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

dove:

$\sum_S$ = tasso di guasti non pericolosi,
$\sum\lambda_S + \sum\lambda_D$ = 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 qualche forma di 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 ad evitare i guasti sistematici ci sono le seguenti:

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

Capitolo 9: sistemi di controllo di sicurezza, considerazioni aggiuntive

Cenni generali

In questo capitolo verranno riportati principi e considerazioni strutturali da tenere presenti durante la progettazione di un sistema di controllo di sicurezza.

Categorie dei sistemi di controllo

Le “Categorie” dei sistemi di controllo derivano dal precedente standard EN 954-1:1996 (ISO 13849-1:1999). Tuttavia, le categorie vengono tuttora spesso utilizzate per descrivere la struttura dei sistemi di controllo di sicurezza e rimarranno parte integrante dello standard (EN) ISO 13849-1 come “Architetture designate”. La descrizione e la discussione dei requisiti delle categorie sono riportate, nella prima parte di questa pubblicazione, con il titolo “Cenni generali su (EN) ISO 13849-1”. Questa sezione intende fornire una guida semplificata ma pratica su come implementare le strutture delle categorie.

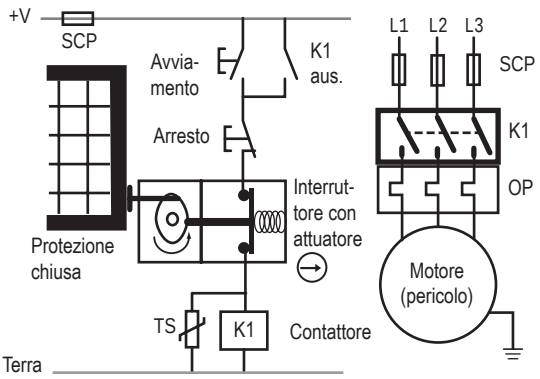
Categoria B

La Categoria B dovrebbe essere considerata come la base su cui sono costruite tutte le altre categorie. Non ha alcuna disposizione o struttura speciale per la sicurezza, a parte i principi di sicurezza base forniti negli allegati da A a D di (EN) ISO 13849-2. Questi rappresentano una buona pratica generale per la progettazione e la selezione dei materiali.

Categoria 1

La Categoria 1 richiede l’uso di componenti di comprovata efficienza e di principi di sicurezza collaudati.

Qui è illustrato un tipico sistema concepito per ottenere la Categoria 1. Interblocco e contattore svolgono il ruolo chiave di scollegare l’alimentazione del motore, quando è necessario accedere al pericolo. L’interblocco con attuatore soddisfa i 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 minimizzare la possibilità di perdita della funzione di sicurezza, ma va sottolineato che un guasto singolo può ancora comportare la perdita della funzione di sicurezza.

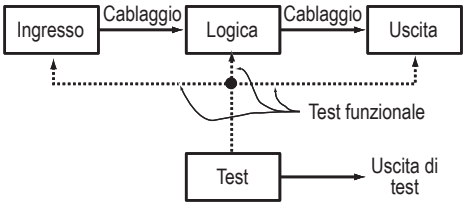


Semplice sistema di sicurezza di Categoria 1

La Categoria 1 mira a prevenire il guasto mediante una progettazione semplice con componenti ad affidabilità elevata. Quando questo tipo di 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 soddisfare i requisiti della Categoria B e ad utilizzare principi di sicurezza di comprovata efficienza, il sistema di sicurezza deve essere sottoposto a test per soddisfare i 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. Se vengono rilevati guasti, una funzione di risposta ai guasti deve assicurare che la macchina rimanga in uno stato di sicurezza.



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:

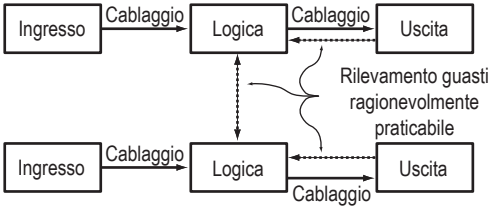
- alla prima accensione della macchina,
- prima della generazione di un pericolo, e
- periodicamente, se ritenuto necessario dalla valutazione dei rischi

Nota: (EN) ISO 138491-1 presuppone che il tasso di domanda della funzione di sicurezza sia 100 volte inferiore al tasso di domanda della funzione di test, con capacità di rilevare un guasto e fermare la macchina in un tempo più breve di quello necessario a raggiungere il pericolo.

In pratica, un sistema o sottosistema di sicurezza deve essere provato per verificare se la sua funzione di sicurezza funziona ancora correttamente. Ciò può essere difficile o impossibile da implementare con tecnologie che hanno caratteristiche meccaniche. Un approccio di Categoria 2 è generalmente più adatto alla tecnologia elettronica. Per PLd deve esserci un'uscita di test in grado di attivare uno stato sicuro in caso di rilevamento di un guasto.

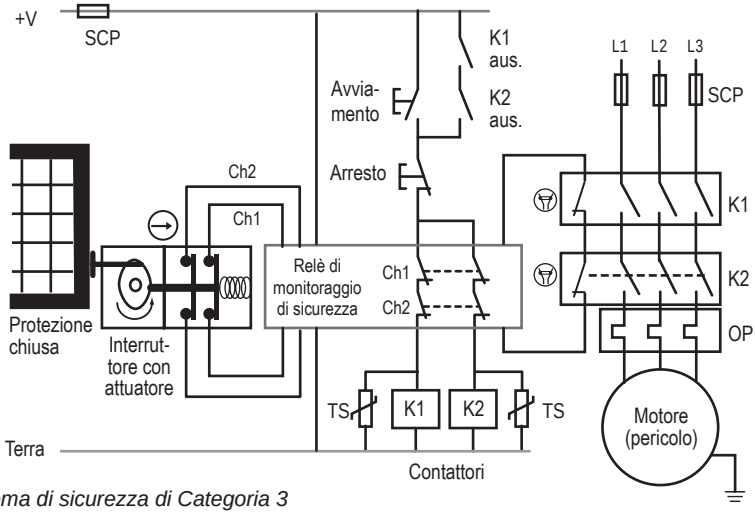
Categoria 3

Oltre a soddisfare i requisiti della Categoria B e i 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.
Alcuni guasti, come quelli incrociati, che non provocano la perdita immediata della funzione di sicurezza possono non essere rilevati. Ciò significa che, per la Categoria 3, un accumulo di guasti non rilevati 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 ed al monitoraggio incrociato e delle uscite.

Sistemi di controllo di sicurezza, considerazioni aggiuntive



Sistema di sicurezza di Categoria 3

Questo è un esempio di sistema di Categoria 3. L'interruttore interbloccato con attuatore ha un set ridondante di contatti. 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 a guida forzata.

Il rilevamento dei guasti deve essere preso in esame per ogni parte del sistema di sicurezza. 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?

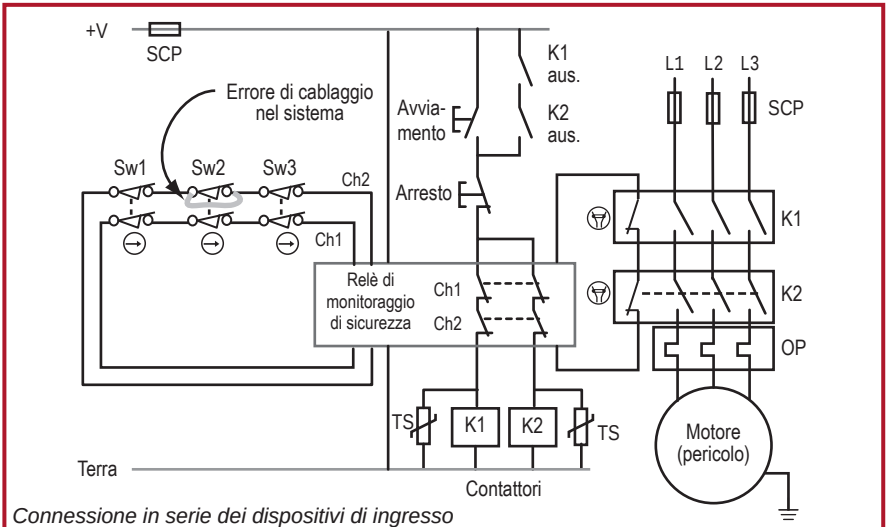
Per i circuiti di Categoria 3, è pratica comune utilizzare singoli interruttori interbloccati con attuatore con set di contatti elettrici ridondanti. Ciò significa che la possibilità di un guasto di un singolo componente nel collegamento di azionamento deve essere esclusa. Se tale guasto non può essere escluso, significa che un guasto singolo può causare la perdita della funzione di sicurezza. È molto importante che qualunque esclusione di guasto sia pienamente giustificata.

Il relè di monitoraggio di sicurezza (MSR) assicura la diagnostica dei guasti per l'interruttore interbloccato con attuatore e per i contattori. L'MSR può facilitare anche altre funzionalità come, ad esempio, un reset manuale. In termini di architettura interna, i relè di monitoraggio di sicurezza sono generalmente PLe o SIL3.

I due contattori dovrebbero essere protetti da sovraccarichi e cortocircuiti. La probabilità di guasto del contattore per contatti saldati è bassa, ma non impossibile. Un contattore si può guastare anche a causa di contatti di commutazione che rimangono chiusi in seguito al blocco dell'indotto. Se il guasto di un contattore genera uno stato pericoloso, il secondo contattore continua a funzionare ed interrompe l'alimentazione del motore. 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 a guida forzata del contattore guasto rimangono aperti e il relè MSR, non essendo in grado di chiudere i contatti di sicurezza, segnala 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 ad un relè di monitoraggio di sicurezza. Ogni dispositivo contiene due contatti ad azione di apertura diretta, normalmente chiusi. 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 all'interno di questa struttura quando si utilizza lo standard (EN) ISO 13849-1 o IEC 62061. Fino alla pubblicazione di ISO TR 24119 (novembre 2015: valutazione della connessione seriale di mascheramento dei guasti dei dispositivi di interblocco associati a protezioni con contatti puliti) non c'erano specifiche istruzioni definitive in merito, ma era usuale presumere una copertura DC del 60%, a condizione che gli interruttori fossero testati singolarmente a intervalli di tempo adeguati per rilevare i guasti. Se prevedibilmente uno (o più) interruttori non sarebbero mai stati testati singolarmente, la relativa copertura DC avrebbe dovuto essere pari a zero. ISO TR 24119 fornisce istruzioni dettagliate per la determinazione della copertura DC dei dispositivi di interblocco della protezione con contatti puliti collegati in serie. La tabella che segue fornisce una descrizione di base. È indispensabile studiare a fondo il documento per determinare l'effettiva copertura DC ammissibile massima di qualunque particolare architettura e applicazione.

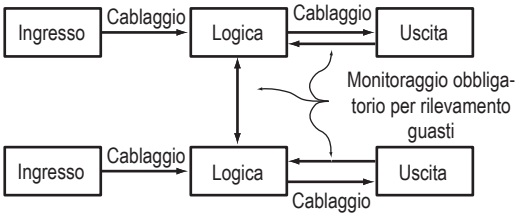
Numero di protezioni mobili utilizzate frequentemente[1]	Numero di protezioni mobili aggiuntive	Probabilità di mascheratura	Copertura diagnostica	PL massimo ottenibile
0	da 2 a 4	Bassa	Media	PL d
	da 5 a 30	Media	Bassa	PL d
	>30	Alta	Nessuno	PL c
1	1	Bassa	Media	PL d
	da 2 a 4	Media	Bassa	PL d
	≥5	Alta	Nessuno	PL c
>1	--	Alta	Nessuno	PL c

[1] Frequenza di commutazione superiore ad una volta all'ora

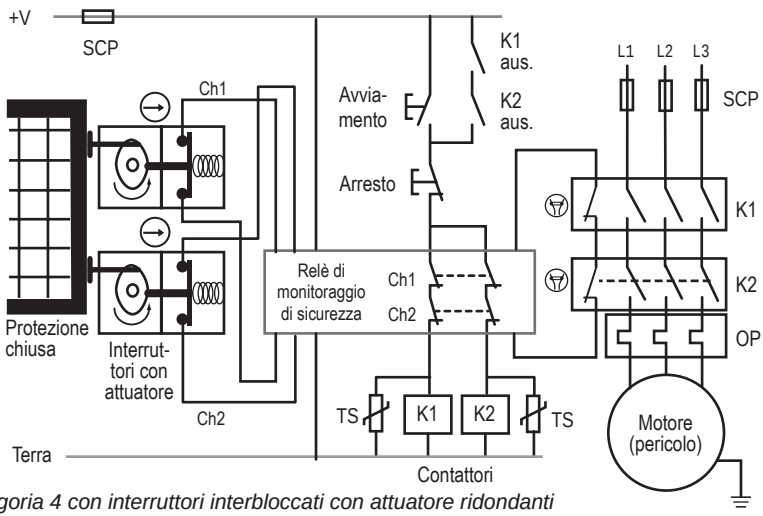
La connessione in serie dei contatti elettromeccanici può arrivare al massimo a PLd e, in alcuni casi, può essere limitata a PLc. In ogni caso va sottolineato che, se è prevedibile la mascheratura dei guasti (ad es. diverse protezioni mobili si apriranno allo stesso tempo nell'ambito del normale funzionamento o durante gli interventi di assistenza), la copertura DC sarà limitata a "Nessuna".
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 gli standard sulla sicurezza funzionale.

