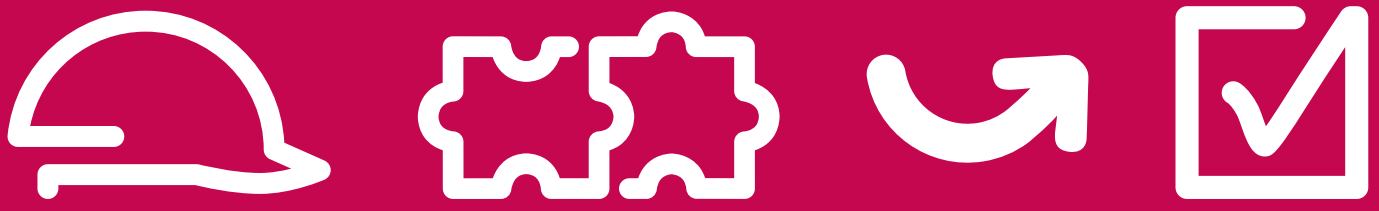
Guida Applicativa
Sicurezza Macchine



Schneider Electric™

Sommario

Introduzione

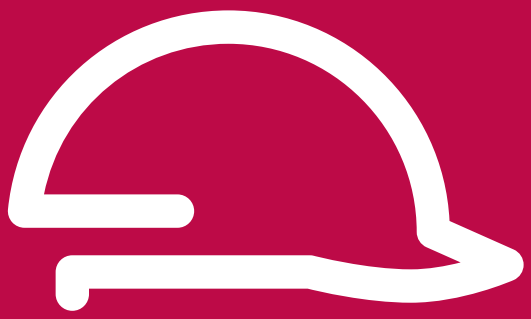
Molte guide alla legislazione in materia di sicurezza macchine tendono a presentare una visione distorta dei requisiti della normativa vigente.

Questa guida offre informazioni aggiornate e obiettive con lo scopo di aiutare i costruttori di macchine e gli utenti finali a garantire la sicurezza dei lavoratori con macchine sicure, a norma ed efficienti.

Non pretende di essere una guida esaustiva sulla rispondenza e conformità alla normativa vigente in materia di sicurezza, né di poter sostituire in alcun modo la consultazione delle norme stesse.

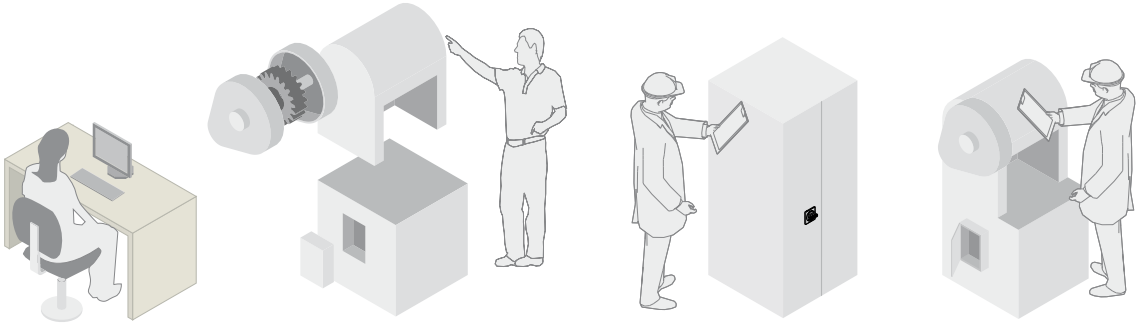
L'obiettivo di questa guida è seguire passo passo attraverso un percorso logico l'analisi dei diversi aspetti della sicurezza macchine, indicando le fonti di informazione più rilevanti.

Le Direttive Europee



Oltre all'obbligo morale di evitare danni alle persone, la normativa specifica impone macchine sicure, esistono poi valide ragioni economiche per prevenire gli incidenti.

La sicurezza deve essere implementata a partire dalla progettazione e deve riguardare tutto il ciclo di vita di una macchina: progettazione, costruzione, installazione, regolazione, funzionamento, manutenzione e rottamazione.



Progettazione/Costruzione | Installazione | Regolazione/Funzionamento | Manutenzione

Macchine nuove: la Direttiva Macchine

La Nuova Direttiva Macchine 2006/42/CE è entrata in vigore dal 29 Dicembre 2009.

Stabilisce che i costruttori garantiscano i requisiti minimi di sicurezza per i macchinari e le apparecchiature commercializzati all'interno dell'Unione Europea.

Le macchine devono adeguarsi ai requisiti fondamentali di salute e sicurezza elencati nell'Allegato I della Direttiva, garantendo in tal modo un livello minimo di protezione e sicurezza comune per tutto il mercato europeo.

Prima di immettere sul mercato una nuova macchina i produttori o i loro rappresentanti autorizzati all'interno dell'EU devono garantire che la macchina sia conforme, rendere disponibile un Fascicolo Tecnico in caso di richiesta giustificata da parte di un'autorità, firmare una "Dichiarazione di Conformità" e apporre la marcatura CE.

Macchine esistenti: Direttiva sull'uso delle attrezzature da lavoro

La Direttiva 89/655/CE sull'uso delle attrezzature da lavoro è rivolta agli utilizzatori delle macchine ed è rispettata utilizzando macchine e macchinari conformi alle norme.

Riguarda l'utilizzo di tutte le attrezzature da lavoro, compresi macchinari di sollevamento e attrezzature mobili, in tutti i luoghi di lavoro.

Le attrezzature di lavoro devono essere adatte all'uso e garantire la sicurezza nel tempo, attraverso una corretta manutenzione.

Il costo degli incidenti

Alcuni costi sono evidenti, quali ad esempio l'assenza per malattia del personale infortunato, mentre alcuni costi sono più difficili da identificare. L'impatto finanziario sull'azienda è altissimo: l'aumento dei premi assicurativi, il calo della produzione, la perdita di clienti e della reputazione dell'azienda.

Alcune misure di riduzione del rischio possono effettivamente migliorare la produttività; l'utilizzo ad esempio di barriere fotoelettriche per proteggere i punti di accesso ai macchinari possono permettere un più veloce e sicuro carico e scarico, mentre l'installazione di dispositivi di sezionamento può permettere di isolare alcune parti della macchina, in caso di manutenzione, lasciando operative altre sezioni.

Le norme riguardano tutti i lavoratori, dipendenti o autonomi, e tutti coloro che si occupano della verifica delle attrezzature e delle macchine.

Le Norme Tecniche Europee

Direttiva CE:

> Strumento legale utilizzato per armonizzare le legislazioni degli Stati membri dell'Unione Europea

> Stabilisce i requisiti essenziali per la salute e la sicurezza

> Obbligo di trasposizione nella legislazione nazionale

Norma tecnica:

> Con il termine "norma" si intende una specifica tecnica approvata da un ente normativo riconosciuto a svolgere questa attività di normazione

Norme armonizzate:

> Una norma diventa armonizzata quando viene pubblicata negli Stati membri della comunità

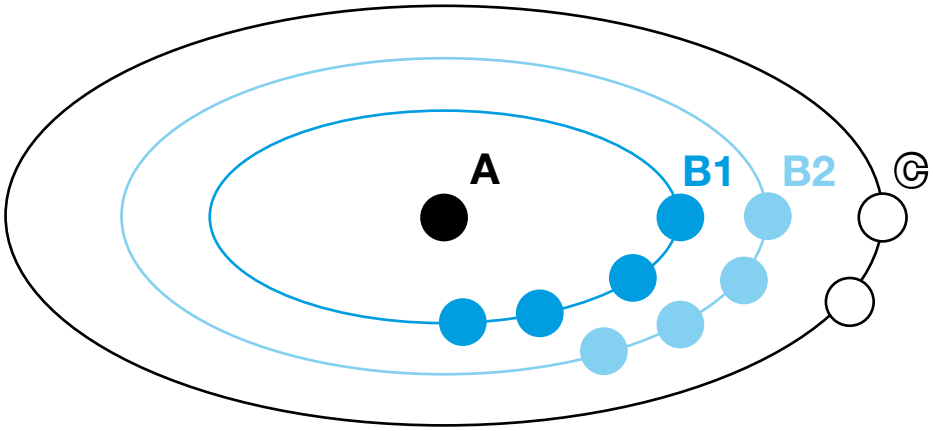
Presunzione di conformità:

Un prodotto costruito in conformità ad una norma armonizzata europea (EN), il cui riferimento è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea per una specifica Direttiva e che risponde ad uno o più dei requisiti essenziali di sicurezza e di tutela della salute, è presunto conforme ai requisiti essenziali di tale Direttiva.

È necessario garantire la conformità a tutti i requisiti applicabili per il conferimento della Presunzione di Conformità.

Norme di tipo A B e C:

Le norme armonizzate in materia di Sicurezza Macchine si dividono in tre tipi come qui di seguito descritto:



Norme di tipo A

> (norme base) contengono i concetti fondamentali, i principi di progettazione e gli aspetti generali applicabili a tutte le macchine;

Norme di tipo B

> (norme gruppo) trattano un aspetto specifico della sicurezza o un dispositivo di sicurezza. Sono suddivise in due gruppi:

- Tipo B1 : riguardano aspetti particolari della sicurezza (ad es. distanze di sicurezza, temperatura della superficie, rumore);
- Tipo B2: riguardano i dispositivi di protezione (ad es. comandi a due dispositivi di interblocco delle protezioni);

Norme di tipo C

> (norme famiglie di macchina) trattano i requisiti di sicurezza per tipologia di macchina.

Quando una norma di tipo C devia da una o più disposizioni di una norma di tipo A o da una norma di tipo B, prevale la norma di tipo C.

Alcuni esempi di norme:		
EN/ISO 12100	**A**	Sicurezza del macchinario. Concetti fondamentali di valutazione e riduzione del rischio
EN 574	**B**	Dispositivo comando a due mani. Aspetti funzionali, principi generali di progettazione
EN/ISO 13850	**B**	Arresto di emergenza - Principi di progettazione
EN/IEC 62061	**B**	Sicurezza di funzionamento di sistemi di controllo elettrici, elettronici, ed elettronici programmabili
EN/ISO 13849-1	**B**	Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza - Parte 1: Principi generali per la progettazione
EN 349	**B**	Spazi minimi per evitare lo schiacciamento di parti del corpo.
EN/SO 13857	**B**	Sicurezza del macchinario - Distanze di sicurezza per impedire il raggiungimento di zone pericolose con gli arti superiori e inferiori
EN/IEC 60204-1	**B**	Sicurezza del macchinario - Componenti elettriche delle macchine Parte 1: Principi generali per la progettazione
EN 999/ISO 13855	**B**	Posizionamento dei dispositivi di protezione in funzione delle velocità di avvicinamento di parti del corpo
EN 1088/ISO 14119	**B**	Dispositivi di interblocco associati ai ripari. Principi di progettazione e di scelta
EN/IEC 61496-1	**B**	Dispositivi elettrosensibili di protezione Parte 1: Requisiti generali e prove
EN/IEC 60947-5-5	**B**	Apparecchiature e quadri di bassa tensione - Parte 5-5: Dispositivi per circuiti di comando ed elementi di manovra. Sezione 5: Dispositivo elettrico di arresto d'emergenza con blocco meccanico.
EN 842	**B**	Segnali visivi di pericolo. Requisiti generali, progettazione e prove
EN 1037	**B**	Protezione contro l'avviamento imprevisto
EN 953	**B**	Requisiti generali per la progettazione e la costruzione di ripari fissi e mobili
EN 201	**C**	Macchine per materie plastiche e gomma. Presse a iniezione. Requisiti di sicurezza
EN 692	**C**	Macchine utensili - Presse meccaniche - Requisiti di sicurezza
EN 693	**C**	Macchine utensili - Presse idrauliche - Requisiti di sicurezza
EN 289	**C**	Macchine per materie plastiche e gomma - Sicurezza - Presse piegatrici idrauliche per la produzione di corpi cavi - Requisiti di progettazione e costruzione
EN 422	**C**	Macchine per soffiaggio per la produzione di corpi cavi - Requisiti di progettazione e costruzione
EN/ISO 10218-1	**C**	Robot per ambienti industriali - Requisiti di sicurezza - Parte 1: Robot
EN 415-4	**C**	Sicurezza macchine per imballare - Parte 4: Pallettizzatori e depallettizzatori.
EN 619	**C**	Apparecchiature e sistemi di movimentazione continua - Requisiti di sicurezza e compatibilità elettromagnetica per le apparecchiature di movimentazione meccanica di carichi unitari
EN 620	**C**	Apparecchiature e sistemi di movimentazione continua - Requisiti di sicurezza e compatibilità elettromagnetica per trasportatori a nastro fissi per materiale sfuso

Responsabilità del costruttore

I costruttori che immettono le macchine sul mercato europeo devono adeguarsi alle disposizioni previste dalla Direttiva Macchine.
Per “immissione sul mercato” si intende anche il caso di un’azienda che fornisce un macchinario a se stessa, per costruire o modificare macchine per proprio uso personale, o ancora l’importazione di macchine nell’ambito della Comunità Europea.

Responsabilità dell’utilizzatore

Spetta agli utilizzatori accertarsi che le nuove macchine acquistate abbiano la marcatura CE e siano accompagnate da una Dichiarazione di Conformità alla Direttiva. Le macchine devono essere utilizzate secondo le istruzioni del fabbricante.

Le macchine esistenti in servizio prima dell’entrata in vigore della Direttiva Macchine sono tenute a garantire la conformità alle regolamentazioni della Direttiva sull’Uso delle Attrezzature di Lavoro (Direttiva Sociale).


Aries

Analisi del rischio

Affinchè una macchina (o altra apparecchiatura) possa essere ritenuta sicura è necessario valutare attentamente i rischi che potrebbero derivare dal suo utilizzo.
La strategia di valutazione del rischio e riduzione dei rischi è oggetto dalla norma EN/ISO 12100.

Esistono molte tecniche di valutazione del rischio, ma nessuna può essere ritenuta la strategia migliore. La normativa specifica ha alcuni principi generali, ma non può indicare esattamente la procedura da seguire per ciascun caso specifico. Sarebbe auspicabile che la normativa potesse fornire un valore o 'punteggio' per ciascun rischio ed un valore ottimale massimo da non superare. Il punteggio assegnabile ad ogni singolo rischio, oltre al livello di rischio tollerabile, dipende da una serie di analisi e può variare in funzione della persona incaricata o in base all'ambiente. I rischi che potrebbero ad esempio essere ragionevoli e tollerabili in un ambiente industriale, con personale specializzato, sarebbero al contrario inaccettabili in uno spazio pubblico con presenza di bambini.
L'analisi storica dei tassi di incidenti e infortuni può essere un indicatore utile, ma non può fornire un'indicazione affidabile sulle percentuali prevedibili di incidenti ed infortuni.

Definire i limiti della macchina

Cosa è importante valutare? Quali sono le velocità, i carichi, le sostanze, ecc. che possono essere coinvolte. Ad esempio quante bottiglie può produrre all'ora una soffiatrice in estrusione continua e quanto materiale viene lavorato e a che temperatura. Non dimenticare di prevedere un uso errato o non idoneo, come ad esempio l'eventuale utilizzo di una macchina al di fuori delle specifiche tecniche. Qual è l'aspettativa di vita di una macchina e dell'applicazione ad essa correlata? Bisogna provvedere in che modo rottamare la macchina al termine del suo ciclo di vita.

