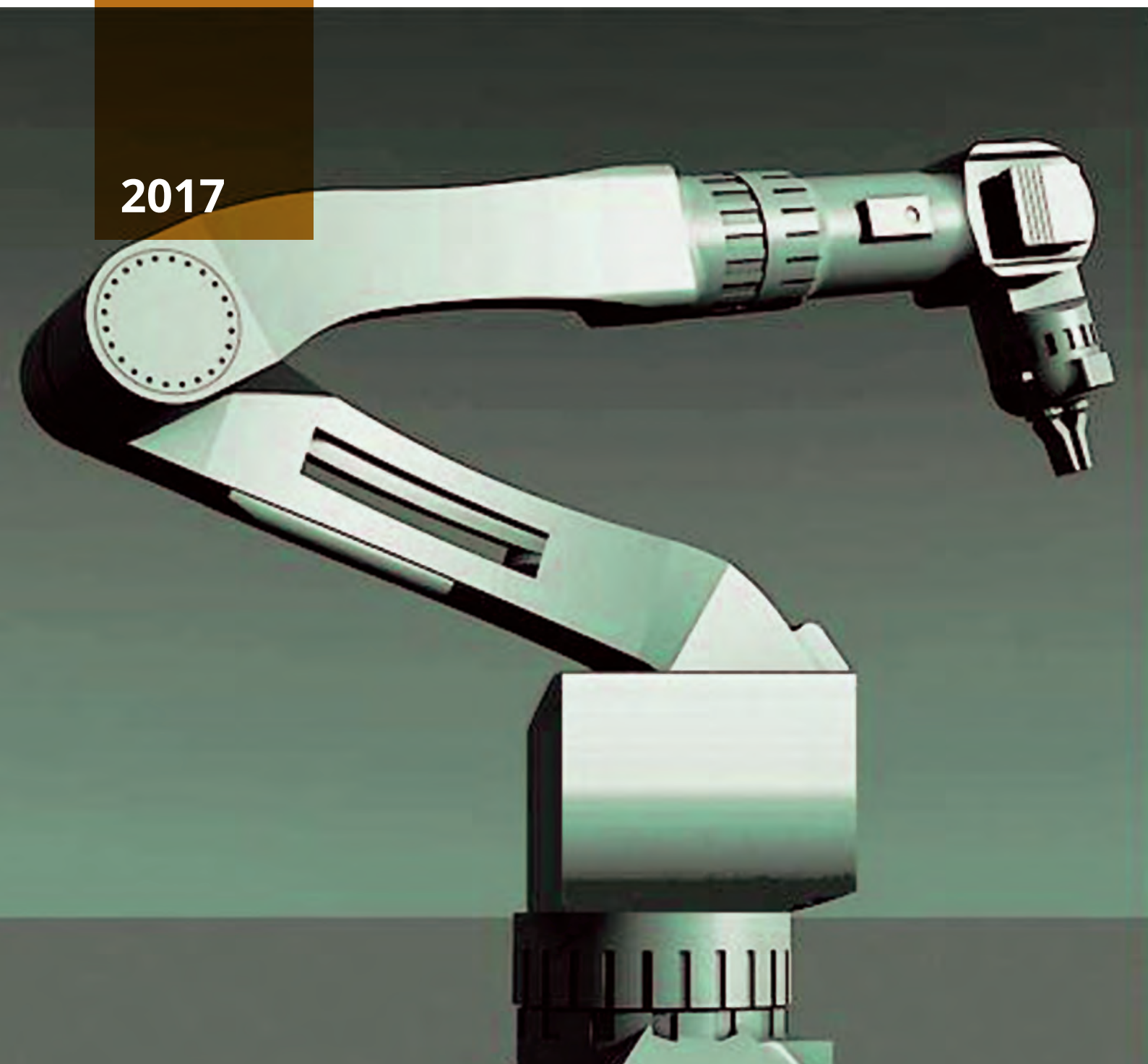
INAIL

I SISTEMI DI COMANDO DELLE MACCHINE SECONDO LE NORME EN ISO 13849-1 E EN ISO 13849-2

2017



INAIL

I SISTEMI DI COMANDO DELLE MACCHINE SECONDO LE NORME EN ISO 13849-1 E EN ISO 13849-2

2017

Pubblicazione realizzata da

Inail
Dipartimento innovazioni tecnologiche
e sicurezza degli impianti, prodotti e insediamenti antropici