Categoria 4

Come la Categoria 3, la Categoria 4 impone che il sistema di sicurezza risponda alla Categoria B, usi principi di sicurezza collaudati 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. In pratica, questo si ottiene con un livello elevato di diagnostica che assicuri che tutti i guasti rilevanti vengano rilevati prima che si accumulino. Quando si considera un accumulo teorico di guasti, 2 guasti possono essere sufficienti anche se, per alcune configurazioni, possono essere necessari 3 guasti.

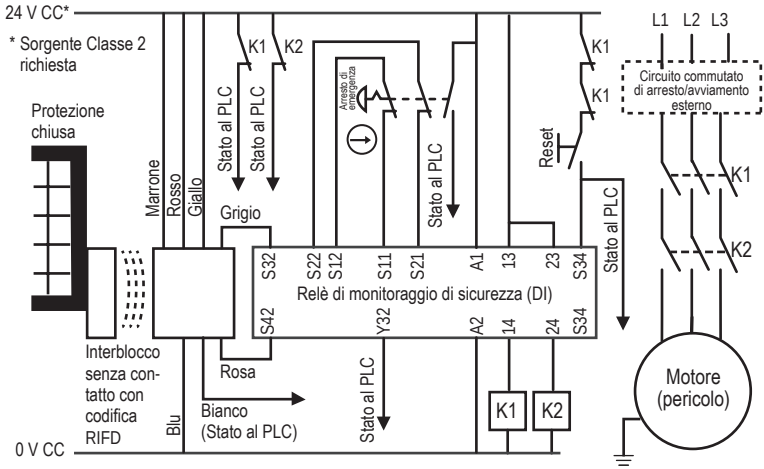


Questo è lo schema a blocchi per la Categoria 4. Il monitoraggio di entrambi i dispositivi di uscita ed il monitoraggio incrociato sono requisiti essenziali. La Categoria 4 ha una copertura diagnostica più alta di quella della Categoria 3.



Categoria 4 con interruttori interbloccati con attuatore ridondanti

Fino a tempi relativamente recenti, i singoli interruttori interbloccati con attuatore con due canali elettrici venivano considerati adatti all'uso in circuiti di Categoria 4. Per utilizzare un singolo interblocco con attuatore in un circuito a canale doppio, è necessario escludere i possibili punti di guasto singolo sul collegamento meccanico tra attuatore e interruttore. Tuttavia, il Report tecnico congiunto ISO TR 23849 ha chiarito che questo tipo di esclusione di guasto non dovrebbe essere utilizzato in sistemi PLe o SIL 3. Se il progettista del sistema di sicurezza preferisce usare interblocchi con attuatore, per soddisfare i requisiti della Categoria 4 è possibile utilizzare due interruttori separati.



Categoria 4 con interblocco senza contatto ad azionamento elettronico RFID

La tecnologia attuale prevede un approccio differente per ottenere un'architettura di Categoria 4 (e PLe/SIL 3). L'uso di elettronica complessa ha permesso di integrare, in modo economicamente conveniente, la tolleranza al guasto ed un alto livello di copertura diagnostica in un singolo dispositivo. Il dispositivo di interblocco illustrato non solo raggiunge la Categoria 4 ma fornisce un livello estremamente elevato di resistenza alla manomissione (esclusione) grazie all'uso della codifica RFID. Può anche essere collegato in serie con altri dispositivi simili senza declassamento della categoria o della copertura diagnostica.

Livello prestazionale (PL) per la classificazione di sistemi e componenti

Le architetture designate (categorie) di (EN) ISO 13849 possono essere utilizzate nelle classificazioni PL sia dei componenti (dispositivi) di sicurezza che 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.
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 ad un relè di monitoraggio di sicurezza.

Alcuni componenti come i relè di monitoraggio di sicurezza ed 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 ed 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 guasto singolo.

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 indipendenti è considerato altamente improbabile e non è affrontato in questa analisi.

Esclusioni dei guasti

(EN) ISO 13849-1 e IEC 62061 consentono 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 ed 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, ISO TR 23849 spiega che 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 (ad 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.

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

Il fatto che il termine “Categoria” venga utilizzato con accezioni diverse in relazione ai sistemi di controllo di 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. Nota: vedere IEC 60204-1 per informazioni sulle Categorie di arresto 1a e 1b.

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

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 ad 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 danni agli utensili ed alla macchina. Per l’arresto di sicurezza, non ci si può affidare ad un PLC standard (non di sicurezza) e, quindi, devono essere considerati altri approcci.

Di seguito sono riportate due possibili soluzioni per l’arresto di Categoria 1:

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 ad ingressi del dispositivo programmabile (ad es. PLC o ingresso di abilitazione dell’azionamento) e le uscite ad azione ritardata sono collegate ad un contattore principale. Quando l’interruttore di inter-blocco 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 ed 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 come GuardLogix.

Requisiti dei sistemi di controllo di sicurezza USA

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.

Note sui sistemi a controllo affidabile

Gli aspetti fondamentali dei sistemi a controllo affidabile sono la tolleranza al singolo guasto ed il monitoraggio (rilevamento guasti). 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, e (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 ed 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.

Capitolo 10: esempi applicativi

Descrizione – funzioni di sicurezza preconfigurate per macchine

Le funzioni di sicurezza delle macchine – che si tratti di arresto di emergenza, protezione o rilevamento accesso – richiedono molteplici elementi tra cui un sensore o un dispositivo di ingresso, un dispositivo logico ed un dispositivo di uscita. Insieme, questi elementi forniscono un livello di protezione calcolato mediante il livello prestazionale, come riportato in (EN) ISO 13849-1.

In questo capitolo, abbiamo selezionato una delle molte funzioni di sicurezza preconfigurate per le macchine che Rockwell Automation ha sviluppato. Ognuno di questi documenti sulle funzioni di sicurezza fornisce istruzioni per una specifica funzione di sicurezza in base al requisito funzionale, alla selezione delle apparecchiature ed al livello prestazionale richiesto, inclusi setup e cablaggio, configurazione, piano di verifica e validazione e calcolo del livello prestazionale.

Le funzioni di sicurezza preconfigurate sono gratuite e possono essere scaricate dal sito web di Rockwell Automation.

www.rockwellautomation.com, in Solutions & Services > Safety Solutions.

La funzione di sicurezza preconfigurata che segue è basata su un interruttore di interblocco di monitoraggio porta con un relè di sicurezza configurabile. I prodotti utilizzati sono: interruttore di interblocco di sicurezza senza contatto SensaGuard con codifica RFID collegato ad un relè di sicurezza configurabile Guardmaster 440C-CR30. I dispositivi di uscita utilizzati sono contattori di sicurezza 100S-C.
La classificazione di sicurezza ottenuta da questa funzione di sicurezza preconfigurata è: CAT. 4, PLe secondo (EN) ISO 13849-1.

Il numero di pubblicazione del documento originale è: SAFETY-AT133C-EN-P

Descrizione della sicurezza funzionale

Il personale è protetto dal movimento pericoloso da una barriera fissa. L'accesso alla zona pericolosa, quando necessario, avviene attraverso una porta oscillante. La porta è monitorata da un interblocco senza contatto SensaGuard, collegato agli ingressi del relè di sicurezza configurabile 440C-CR30. Il relè 440C-CR30 controlla due contattori di sicurezza 100S-C che, collegati in serie, controllano l'alimentazione del motore che aziona il movimento pericoloso. Ogni volta che questa porta monitorata viene aperta, il sistema di sicurezza interrompe l'alimentazione del motore. Il motore ed il movimento

pericoloso che aziona si arrestano per inerzia (arresto di Categoria 0). Il motore non può essere riavviato mentre la porta monitorata è aperta. Una volta che la porta è chiusa, il motore può essere riavviato premendo e rilasciando il pulsante di reset per resettare il relè 440C-CR30 e quindi attivare l'avviamento esterno per ripristinare l'alimentazione del motore controllato dai contattori 100S-C.

L'interruttore SensaGuard monitora lo stato (aperto o chiuso) della porta. L'interruttore SensaGuard monitora anche l'eventuale presenza di guasti sulle sue due uscite OSSD. Il relè 440C-CR30 monitora l'eventuale presenza di guasti sugli ingressi dall'interruttore SensaGuard e lo stato dei segnali di reset e feedback dai contattori 100S-C. Il relè monitora l'eventuale presenza di guasti anche sulle proprie uscite. Queste uscite controllano i contattori 100S-C. Quando viene rilevato un guasto, il relè 440C-CR30 disattiva le sue uscite ed interrompe l'alimentazione del motore. Non procede al ripristino fino alla correzione di quel guasto.

Distinta dei materiali

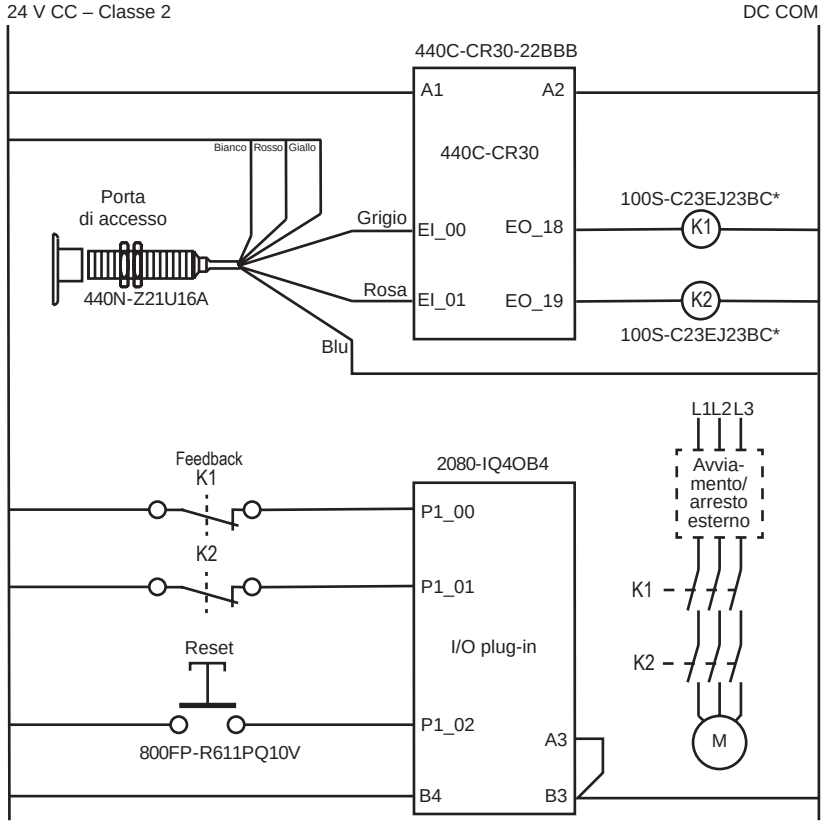
Questa applicazione utilizza i seguenti prodotti.