Identificare i rischi

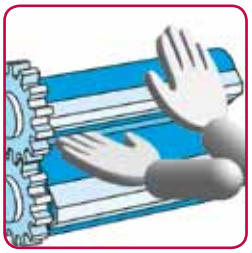
Quali aspetti della macchina possono causare danni o lesioni ad una persona? I pericoli da tenere in considerazione includono la possibilità di intrappolamento, schiacciamento, taglio con attrezzi e utensili, con bordi e spigoli vivi della macchina o con dei materiali lavorati. Occorre inoltre considerare altri fattori quali stabilità della macchina, rumore, vibrazioni, emissione di sostanze tossiche o fumi, radiazioni, superfici calde, agenti chimici o velocità elevate. Questa fase deve includere tutti i rischi riscontrabili durante il ciclo di vita di una macchina, compresa la costruzione, l'installazione e lo smaltimento.

Qui di seguito forniamo alcuni esempi di rischi tipici anche se la lista non pretende di essere esaustiva. Un elenco dettagliato è riportato nella norma EN/ISO 12100.

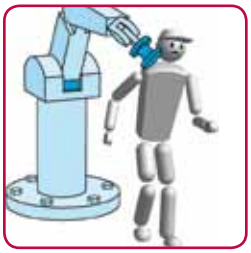
Chi può subire lesioni o danni conseguenti ai rischi identificati e quando?

Chi interagisce con la macchina, quando e perchè? Di nuovo consigliamo di verificare l'uso scorretto ragionevolmente prevedibile, compresa la possibilità di utilizzo di una macchina da parte di personale inesperto; non solo gli operatori ma anche il personale addetto alle pulizie, alla sicurezza o il pubblico.

Foratura, perforazione, puntura, tranciatura, taglio



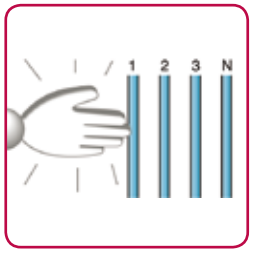
Impigliamento, trascinamento e intrappolamento



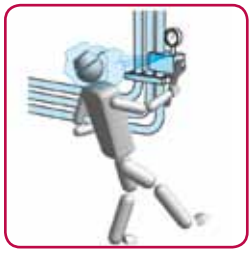
Urto

Schiacciamento

Qui a lato sono illustrati alcuni esempi di rischi tipici.



Folgorazione



Emissione di sostanze pericolose

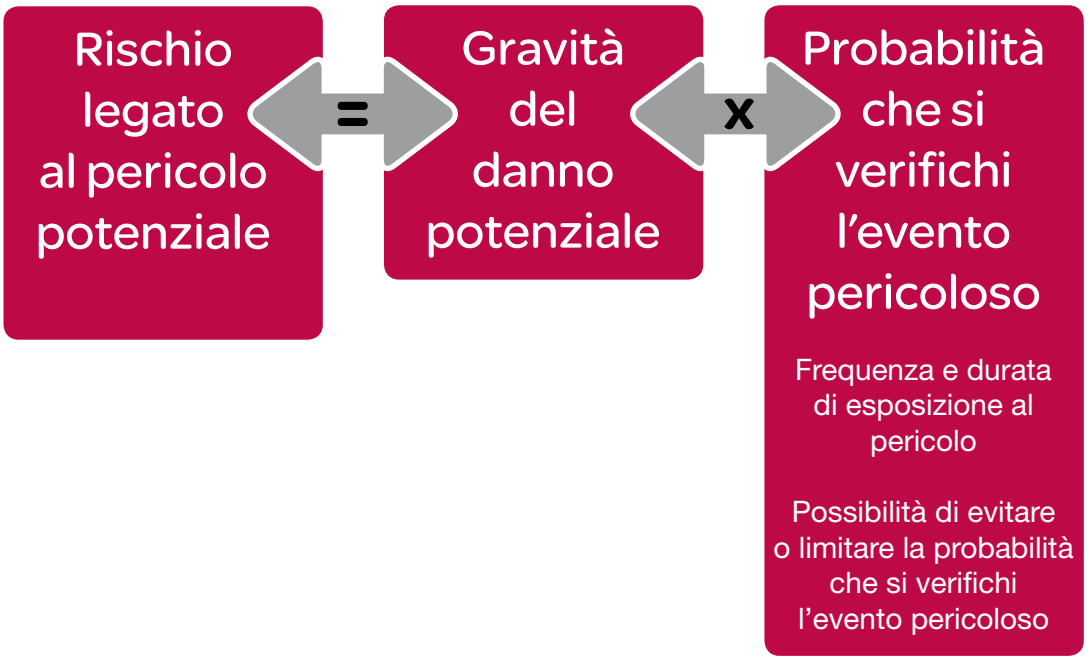
Scottature

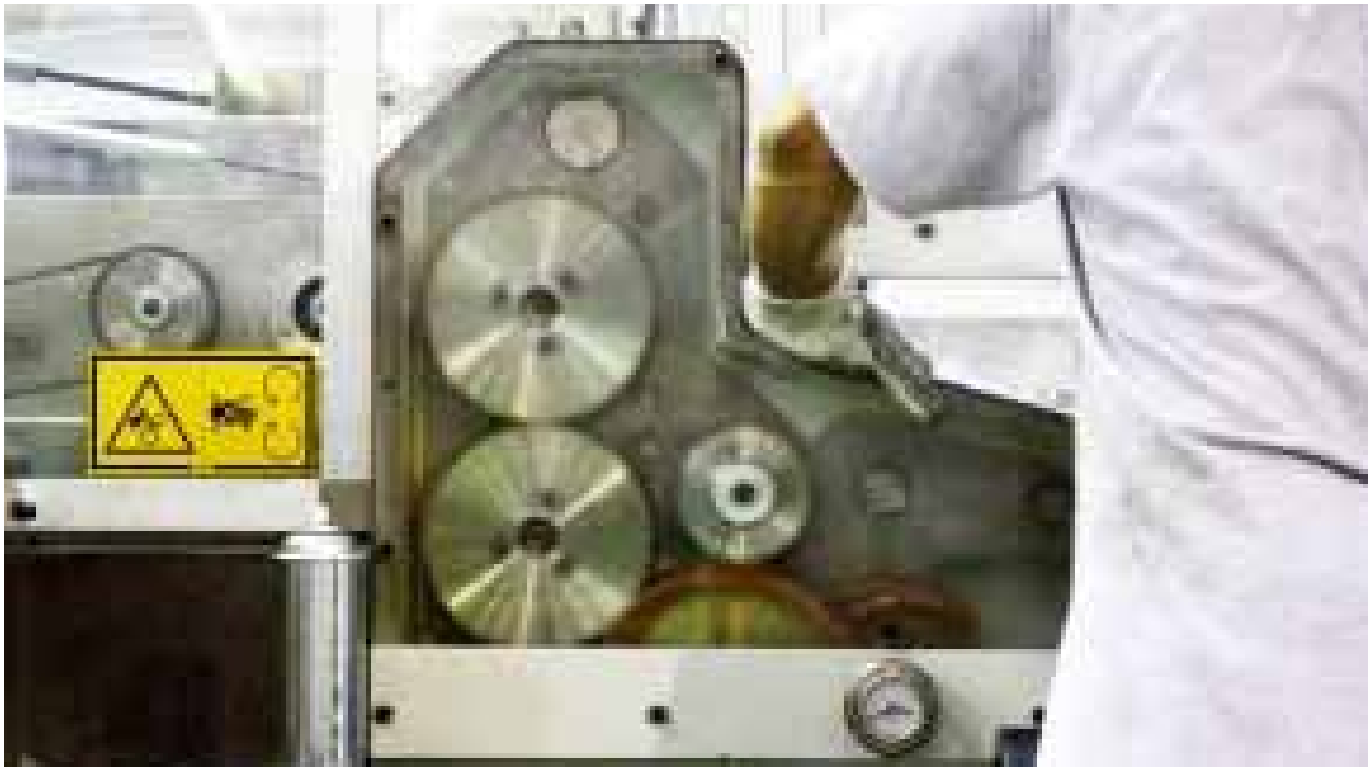
Stabilire un ordine di priorità in base dalla gravità del rischio

La norma EN/ISO 12100 contiene le istruzioni a livello globale per la valutazione dei rischi. La stima dei rischi può essere valutata considerando il danno potenziale che potrebbe derivare dal rischio in base all'esposizione al rischio stesso ed il numero di persone esposte al pericolo.

Resta comunque difficile stimare il danno potenziale, ammettendo sempre la possibilità che qualsiasi incidente possa portare a danni con effetti irreversibili. Tuttavia anche nella maggior parte dei casi che presentano più di una possibile conseguenza, una sola è quella più probabile. Occorre sempre prendere in considerazione tutte le conseguenze plausibili, non solo il caso più grave.

Il risultato del processo di Valutazione del rischio dovrà portare ad una tabella dei vari rischi legati alla macchina con indicazione della gravità di ciascuno. Non esiste un unico "tasso di rischio" o un'unica "categoria di rischio" per una macchina: ogni rischio deve essere considerato e valutato singolarmente. La gravità del rischio può essere solo stimata: la Valutazione dei Rischi non è una scienza esatta, l'obiettivo della Valutazione del rischio deve essere una corretta strategia di riduzione dei rischi.





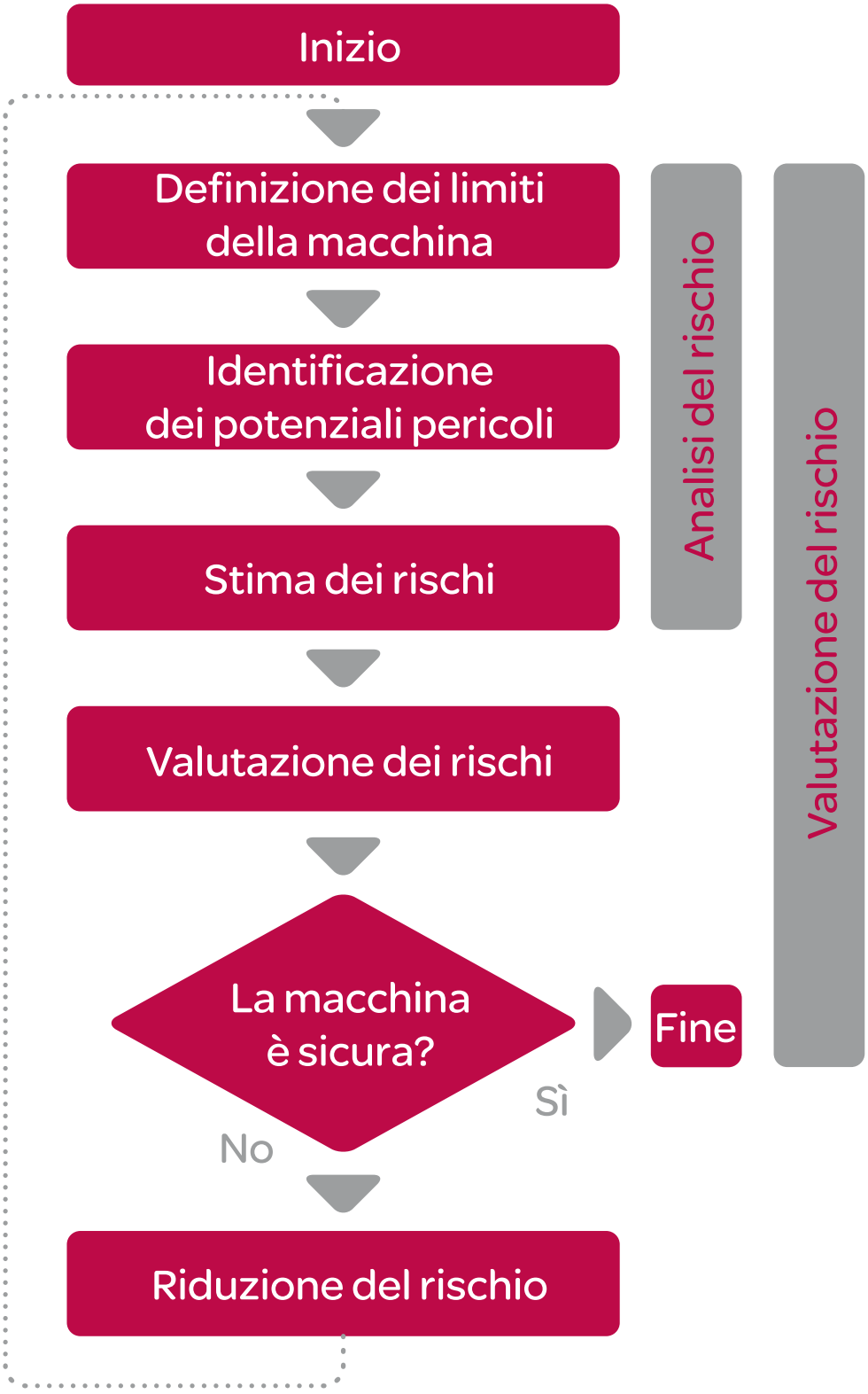
Riduzione del rischio

La norma EN/ISO 12100 definisce una strategia di riduzione dei rischi.

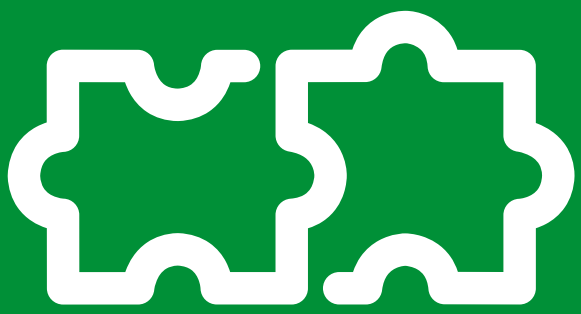
La riduzione dei rischi è definita in termini di eliminazione e neutralizzazione del rischio: “le misure adottate devono avere lo scopo di eliminare ogni rischio durante l’esistenza prevedibile della macchina, incluse le fasi di trasporto, montaggio, smontaggio, smantellamento messa fuori servizio e rottamazione.”

Come regola generale, se un rischio può essere ridotto è necessario adottare tutte le possibili misure per ridurlo. Questo compatibilmente con ogni singola realtà economica aziendale; le norme utilizzano termini quali “ragionevole” per indicare che potrebbe esistere la possibilità che alcuni rischi non siano eliminabili senza interventi economicamente molto gravosi.

La valutazione dei rischi è un processo interattivo che deve essere realizzato in diverse fasi del ciclo di vita della macchina: i rischi devono essere identificati, gestiti secondo un ordine di priorità, quantificati, adottando misure opportune per eliminare i pericoli o ridurre i rischi connessi con misure opportune (per prima cosa con una costruzione sicura, quindi con l’adozione di misure tecniche di sicurezza). Questo processo dovrà quindi essere ripetuto per valutare se e in che modo i singoli rischi siano stati ridotti ad un livello accettabile, accertandosi che non siano stati introdotti rischi ulteriori.
Nelle pagine che seguono esamineremo la progettazione e costruzione sicura e l’adozione delle misure di sicurezza.