Autori
Fabio Pera
Giovanni Luca Amicucci

Collaboratori
Laura di Lollo
David Ranieri

per informazioni
Inail
Dipartimento innovazioni tecnologiche
e sicurezza degli impianti, prodotti e insediamenti antropici
Via Roberto Ferruzzi n. 38/40 - 00143 Roma
dit@inail.it
www.inail.it

ISBN 978-88-7484-548-4

Tipolitografia Inail - Milano, aprile 2017

Prefazione

Secondo quanto definito dal Testo Unico sulla Sicurezza del lavoro (d.lgs. 81/08 e s.m.i.), è fatto obbligo al datore di lavoro di provvedere affinché le attrezzature di lavoro messe a disposizione dei lavoratori siano conformi alle specifiche disposizioni legislative e regolamentari di recepimento delle direttive comunitarie di prodotto a esse applicabili (d.lgs. 81/08, art. 70).
Tali attrezzature, che devono essere idonee ai fini della salute e sicurezza e adeguate al lavoro da svolgere o adattate a tali scopi, devono essere utilizzate conformemente alle disposizioni legislative di recepimento delle direttive comunitarie (d.lgs. 81/08, art. 71).

Le attrezzature di lavoro conformi alla Direttiva Macchine (2006/42/EC) devono soddisfare i requisiti di sicurezza di tale direttiva. Nell'Allegato I alla direttiva esiste un intero capitolo (1.2) relativo ai requisiti di sicurezza dei sistemi di comando delle macchine. In particolare:

"I sistemi di comando devono essere progettati e costruiti in modo da evitare l'insorgere di situazioni pericolose. In ogni caso essi devono essere progettati e costruiti in modo tale che:
- resistano alle previste sollecitazioni di servizio e agli influssi esterni,
- un'avaria nell'hardware o nel software del sistema di comando non crei situazioni pericolose,
- errori della logica del sistema di comando non creino situazioni pericolose,
- errori umani ragionevolmente prevedibili nelle manovre non creino situazioni pericolose […]"

(Requisito 1.2.1 – Sicurezza ed affidabilità dei sistemi di comando – All. I, direttiva 2006/42/EC)

La norma ISO 13849-1 fissa i criteri e i principi di progettazione dei sistemi di controllo delle macchine. Essendo armonizzata alla Direttiva Macchine, riveste interesse sia per i costruttori che per i comitati tecnici che si occupano di produrre norme di tipo B2 o di tipo C per la conformità ai requisiti essenziali di sicurezza dell'Allegato I alla Direttiva Macchine.
La ISO 13849-2 riguarda la validazione delle parti dei sistemi di controllo relative alla sicurezza, progettate secondo le procedure indicate nella parte 1 della norma stessa. Pertanto, contiene la metodologia, i criteri e gli strumenti per verificare se sono soddisfatti i requisiti specifici di sicurezza per la corretta progettazione contenuti nella parte 1.

L'Inail ha preso parte all'evoluzione della normativa e svolge attività di ricerca e di formazione sull'argomento.

Il presente lavoro è il risultato del monitoraggio, dell'analisi e del contributo portato nello sviluppo dei citati documenti e ha lo scopo di presentare:

- la norma ISO 13849-1, edizione 2015, contenente le modifiche effettuate nel processo di Amendment e, in particolare:
  - la procedura per la valutazione del livello di prestazione richiesto per la parte del sistema di controllo che implementa una data funzione di sicurezza derivante dall'applicazione del processo di riduzione del rischio;
  - la procedura per la valutazione del livello di prestazione sulla base di specifici parametri della parte del sistema di controllo relativa alla sicurezza;
  - le procedure per la valutazione dei parametri di interesse ($MTTF_D$ del canale, copertura diagnostica);
  - la procedura per stimare se eventuali guasti di causa comune siano al di sotto di una certa frazione massima dei guasti pericolosi;
  - le misure per limitare gli effetti dei guasti sistematici.
- La norma ISO 13849-2, edizione 2012, e, in particolare:
  - le procedure di validazione della funzione di sicurezza, delle Categorie, del PL, ecc.;
  - i principi base di sicurezza ed i principi di sicurezza ben provati.