Numero di catalogo	Descrizione	Quantità
440N-Z21S16B	Interruttore SensaGuard in plastica da 18 mm, 2 x PNP, 0,2 A max., uscita di sicurezza, 10 m di cavo	1
800FP-R611	Pulsante di reset 800F in plastica rotondo (type 4/4X/13, IP66), blu, R, confezione standard	1
2080-IQ4OB4	Modulo I/O digitale combinato a 4 canali	1
1761-CBL-PM02	Cavo; tra il relè di sicurezza configurabile 440C-CR30 ed il personal computer, cavo stampante	1
440C-CR30-22BBB	Relè di sicurezza Guardmaster 440C-CR30 configurato tramite software, PLe SIL 3, 22 I/O di sicurezza, porta seriale integrata, porta di programmazione USB, 2 slot plug-in, 24,0 V CC	1
100S-C23EJ23BC	Contattore di sicurezza MCS 100S-C, 23 A, 24 V CC (con bobina elettrica), contatto biforcato	2

Descrizione del sistema

L'interruttore di interblocco SensaGuard viene utilizzato per verificare che la porta di protezione sia in posizione chiusa e sicura. Ogni volta che questa porta non è chiusa, il movimento pericoloso viene interrotto o impedito. Oltre a monitorare lo stato della porta di protezione, l'interruttore SensaGuard monitora le eventuali condizioni di guasto sulle sue uscite. Il relè di sicurezza configurabile 440C-CR30 rileva anche i guasti per filo interrotto, canale singolo o cortocircuito a 0 V in corrispondenza degli ingressi dell'interruttore SensaGuard.

Il relè di sicurezza configurabile 440C-CR30 monitora le condizioni di guasto delle uscite testate ad impulsi che azionano le bobine del contattore di sicurezza. Lo stato di sicurezza dei contattori di sicurezza, K1 e K2, viene verificato dal relè di sicurezza configurabile 440C-CR30 che monitora i segnali di feedback a SMF2 all'avviamento.



**ISO 13849-2 richiede la soppressione dei transitori elettrici attraverso il carico come principio di sicurezza di base. La bobina elettronica "EJ" assicura una soppressione adeguata.*

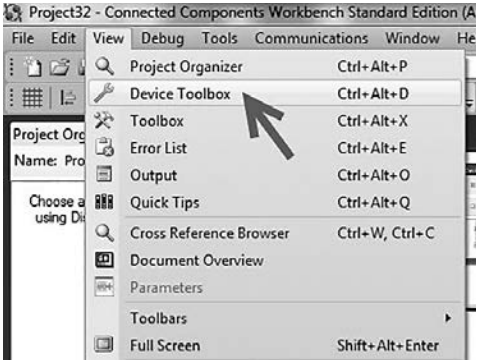
Configurazione

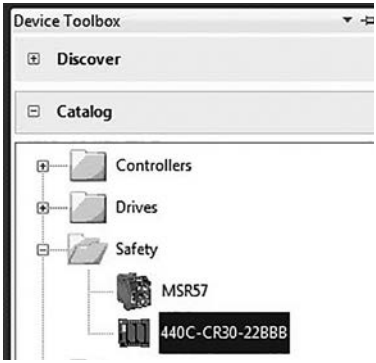
Il relè 440C-CR30 viene configurato con il software Connected Components Workbench™, versione 6.01 o successiva. In questo documento non è possibile fornire una descrizione dettagliata di tutte le fasi. e, di conseguenza, si presume la conoscenza del software Connected Components Workbench.

Configurazione del relè 440C-CR30

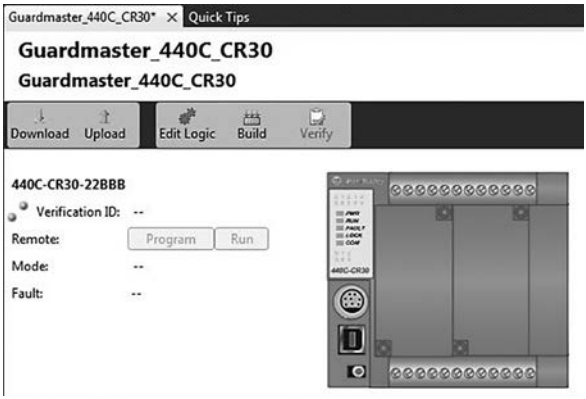
Per configurare il relè Guardmaster 440C-CR30 nel software Connected Components Workbench, procedere come segue.

1. Nel software Connected Components Workbench, selezionare View e quindi Device Toolbox. In Device Toolbox, selezionare 440C-CR30-22BBB.

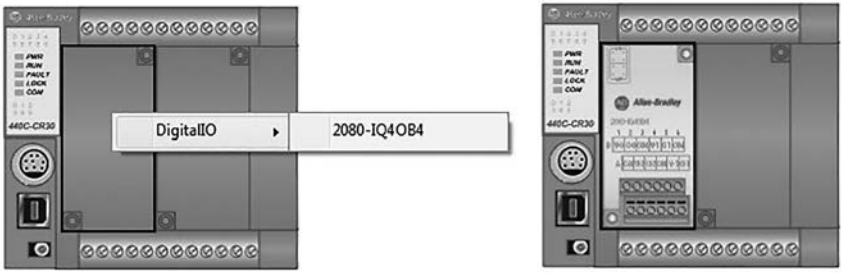




2. In Project Organizer, fare doppio clic su Guardmaster_400C_CR30 *.

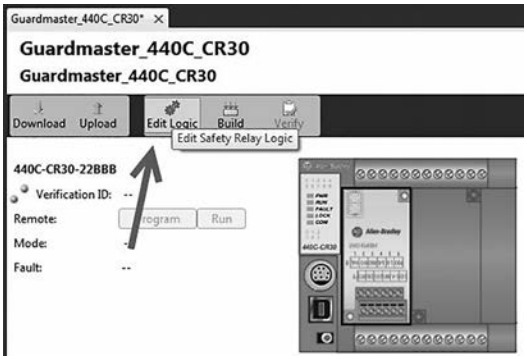


3. Per aggiungere il modulo I/O plug-in definito in questo circuito, fare clic con il pulsante destro del mouse nell'area del modulo plug-in di sinistra e scegliere il modulo 2080-IQ4OB4.

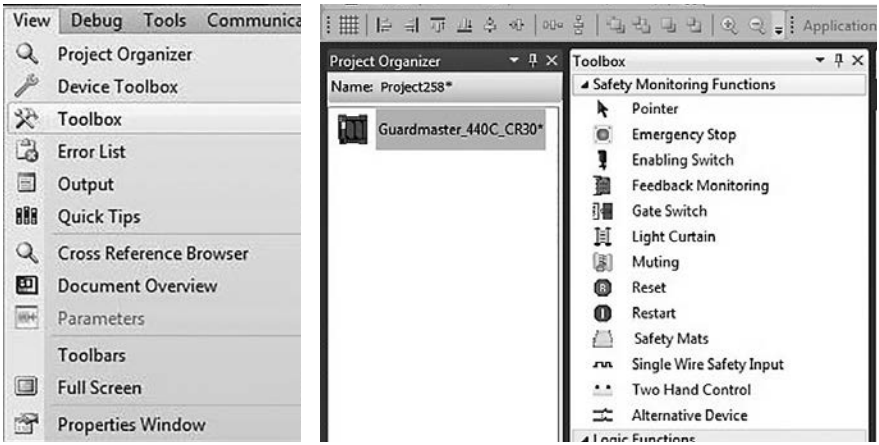


SUGGERIMENTO: il modulo I/O è visualizzato in grigio perché non è un modulo I/O di sicurezza. In questa applicazione, ciò è ammissibile perché non serve a collegare segnali di sicurezza. Gli ingressi come i pulsanti di feedback e reset non sono considerati strettamente segnali di sicurezza. L'utilizzo di I/O standard per questi segnali non legati a sicurezza consente di riservare il limitato numero di ingressi ed uscite di sicurezza per segnali realmente di sicurezza.

4. Fare clic sul pulsante Edit Logic per aprire l'area di lavoro di Connected Components Workbench. Viene visualizzata un'area di lavoro vuota.



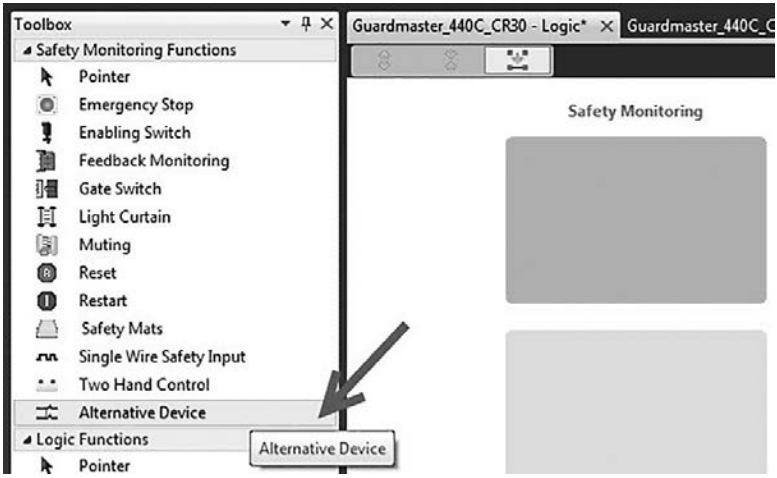
5. Dal menu a tendina View, selezionare Toolbox. Viene visualizzata la finestra Toolbox.



Configurazione degli ingressi

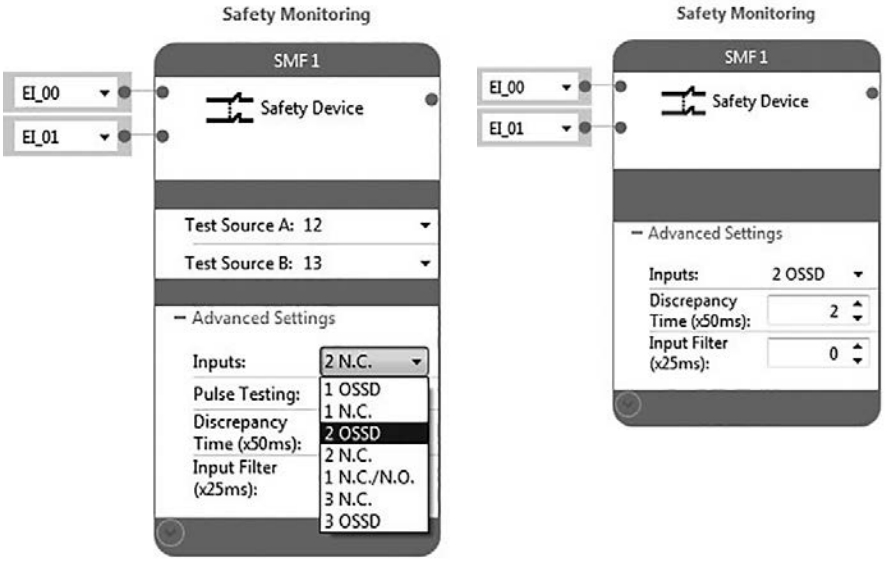
Nella finestra Toolbox non è presente una funzione di monitoraggio di sicurezza SensaGuard. Per configurarne una, procedere come segue.

1. Selezionare Alternative Device. Trascinarlo nel blocco verde della colonna Safety Monitoring e rilasciarlo.

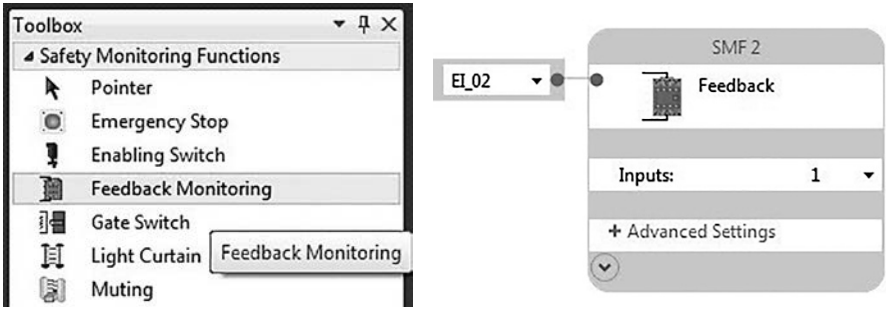


Il software Connected Components Workbench assegna automaticamente al dispositivo i primi due ingressi disponibili, EI_00 e EI_01. Lasciare assegnati tali ingressi. Il software Connected Components Workbench assegna automaticamente a questo blocco SMF 1 come nome della funzione. Per default, il software presume un dispositivo elettromeccanico e assegna gli ingressi di test (Test Sources). L'interruttore SensaGuard ha due uscite OSSD e non richiede Test Sources.