Inizio
Definizione dei limiti della macchina
Identificazione dei potenziali pericoli
Stima dei rischi
Valutazione dei rischi
La macchina è sicura?
Sì
No
Fine
Riduzione del rischio
Analisi del rischio
Valutazione del rischio

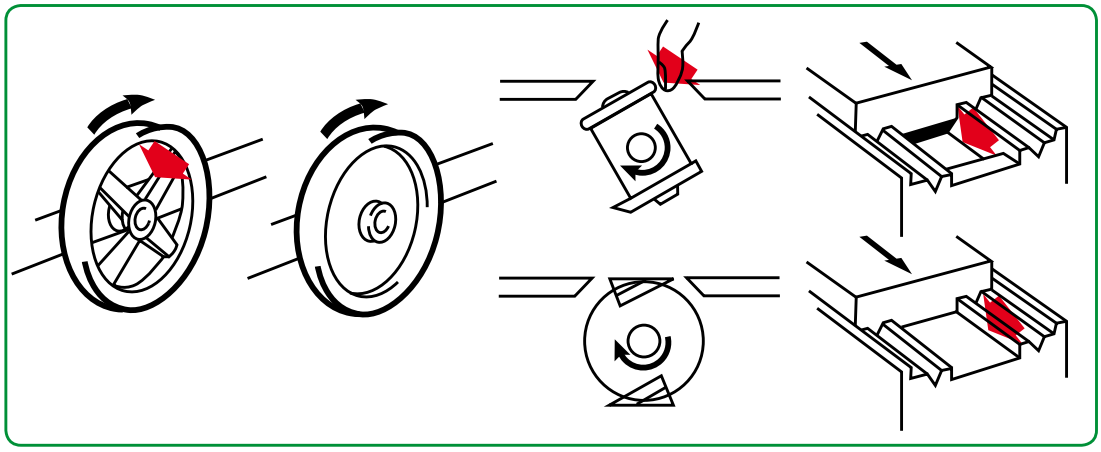
Progettazione delle funzioni di sicurezza



Concetto di costruzione sicura (secondo EN/ISO 12100)

> Alcuni rischi possono essere evitati adottando semplici misure; è possibile eliminare all'origine il rischio? Talvolta è possibile eliminare il rischio automatizzando alcune operazioni quali ad esempio il carico della macchina.
Ad esempio l'utilizzo di un solvente non infiammabile per le operazioni di pulizia dei macchinari può evitare i rischi di incendio causati da sostanze infiammabili.
Questa fase viene definita con il termine di **Costruzione conforme ai principi di progettazione sicura** e rappresenta l'unico modo per **azzerare il rischio**.

Togliere la trasmissione dal rullo terminale di un trasportatore permette di ridurre la possibilità che qualcuno venga intrappolato. Sostituire le pulegge a raggi con dischi lisci consente di ridurre i rischi di taglio. Eliminare bordi e spigoli taglienti, angoli o sporgenze consente di evitare tagli ed ecchimosi. L'aumento delle distanze minime dalla macchina può permettere di evitare lo schiacciamento di parti del corpo.
La limitazione di forze, velocità e pressioni può ridurre il rischio di lesioni.



Eliminazione delle cesoie a ghigliottina con misure appropriate di progettazione sicura. Fonte: BS PD 5304

> Fare attenzione ad evitare di sostituire un rischio con un altro. Gli utensili alimentati ad aria permettono ad esempio di evitare i rischi legati all'elettricità, ma possono implicare altri rischi legati all'uso dell'aria compressa, quali l'iniezione d'aria e il rumore del compressore.

Norme e leggi indicano una gerarchia distinta per i controlli. L'eliminazione dei rischi o la riduzione dei rischi ad un livello tollerabile con appropriate misure di sicurezza rappresenta la priorità.

Misure tecniche di sicurezza e dispositivi di protezione aggiuntivi (secondo EN/ISO 12100)

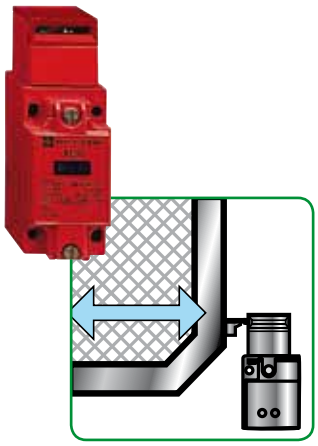
> Ove non sia possibile la costruzione conforme a principi di progettazione sicura, il passo successivo è l'adozione di **misure tecniche di sicurezza**. Queste possono prevedere ad esempio l'installazione di ripari fissi o mobili, rilevatori di presenza per evitare avviamenti inattesi, ecc.
Le misure tecniche di sicurezza devono impedire a chiunque l'accesso o il contatto involontario con un elemento pericoloso che implica un rischio di lesione personale, oppure ridurre il rischio portandolo ad uno stato sicuro prima che la persona possa entrare in contatto con esso.

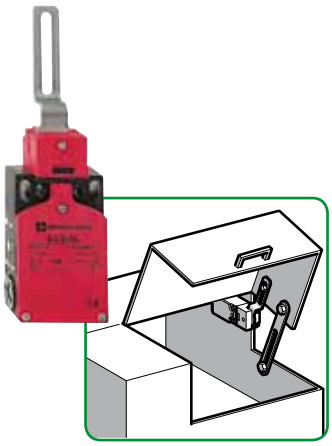
I ripari possono essere fissi per limitare o mantenere la distanza da un pericolo, o mobili (interbloccati o regolabili manualmente o automaticamente).

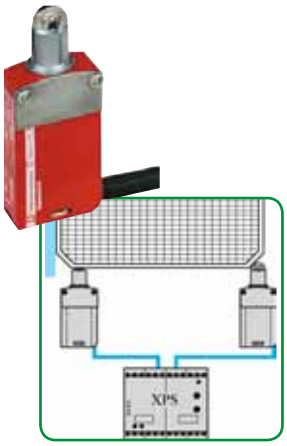
I dispositivi di protezione utilizzati per creare un sistema di sicurezza comprendono:

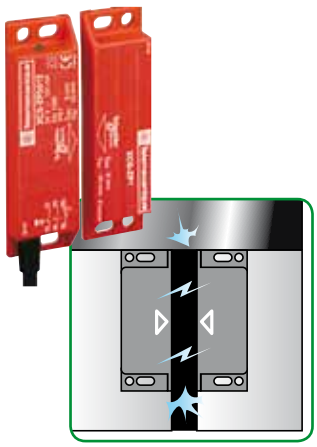
> Dispositivi di interblocco che rilevano e controllano la posizione dei ripari mobili, utilizzati generalmente per consentire le operazioni di carico e scarico, pulizia, impostazione, regolazione, ecc.

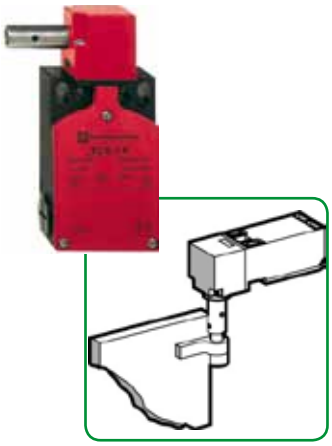
La protezione degli operatori è assicurata dall'arresto della macchina quando l'attuatore è fuori dalla testa dell'interruttore, quando la leva o il pistone è attivato, quando il riparo è aperto o la cerniera del riparo ruotata di 5° , generalmente su macchine a bassa inerzia (ad esempio con tempi di arresto rapidi)



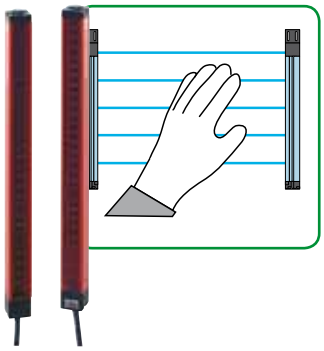








Barriere fotoelettriche di sicurezza per il rilevamento degli accessi alle zone pericolose



> Rilevamento dita, mani o corpo (capacità di rilevamento fino a 14mm, fino a 30mm e oltre 30mm)

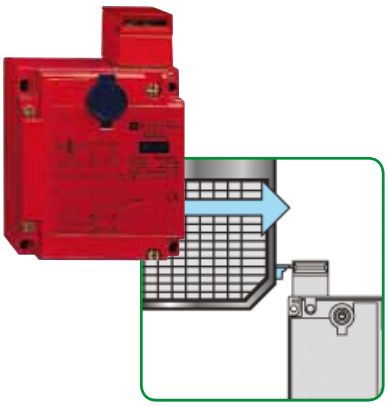
Le barriere fotoelettriche di sicurezza vengono utilizzate generalmente nelle applicazioni di movimentazione materiali, confezionamento e imballaggio, nastri trasportatori, immagazzinaggio ecc. Le barriere sono sensori di presenza fotoelettrici concepiti specificatamente per proteggere il personale dai movimenti pericolosi delle macchine. Sono perfette per le applicazioni in cui il personale necessita di accedere frequentemente a un punto di lavoro pericoloso. L'assenza di porte o schermi di protezione facilita l'accesso riducendo i tempi necessari alle operazioni di carico, ispezione o regolazione, pur garantendo un livello di sicurezza ottimale e un'elevata produttività.

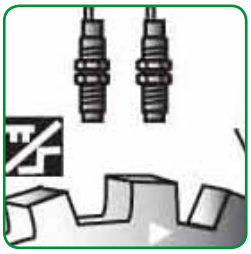
Tappeti di sicurezza sensibili alla pressione

> Rilevamento avvicinamento o stazionamento nell'area pericolosa

I tappeti o pedane sensibili alla pressione sono spesso usati davanti o intorno ad un'area con macchine o robot potenzialmente pericolosi. Servono a proteggere l'area intorno alla macchina, impedendo movimenti pericolosi se l'operatore si avvicina dalla zona pericolosa.
Sono concepiti per garantire la sicurezza del personale e vengono spesso associati alle barriere fotoelettriche per consentire il libero accesso per operazioni di carico e scarico delle macchine.
Non impediscono l'accesso ma si attivano quando lo rilevano: la pressione esercitata sul tappeto interrompe il movimento pericoloso.

Interruttori di sicurezza con elettroserratura (bobina) per prevenire l'apertura delle protezioni mobili





> Per le fasi pericolose, a differenza degli interruttori senza blocco, gli interruttori con bobina sono utilizzati su macchine con inerzia elevata, ad esempio con tempi di arresto lunghi e sono consigliati per il controllo degli accessi previo arresto del movimento pericoloso. Sono spesso utilizzati con i moduli Preventa temporizzati (con tempi di arresto macchina definiti) o di rilevamento velocità nulla (con tempi di arresto variabili) per consentire l'accesso solo quando sono soddisfatte le condizioni di sicurezza.

La scelta e l'installazione degli interruttori di sicurezza deve consentire di ridurre al minimo la possibilità di guasto ed errore, mentre il dispositivo di protezione non deve impedire le lavorazioni e la produzione.
Per raggiungere questo obiettivo sono necessari:

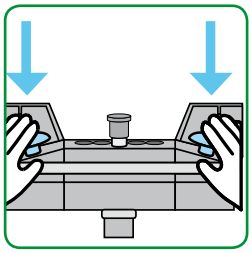
- dispositivi di protezione fissati solidamente; il loro montaggio/smontaggio o regolazione deve richiedere un utensile;

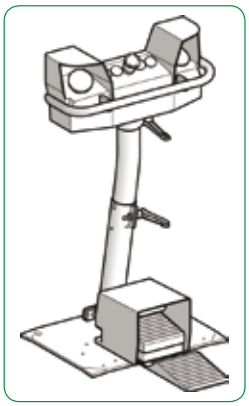
- dispositivi o sistemi bloccati codificati per l'interblocco del comando o dell'alimentazione (meccanico, elettrico, magnetico o ottico)

- impedimento fisico o schermo di protezione per prevenire l'accesso al dispositivo di interblocco con riparo aperto;

- il supporto dei dispositivi deve essere sufficientemente rigido per assicurare il loro corretto funzionamento

Pulpito di comando a due mani e interruttori a pedale





> Evitano all'operatore l'accesso ad una macchina mentre questa si trova in una condizione pericolosa (es. comando presse).

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. Per la protezione del resto del personale è necessario prevedere altre misure di sicurezza quali ad esempio l'installazione di barriere fotoelettriche.

Comando ad azione mantenuta per accesso in condizioni specifiche di rischio ridotto

> Permettono all'operatore di accedere ad un'area pericolosa in caso di operazioni di ricerca guasti, manutenzione, messa in servizio, ecc. (ad es. manovra ad impulsi). Sono dotati di interruttori a tre posizioni: attivati in posizione centrale e disattivati nelle altre due posizioni (rilasciato o completamente premuto).

Monitoraggio dei segnali di sicurezza: i sistemi di controllo

I segnali emessi dai dispositivi di sicurezza in campo vengono generalmente monitorati con componenti quali moduli di sicurezza, configuratori o PLC di sicurezza (definiti “dispositivi logici di sicurezza”), che vengono utilizzati per comandare (e talvolta monitorare) i dispositivi di uscita quali i contattori.

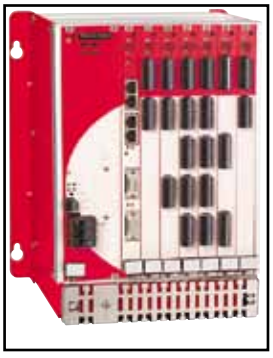
La scelta di un dispositivo logico dipende da molti fattori tra i quali il numero di ingressi di sicurezza da elaborare, il costo, la complessità delle funzioni di sicurezza, dall’esigenza di ridurre il cablaggio con un bus di campo quali AS-Interface Safety at Work o SafeEthernet, o infine dalla necessità di inviare segnali/dati di sicurezza su lunghe distanze attraverso macchine di grandi dimensioni o tra macchinari in siti particolarmente estesi. L’attuale diffuso utilizzo di dispositivi elettronici complessi e software nei controllori o PLC di sicurezza ha in parte influenzato l’evoluzione delle normative in materia di sicurezza relative ai sistemi di controllo.

Tra le norme di riferimento più recenti ricordiamo la EN/ISO 13849-1 (che sostituisce la EN 954-1) e la EN/IEC 62061.


Modulo di sicurezza


Configuratore di sicurezza


PLC di sicurezza compatto


PLC di sicurezza modulare

La funzione di protezione prevede generalmente l’utilizzo di un sistema di comando e controllo, relativamente al quale la Direttiva Macchine indica diversi requisiti prestazionali. In particolare la norma specifica che “i sistemi di comando devono essere progettati e costruiti in modo da evitare l’insorgere di situazioni pericolose”. La Direttiva Macchine non chiede in modo specifico l’applicazione di uno standard; tuttavia l’utilizzo di un sistema di comando conforme ai requisiti delle norme armonizzate è un modo per dimostrare la conformità al requisito della Direttiva Macchine. Due norme che rivedono i princìpi generali per la progettazione dei sistemi di comando relativi alla sicurezza, sono la EN/ISO 13849-1 (in sostituzione alla norma EN 954-1) e la EN/IEC 62061.