Indice

1. La norma EN ISO 13849-1

1.1. Introduzione

Il progettista può scegliere di raggiungere una certa riduzione del rischio per una macchina adottando ripari e/o protezioni (*safeguards*) che utilizzano una o più funzioni di sicurezza.

La norma EN ISO 13849-1 definisce le parti di un sistema di controllo di una macchina che servono per realizzare le funzioni di sicurezza come *parti del sistema di controllo relative alla sicurezza* (S*afety-Related Parts of Control Systems* – SRP/CSs).
Tali parti possono essere integrate nel sistema di controllo della macchina o esserne separate. Oltre a realizzare le funzioni di sicurezza, tali parti possono essere utilizzate per realizzare funzioni operative.

L'abilità delle parti del sistema di controllo relative alla sicurezza di realizzare una data funzione di sicurezza sotto condizioni note è misurata con una scala a cinque livelli (*Performance Level* – PL). Tali livelli prestazionali sono definiti in termini di probabilità di guasti pericolosi per ora.

La probabilità che una SRP/CS abbia un malfunzionamento pericoloso dipende da molti fattori, incluse la struttura dell'hardware e del software, la capacità di rilevazione del dispositivo di diagnostica (*Diagnostic Coverage* – DC), l'affidabilità dei componenti (*Mean Time to Dangerous Failure* – MTTF), i malfunzionamenti di causa comune (*Common Cause Failure* – CCF), la progettazione, le sollecitazioni durante il funzionamento, le condizioni ambientali e le procedure lavorative.

Per aiutare il progettista e semplificare la valutazione del livello prestazionale (PL) raggiunto, la EN ISO 13849-1 usa un metodo basato sulle Categorie, ovvero su strutture/architetture del sistema di controllo determinate o meglio "designate", che utilizzano specifici criteri di progetto e hanno specifici comportamenti in caso di guasto.

Come già accennato la ISO 13849-1 stabilisce i requisiti per il progetto e la realizzazione dei sistemi di controllo relativi alla sicurezza delle macchine per tutte le tecnologie. Per la sola tecnologia elettrica ed elettronica programmabile lo stesso compito viene svolto dalla norma IEC 62061.
Possono essere progettati sistemi di controllo relativi alla sicurezza utilizzando una qualsiasi delle due norme, integrando tra loro SRP/CS o sottosistemi, per usare un termine equivalente (impiegato nella IEC 62061), non complessi, ove per non complesso si intende un qualcosa le cui modalità di guasto sono ben definite e il cui il comportamento in condizioni di avaria può essere definito completamente (una logica programmabile è un componente complesso).
Entrambe le norme possono essere utilizzate per integrare nei sistemi di controllo relativi alla sicurezza sottosistemi progettati in conformità alla IEC 61508, che è la norma generale dalla quale sono state derivate come applicazione per le macchine.

I metodi per determinare il SIL o il PL_r richiesto, contenuti negli Allegati A delle rispettive norme, presentano delle diversità anche se è emerso un buon livello di corrispondenza tra gli stessi in certi casi. Indipendentemente dal metodo utilizzato è importante prestare la dovuta attenzione alla valutazione appropriata dei parametri di rischio applicabili a una specifica funzione di sicurezza. Tale valutazione è svolta più efficacemente riunendo personale con competenze diverse (progettisti, manutentori, operatori) per accertare l'adeguata comprensione dei rischi presenti sulla macchina.