2. Per configurare correttamente il blocco, aprire Advanced Settings e selezionare 2 OSSD dal menu a tendina Inputs. Il blocco risultante appare come illustrato.

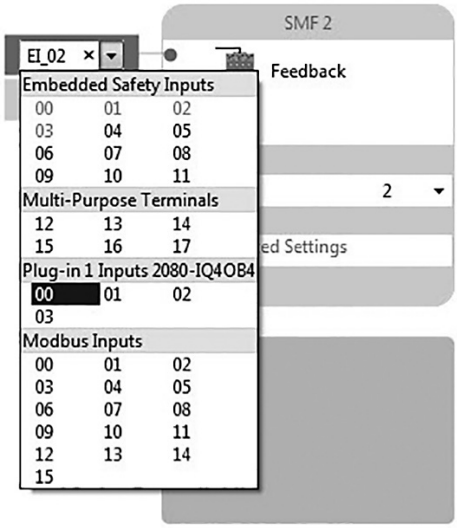


3. Fare clic, trascinare e rilasciare una funzione di monitoraggio della sicurezza Feedback Monitoring nel blocco Safety Monitoring, sotto il blocco SensaGuard nell'area di lavoro.

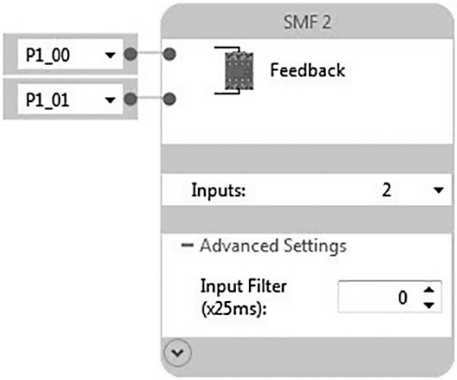


Prendere nota che il software Connected Components Workbench assegna questo al morsetto di ingresso EI_02, il successivo morsetto di ingresso di sicurezza disponibile. Il software presume che questo sia un ingresso singolo ed assegna automaticamente SMF 2, come nome della funzione, a questo blocco.

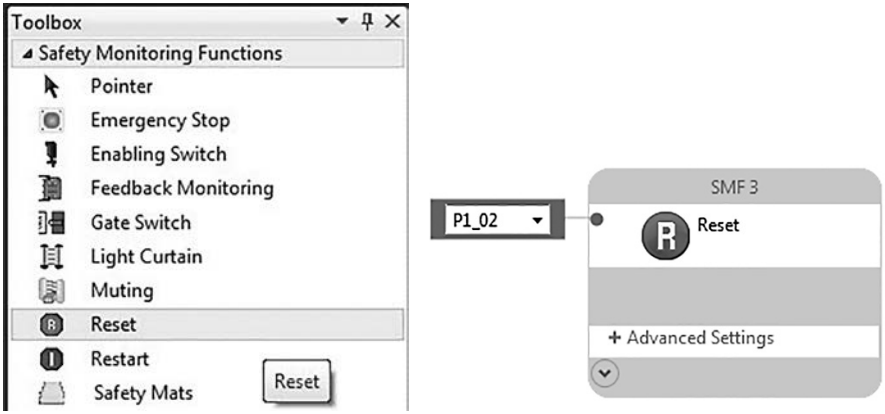
4. Dato che il circuito richiede due ingressi, uno da ogni contattore, cambiare il numero di ingressi a 2, uno per il contatto NC di ogni contattore 100S.



5. Assegnare gli ingressi ai morsetti plug-in PI_00 e PI_01. Questo evita di usare inutilmente gli ingressi di sicurezza per i segnali di feedback.



6. Fare clic, trascinare e rilasciare una funzione di monitoraggio della sicurezza Reset nel blocco Safety Monitoring, sotto il blocco Feedback Monitoring nell'area di lavoro.

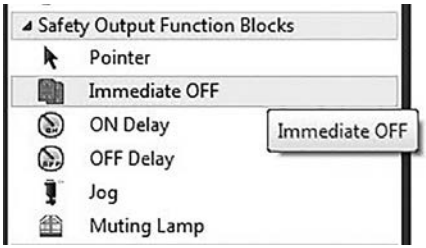


Il software Connected Components Workbench assegna automaticamente a questo blocco SMF 3 come nome della funzione. Riassegnare l'ingresso Reset al morsetto plug-in PI_02.

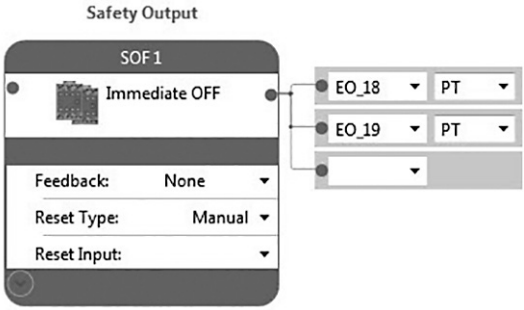
Configurazione delle uscite

Per configurare le uscite, procedere come segue.

1. Fare clic su Immediate OFF per trascinarlo dalla sezione Safety Output Function Blocks della Toolbox.

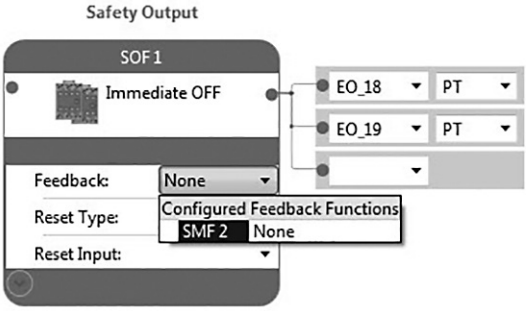


2. Rilasciarlo sul blocco superiore della colonna Safety Output dell'area di lavoro.

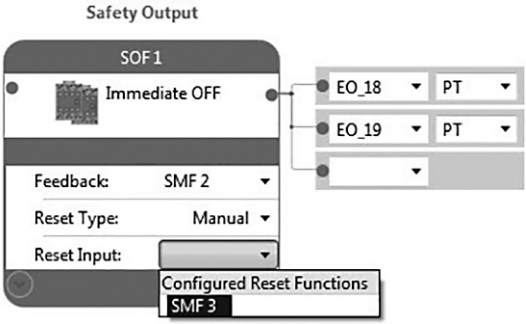


Il software Connected Components Workbench assegna automaticamente i morsetti di uscita EO_18 e EO_19. Pulse Testing è il valore di default di questi morsetti. Il Reset Type di default è Manual. Lasciare queste impostazioni ai loro valori di default.

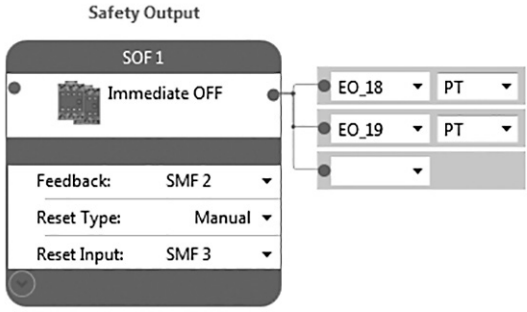
3. Selezionare SMF 2 nel menu a tendina Feedback.



4. Selezionare SMF 3 nel menu a tendina Reset Input.



La configurazione delle uscite di sicurezza è completa.

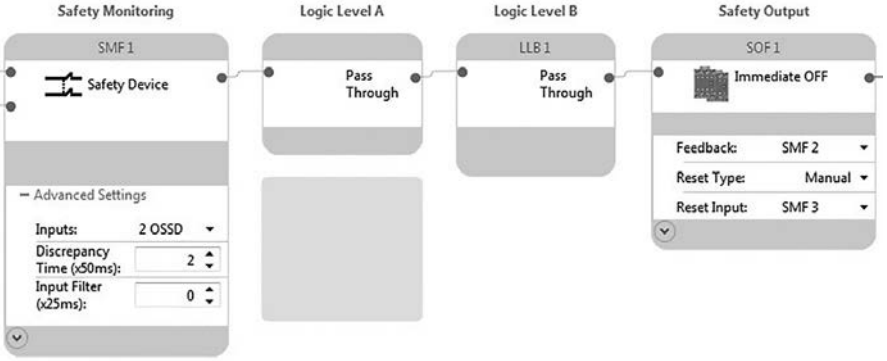


Configurazione della logica

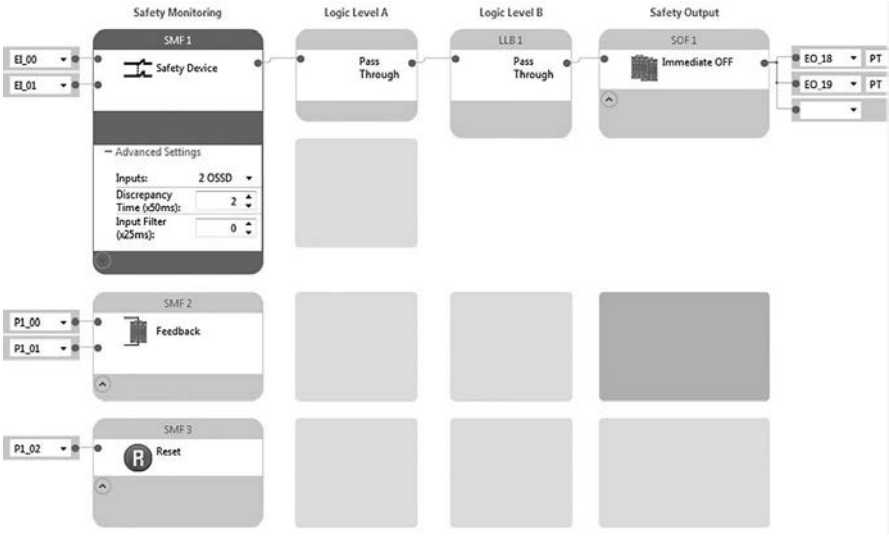
La sezione Logic determina il modo in cui le uscite di sicurezza rispondono agli ingressi di monitoraggio di sicurezza. In questo caso, l'uscita di sicurezza segue direttamente l'ingresso di monitoraggio di sicurezza.

1. Fare clic sul punto blu del lato destro del blocco di ingresso Safety Monitoring di SensaGuard. Il punto diventa grigio.

2. Fare clic sul punto blu del lato sinistro del blocco Safety Output per collegare la logica.

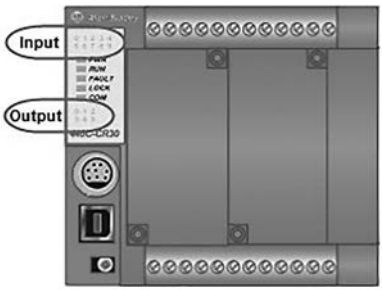


La logica completata si presenta come illustrato di seguito.



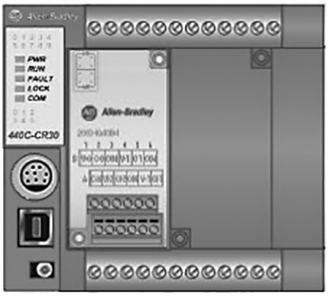
Configurazione degli indicatori di stato

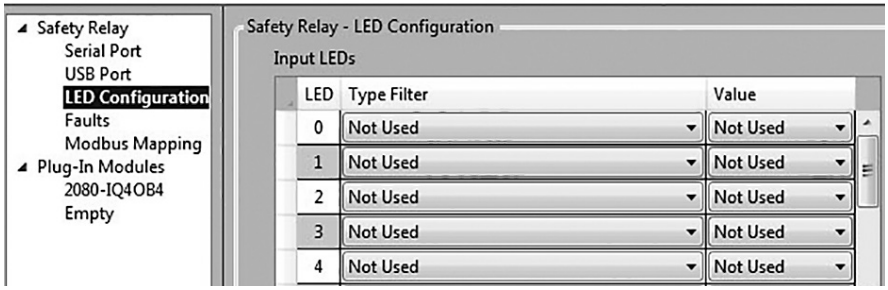
Il relè di sicurezza configurabile 440C-CR30 mette a disposizione dieci LED di stato degli ingressi e sei LED di stato delle uscite configurabili dall'utilizzatore. In molti casi, possono rivelarsi estremamente utili nelle fasi di installazione, messa in servizio, monitoraggio e ricerca guasti di un sistema di relè di sicurezza configurabili 440C-CR30. Non incidono in alcun modo sul funzionamento del sistema e non è necessario configurarli, ma sono facili da configurare e si raccomanda di utilizzarli.