Misure di protezione e dispositivi complementari: Arresti di emergenza

Malgrado i dispositivi di arresto d'emergenza siano richiesti per qualsiasi tipo di macchina (la Direttiva Macchine prevede due eccezioni specifiche) la norma li considera "apparecchiature di protezione complementari". Poiché non impediscono e non rilevano l'accesso a un pericolo, non sono considerati dispositivi di protezione primari. Sono generalmente usati per proteggere le persone e le macchine **solo in caso di pericoli improvvisi ed emergenze**.
Devono essere robusti, affidabili e immediatamente accessibili e disponibili in tutte le modalità di funzionamento della macchina e in tutte le posizioni in cui possa essere necessario azionarli.

La norma EN/IEC 60204-1 suddivide gli arresti in tre categorie:

– Categoria 0: arresto con immediata apertura dell'alimentazione degli attuatori della macchina (arresti non controllati);

– Categoria 1: arresto con alimentazione disponibile affinché gli attuatori della macchina eseguano l'arresto; l'alimentazione viene rimossa dopo l'arresto;

– Categoria 2: arresto comandato con alimentazione disponibile per gli attuatori della macchina, anche dopo l'arresto.

La Categoria 2 non è generalmente considerata adatta ad un arresto d'emergenza.

Gli arresti d'emergenza devono essere conformi alla norma EN/IEC 60947-5-5.

Rischi residui

Dopo aver eliminato o ridotto i rischi il più possibile attraverso la progettazione e costruzione di macchine intrinsecamente sicure e con l'installazione dei sistemi e delle misure di protezione necessari, il processo di valutazione dei rischi deve essere ripetuto per verificare che non siano stati introdotti nuovi rischi (ad esempio l'installazione di ripari mobili può implicare rischi di schiacciamento) e per valutare se ciascun rischio sia stato ridotto entro limiti tollerabili. Tuttavia pur ripetendo più volte il processo interattivo di valutazione e riduzione dei rischi può accadere facilmente che sussistano rischi residui.

Ad eccezione delle macchine costruite in conformità con una norma di tipo C (automatica presunzione di conformità con i requisiti essenziali di sicurezza e salute) spetta al progettista giudicare il livello di tollerabilità del rischio residuo o le eventuali ulteriori misure da prendere, fornendo informazioni ed indicazioni specifiche riguardo ai rischi residui sotto forma di iscrizioni e/o targhe con le istruzioni per l'uso, ecc. Le istruzioni dovranno altresì specificare le misure da adottare, quali ad esempio i dispositivi di protezione personale (DPP) o procedure operative particolari, anche se queste ultime non saranno mai affidabili quanto le misure implementate direttamente dal progettista della macchina.

Sicurezza funzionale

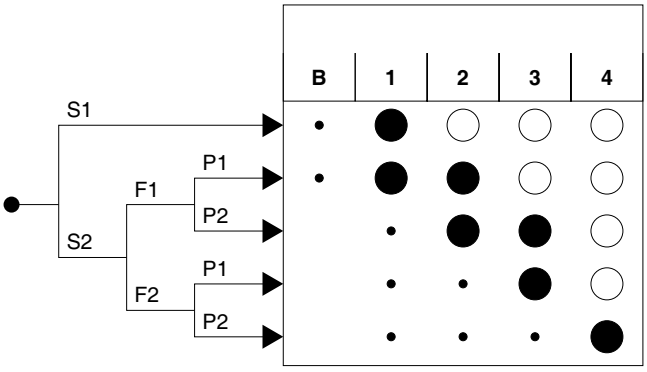
Sicurezza funzionale

Negli ultimi anni sono state pubblicate numerose norme che utilizzano il concetto di sicurezza funzionale. Tra queste ricordiamo le norme IEC 61508, IEC 62061, IEC 61511, ISO 13849-1 e la IEC 61800-5-2, tutte entrate in vigore in Europa e pubblicate come norme EN.

Il concetto di sicurezza funzionale è relativamente recente e sostituisce le vecchie Categorie definite dalla norma EN 954-1 a cui spesso si fa erroneamente riferimento come 'Categorie di sicurezza'.

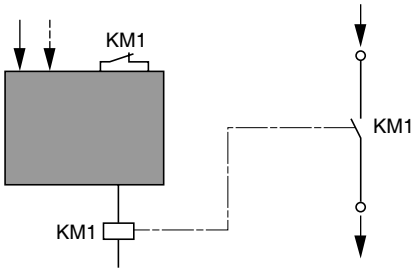
Promemoria dei principi della norma EN 954-1

Chi conosce la norma EN 954-1 avrà sicuramente familiarità con il vecchio "diagramma di rischio" da molti utilizzato in passato per progettare le parti dei sistemi di comando legate alla sicurezza in base alle categorie B da 1 a 4. All'utilizzatore veniva richiesto di valutare in modo soggettivo la gravità del danno, la frequenza e/o il tempo di esposizione al pericolo e la possibilità di evitarlo. La gravità della lesione veniva valutata con i parametri da lieve a seria, e l'esposizione al rischio da rara a frequente, da possibile in determinate condizioni a virtualmente impossibile. L'obiettivo era di arrivare alla categoria richiesta per ogni parte del sistema legata alla sicurezza.

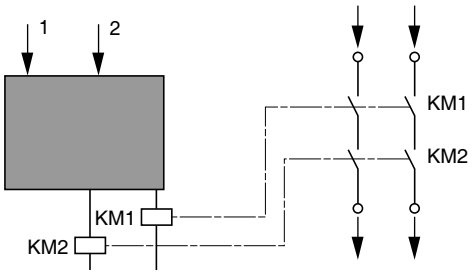


La teoria è che più la riduzione dei rischi dipende dal funzionamento corretto del sistema di controllo elettrico di sicurezza e più questo dovrà essere in grado di resistere ai guasti (quali cortocircuiti, saldatura dei contatti, ecc.).

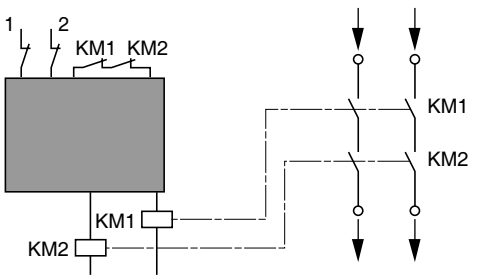
Il comportamento delle categorie in condizioni di guasto era definito nel modo seguente:
- Categoria B: non prevede misure per la sicurezza. Rappresenta la base per le altre categorie. Quando si verifica un guasto, questo può comportare una perdita della funzione di sicurezza.
- Categoria 1: Come per la categoria B anch'essa può portare ad una perdita della funzione di sicurezza ma con una più alta affidabilità.
- Categoria 2: La perdita della funzione di sicurezza è rilevata dal controllo. Il verificarsi di un guasto può comportare la perdita della funzione di sicurezza tra gli intervalli di controllo.



- Categoria 3: Quando si verifica un singolo guasto, la funzione di sicurezza viene sempre garantita. Alcuni ma non tutti gli errori vengono rilevati. Un accumulo di errori non rilevati può comportare la perdita della funzione di sicurezza.



- Categoria 4: La funzione di sicurezza viene sempre garantita anche in caso di uno o più guasti. I guasti vengono rilevati in tempo utile per prevenire la perdita della funzione di sicurezza.
Per monitorare le prestazioni della funzione di sicurezza si ricorre alla ridondanza e al controllo incrociato delle uscite.



> La Sicurezza Funzionale viene definita come **"parte della sicurezza della macchina e del suo sistema di controllo che dipende dal funzionamento corretto dello SRECS*, di altri sistemi con tecnologia relativa alla sicurezza e ad impianti esterni per la riduzione del rischio"**.

* SRECS (Sistema Elettrico di Controllo Relativo alla Sicurezza): Sistema elettrico di controllo di una macchina il cui gusto può produrre un immediato aumento del rischio.

Occorre inoltre ricordare che con "funzionamento corretto" si intende che il sistema deve eseguire correttamente una funzione di sicurezza: questo significa che **le funzioni devono essere scelte correttamente**. In passato si tendeva a scegliere sempre componenti con una categoria superiore specificata dalla norma EN 954-1 al posto di componenti di categoria inferiore, anche se questi ultimi potevano presentare funzioni più adatte allo scopo. Questo può essere imputabile all'erroneo concetto gerarchico delle categorie, ove ad esempio la categoria 3 veniva considerata sempre "migliore" rispetto alla categoria 2 e così via. Le norme relative alla sicurezza funzionale mirano ad incoraggiare i progettisti a focalizzarsi maggiormente sulle funzioni effettivamente necessarie a ridurre ogni singolo rischio, oltre che sui livelli prestazionali richiesti a ciascuna funzione, piuttosto che fare semplicemente affidamento su componenti specifici.

Quali norme sono applicabili alla funzione di sicurezza?

Attualmente la norma EN 954-1 può dirsi quasi superata, mentre le valide alternative disponibili cui fare riferimento sono la norma EN/IEC 62061 e EN/ISO 13849-1.

Entrambe le norme permettono una valutazione precisa delle prestazioni di ogni singola funzione e degli elementi di rischio, anche se in modo diverso.
In base alla norma EN/IEC 62061 si determina il livello di integrità della sicurezza richiesto (SIL) mentre sulla base della EN/ISO 13849-1 si calcola il Performance Level (PL).

In entrambi i casi l'architettura del circuito di controllo che realizza la funzione di sicurezza è un fattore, ma diversamente dalla EN 954-1 le nuove norme prendono in considerazione l'affidabilità dei componenti scelti.

EN/IEC 62061

È importante considerare nel dettaglio ogni singola funzione; la norma EN/IEC 62061 richiede la stesura di una specifica dei requisiti di sicurezza (Safety Requirements Specification o SRS). Questa comprende una specifica funzionale (cosa fa in dettaglio) ed una specifica dell'integrità della sicurezza che definisce la probabilità richiesta che una funzione venga eseguita nelle condizioni specificate.

Un esempio spesso utilizzato è "l'arresto della macchina all'apertura del riparo", che richiede naturalmente un'analisi più attenta e dettagliata, in primo luogo della specifica funzionale. Ad esempio, è possibile ottenere l'arresto della macchina togliendo l'alimentazione della bobina di un contattore o riducendo la velocità con un variatore di velocità? Occorre mantenere il riparo bloccato in posizione chiuso fino all'arresto del movimento pericoloso? Potrà essere necessario disattivare altri dispositivi a monte o a valle del circuito? Come sarà possibile rilevare l'apertura del riparo?

La specifica dell'integrità di sicurezza deve prendere in considerazione sia i guasti occasionali dei componenti hardware che i guasti sistematici. Questi ultimi sono quelli imputabili a cause specifiche e possono essere evitati solo eliminando la causa, generalmente apportando modifiche progettuali. In pratica la maggior parte dei guasti reali sono guasti di tipo sistematico risultanti da specifiche non corrette.

Parte integrante dei normali processi di progettazione, questa specifica deve guidare alla scelta delle corrette misure di progettazione; ad esempio ripari pesanti e non allineati possono provocare il danneggiamento degli interruttori di blocco se non si prevede l'installazione di appositi respingenti o dispositivi di assorbimento degli urti e di sistemi di allineamento, mentre i contattori dovranno essere dimensionati correttamente e protetti contro i sovraccarichi.

Con quale frequenza verrà aperta la protezione? Quali potranno essere le conseguenze di un guasto della funzione? Quali saranno le condizioni ambientali (temperatura, vibrazioni, umidità, ecc)?

Nella norma EN/IEC 62061 un requisito di integrità di sicurezza viene espresso con un valore limite di guasto prestabilito per la probabilità di guasto pericoloso all'ora di ogni funzione di controllo relativa alla sicurezza (SRCF). Questo può essere calcolato in base a dati attendibili per ciascun componente o sottosistema ed è correlato al SIL come mostrato dalla Tabella 3 della norma:

Livello di integrità della sicurezza (SIL)	Probabilità di guasto pericoloso per ora PFH_D
3	da $>10^{-8}$ a $<10^{-7}$
2	da $>10^{-7}$ a $<10^{-6}$
1	da $>10^{-6}$ a $<10^{-5}$

Tabella 1: Rapporto tra SIL e probabilità di guasto

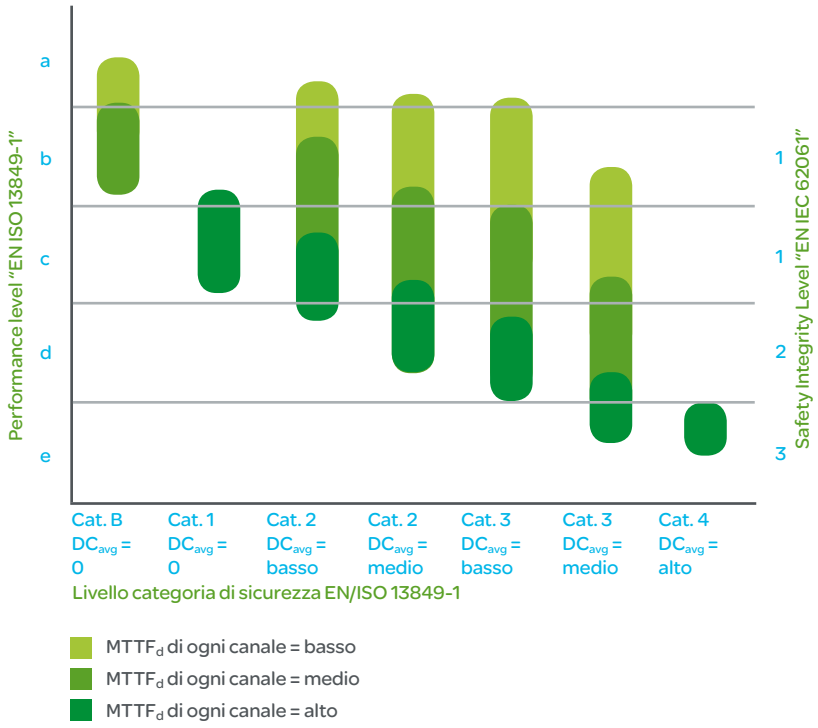
EN ISO 13849-1

La norma EN ISO 13849-1 utilizza una combinazione tra Tempo Medio dei Guasti Pericolosi ($MTTF_d$), Copertura Diagnostica (DC) e architettura (categoria) per determinare il Performance Level PL (a, b, c, d, e). La Tabella 7 della norma mostra un metodo semplificato di valutazione del PL. Le categorie sono le stesse della norma EN 954-1, come illustrato nell'Allegato 2.