1.2. Scopo della norma

La EN ISO 13849-1 fornisce i requisiti di sicurezza e una guida alla progettazione e all'integrazione di parti del sistema di controllo relative alla sicurezza (SRP/CS), inclusa la progettazione del software. Per le SRP/CS sono specificate le caratteristiche e il livello di prestazione richiesto (PL_r) per realizzare la funzione di sicurezza. La norma si applica a tali parti indipendentemente dal tipo di tecnologia ed energia usati (elettrica, idraulica, pneumatica, meccanica) per qualsiasi livello di complessità.
Nella norma sono forniti i principi base, ma non sono descritte funzioni di sicurezza o livelli di prestazione per applicazioni specifiche, infatti è una norma di tipo B1.
La EN ISO 13849-1 si applica a SRP/CS con un'alta frequenza di domanda (*high demand*) o per un uso continuo (*continuous mode*).

1.3. Strategia per la riduzione del rischio

Al fine di riuscire a raggiungere gli obiettivi di sicurezza e quelli funzionali della macchina, è opportuno seguire una procedura strutturata e organizzata anche dal punto di vista gestionale per la progettazione.
Le SRP/CS devono essere progettate e costruite in modo da rispettare i principi della ISO 12100.
In base a tale norma deve essere messo in atto un processo iterativo per la valutazione del rischio e la sua riduzione, fino al raggiungimento di un livello di rischio adeguato (figura 1).
Questo processo iterativo deve essere eseguito separatamente per ogni pericolo, considerando tutte le possibili condizioni d'uso della macchina.

Una volta identificati i pericoli, la riduzione del rischio è ottenuta progettando adeguatamente le SRP/CS che devono realizzare le funzioni di sicurezza per ciascuno di essi (figura 2).
Tutti gli usi previsti e gli usi errati ragionevolmente prevedibili devono essere considerati.

Il progetto delle SRP/CS prevede all'interno della valutazione del rischio della macchina un sottoinsieme specifico di attività all'interno della procedura globale stessa, da svolgere al fine di ottenere la riduzione del rischio richiesta.

La strategia per la riduzione del rischio associato a una macchina deve coprire l'intero ciclo di vita della macchina ed è descritta in dettaglio nei punti 6.1, 6.2, 6.3 e 6.4 della ISO 12100.

Il processo di riduzione dei rischi richiede un'analisi dei pericoli che devono essere eliminati o ridotti per mezzo di una gerarchia di misure da adottare:
- eliminazione dei pericoli o riduzione del rischio per mezzo della progettazione (ISO 12100, punto 6.2: misure per la progettazione a sicurezza intrinseca);
- riduzione del rischio per mezzo di ripari, dispositivi di protezione o di misure di protezione complementari (ISO 12100, punto 6.3: ripari e misure di protezione complementari);
- riduzione del rischio realizzata fornendo informazioni sui rischi residui durante l'uso (ISO 12100, punto 6.4).

1.3.1. Specifiche delle funzioni di sicurezza

Quando si vanno a identificare le specifiche delle funzioni di sicurezza (cioè tutti i parametri qualitativi e quantitativi atti a definirle univocamente per l'applicazione definita) si devono considerare almeno i seguenti aspetti:
a) risultati della valutazione dei rischi per ogni pericolo o situazione pericolosa;
b) caratteristiche della macchina durante il funzionamento:
   - uso previsto della macchina e uso errato ragionevolmente prevedibile;
   - modi di funzionamento (ad es.: modo manuale, modo automatico, modo relativo a una parte della macchina);

  - tempo di ciclo;
  - tempo di risposta;

c) operazioni di emergenza;
d) descrizione dell'interazione tra i diversi processi di lavoro e le attività manuali (riparazione, impostazione, pulizia, risoluzione di problemi);
e) il comportamento della macchina che deve essere ottenuto o evitato per mezzo della funzione di sicurezza;
f) il comportamento della macchina a seguito di perdita dell'alimentazione (la SRP/CS deve continuare a fornire la funzione di sicurezza o inviare segnali ad altre parti in grado di portare e mantenere la macchina in uno stato sicuro; in alcune applicazioni potrebbe essere necessario duplicare le funzioni di sicurezza: una per quando la potenza è disponibile e una per quando non lo è);
g) le condizioni (durante ciascun modo di funzionamento) al verificarsi delle quali la macchina è in azione o disattivata;
h) la frequenza di funzionamento;
i) la priorità delle funzioni che possono essere attive contemporaneamente e che possono causare conflitti di funzionamento.