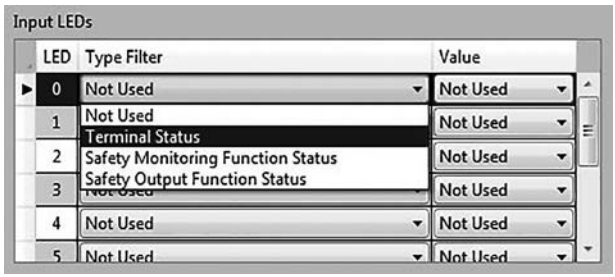
1. Fare clic su Guardmaster_440C_CR30*.

2. Selezionare LED Configuration.

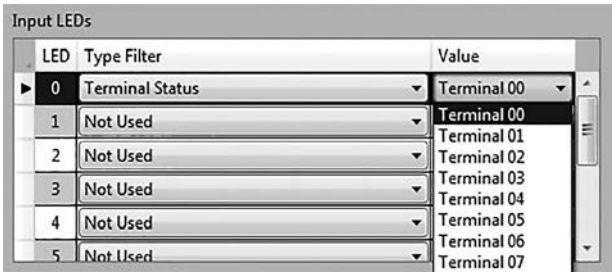




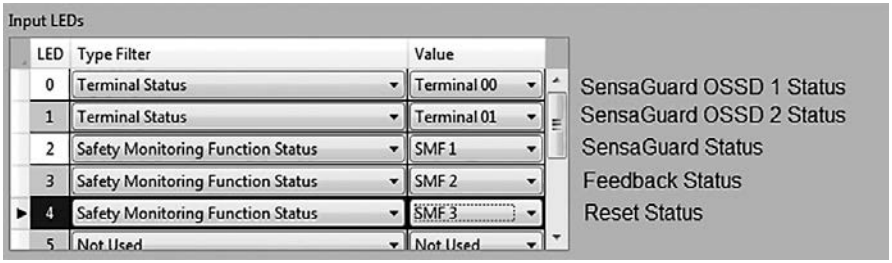
3. Per Type Filter, selezionare Terminal Status per il LED 0.



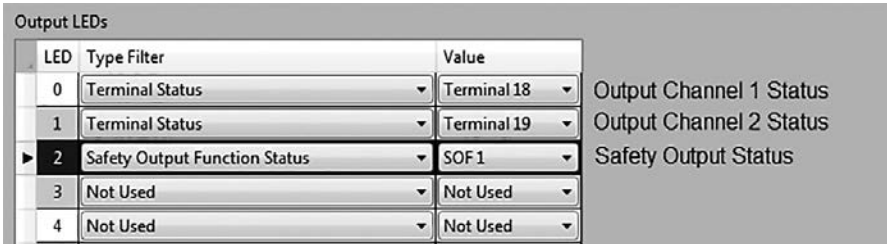
4. Per il LED 0, selezionare Terminal 00 dal menu a tendina Value. Il LED indicatore di stato 0 è ora configurato per indicare lo stato del morsetto 00.



5. Assegnare i successivi quattro LED (1…4) di stato degli ingressi nello stesso modo. I LED di stato degli ingressi ora sono configurati.



6. Assegnare i tre LED di uscita come segue.

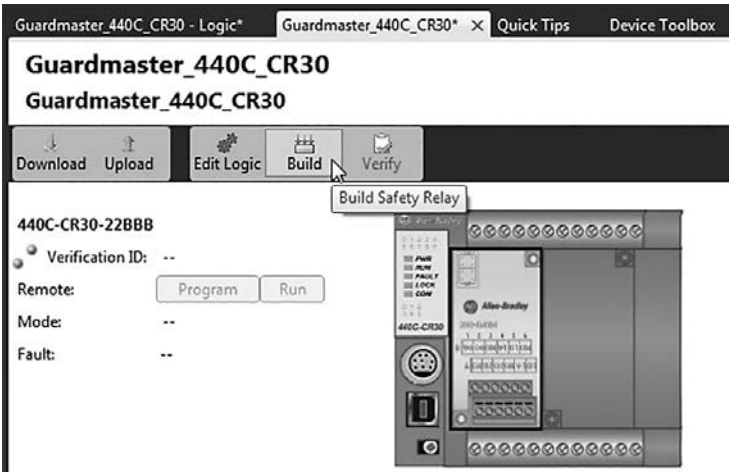


Verifica della validità della compilazione

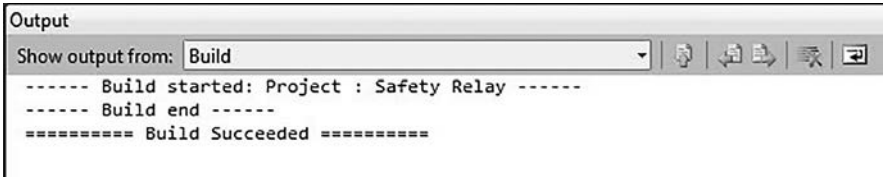
Per verificare la validità della logica usando la funzione Build nel software Connected Components Workbench, procedere come segue.

1. Fare clic su Guardmaster_440C_CR30 nella barra sopra l'area di lavoro.

2. Fare clic su Build.



Il messaggio Build Succeeded conferma che la configurazione è valida.



In caso di rilevamento di un errore o di un'omissione durante la compilazione, viene visualizzato un messaggio che descrive l'errore in modo che possa essere corretto. Dopo aver corretto l'errore, è necessario ripetere la compilazione.

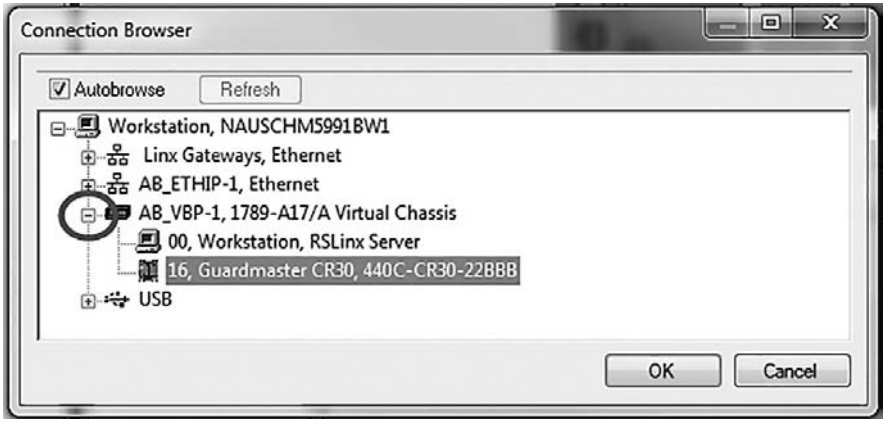
Salvataggio e download del progetto

Per salvare e scaricare il progetto, procedere come segue.

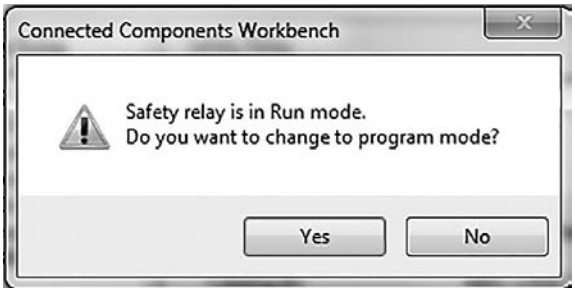
1. Dal menu File, selezionare Save as per salvare il progetto.
2. Nella finestra Project Organizer, fare doppio clic su Guardmaster_440C_CR30 per aprire l'area di lavoro.
3. Accendere il relè di sicurezza 440C-CR30.
4. Collegare il cavo USB al relè 440C-CR30.

5. Fare clic su Download.

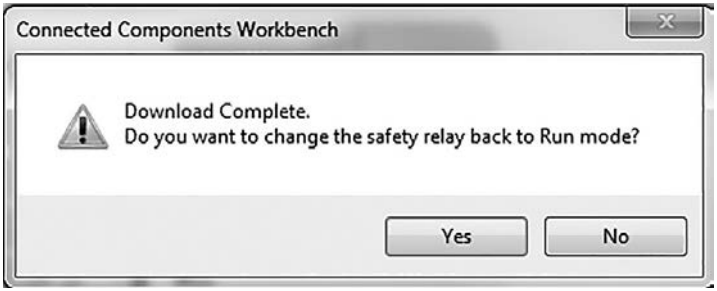
6. In Connection Browser, espandere AB_VBP-1 Virtual Chassis e selezionare Guardmaster 440C-CR30-22BBB. Fare clic su OK.



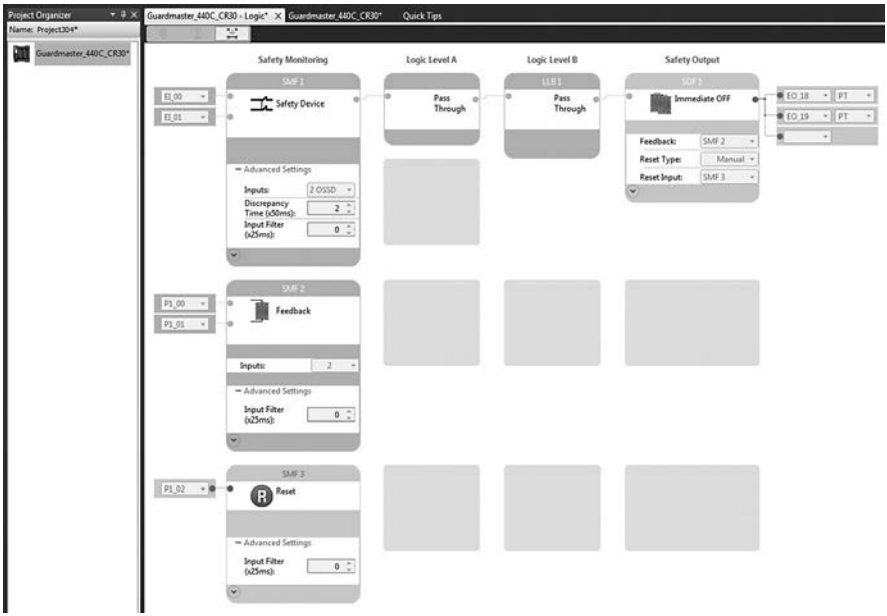
7. Fare clic su Yes per passare dalla modalità Run alla modalità Program.



8. Terminato il download, fare clic su Yes per passare dalla modalità Program alla modalità Run.



9. Fare clic su Edit Logic per vedere la diagnostica online.

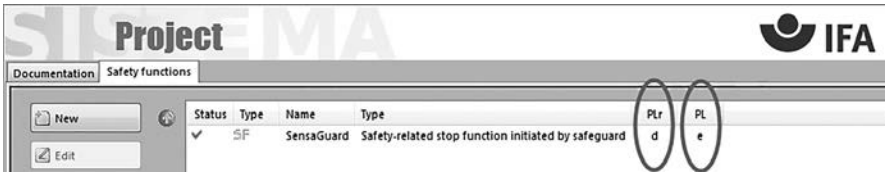


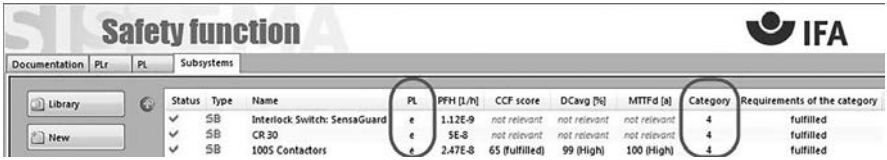
Il colore verde indica che un blocco è True o che un morsetto di ingresso o uscita è ON. Verde lampeggiante indica che la funzione di un'uscita di sicurezza è pronta per il reset.
La modalità diagnostica online del relè 440C-CR30 può essere molto utile durante il processo di verifica.