Categoria	B	1	2	2	3	3	4
DC_{avg}	Nessuna	Nessuna	Basso	Medio	Basso	Medio	Alto
$MTTF_d$ di ogni canale							
Basso	a	Non rilev.	a	b	b	c	Non rilev.
Medio	b	Non rilev.	b	c	c	d	Non rilev.
Alto	Non rilev.	c	c	d	d	d	e

Tabella 2: Procedura semplificata di valutazione del PL eseguita dal SRP/CS

Dalla tabella sopra riportata si può vedere che per ottenere il PLe è necessario utilizzare un'architettura di categoria 4, ma è tuttavia possibile ottenere PL più bassi utilizzando categorie diverse in base alla combinazione di $MTTF_d$ e DC dei componenti utilizzati.



Indice	MTTFd
Basso	da >3 anni a <10 anni
Medio	da >10 anni a <30 anni
Alto	da >30 anni a <100 anni

Tabella 3: Livelli MTTFd

- Lo standard propone tre metodi per determinare il Tempo Medio prima di un guasto pericoloso ($MTTF_d$) di un componente:
  1. Dati del costruttore ($MTTF_d$, B10 o $B10_d$)
  2. Utilizzo degli Allegati C e D della EN/ISO 13849-1che forniscono i tassi di guasto dei componenti
  3. Uso di un valore di default di 10 anni.

- La copertura diagnostica (DC) rappresenta l'efficacia del monitoraggio dei guasti di un sistema o sottosistema. DC indica quanti sono, tra i possibili guasti pericolosi, quelli rilevati: è il rapporto tra il tasso di guasti pericolosi rilevati e il tasso totale dei guasti pericolosi. Il livello di sicurezza può essere migliorato in modo significativo con sottosistemi che effettuano l'autodiagnostica sui propri componenti interni.

Indice	Copertura diagnostica
Nessuno	<60%
Basso	da >60% a <90%
Medio	da >90% a <99%
Alto	>99%

Tabella 4: Livelli di Copertura Diagnostica

- I guasti per causa comune (CCF) si verificano quando una singola causa esterna (ad esempio un guasto) rende inutilizzabili un certo numero di componenti, indipendentemente dal Tempo medio dei guasti pericolosi MTTFd. Le azioni da adottare per ridurre il CCF comprendono:

  - Diversità dei componenti utilizzati e delle modalità di utilizzo
  - Prevenzione contro rischi ambientali
  - Separazione
  - Miglioramento della compatibilità elettromagnetica

Quale norma utilizzare?

A meno che una norma di tipo C specifichi un livello SIL o PL richiesto, il progettista è libero di utilizzare indifferentemente le specifiche dell norma EN/IEC 62061 o della norma EN/ISO 13849-1, o anche di altre normative. Sia la norma EN/IEC 62061 che la EN/ISO 13849-1 sono norme armonizzate che assicurano un'automatica presunzione di conformità ai requisiti Essenziali della Direttiva Macchine. Tuttavia occorre ricordare che qualsiasi norma venga scelta questa dovrà essere utilizzata integralmente e che non è possibile mischiare i requisiti di più norme in un unico sistema.

Attualmente è in corso uno studio che punta ad un' integrazione degli standard IEC e ISO per la redazione di un Allegato comune ad entrambi gli standard, con l'obiettivo finale di produrre eventualmente un'unica norma di riferimento.

La norma EN/IEC 62061 è forse più completa in materia di responsabilità relative alla specifica e alla gestione della sicurezza, mentre la EN/ISO 13849-1 è concepita in modo specifico per permettere una più facile transizione dalla EN 954-1.

Certificazione

Alcuni componenti sono forniti con certificazione ad uno specifico livello SIL o PL. Occorre tuttavia ricordare che tali certificazioni rappresentano solo un'indicazione del massimo livello SIL o PL ottenibile da un sistema che utilizza un determinato componente in una data configurazione, senza peraltro garantire che l'intero sistema soddisfi uno specifico livello SIL o PL.

Esempi pratici di applicazione

Forse il modo migliore per comprendere l'applicazione delle norme EN/IEC 62061 e EN/ISO 13849-1 è quello di fornire esempi pratici.

Per entrambe le norme utilizzeremo l'esempio di un'apertura della protezione con conseguente arresto delle parti mobili di una macchina, ove il mancato arresto potrebbe comportare la rottura di un braccio o l'amputazione di un dito dell'operatore.

Esempio pratico di applicazione della norma EN/IEC 62061

“Sicurezza del macchinario – Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza”

I sistemi di controllo elettrici di sicurezza delle macchine (SRECS) svolgono un ruolo chiave nell’assicurare la sicurezza totale delle macchine ed utilizzano sempre più spesso apparecchi elettronici complessi. Questa norma è rivolta in modo specifico al settore delle macchine e deriva della norma EN/IEC 61508.

Fornsice i requisiti per l’integrazione di sottosistemi realizzati in conformità con la norma EN/ISO 13849-1. Non specifica tuttavia i requisiti di funzionamento dei componenti non elettrici di controllo delle macchine (esempio: componenti idraulici, pneumatici).

Approccio funzionale alla sicurezza

Il procedimento parte dall’analisi dei rischi (EN/ISO 12100) per stabilire i requisiti di sicurezza. Una caratteristica specifica della norma EN/IEC 62061 è quella di spingere in prima istanza l’utilizzatore ad effettuare un’analisi dell’architettura necessaria a realizzare le funzioni di sicurezza, quindi a prendere in considerazione le sottofunzioni e ad analizzare le interazioni prima di procedere alla scelta di una soluzione hardware per il sistema di controllo elettrico di sicurezza della macchina (SRECS).

Per ogni progetto la norma richiede un Piano di sicurezza funzionale documentato che includa:

Lo sviluppo della specifica della funzione di comando di sicurezza (SRCF) divisa in due parti:

- Specifica dei requisiti funzionali con descrizione di funzioni e interfacce, modi operativi, priorità di funzionamento, frequenza di utilizzo, ecc.

- Specifica dei requisiti di integrità della sicurezza per ogni funzione, espressi in livelli di integrità della sicurezza (SIL o Livello di integrità della sicurezza).

- La Tabella 1 sotto riportata mostra le probabilità di guasto pericoloso per ogni livello SIL.

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

- Il processo di progettazione e documentazione del sistema di controllo elettrico di sicurezza della macchina (SRECS),

- Le procedure e risorse per la registrazione e l’aggiornamento delle informazioni,

- Il processo di gestione e modifica della configurazione, che tenga conto dell’organizzazione e del personale autorizzato,

- Il piano di verifica e validazione.

I vantaggi di questo approccio sono rappresentati dalla possibilità di offrire un metodo di calcolo comprendente tutti i parametri che possono influire sull'affidabilità dei sistemi di controllo. Il metodo consiste nell'assegnare un livello SIL ad ogni funzione, tenendo conto dei seguenti parametri:

- La probabilità di guasto pericoloso dei componenti (PFH_D),

- Il tipo di architettura (A, B, C o D), ovvero:
  con o senza ridondanza,
  con o senza funzioni di diagnostica che permettono il controllo di alcuni dei guasti pericolosi,

- Cause Comuni di Guasto (CCF), comprendenti:
  Cortocircuito tra i canali,
  Sovratensione,
  Interruzione dell'alimentazione, ecc.,

- Probabilità di trasmissione di errori pericolosi in caso di utilizzo di comunicazione digitale,

- Interferenze elettromagnetiche (EMC).

La procedura di progettazione di un sistema prevede cinque fasi successive alla realizzazione del piano di sicurezza funzionale:

1. In base alla valutazione del rischio assegnare un livello di integrità della sicurezza (SIL) e identificare la struttura base del sistema di controllo elettrico (SRECS), descrivendo inoltre ogni funzione di controllo relativa alla sicurezza (SRCF) ad esso correlata,

2. Scomporre ogni funzione di controllo relativa alla sicurezza (SRCF) in blocchi funzionali (FB)

3. Dettagliare le prescrizioni di sicurezza per ogni blocco funzionale, assegnando i blocchi funzionali ai sottosistemi dello SRECS,

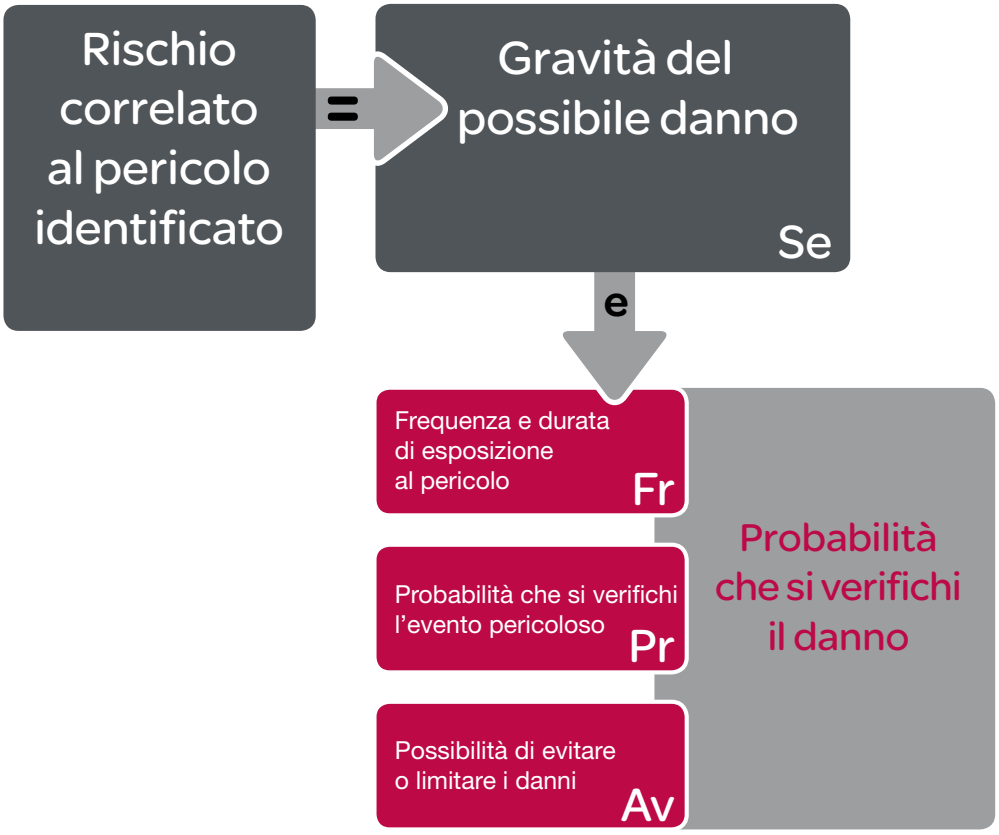
4. Selezionare il dispositivo per ciascun sottosistema,

5. Progettare le funzioni diagnostiche come prescritto e verificare il raggiungimento del livello di integrità (SIL) specificato.

Il nostro esempio prende in considerazione una funzione di interruzione dell'alimentazione di un motore successiva all'apertura di un riparo o protezione. Se la funzione fallisce si verifica la perdita dello stato sicuro con possibilità di infortunio grave dell'operatore (rottura del braccio o amputazione di un dito).

Fase 1 - Asssegnazione di un livello di integrità della sicurezza (SIL) e identificazione della struttura dello SRECS proposto

In base alla valutazione del rischio eseguita in conformità con la norma EN/ISO 12100, viene effettuata la stima del livello di integrità della sicurezza SIL richiesto per ogni funzione di controllo relativa alla sicurezza (SRCF), scomponendola successivamente in parametri, come mostrato dallo schema sottostante.



Gravità o severità Se

La gravità dei possibili danni o lesioni alla salute può essere valutata in base alle conseguenze della ferita che può essere leggera (di solito reversibile), seria (di solito irreversibile) o portare alla morte. La classificazione consigliata è indicata nella tabella sottostante:

Conseguenze	Gravità (Se)
Irreversibile: Morte, perdita di un occhio o di un braccio	4
Irreversibile: rottura di un arto, perdita delle dita	3
Reversibile: necessità di intervento medico	2
Reversibile: pronto soccorso	1

Probabilità di lesioni

Ciascuno dei tre parametri di rischio Fr, Pr, Av viene stimato separatamente basandosi sul caso più grave per ogni fattore. E' consigliabile effettuare un'analisi attenta della funzione per garantire che la stima della probabilità di lesione sia valutata in modo corretto.

Frequenza e durata di esposizione Fr

Il livello di esposizione al rischio è legato alla necessità di accedere alla zona pericolosa (funzionamento normale, manutenzione, ecc...) e alla modalità di accesso (alimentazione manuale, regolazione, ecc...). E' quindi possibile stimare la frequenza e durata media di esposizione. La classificazione consigliata è indicata nella tabella sottostante:

Frequenza di esposizione	Durata > 10 min
< 1 ora	5
> 1ora a < 1 giorno	5
> 1 giorno a < 2 settimane	4
> 2 settimane a < 1 anno	3
> 1 anno	2

Probabilità che si verifichi un evento pericoloso Pr

Occorre prendere in considerazione due concetti fondamentali:

la prevedibilità dei componenti pericolosi nelle diverse parti della macchina e nei diversi modi operativi (normale, manutenzione, ricerca e riparazione dei guasti), prestando particolare attenzione agli avviamenti inattesi;

comportamento delle persone che interagiscono con la macchina, quali tensioni psichiche (stress), fatica, inesperienza, ecc.

Probabilità che si verifichi un evento pericoloso	Probabilità (Pr)
Molto alta	5
Probabile	4
Possibile	3
Scarsa	2
Trascurabile	1

Probabilità di evitare o limitare il danno Av

Questo parametro è legato alla progettazione della macchina. Tiene conto del verificarsi improvviso dell'evento pericoloso, del tipo di rischio (taglio, temperatura, scossa elettrica), della possibilità di evitare fisicamente il pericolo e della possibilità per una persona di identificare un fenomeno pericoloso.

Probabilità di evitare o limitare il danno (AV)	
Impossibile	5
Scarsa	3
Probabile	1

Assegnazione del SIL:

La stima può essere effettuata servendosi della tabella sottostante.

Nel nostro esempio abbiamo un grado di severità (Se) 3 poichè esiste il rischio di amputazione di un dito; questo valore è indicato nella prima colonna della tabella. Successivamente occorre sommare tra loro tutti gli altri parametri per scegliere una delle classi (colonne verticali della tabella). In tal modo otterremo:

Fr = 5 accesso più volte al giorno
Pr = 4 evento pericoloso probabile
Av = 3 probabilità di evitare il danno quasi impossibile

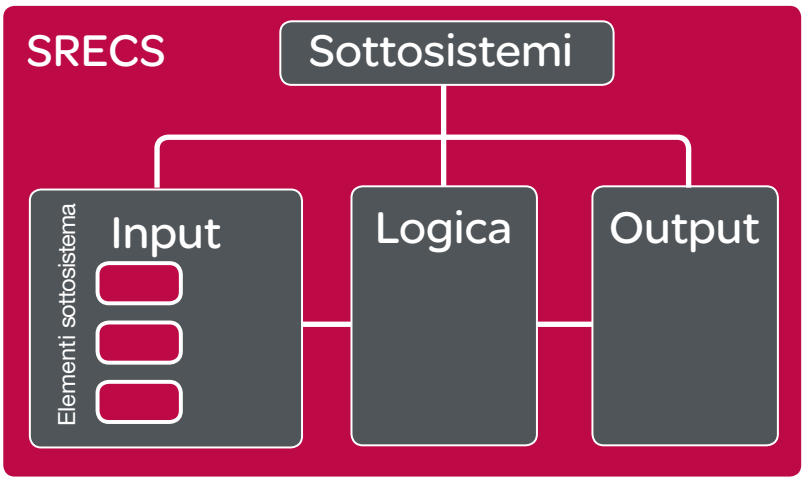
Di conseguenza avremo una classe **Cl = 5 + 4 + 3 = 12**

Il sistema elettrico di controllo relativo alla sicurezza (SRECS) della macchina deve realizzare questa funzione con un livello di integrità SIL 2.