1.3.2. Contributo del sistema di controllo alla riduzione del rischio

La SRP/CS fornisce la funzione di sicurezza con un certo livello di prestazione (*Performance Level* – PL: un livello discreto utilizzato per specificare la capacità della SRP/CS di eseguire la funzione di sicurezza in condizioni determinate).
Durante il processo di valutazione del rischio il progettista stabilisce il contributo alla riduzione del rischio che deve essere fornito da ciascuna funzione di sicurezza realizzata dalla SRP/CS. Tale contributo non copre il rischio globale della macchina, ma solo quella parte di rischio che è ridotto dall'applicazione di quella particolare funzione di sicurezza.
L'entità del PL ottenuta permette il raggiungimento della riduzione del rischio richiesta.
La riduzione del rischio può essere ottenuta applicando misure di protezione differenti (realizzate utilizzando o non utilizzando SRP/CS) allo scopo di raggiungere una condizione di sicurezza.
Non c'è bisogno di applicare la riduzione del rischio a elementi di controllo che non sono SRP/CS o sono elementi puramente funzionali.
Per ogni funzione di sicurezza le caratteristiche e il livello di prestazione richiesto devono essere specificate e documentate nelle specifiche dei requisiti di sicurezza.

1.3.3. Livelli di prestazione

I livelli di prestazione (PL) sono cinque livelli (da "a" a "e"), definiti in termini di opportuni intervalli di probabilità oraria di malfunzionamento pericoloso "PFH_D" (tabella 1). Per raggiungere un certo livello è necessario soddisfare anche aspetti qualitativi (La funzione di sicurezza deve essere fornita per un intervallo noto di condizioni ambientali, i malfunzionamenti sistematici e quelli relativi al software devono essere evitati o controllati, il comportamento della funzione di sicurezza in caso di guasto deve essere noto e non compromettere la riduzione del rischio raggiunta).

TABELLA 1: LIVELLI DI PRESTAZIONE (PL) E LORO CORRISPONDENZA CON I LIVELLI DI INTEGRITÀ DI SICUREZZA (SIL)

PL	Probabilità oraria media di malfunzionamento pericoloso (PFH_D) [1/h]	SIL
a	$10^{-5} \leq PFH_D < 10^{-4}$	non applicabile
b	$3\times10^{-6} \leq PFH_D < 10^{-5}$	1
c	$10^{-6} \leq PFH_D < 3\times10^{-6}$	1
d	$10^{-7} \leq PFH_D < 10^{-6}$	2
e	$10^{-8} \leq PFH_D < 10^{-7}$	3