10. Prima di procedere alla verifica della configurazione, esaminare le informazioni contenute in "Calcolo del livello prestazionale" e "Piano di verifica e validazione".

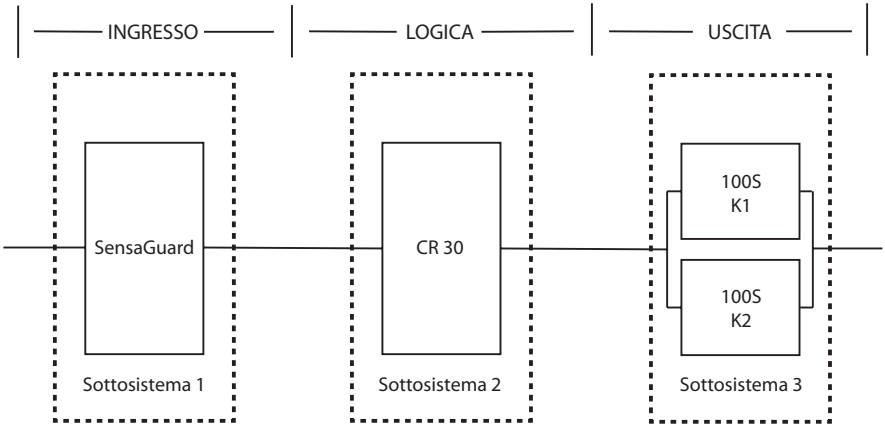
Calcolo del livello prestazionale

Quando correttamente implementata, questa funzione di arresto di sicurezza può ottenere una classificazione di sicurezza di Categoria 4, Livello prestazionale e (CAT. 4, PLe), secondo ISO 13849-1:2008, come calcolato usando lo strumento di calcolo del PL del software SISTEMA.
In base alla valutazione dei rischi, il minimo livello prestazionale richiesto (PLr) per questa funzione di sicurezza è PLd.





Questo arresto di sicurezza attivato da una funzione di sicurezza della protezione può essere modellato come segue:



Trattandosi di dispositivi elettromeccanici, i dati dei contattori di sicurezza includono quanto segue:

- Tempo medio tra i guasti, pericolosi ($MTTF_D$)
- Copertura diagnostica (DCmed)
- Guasto per causa comune (CCF)

Le valutazioni sulla sicurezza funzionale dei dispositivi elettromeccanici considerano quanto segue:

- Frequenza di azionamento
- Efficace monitoraggio dei guasti
- Corretta specifica e installazione

SISTEMA calcola l'MTTFd usando i dati B10d forniti per i contattori e la frequenza stimata di utilizzo, inserita durante la creazione del progetto SISTEMA.

La copertura DCmed (99%) dei contattori viene selezionata dalla tabella "Dispositivo di uscita" di ISO 13849-1 Allegato E, Monitoraggio diretto.

Il valore CCF viene generato usando il processo di punteggio descritto nell'Allegato F di ISO 13849-1. Il processo di punteggio dei guasti per causa comune (CCF) deve essere eseguito quando si implementa effettivamente un'applicazione ed è necessario raggiungere un punteggio minimo di 65.

Piano di verifica e validazione

La verifica e la validazione svolgono un ruolo importante nell'evitare errori nel processo di progettazione e sviluppo di un sistema di sicurezza. ISO 13849-2 stabilisce i requisiti per la verifica e la validazione. Lo standard richiede un piano documentato per verificare che siano stati rispettati tutti i requisiti funzionali di sicurezza.

La verifica è un'analisi del sistema di controllo di sicurezza risultante. Il livello prestazionale (PL) del sistema di controllo di sicurezza viene calcolato per verificare che il sistema risponda al livello prestazionale richiesto (PLr) specificato. Il software SISTEMA viene generalmente utilizzato per eseguire i calcoli ed assicurare il rispetto dei requisiti di ISO 13849-1.

La validazione è un test funzionale del sistema di controllo di sicurezza per dimostrare che il sistema è conforme ai requisiti specificati della funzione di sicurezza. Il sistema di controllo di sicurezza viene testato per verificare che tutte le uscite di sicurezza rispondano adeguatamente agli ingressi di sicurezza corrispondenti. Il test funzionale include le normali condizioni di funzionamento oltre all'iniezione dei guasti potenziali delle modalità di guasto. Per documentare la validazione del sistema di controllo di sicurezza, viene generalmente utilizzata una checklist.

Prima di validare il sistema, verificare che il relè di sicurezza configurabile Guardmaster 440C-CR30 sia stato cablato e configurato nel rispetto delle istruzioni di installazione.

Checklist di verifica e validazione

Informazioni generali sulla macchina Descrizione	
Nome/modello della macchina	
Numero di serie della macchina	
Nome del cliente	
Data del test	
Nomi dei responsabili del test	
Numero dello schema	
Dispositivi di ingresso	440N-Z21S16B
Relè di sicurezza configurabile	440C-CR30-22BBB
Convertitore di frequenza	
Contattore di sicurezza	100S-C23EJ23BC

Configurazione relè e cablaggio di sicurezza			
Passo del test	**Verifica**	**Superato/ Non superato**	**Cambiamenti/ modifiche**
1	Verificare che le specifiche di tutti i componenti siano adatte all'applicazione. Consultare i principi di sicurezza base e principi di sicurezza collaudati di ISO 13849-2.		
2	Ispezionare visivamente il circuito del relè di sicurezza per verificare che sia cablato come documentato negli schemi.		
3	Verificare che la configurazione del relè di sicurezza configurabile 440C-CR30 sia quella corretta e prevista.		

Verifica del normale funzionamento – il sistema di sicurezza risponde correttamente a tutti i normali comandi di avviamento, arresto, reset e arresto di emergenza e agli ingressi dell'interruttore SensaGuard.			
Passo del test	**Verifica**	**Superato/ Non superato**	**Cambiamenti/ modifiche**
1	Verificare che nessuno si trovi nell'area protetta.		
2	Verificare che il movimento pericoloso si sia fermato.		
3	Verificare che la porta sia chiusa.		
4	Alimentare il sistema di sicurezza.		
5	Verificare che i LED di stato degli ingressi del morsetto 00, del morsetto 01 e di SMF1 del relè di sicurezza 440C-CR30 siano verdi. Verificare che gli indicatori di stato di tutte le uscite siano OFF. Verificare che i LED di stato Power e Run siano verdi. Monitorare il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
6	Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. Verificare che i LED di stato delle uscite del morsetto 18, del morsetto 19 e di SOF1 siano verdi. Monitorare il corretto funzionamento dei LED di stato ed il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
7	Verificare che il movimento pericoloso non si avvii all'accensione.		

8	Premere e rilasciare il pulsante Start dell'azionamento. Verificare che il movimento pericoloso inizi e che la macchina inizi a funzionare.		
9	Premere il pulsante di arresto esterno. La macchina deve fermarsi nel modo normale configurato. Il sistema di sicurezza non deve intervenire.		
10	Premere e rilasciare il pulsante di avviamento esterno. Verificare che il movimento pericoloso inizi e che la macchina inizi a funzionare.		
11	Aprire la porta di protezione. Il sistema di sicurezza deve intervenire. Il movimento pericoloso deve fermarsi in meno di 0,7 secondi. Monitorare il corretto funzionamento dei LED di stato ed il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
12	Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. Il relè di sicurezza configurabile 440C-CR30 non deve intervenire. Monitorare il corretto funzionamento dei LED di stato ed il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
13	Chiudere la porta di protezione. La macchina non deve avviarsi. Il relè di sicurezza 440C-CR30 non deve intervenire. Monitorare il corretto funzionamento dei LED di stato ed il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
14	Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. L'uscita SOF1 del relè di sicurezza 440C-CR30 deve eccitarsi. Il movimento pericoloso non deve essere avviato. Monitorare il corretto funzionamento dei LED di stato ed il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
15	Premere e rilasciare il pulsante di avviamento esterno. Verificare che il motore si avvii e che la macchina inizi a funzionare.		

Validazione della risposta di sicurezza al funzionamento anomalo – il sistema di sicurezza risponde correttamente a tutti i guasti prevedibili con la diagnostica corrispondente.

Test di SensaGuard e dei relè di sicurezza configurabili 440C-CR30

Passo del test	Verifica	Superato/ Non superato	Cambiamenti/ modifiche
1	Mantenere chiusa la porta di protezione. Mentre il movimento pericoloso è in corso, staccare il filo dell'uscita OSSD1 di SensaGuard in corrispondenza del morsetto EI_00 del relè di sicurezza 440C-CR30. Il relè di sicurezza 440C-CR30 deve intervenire immediatamente. Il LED rosso dello stato di guasto sul relè deve lampeggiare. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
2	Ricollegare il filo a E1_00. Il relè di sicurezza 440C-CR30 non deve intervenire. Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. Il relè di sicurezza 440C-CR30 non deve intervenire. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
3	Aprire e chiudere la porta di protezione. Il LED rosso dello stato di guasto deve essere spento. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		

4	Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. L'uscita SOF 1 sul relè 440C-CR30 deve eccitarsi. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
5	Premere il pulsante di avviamento esterno. La macchina deve iniziare a funzionare. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench. Questo passo è opzionale nei seguenti test di validazione di SensaGuard (passi da 6 a 27).		
6	Con la porta di protezione chiusa, collegare OSSD 1 a 24 V CC. Dopo circa 40 secondi, l'interruttore SensaGuard interviene. Il relè di sicurezza 440C-CR30 interviene. Il LED rosso dello stato di guasto sul relè di sicurezza 440C-CR30 deve lampeggiare. L'indicatore di stato sull'interruttore SensaGuard lampeggia in rosso. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
7	Scollegare OSSD 1 da 24 V CC. Né l'interruttore SensaGuard né il relè di sicurezza 440C-CR30 intervengono. Premere e rilasciare il pulsante di riavviamento sul relè di sicurezza 440C-CR30. Né l'interruttore SensaGuard né il relè di sicurezza 440C-CR30 intervengono. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
8	Spegnere e riaccendere l'interruttore SensaGuard. Cinque secondi circa dopo il ripristino dell'alimentazione dell'interruttore SensaGuard, il suo LED di stato diventa verde fisso. Il LED rosso lampeggiante dello stato di guasto sul relè di sicurezza 440C-CR30 si spegne. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
9	Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
10	Collegare OSSD 1 a DC COM. Il relè di sicurezza 440C-CR30 interviene immediatamente. La luce rossa di arresto in sicurezza della torretta luminosa si accende. La luce arancione della torretta luminosa del riparo 1 si accende. Il LED rosso dello stato di guasto sul relè di sicurezza 440C-CR30 deve lampeggiare. L'indicatore di stato sull'interruttore SensaGuard lampeggia in rosso.		
11	Scollegare OSSD1 da DC COM. Né l'interruttore SensaGuard né il relè di sicurezza 440C-CR30 intervengono. Premere e rilasciare il pulsante di riavviamento sul relè di sicurezza 440C-CR30. Né l'interruttore SensaGuard né il relè di sicurezza 440C-CR30 intervengono.		
12	Spegnere e riaccendere l'interruttore SensaGuard. Cinque secondi circa dopo il ripristino dell'alimentazione dell'interruttore SensaGuard, il suo LED di stato diventa verde fisso. La luce arancione della torretta luminosa del riparo 1 si spegne. La luce rossa di safe-off della torretta luminosa rimane accesa. Il LED rosso lampeggiante dello stato di guasto sul relè di sicurezza 440C-CR30 si spegne.		
13	Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. L'uscita SOF 1 del relè di sicurezza 440C-CR30 deve eccitare i contattori. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
da 14 a 27	Ripetere i passi da 1 a 13 usando EI_01 al posto di EI_00 e OSSD 2 al posto di OSSD 1.		