Severità (Se)	Classe (Cl)				
	3-4	5-7	8-10	11-13	14-15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Struttura base del sistema di controllo SRECS

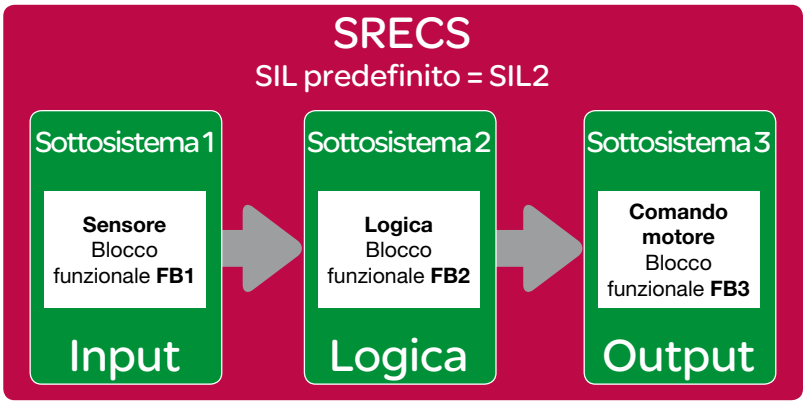
Prima di analizzare in dettaglio i componenti hardware da utilizzare il sistema viene suddiviso in due sottosistemi. In questo esempio sono necessari 3 sottosistemi per l'esecuzione delle funzioni di input, elaborazione e output. Lo schema sottostante mostra questa fase, indicando i termini esatti della normativa.



Fase 2 - Suddivisione di ogni funzione di sicurezza in blocchi funzionali (FB)

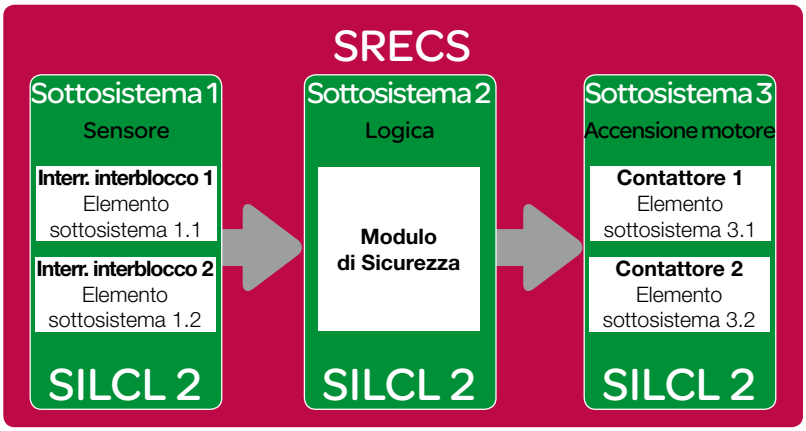
Un blocco funzionale (FB) è il risultato di una scomposizione dettagliata della funzione relativa alla sicurezza.

La struttura del blocco funzionale mostra il concetto iniziale dell'architettura dello SRECS.
I requisiti di sicurezza di ogni blocco derivano dalla specifica dei requisiti di sicurezza della funzione di controllo relativa alla sicurezza.



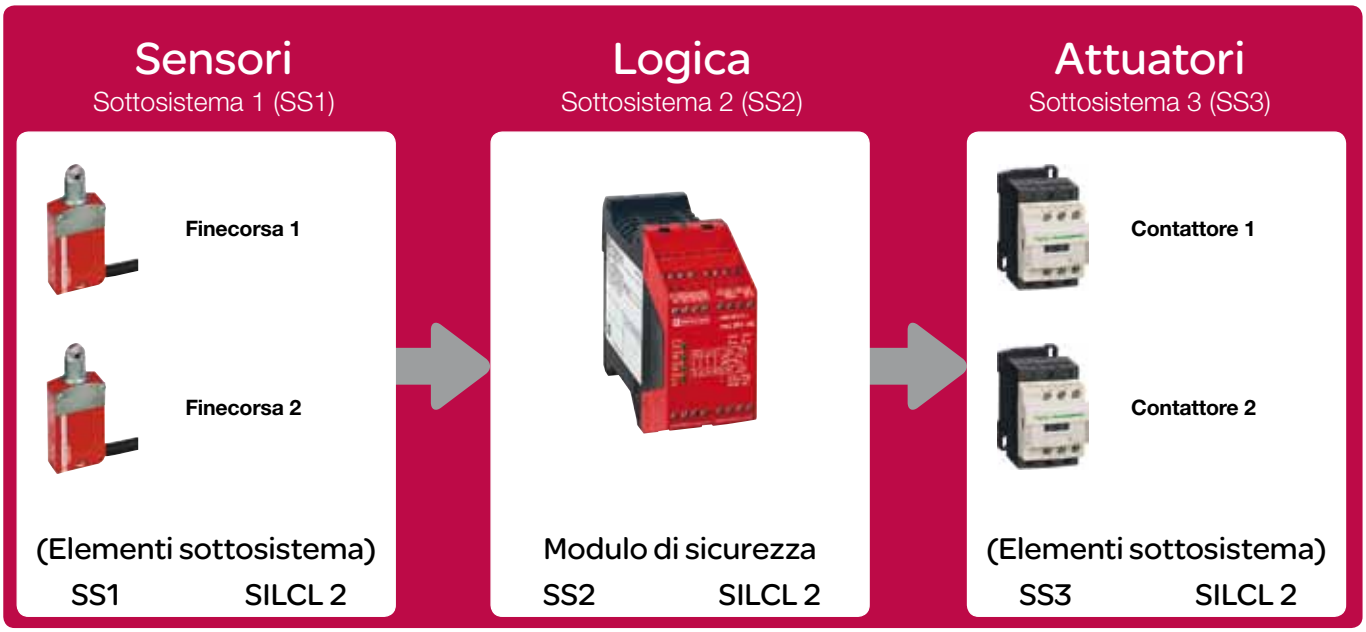
Fase 3 - Dettagliare le prescrizioni di sicurezza per ogni blocco funzionale ed assegnare i blocchi funzionali ai sottosistemi dell'architettura.

Ciascun blocco funzionale viene assegnato ad un sottosistema dell'architettura del sistema SRECS. La norma utilizza 'sottosistema' nel significato strettamente gerarchico del termine. Le parti che costituiscono un sottosistema si definiscono invece "elementi del sottosistema". Ovviamente, se un sottosistema si guasta si ha il mancato funzionamento della funzione di controllo relativa alla sicurezza. Ad ogni sottosistema è possibile assegnare più di un blocco funzionale. Ogni sottosistema può comprendere elementi del sottosistema e, se necessario, funzioni di diagnostica per assicurare che i guasti possano essere rilevati per consentire di intraprendere un'azione immediata corretta. Le funzioni di diagnostica sono considerate funzioni separate e possono essere elaborate dal sottosistema o da un altro sottosistema. I sottosistemi devono raggiungere almeno la stessa capacità SIL assegnata all'intera funzione di controllo relativa alla sicurezza (SRCF), ciascuna limitatamente al proprio SIL Claim Limit (SILCL). Nel nostro caso il SILCL di ciascun sottosistema deve essere 2.



Fase 4 - Selezionare i componenti di ciascun sottosistema

> Vengono scelti i prodotti mostrati qui di seguito.



Componente	Numero di manovre (B10)	% guasti pericolosi	Durata
Finecorsa XCS	10.000.000	20%	10 anni
Moduli di sicurezza XPS AK	$PFH_D = 7.389 \times 10^{-9}$		
Contattore TeSys LC1	1 000 000	73%	20 anni

L'affidabilità dei dati è garantita dal costruttore.

La durata del ciclo nel nostro esempio è di 450 secondi, il ciclo di azionamento **C** è di 8 manovre all'ora: la protezione verrà quindi aperta 8 volte all'ora.

Fase 5 - Progettare la funzione di diagnostica

Il SIL raggiunto dal sottosistema non dipende solamente dai componenti ma anche dall'architettura scelta. Nel nostro esempio sceglieremo architetture B per le uscite contattore e D per i finecorsa (Vedere Allegato 1 di questa Guida per la spiegazione delle architetture A, B, C e D).

In questa architettura il modulo logico di sicurezza esegue l'autodiagnostica e verifica anche i finecorsa. Vi sono tre sottosistemi per i quali determinare il SILCL (SIL Claim Limits) :

SS1: due finecorsa in un sottosistema con architettura di tipo D (ridondante);
SS2 di sicurezza: un modulo logico SILCL 3 (scelto in base ai dati, incluso il PFH_D, , forniti dal costruttore);
SS3: due contattori utilizzati in associazione con un'architettura tipo B (ridondante senza feedback)

Il calcolo tiene conto dei seguenti parametri:

B10: numero di cicli operativi dopo i quali il 10% dei dispositivi si sono guastati.
C: Ciclo di azionamento (numero di manovre all'ora).

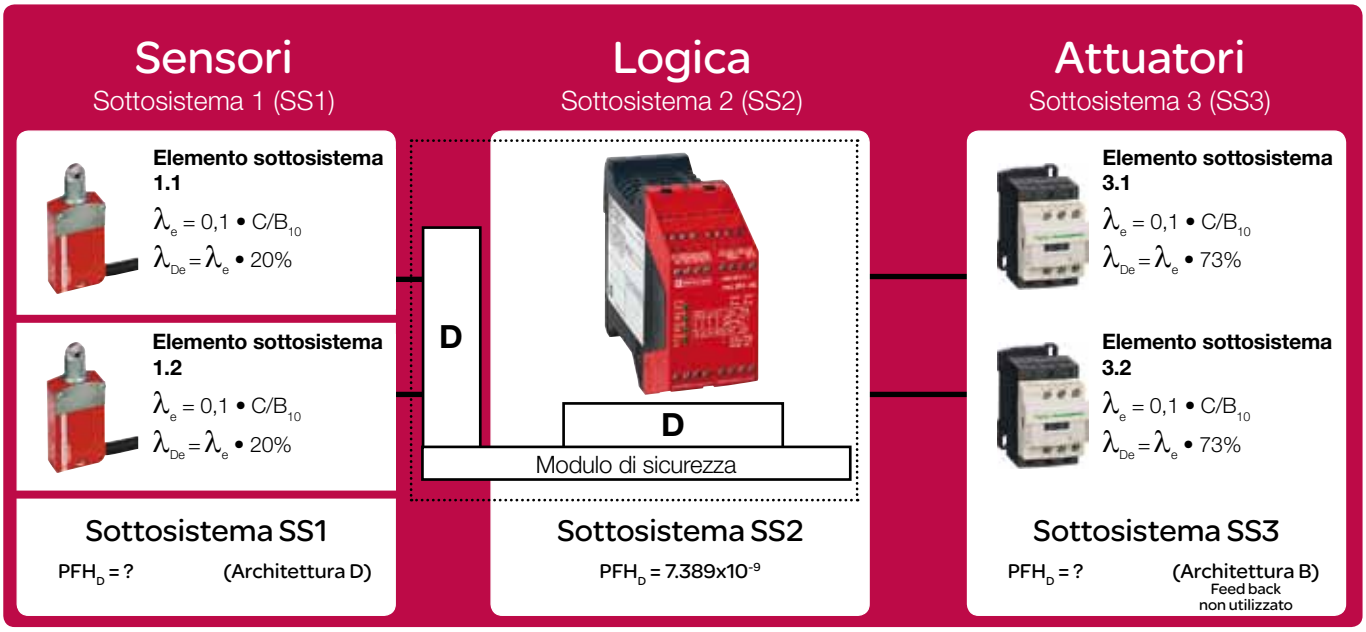
λ_D**:** percentuale di guasti pericolosi (λ = x tasso di guasti pericolosi).

β**:** Fattore di Causa Comune, vedere Allegato F della norma.

T1: Intervallo di verifica periodica o tempo di vita (il valore minore dei due specificato dal costruttore). La norma specifica che il progettista preveda una durata di 20 anni, per evitare l'utilizzo di intervalli di verifica funzionale periodica non realistici allo scopo di migliorare il SIL. Tuttavia riconosce che i componenti elettromeccanici possano richiedere una sostituzione al raggiungimento del numero di manovre specificato. Il valore utilizzato per T1 può quindi essere il tempo di vita indicato dal costruttore o, nel caso di componenti elettromeccanici, il valore $B10_D$ del dispositivo diviso per il ciclo di azionamento C.

T2: Intervallo delle prove diagnostiche.

DC: Copertura Diagnostica = λ_{DD} / λ_{Dtotal}, ovvero il rapporto tra il tasso di guasto pericoloso rilevabile e il tasso di guasto pericoloso totale.



Il tasso di guasto λ di un elemento del sottosistema elettromeccanico è definito con la formula λe = 0,1 x C / B10 , ove C rappresenta il numero di operazioni all'ora dell'applicazione e B10 è il numero previsto di cicli operativi dopo i quali il 10% dei dispositivi si sono guastati. In questo esempio considereremo C = 8 operazioni all'ora.

			SS1 controllo di 2 finecorsa	SS3 2 contattori senza diagnostica
Tasso di guasto per ciascun elemento λ_e	$\lambda_e = 0.1\ C/B_{10}$			
Tasso di guasto pericoloso per ciascun elemento λ_{De}	$\lambda_{De} = \lambda_e$ x probabilità di guasti pericolosi			
DC			99%	Non applicabile
Fattore di causa comune β			Si presume il caso peggiore del 10%	
T1 min (tempo di vita B10d/C)	$T1 = B_{10D}/C$		(10 000 000/20%)/8 = 87 600	(10 000 000/73%)/8 = 171 232
Intervallo prove diagnostiche T2			Ogni richiesta, ad es. 8 volte/ora, = 1/8 = 0.125 h	Non applicabile
Tasso di guasto pericoloso per ogni sottosistema	Formula per architettura B: $\lambda_{DssB} = (1-\beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$	Formula per architettura D $\lambda_{DssD} = (1-\beta)^2 \{[\lambda_{De2} \times {}^2 \times DC] \times T_2/2 + [\lambda_{De2} \times (1-DC)] \times T_1\} + \beta \times \lambda_{De}$		$\lambda_{DssB} = (1-0.9)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$

> Per quanto riguarda i contattori di uscita di un sottosistema SS3 occorre calcolare il PFH_d. Per un'architettura di tipo B (a prova di guasto singolo senza diagnostica) la probabilità di guasto pericoloso del sottosistema è:

$\lambda_{DssB} = (1 - \beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$
[Equazione B della norma]

$PFHDssB = \lambda_{DssB} \times 1h$

In questo esempio abbiamo $\beta = 0.1$
$\lambda_{De1} = \lambda_{De2} = 0.73\ (0.1 \times C / 1\ 000\ 000) = 0.73(0.8/1\ 000\ 000) = 5.84 \times 10^{-7}$
T1 = min(tempo di vita, $B10_D/C$) = min (175 200*, 171 232) = 171 232 ore
* Tempo di vita 20 anni min 175 200 ore

$\lambda_{DssB} = (1 - 0.1)^2 \times 5.84 \times 10^{-7} \times 5.84 \times 10^{-7} \times 171\ 232 + 0.1 \times ((5.84 \times 10^{-7}) + (5.84 \times 10^{-7}))/2$

$= 0.81 \times 5.84 \times 10^{-7} \times 5.84 \times 10^{-7} \times 171\ 232 + 0.1 \times 5.84 \times 10^{-7}$
$= 0.81 \times 3.41056 \times 10^{-13} \times 171\ 232 + 0.1 \times 5.84 \times 10^{-7}$
$= (3.453 \times 10^{-8}) + (5.84 \times 10^{-8}) = 1.06 \times 10^{-7}$
Dal momento che $PFH_{DssB} = \lambda_{DssB} \times 1h$, PFH_D per i contattori di un sottosistema SS3 = 1.06×10^{-7}

> Per i finecorsa di un sottosistema SS1 dobbiamo calcolare il PFH_D. Si sceglie un'architettura tipo D a prova di guasto singolo con funzione di diagnostica.
Questa architettura consente un singolo guasto di un elemento del sottosistema senza perdita della funzione di controllo relativa alla sicurezza (SRCF), ove

T_2 è l'intervallo prove diagnostiche;
T_1 è l'intervallo di verifica periodica o tempo di vita (il valore minore dei due).
β è il fattore di Causa Comune; $\lambda_D = \lambda_{DD} + \lambda_{DU}$; ove λ_{DD} è il tasso di guasti pericolosi rilevabili e λ_{DU} il tasso di guasti pericolosi non rilevabili.
$\lambda_{DD} = \lambda_D \times DC$
$\lambda_{DU} = \lambda_D \times (1 - DC)$
Per gli elementi del sottosistema di identica progettazione:
λ_{De} indica il tasso di guasto pericoloso dell'elemento del sottosistema;
DC è la Copertura Diagnostica dell'elemento del sottosistema.

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

D.2 della norma

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

λ_e= 0,1 •C / B10 = 0.1 x 8/10 000 000 = 8×10^{-8}

$\lambda_{De} = \lambda_e$ x 0.2 = 1.6×10^{-8}

DC = 99%

β = 10% (caso peggiore)

T_1 = min (tempo di vita, $B10_D$/C) = min[87600*,(10 000 000/20%)] = 87 600 ore

T_2 = 1/C = 1/8 = 0.125 hour

* Tempo di vita 10 anni min 87 600 ore

Da D.2:

$\lambda_{DssD} = (1 - 0.1)^2$ {[$1.6 \times 10^{-8} \times 1.6 \times 10^{-8} \times 2 \times 0.99$] x 0.125 /2 + [1.6 x 10-8 x 1.6×10^{-8} x (1 – 0.99)] x 87 600} + $0.1 \times 1.6 \times 10^{-8}$

= 0.81 x {[5.0688×10^{-16}] x 0.0625 + [2.56 x 10-16 x(0.01)] x 87 600} + 1.6×10^{-9}

= 0.81 x {3.168×10^{-17} + [2.56 x 10-18] x 87 600} + 1.6×10^{-9}

= $1.82\ 10^{-13}$

= 1.6×10^{-9}

Dal momento che $PFH_{DssD} = \lambda_{DssD}$ x 1h, il PFHD dei finecorsa di un sottosistema SS1 = 1.63×10^{-9}

Sappiamo già che per un sottosistema SS2, il PFH_D del blocco funzionale logico (implementato con il modulo di sicurezza XPSAK) è 7.389×10^{-9} (dati costruttore)
Il PFH_D totale del sistema di controllo con relè di sicurezza (SRECS) è la somma del PFH_D di tutti i blocchi funzionali, quindi:

$PFH_{DSRECS} = PFH_{DSS1} + PFH_{DSS2} + PFH_{DSS3}$ =
$1.6\ 10^{-9} + 7.389\ 10^{-9} + 1.06\ 10^{-7}$

= 1.15×10^{-7}, che, come indicato dalla tabella sottostante estratta dalla norma, è compreso entro i limiti di SIL 2.

Safety integrity level	Probabilità di guasto pericoloso all'ora PFH_D
3	da $>10^{-8}$ a $<10^{-7}$
2	da $>10^{-7}$ a $<10^{-6}$
1	da $>10^{-6}$ a $<10^{-5}$

Notare che se vengono utilizzati i contatti mirror dei contattori l'architettura della funzione di controllo diventerà di tipo D (ridondante con feedback) e il SIL claim limit passerà da SIL2 a SIL 3.

Questo implica un ulteriore riduzione della probabilità di rischio di guasto della funzione di sicurezza, in linea con il concetto di riduzione del rischio al livello più basso ragionevolmente praticabile.

Contattori TeSys LC1D con contatti mirror

Esempio pratico di applicazione della norma EN/ISO 13849-1

Sicurezza delle macchine – Componenti legati alla sicurezza dei sistemi di controllo" Parte 1: Principi generali di progettazione

- Come appena visto per la norma EN/IEC 62061, il procedimento prevede una successione di sei fasi logiche

FASE 1: Valutazione del rischio e identificazione delle funzioni di sicurezza necessarie.

FASE 2: Determinazione del Performance Level richiesto (PLr) per ciascuna funzione di sicurezza.

FASE 3: Identificazione della combinazione delle parti del controllo relative alla sicurezza che svolgono la funzione di sicurezza.

FASE 4: Valutazione del Performance Level PL di tutte le parti del controllo relative alla sicurezza.

FASE 5: Verifica che il PL del SRP/CS* per la funzione di sicurezza sia almeno pari al Performance Level richiesto PLr.

FASE 6: Confermare che siano soddisfatti tutti i requisiti (vedere EN/ISO 13849-2).

*Parti del sistema di controllo relativo alla sicurezza (ai sensi della norma EN ISO 13849-1).

Per maggiori dettagli fare riferimento all'Allegato 2 di questa Guida.

- FASE 1: Come per l'esempio precedente prendiamo in considerazione una funzione di sicurezza che comandi l'interruzione dell'alimentazione di un motore in seguito all'apertura di un riparo o protezione.

- FASE 2: Servendosi del "diagramma di rischio" della Figura A.1 della norma EN/ISO 13849-1 e degli stessi parametri dell'esempio precedente, il Performance Level richiesto sarà d
(attenzione: PL=d è spesso indicato come "equivalente" al livello SIL 2).

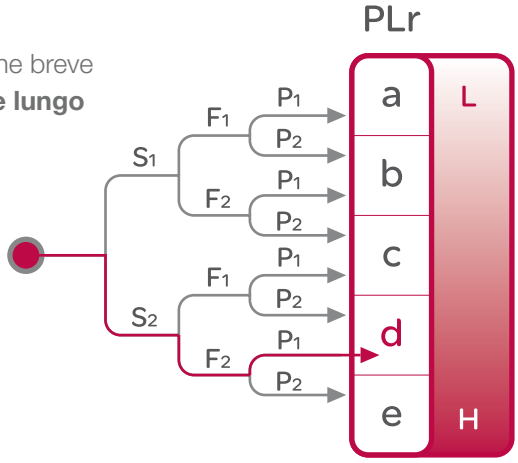
H = Alto contributo alla riduzione del rischio del sistrema di controllo

L = Basso contributo alla riduzione del rischio del sistrema di controllo

S = Gravità del danno o della lesione
S1 = Lesione leggera (generalmente reversibile)
S2 = Lesione seria (generalmente irreversibile, incluso il decesso)

F = Frequenza e/o tempo di esposizione al pericolo
F1 = raramente o poco frequente e/o tempo di esposizione breve
F2 = Frequente o continuo e/o tempo di esposizione lungo

P = Possibilità di evitare o limitare il danno
P1 = Possibile in alcune circostanze
P2 = Quasi impossibile



FASE 3: Prendiamo in considerazione la stessa architettura dell'esempio precedente relativo alla norma EN/IEC 62061, in altri termini un'architettura di categoria 3 senza feedback

FASE 4: Il PL delle parti del controllo relative alla sicurezza (SRP/CS) viene determinato valutando i seguenti parametri: (vedere Allegato 2):

- La CATEGORIA (struttura del sistema di sicurezza) (vedere clausola 6 dello standard EN/ISO 13849-1). In questo esempio l'utilizzo di un'architettura di categoria 3 indica che i contatti mirror dei contattori non vengono utilizzati.

- Il tempo medio prima di un guasto pericoloso $MTTF_d$ dei singoli componenti (vedere Allegati C e D della norma EN/ISO 13849-1)

- La Copertura Diagnostica (vedere Allegato E della norma EN/ISO 13849-1)

- Le Cause Comuni di Guasto (CCF) (vedere punteggio nell'Allegato F della EN/ISO 13849-1)

Il costruttore fornisce i seguenti dati relativi ai componenti:

Esempio di SRP/CS	B10 (operazioni)	$MTTF_d$ (anni)	DC
Finecorsa	10.000.000		99%
Modulo di sicurezza XPSAK		154.5	99%
Contattori	1.000.000		0%

Dal momento che il costruttore non può conoscere i dettagli dell'applicazione e in modo specifico il ciclo di azionamento (numero di operazioni) dei dispositivi elettromeccanici, potrà fornire solo il valore B10 o $B10_d$. Questo spiega il motivo per cui nessun costruttore è in grado di indicare un tempo medio prima di un guasto pericoloso (MTTFd) per un dispositivo elettromeccanico.

Il Tempo medio prima di un guasto pericoloso ($MTTF_d$) dei componenti può essere ricavato con la seguente formula:

$MTTF_d = B10d / (0.1 \times n_{op})$

Ove n_{op} rappresenta il numero medio di operazioni all'anno.

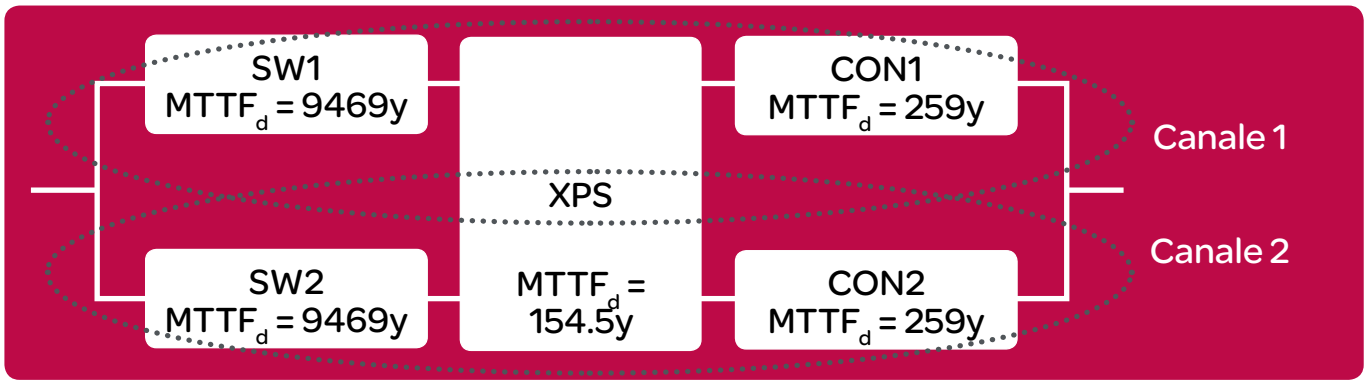
Il valore B10 è il numero di cicli operativi dopo i quali il 10% dei dispositivi si sono guastati. B10d è il numero di cicli operativi dopo i quali il 10% dei dispositivi hanno avuto guasti pericolosi. Senza conoscere in modo specifico il modo di utilizzo di un componente e quindi cosa può rappresentare un guasto pericoloso, la percentuale di guasto pericoloso di un finecorsa è del 20%, quindi $B10_d = B10/20\%$
Ammettendo che la macchina sia utilizzata per 8 ore al giorno, 220 giorni all'anno, con un tempo di ciclo di 120 secondi, il numero di manovre n_{op} sarà pari a 52800 operazioni/anno.

Supponendo che B10d = B10/20%, la tabella sarà:

Esempio di SRP/CS	B10 (operazioni)	B10d	MTTFd (anni)	DC
Finecorsa	10.000.000	50.000.000	9469	99%
Modulo di sicurezza XPSAK			154.5	99%
Contattori	1.000.000	1.369.863	259	0%

I valori $MTTF_d$ indicati in rosso sono ricavati dai dati applicativi utilizzando i dati relativi ai cicli di azionamento e al valore $B10_d$.

L' $MTTF_d$ può essere calcolato per ogni canale utilizzando il metodo di calcolo indicato nell'Allegato D della norma.



In questo esempio il calcolo sarà il medesimo per entrambi i canali 1 e 2:

$$\frac{1}{MTTFd} = \frac{1}{9469\ anni} + \frac{1}{154.5\ anni} + \frac{1}{259\ anni} = \frac{1}{95.85\ anni}$$

Il Tempo medio prima di un guasto pericoloso ($MTTF_d$) di ogni canale è quindi 85 anni, corrispondente ad un MTTFd "alto" in base alla Tabella 3

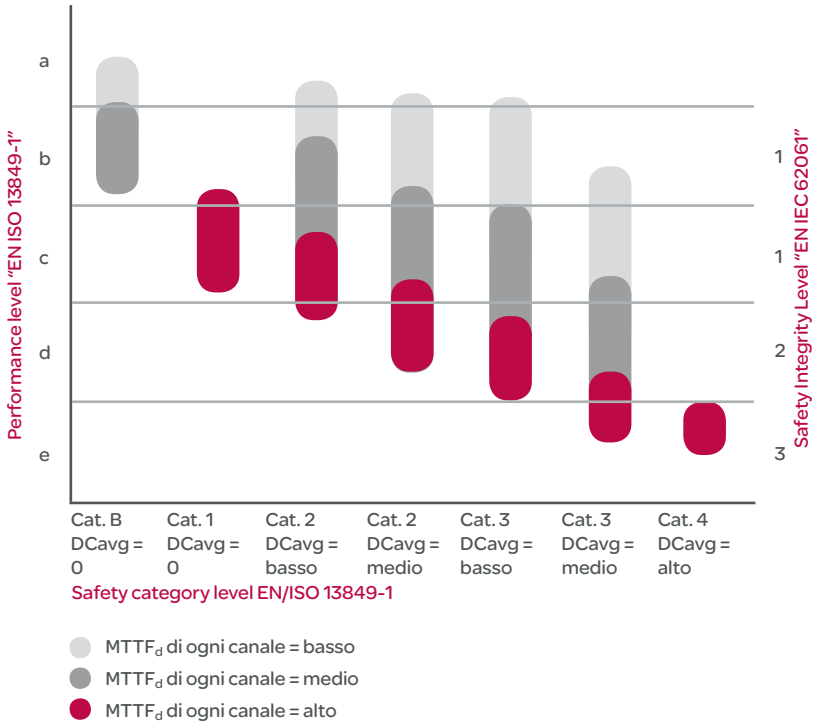
Dalle equazioni dell'Allegato E della norma è possibile stabilire che $DC_{avg} = 62.4\%$, ovvero un valore "basso" in base alla Tabella 4

FASE 5: Verificare che il PL del sistema sia conforme al Performance Level richiesto (PLr)

Poiché l'architettura utilizzata corrisponde alla categoria 3, e avendo un alto $MTTF_d$ e una bassa Copertura Diagnostica (DC_{avg}), possiamo rilevare dalla tabella sotto riportata (fig. 5 della norma) che PL=d, ovvero abbiamo soddisfatto il requisito previsto PL=d.