28	Collegare OSSD 1 a OSSD 2 (il morsetto EI_00 al morsetto EI_01). Dopo circa 50 secondi, l'interruttore SensaGuard interviene. Il relè di sicurezza 440C-CR30 interviene. L'indicatore di stato sull'interruttore SensaGuard lampeggia in rosso. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
29	Scollegare OSSD 1 da OSSD 2. Né l'interruttore SensaGuard né il relè di sicurezza 440C-CR30 intervengono. Premere e rilasciare il pulsante di riavviamento sul relè di sicurezza 440C-CR30. Né l'interruttore SensaGuard né il relè di sicurezza 440C-CR30 intervengono.		
30	Spegnere e riaccendere l'interruttore SensaGuard. Cinque secondi circa dopo il ripristino dell'alimentazione dell'interruttore SensaGuard, il suo LED di stato diventa verde fisso. Il LED rosso lampeggiante dello stato di guasto sul relè di sicurezza 440C-CR30 si spegne. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
31	Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. La luce rossa di arresto in sicurezza della torretta luminosa deve essere spenta. L'uscita SOF1 del relè di sicurezza 440C-CR30 deve eccitare i contattori. Monitorare il corretto funzionamento di tutti i LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		

Validazione della risposta di sicurezza al funzionamento anomalo – il sistema di sicurezza risponde correttamente a tutti i guasti prevedibili con la diagnostica corrispondente.

Contattore – test del relè di sicurezza configurabile 440C-CR30

Passo del test	Verifica	Superato/ Non superato	Cambiamenti/ modifiche
1	Mentre la macchina continua a funzionare, aprire la connessione tra il morsetto EO_18 del relè di sicurezza configurabile 440C-CR30 e il morsetto A1 della bobina K1. Il movimento pericoloso deve arrestarsi per inerzia.		
2	Premere il pulsante di arresto esterno. Ripristinare la connessione. Premere il pulsante di avviamento esterno per riprendere il movimento pericoloso.		
3	Mentre il movimento pericoloso continua, collegare il morsetto A1 della bobina K1 a 24 V CC. Dopo circa 18 secondi, il relè di sicurezza 440C-CR30 deve intervenire. K2 deve diseccitarsi. Il movimento pericoloso si arresta per inerzia. Il LED rosso dello stato di guasto sul relè di sicurezza 440C-CR30 è acceso.		
4	Scollegare il morsetto A1 della bobina K1 da 24 V CC. Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. Il relè di sicurezza 440C-CR30 non deve intervenire.		
5	Spegnere e riaccendere il relè di sicurezza 440C-CR30. Il relè risponde. Il LED indicatore dello stato di guasto del relè di sicurezza 440C-CR30 è spento.		
6	Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. Premere il pulsante di avviamento esterno. Il movimento pericoloso deve riprendere.		
7	Mentre la macchina continua a funzionare, cortocircuitare il morsetto A1 della bobina K1 con DC COM. Il relè di sicurezza 440C-CR30 deve intervenire. Il LED rosso dello stato di guasto sul relè di sicurezza 440C-CR30 è acceso.		

8	Scollegare il morsetto A1 della bobina K1 da DC COM. Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. Il relè di sicurezza 440C-CR30 non deve intervenire.		
9	Spegnere e riaccendere il relè di sicurezza 440C-CR30. Il relè di sicurezza 440C-CR30 risponde. Il LED indicatore dello stato di guasto sul relè di sicurezza 440C-CR30 è spento.		
10	Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. Premere il pulsante di avviamento esterno. Il movimento pericoloso riprende.		
da 11 a 21	Ripetere i passi da 1 a 10 usando EO_19 al posto di EO_18 e K2 al posto di K1.		
22	Collegare il morsetto A1 di K1 al morsetto A1 di K2. Dopo circa 18 secondi, il relè di sicurezza 440C-CR30 deve intervenire. Il movimento pericoloso si arresta per inerzia. Il LED rosso dello stato di guasto sul relè di sicurezza 440C-CR30 è acceso.		
23	Scollegare il morsetto A1 di K1 dal morsetto A1 di K2. Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. Il relè di sicurezza 440C-CR30 non deve intervenire.		
24	Spegnere e riaccendere il relè di sicurezza 440C-CR30. Il relè risponde. Il LED indicatore dello stato di guasto sul relè di sicurezza 440C-CR30 è spento.		
25	Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. Premere il pulsante di avviamento esterno. Il movimento pericoloso deve riprendere.		

Validazione della risposta di sicurezza al funzionamento anomalo – il sistema di sicurezza risponde correttamente a tutti i guasti prevedibili con la diagnostica corrispondente.

Feedback del contattore – test del relè di sicurezza configurabile 440C-CR30

Passo del test	Verifica	Superato/ Non superato	Cambiamenti/ modifiche
1	Mentre la macchina è in funzione, rimuovere la connessione del feedback K1 al morsetto P1_00. La macchina deve continuare a funzionare.		
2	Aprire la porta di protezione. Il sistema di sicurezza deve intervenire. Il movimento pericoloso deve fermarsi in meno di 0,7 secondi. Monitorare il corretto funzionamento dei LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
3	Chiudere la porta di protezione. La macchina non deve avviarsi. Il relè 440C-CR30 non deve intervenire. Monitorare il corretto funzionamento dei LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
4	Premere e rilasciare il pulsante di reset sul relè di sicurezza 440C-CR30. Il relè 440C-CR30 non deve intervenire. Monitorare il corretto funzionamento dei LED di stato e il corretto stato del relè di sicurezza 440C-CR30 con il software Connected Components Workbench.		
5	Ripristinare la connessione a P1_00. Spegnere e riaccendere il relè 440C-CR30. Premere il pulsante di reset sul relè 440C-CR30. Le uscite del relè 440C-CR30 devono eccitarsi. Premere e rilasciare il pulsante di avviamento esterno. Verificare che il motore si avvii e che la macchina inizi a funzionare.		
6	Ripetere i passi da 1 a 5 usando la connessione del feedback K2 al morsetto P1_01.		

Verifica della configurazione

Il sistema deve verificare la configurazione di ogni singola applicazione con il comando Verify. Se non viene verificato, il relè di sicurezza configurabile 440C-CR30 andrà in guasto dopo 24 ore di funzionamento.

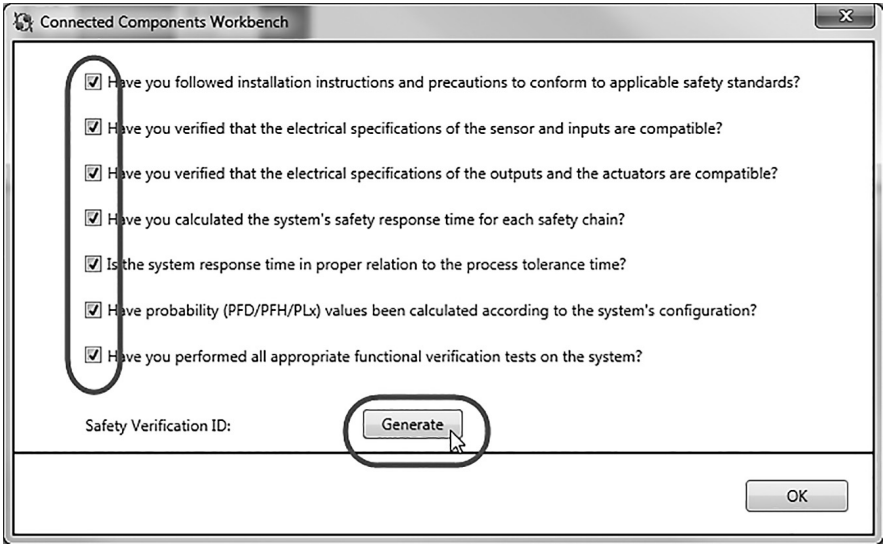
ATTENZIONE: il processo di verifica dovrebbe essere documentato nel fascicolo tecnico del sistema di sicurezza.

Per scaricare e verificare la configurazione, procedere come segue.

1. Verificare che il relè 440C-CR30 sia alimentato e collegato alla stazione di lavoro tramite il cavo USB.
2. Verificare che l'angolo in alto a destra della scheda Project di Connected Components Workbench indichi che il relè 440C-CR30 è collegato. In caso contrario, fare clic su Connect to Device per stabilire la connessione software.

3. Fare clic su Verify.

4. Rispondere a tutte le domande e selezionare ogni casella, se completato. Fare clic su Generate.

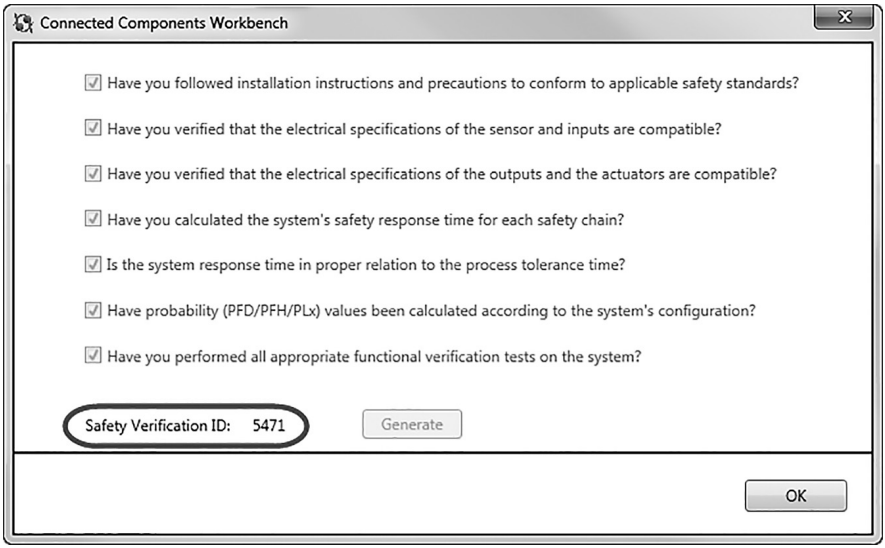


IMPORTANTE: per generare l'ID di verifica, devono essere selezionate tutte le caselle.

6. Fare clic su Yes per procedere alla verifica.

7. Fare clic su Yes per passare alla modalità RUN.

8. Registrare l'ID di verifica della sicurezza nella documentazione della macchina.



Questo processo rappresenta il feedback al relè 440C-CR30 in merito al completamento della verifica del sistema e dei test funzionali. L'ID di verifica è univoco e può essere utilizzato per controllare se sono state apportate modifiche ad un file di configurazione. Eventuali modifiche alla configurazione comportano la rimozione dell'ID di verifica della sicurezza. Le successive azioni di verifica generano un ID di verifica differente. L'ID di verifica della sicurezza viene visualizzato nel software Connected Components Workbench solo quando si è collegati al relè 440C-CR30.

Capitolo 11: prodotti, strumenti e servizi

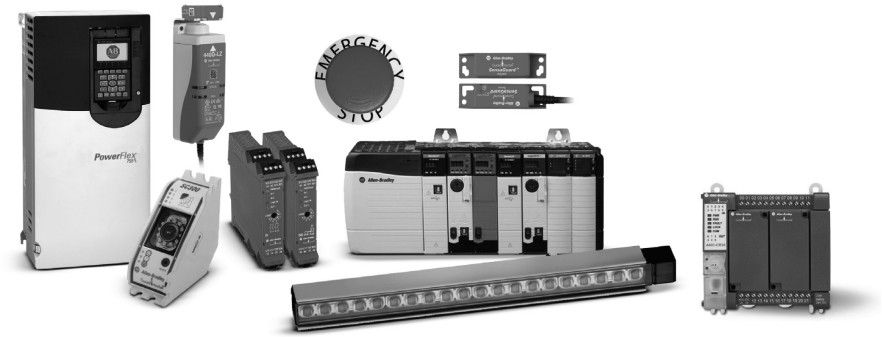
Cenni generali

Rockwell Automation, tra i principali fornitori a livello globale di soluzioni industriali di potenza, controllo e informative, supporta i suoi clienti in diversi settori da oltre 100 anni. Nel suo portafoglio di automazione industriale rientrano tecnologie, strumenti e servizi per la sicurezza delle macchine.

Prodotti e le tecnologie per ogni applicazione

Rispetto agli altri fornitori di soluzioni per la sicurezza delle macchine, Rockwell Automation dispone di portafoglio più ampio e può fornire tutte e tre le parti di un sistema di sicurezza (dispositivo di ingresso, controllo della logica ed elemento di potenza finale).

I prodotti e le tecnologie disponibili includono:



Dispositivi di ingresso di sicurezza

- **Dispositivi di sicurezza per il rilevamento dell'accesso**
  I dispositivi di sicurezza per il rilevamento dell'accesso rilevano la posizione di oggetti o persone vicino a zone pericolose. Queste includono: barriere fotoelettriche di sicurezza, laser scanner di sicurezza, sensori di sicurezza di rilevamento mani, pedane e bordi sensibili alla pressione

- **Interruttori di interblocco di sicurezza**
  Gli interruttori di sicurezza sono concepiti e costruiti facendo riferimento a standard globali in materia di affidabilità, stabilità e qualità. Gli interruttori di sicurezza includono interruttori di finecorsa e di interblocco e pulsanti di arresto di emergenza.

- **Dispositivi di arresto di emergenza e di protezione**
  Gli interruttori di arresto di emergenza includono una gamma di pulsanti a fungo con contatti a guida forzata. Gli interruttori di abilitazione e gli interruttori a fune assicurano la funzione di emergenza nell'ambito di un'applicazione o sono vincolati per consentire il movimento dell'operatore nell'applicazione di sicurezza.

- **Interfaccia operatore**
  I dispositivi di interfaccia operatore consentono all'operatore di interagire con l'applicazione ed offrono funzionalità di sicurezza specifiche aggiuntive.

Controllori logici di sicurezza

- **Relè di sicurezza (a funzione singola o configurabili)**
  I relè di sicurezza controllano e monitorano un sistema di sicurezza e permettono alla macchina di avviarsi o eseguono comandi per arrestarla. I relè di sicurezza a funzione singola 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 ed un controllo di zona minimo.

- **Controllori di sicurezza integrati**
  I PLC di sicurezza apportano alle applicazioni di sicurezza i vantaggi dei sistemi PLC tradizionali, sostituendo i sistemi a relè cablati che sono normalmente necessari per portare i processi automatizzati in uno stato di sicurezza. I PLC di sicurezza consentono ai programmi standard e di sicurezza di risiedere nello chassis di un unico controllore, favorendo la flessibilità di programmazione ed offrendo ai programmatori un ambiente di programmazione familiare e facile da usare. Le soluzioni basate su controllori di sicurezza permettono un controllo aperto ed integrato che contribuisce a garantire la sicurezza delle macchine e la protezione degli asset.

- **Dispositivi I/O di sicurezza**
  I prodotti di sicurezza Guard I/O™ offrono tutti i vantaggi dei tradizionali I/O distribuiti ma sono concepiti per sistemi di sicurezza. Riducono i costi di cablaggio ed il tempo di messa in servizio di macchine e celle e sono disponibili con una varietà di funzioni per applicazioni In-Cabinet e On-Machine.

Attuatori di sicurezza

- **Avviatori e contattori di sicurezza**
  Gli avviatori statici distribuiti ArmorStart® riescono a raggiungere funzionalità di sicurezza di Categoria 4 fornendo, nel contempo, una soluzione di sicurezza integrata nell'installazione di sicurezza DeviceNet™ On-Machine™. Contattori di sicurezza e relè ausiliari IEC aiutano a proteggere il personale da avviamenti accidentali della macchina e dalla perdita della funzione di sicurezza.

- **Convertitori di frequenza PowerFlex®**
  I convertitori di frequenza PowerFlex sono disponibili con diverse funzioni di sicurezza. Nei convertitori di frequenza PowerFlex 525, Safe Torque-off è una funzione integrata di serie, ma è una funzione opzionale nei convertitori di frequenza PowerFlex 40P, 70, 700H, 700S e 750 che supportano anche la funzionalità Safe Speed Monitor.

- **Kinetix® Integrated Motion**
  I servoazionamenti Kinetix 300, 6000, 6200, 6500 e 7000 sono tutti dotati di funzionalità di sicurezza integrata. Con Safe Torque-off, un'uscita del servoazionamento viene disabilitata per rimuovere la coppia motrice senza interrompere l'alimentazione dell'intera macchina. Safe Speed Monitoring permette agli utilizzatori di ridurre e monitorare la velocità dell'applicazione per aiutare l'operatore ad eseguire in sicurezza alcuni tipi di lavoro senza arrestare completamente la macchina.

Sistemi/reti di collegamento

- **Sistemi di connessione QuickConnect**
  Porte a T/splitter, scatole di distribuzione e spine di cortocircuitazione di sicurezza Guardmaster® fanno parte di un sistema di scollegamento rapido dedicato alla sicurezza delle macchine.

- **GuardLink™**
  GuardLink è un protocollo di comunicazione di sicurezza che utilizza un cablaggio standard in una topologia a "dorsale/discesa" con connessioni "plug and play". Permette la comunicazione dei dispositivi di sicurezza per la diagnostica ed il controllo, come comandi di reset e blocco remoto, su un unico cavo. Su un tratto di cavo che può arrivare a 1.000 metri, è possibile collegare fino a 32 dispositivi. I dispositivi di sicurezza Allen-Bradley con tecnologia

GuardLink permettono di accedere alle informazioni del sistema di sicurezza su EtherNet/IP. GuardLink può aiutare a semplificare la configurazione del sistema, ridurre il cablaggio ed aumentare le informazioni diagnostiche relative ad uso e manutenzione.

- **Sicurezza su EtherNet/IP**
  La rete EtherNet/IP™ consente di costruire sistemi di rete a livello di impianto che usano tecnologie di rete standard ed aperte. Assicura controllo ed informazione in tempo reale nelle applicazioni discrete, di processo continuo, batch, sicurezza, azionamento, controllo assi e ad alta disponibilità. Le reti EtherNet/IP collegano dispositivi quali avviatori motore e sensori ai controllori ed ai dispositivi di interfaccia operatore, oltre che a tutti i livelli aziendali. Inoltre, supportano sistemi di comunicazione industriali e non industriali su una singola infrastruttura di rete comune.

Strumenti di supporto

Ampia gamma di strumenti che supportano la conformità agli standard di sicurezza, riducono il rischio di infortuni e migliorano la produttività.

Safety Automation Builder

Safety Automation Builder è un software GRATUITO che semplifica la progettazione e la validazione dei sistemi di sicurezza delle macchine, riducendo tempi e costi. L'integrazione con il software di valutazione dei rischi RASWin fornisce agli utilizzatori una gestione coerente, affidabile e documentata del ciclo di vita della sicurezza funzionale. Safety Automation Builder ottimizza la progettazione del sistema di sicurezza favorendo la messa in conformità e la riduzione dei costi e guidando gli utilizzatori nello sviluppo del sistema di sicurezza, attraverso le fasi di layout, selezione dei prodotti ed analisi della sicurezza, permettendo di ottenere i livelli prestazionali (PL) di sicurezza macchine richiesti dalla norma globale (EN) ISO 13849-1.

RASWin

Il software RASWin consente agli utenti di gestire l'avanzamento attraverso il ciclo di vita della sicurezza funzionale, organizzando le informazioni provenienti da ogni fase del processo e la validazione delle macchine. RASWin collega le fasi del ciclo di vita della sicurezza per evitare guasti sistematici, includendo specifiche delle funzioni di sicurezza, assegnazione dei requisiti del livello prestazionale (PLr) e calcolo del livello PLr, validazione del circuito di sicurezza e documentazione.

Strumento di calcolo dei livelli prestazionali Sistema

Lo strumento SISTEMA, sviluppato da Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA), automatizza il calcolo del livello prestazionale raggiunto dalle parti di sicurezza del sistema di controllo di

una macchina secondo (EN) ISO 13849-1. I dati dei prodotti per la sicurezza delle macchine Rockwell Automation sono disponibili in una libreria utilizzabile con lo strumento di calcolo SISTEMA. La combinazione di queste due soluzioni consente ai progettisti di macchine e sistemi di risparmiare tempo nel valutare la sicurezza secondo (EN) ISO 13849-1. Una funzione di esportazione da Safety Automation Builder consente di importare facilmente in SISTEMA il progetto del sistema di sicurezza, in modo da ricevere una verifica di terze parti del livello prestazionale richiesto.

Funzioni di sicurezza preconfigurate per le macchine

Le funzioni di sicurezza delle macchine richiedono numerosi elementi tra cui un sensore o dispositivo di ingresso, un dispositivo logico e un dispositivo di uscita. Insieme, questi elementi forniscono un livello di protezione calcolato dal livello prestazionale, come riportato in (EN) ISO 13849-1. Rockwell Automation ha sviluppato diversi documenti per le funzioni di sicurezza, ognuno dei quali fornisce istruzioni per una specifica funzione di sicurezza in base al requisito funzionale, alla selezione delle apparecchiature e al requisito del livello prestazionale. Comprendono setup e cablaggio, configurazione, piano di verifica e validazione e calcolo del livello prestazionale.

Strumento Safety Maturity Index

Safety Maturity Index™ è uno strumento completo che permette di quantificare le prestazioni a livello di cultura della sicurezza, procedure di conformità e investimenti di capitale nelle tecnologie per la sicurezza e aiuta le aziende a valutare le proprie prestazioni attuali e a determinare le iniziative che possono intraprendere per migliorare la sicurezza e la redditività.

Servizi ed esperienza a vostra disposizione

Essendo il più grande fornitore in materia di sicurezza industriale, Rockwell Automation può contribuire a ridurre infortuni e costi migliorando, nel contempo, la produttività in ogni fase del ciclo di vita della sicurezza.

I servizi di sicurezza vengono forniti da uno staff esperto e qualificato in sicurezza, spesso in possesso di certificazioni TÜV Rheinland per la sicurezza delle macchine. Per aiutare i clienti a gestire in modo olistico il ciclo di vita della sicurezza, Rockwell Automation si affida ad ingegneri, tecnici ed esperti in sicurezza funzionale TÜV.

Il ciclo di vita della sicurezza è un processo chiaramente definito che contribuisce ad aumentare la produttività e a migliorare la sicurezza identificando le misure necessarie per valutare ed attenuare i rischi connessi ai macchinari. Il ciclo di vita della sicurezza può essere visualizzato e scaricato in questo documento.

Alcuni dei servizi a disposizione sono:

- **Valutazioni della sicurezza**
  Servizi che aiutano a valutare il rischio dell'impianto e supportano l'adozione di decisioni basate su solide informazioni che aiutano a migliorare la sicurezza di collaboratori e macchine.

- **Servizi di progettazione**
  Progettazione completa dei circuiti, applicazione corretta dei dispositivi ed analisi dei progetti, per aiutare a migliorare la sicurezza globale.

- **Servizi di installazione e validazione**
  Verifica che i sistemi stiano funzionando entro i parametri e gli standard definiti.

- **Formazione sulla sicurezza**
  Programmi di formazione completi, forniti da esperti leader del settore.

- **Servizi personalizzati**
  Copertura di applicazioni, tecnologie, applicazioni, piattaforme e configurazioni specifiche.

Perché scegliere Rockwell Automation

Integrare sicurezza e automazione può migliorare la produttività in molti stadi del processo di produzione, dalle fasi di progettazione e collaudo a quelle di installazione e messa in servizio, fino ad arrivare ad uso, manutenzione, modifica o dismissione. Tutte le fasi possono essere ottimizzate attraverso soluzioni di sicurezza correttamente applicate.

In qualità di leader mondiale per le soluzioni di automazione e sicurezza industriale e nella sua veste di innovatore tecnologico, Rockwell Automation è nella posizione ideale per supportare lo sviluppo di soluzioni di produzione più efficienti, sicure e produttive.

Avendo alle spalle molti anni di esperienza in automazione e sicurezza, conoscenze applicative e know-how nell'applicazione dei principi guida innovativi di standard di sicurezza come ISO 12000, (EN) ISO 13849-1 e IEC 62061, Rockwell Automation può assistervi nelle attività di selezione, integrazione, formazione e supporto in materia di soluzioni per la sicurezza delle macchine, la sicurezza dei processi e la sicurezza elettrica.

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, Via Cantonale 27, 6928 Manno, Tel: 091 604 62 62, Fax: 091 604 62 64, Customer Service: Tel: 0848 000 279

Pubblicazione: SAFEBK-RM002C-IT-P – Novembre 2016