Proprio come per l'esempio pratico di applicazione della norma EN/IEC 62061, dipende solo dai contatti ausiliari mirror dei due contattori il passaggio dell'architettura in categoria 4. Questo porta il valore di DCavg a 99% , ovvero ad un parametro "alto" in base alla Tabella 4

Avendo un'architettura di categoria 4, un $MTTF_d$ alto ed un'alta copertura Diagnostica (DC_{avg}), dalla Tabella 7 della norma possiamo dedurre che il Performance Level risultante sarà PL=e, che soddisfa il requisito previsto PLr.



FASE 6: Validazione e controllo della realizzazione dei requisiti di sicurezza e pianificazione Test e verifiche ove necessario (EN/ISO 13849-2).

Fonti di informazione

Legislazione

- Direttiva Macchine 2006/42/EC
- EN/ISO 12100 Sicurezza del macchinario. Principi generali di progettazione
- EN/IEC 60204-1 Sicurezza del macchinario. Equipaggiamento elettrico delle macchine. Regole generali
- EN/IEC 13850 Sicurezza del macchinario. Arresti d'emergenza. Principi di progettazione
- EN/IEC 62061 Sicurezza del macchinario. Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza
- EN/IEC 61508 Sicurezza funzionale di sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza
- EN/ISO 13849-1 Sicurezza del macchinario. Parti dei sistemi di comando legate alla sicurezza.
  Parte 1: Principi generali di progettazione

Documenti Schneider Electric

- Catalogo: Soluzioni per applicazioni di sicurezza
- Sito Internet: www.schneider-electric.com

Allegati

Allegato 1

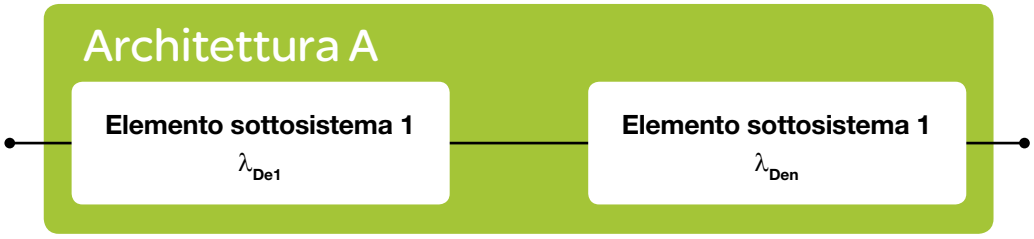
Architetture dei sottosistemi designate in conformità alla norma EN/IEC 62061

> Architettura Sottosistema A: zero tolleranza all'avaria senza funzione diagnostica

Dove: λ_{De} è il tasso di guasto pericoloso dell'elemento del sottosistema

$$\lambda_{DSSA} = \lambda_{DE1} + \ldots + \lambda_{Den}$$

$$PFH_{DSSA} = \lambda_{DSSA} \bullet 1h$$



Rappresentazione logica del sottosistema

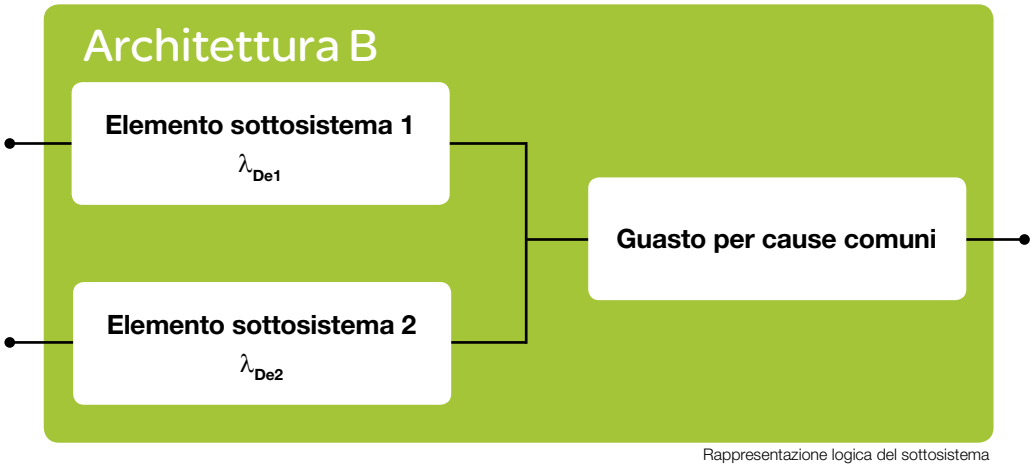
> Architettura Sottosistema B: singola tolleranza all'avaria senza funzione diagnostica

Dove: T_1 è l'intervallo di verifica periodica o tempo di vita (il minore tra i due)
(Fornito dal costruttore o calcolato per i componenti elettromeccanici con la formnula: $T_1 = B_{10}/C$)

β è il fattore di Causa Comune
(β viene determinato con la Tabella F.1 della norma EN/IEC 62061)

$$\lambda_{DSSB} = (1 - \beta)^2 \bullet \lambda_{De1} \bullet \lambda_{De2} \bullet T_1 + \beta \bullet (\lambda_{De1} + \lambda_{De2})/2$$

$$PFH_{DSSB} = \lambda_{DSSB} \bullet 1h$$



Rappresentazione logica del sottosistema

> Architettura Sottosistema C: zero tolleranza all'avaria con funzione diagnostica

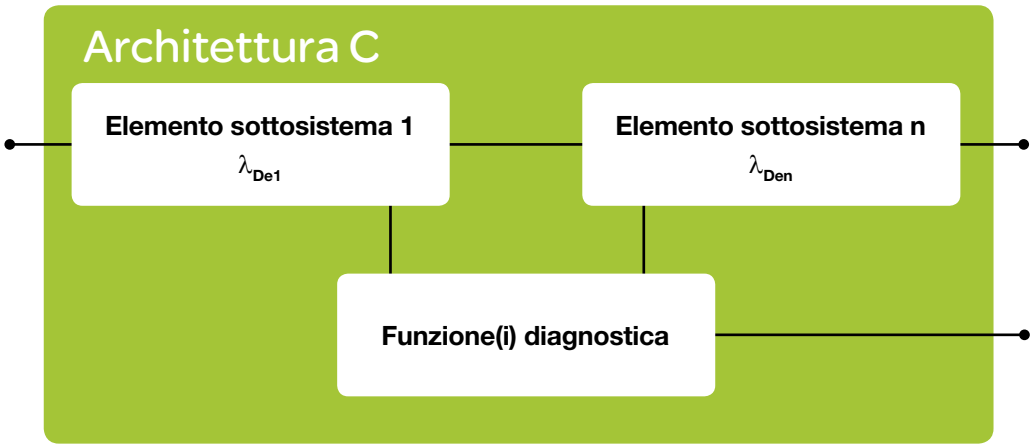
Dove: DC rappresenta la Copertura Diagnostica = $\Sigma \lambda_{DD}/\lambda_D$

λ_{DD} è il tasso di guasto pericoloso rilevato e λ_D è il tasso di guasto pericoloso totale

Il valore DC dipende dall'efficacia della funzione di diagnostica utilizzata dal sottosistema

$\lambda_{DSSC} = \lambda_{De1} \bullet (1 - DC_1) + ... + \lambda_{Den} \bullet (1 - DC_n)$

$PFH_{DSSC} = \lambda_{DSSC} \bullet 1h$



Rappresentazione logica del sottosistema

> Architettura Sottosistema D: singola tolleranza all'avaria con funzione diagnostica

Dove: T_1 è l'intervallo di verifica periodica o tempo di vita (il minore tra i due)

T_2 è l'intervallo prove diagnostiche

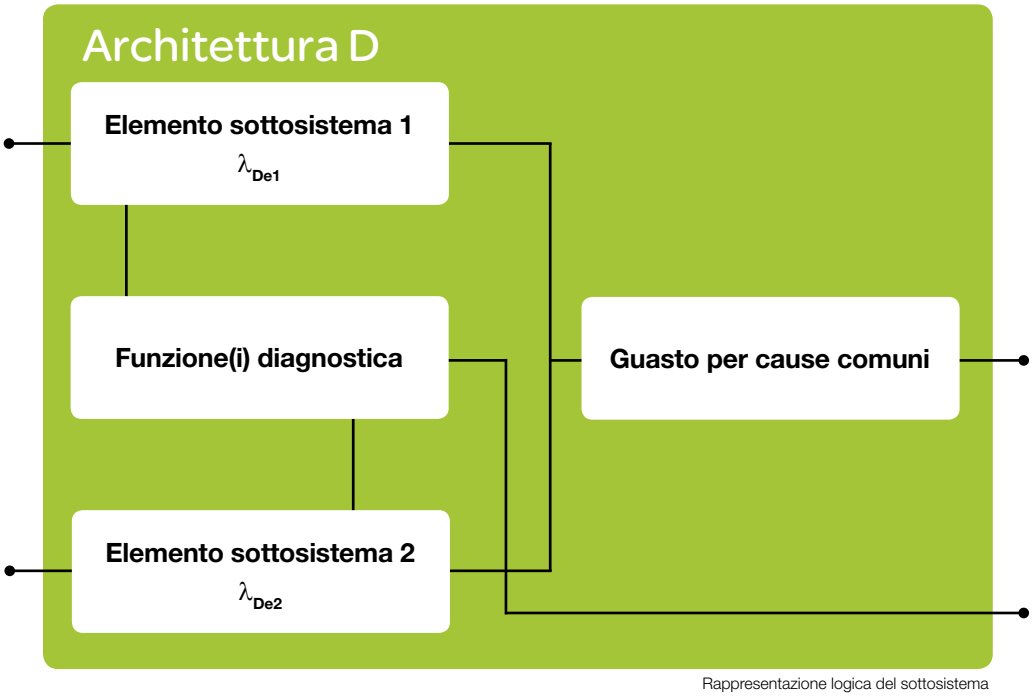
(Almeno equivalente all'intervallo di tempo tra i le richieste della funzione di sicurezza)

β è il fattore di Causa Comune

(determinabile con la tabella dell'Allegato F della norma EN/IEC 62061)

DC rappresenta la Copertura Diagnostica = $\Sigma \lambda_{DD}/\lambda_D$

(λ_{DD} è il tasso di guasto pericoloso rilevato e λ_D è il tasso di guasto pericoloso totale)



Rappresentazione logica del sottosistema

Per gli elementi del sottosistema di progettazione diversa

λ_{De1} = tasso di guasto pericoloso dell'elemento sottosistema 1; DC_1 = copertura diagnostica dell'elemento sottosistema 1

λ_{De2} = tasso di guasto pericoloso dell'elemento sottosistema 2; DC_2 = copertura diagnostica dell'elemento sottosistema 2

$$\lambda_{DSSD} = (1-\beta)^2 \{[\lambda_{De1} \bullet \lambda_{De2} (DC_1 + DC_2)] \bullet T_2/2 + [\lambda_{De1} \bullet \lambda_{De2} \bullet (2-DC_1-DC_2)] \bullet T_1/2\} + \beta \bullet (\lambda_{De1} + \lambda_{De2})/2$$

$$PFH_{DSSD} = \lambda_{DSSD} \bullet 1h$$

Per gli elementi del sottosistema di progettazione identica

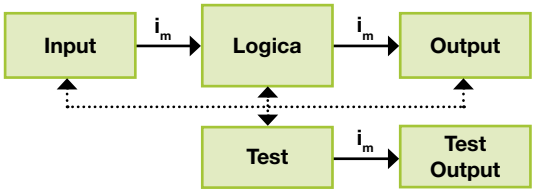
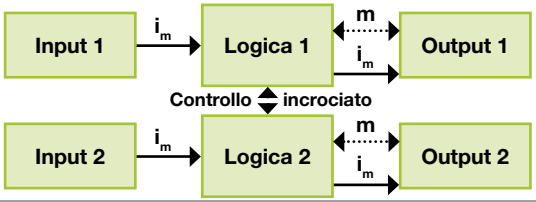
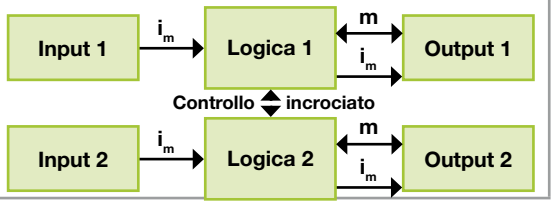
λ_{De} = tasso di guasto pericoloso dell'elemento sottosistema 1 o 2; DC = copertura diagnostica dell'elemento sottosistema 1 o 2

$$\lambda_{DSSD} = (1-\beta)^2 \{[\lambda_{De}^2 \bullet 2 \bullet DC] T_2/2 + [\lambda_{De}^2 \bullet (1-DC)] \bullet T_1\} + \beta \bullet \lambda_{De}$$

$$PFH_{DSSD} = \lambda_{DSSD} \bullet 1h$$

Allegato 2

Categorie della norma EN/ISO 13849-1

Categoria	Descrizione	Esempio
Categoria B	Un guasto può portare alla perdita della funzione di sicurezza.	
Categoria 1	Un guasto può portare alla perdita della funzione di sicurezza, ma l' $MTTF_d$ di ogni canale in Categoria 1 è più alto che nella Categoria B quindi la probabilità è inferiore rispetto a quest'ultima.	
Categoria 2	Un guasto può portare alla perdita della funzione di sicurezza tra un controllo e l'altro. La perdita della funzione di sicurezza è rilevata dal controllo.	
Categoria 3	Le parti relative alla sicurezza devono essere progettate in modo che un singolo guasto non porti alla perdita della funzione di sicurezza, il singolo guasto deve essere se possibile rilevato.	
Categoria 4	Le parti relative alla sicurezza devono essere progettate in modo che un singolo guasto non porti alla perdita della funzione di sicurezza e il guasto deve essere rilevato prima che uno successivo possa portare alla perdita della funzione di sicurezza. Se ciò non è possibile, l'accumulo di guasti non rilevati non deve portare alla perdita della funzione di sicurezza.	

Make the most of your energy℠

Schneider Electric S.p.A.
Sede Legale e Direzione Centrale
Via Circonvallazione Est, 1
24040 STEZZANO (BG)
www.schneider-electric.com

Supporto amministrativo
Tel. 011 4073333

Supporto tecnico
Tel. 011 2281203