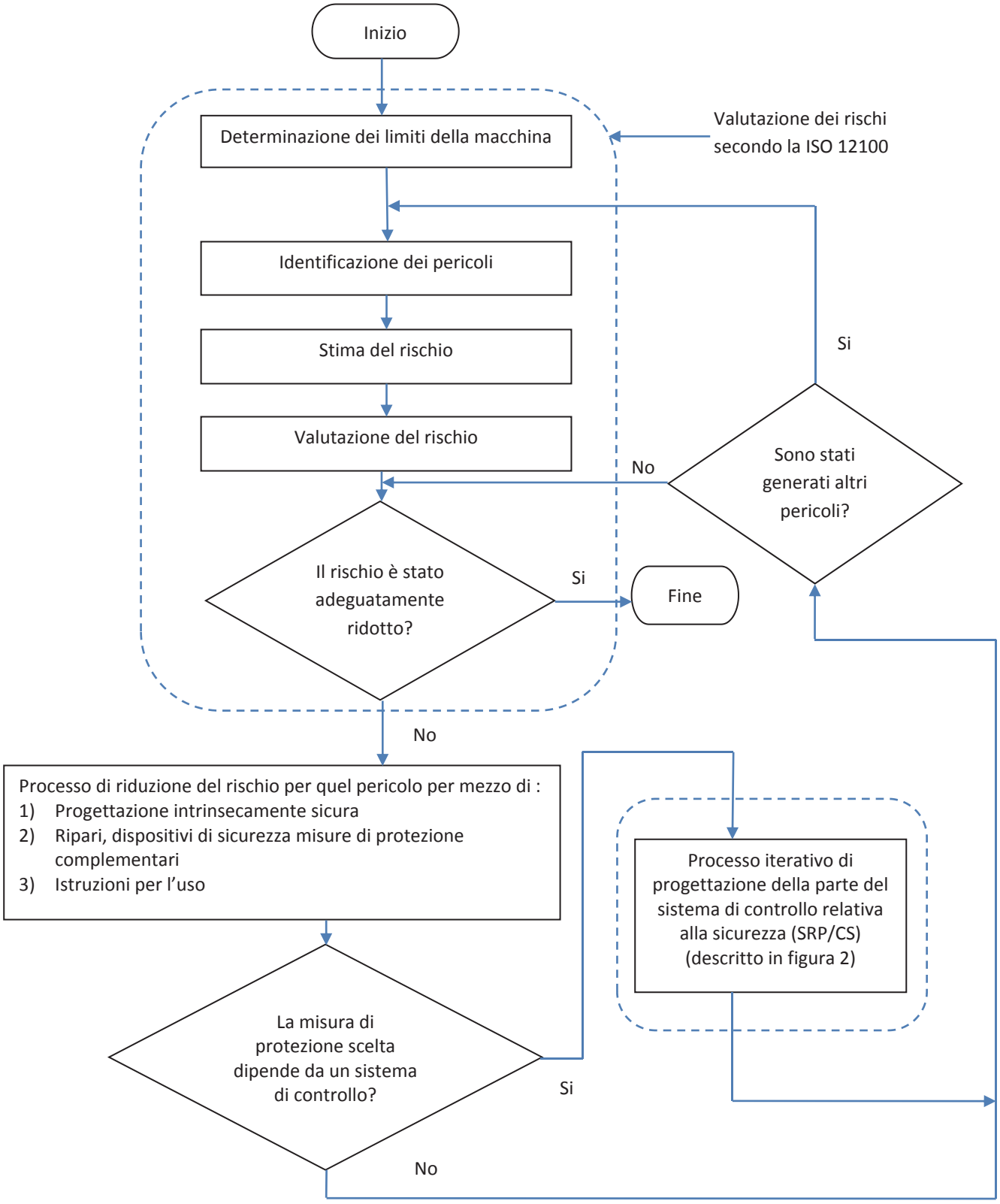


Fig. 1: Processo iterativo per la valutazione del rischio e la sua riduzione

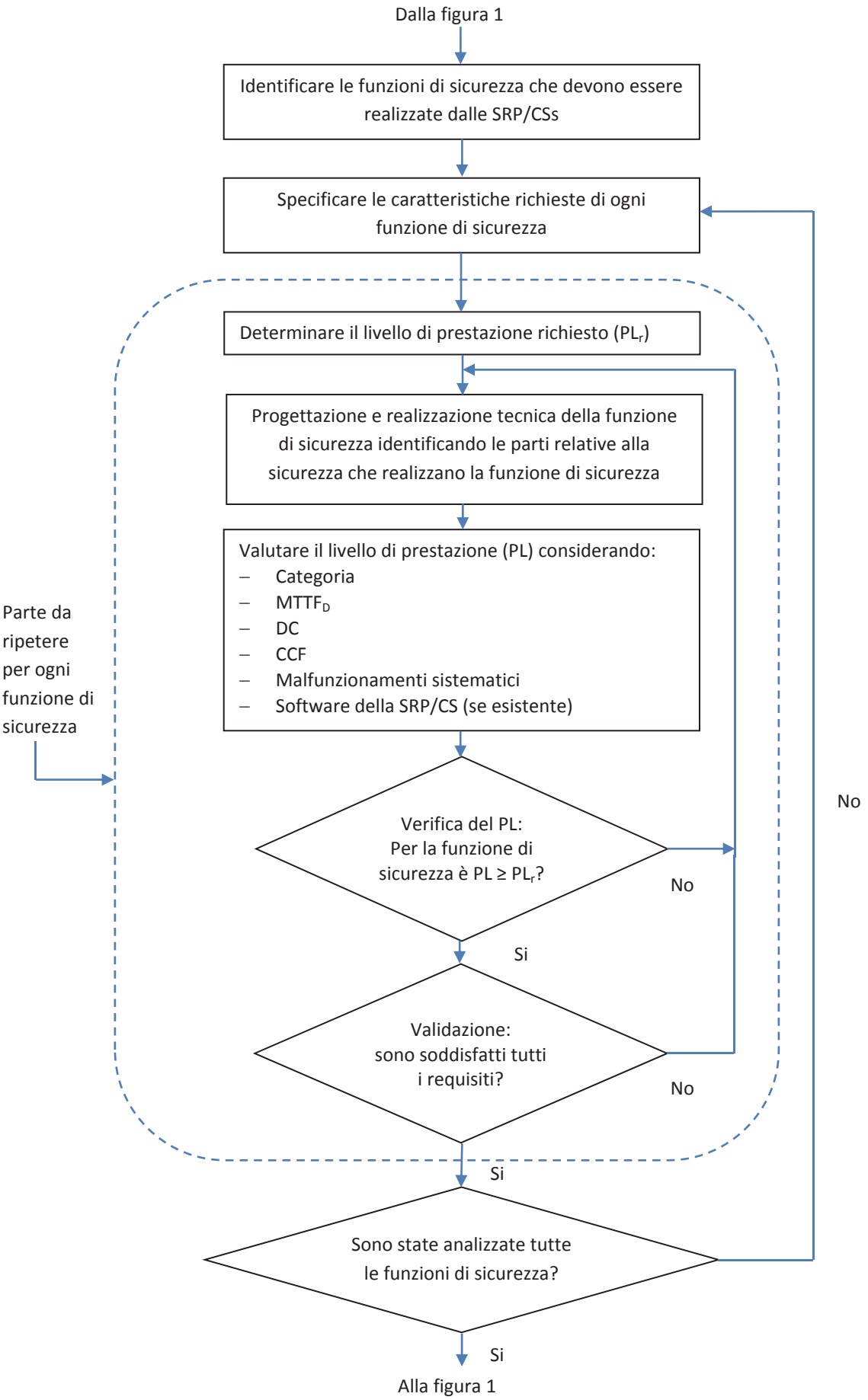


Fig. 2: Processo per la progettazione di una parte di sistema di controllo relativa alla sicurezza

1.4. Determinazione del livello di prestazione richiesto (PL_r)

Determinare le funzioni di sicurezza della macchina fa parte del processo di riduzione del rischio.
Una funzione di sicurezza può essere realizzata da una o più SRP/CS, e molte funzioni di sicurezza possono condividere una o più SRP/CS (ad esempio l'unità logica, le unità di alimentazione).
È anche possibile che una SRP/CS sia utilizzata per realizzare sia funzioni di sicurezza che funzioni di controllo ordinarie.
Il progettista può usare qualsiasi tecnologia disponibile, da sola o in combinazione con altre.
Per una data macchina è importante distinguere le differenti funzioni di sicurezza e le relative SRP/CS che realizzano tali funzioni.

Per ogni funzione di sicurezza che deve essere eseguita da una SRP/CS, deve essere determinato e documentato il livello di prestazione richiesto (*Required Performance Level* – PL_r: il livello di prestazione da realizzare per ottenere la riduzione del rischio richiesta per la funzione di sicurezza data).
Un metodo qualitativo per la determinazione del PL_r è contenuto nell'Allegato A della ISO 13849-1 (si veda al riguardo anche il paragrafo 1.4.1 seguente).
La determinazione del PL_r è il risultato di un processo di valutazione del rischio basato sui parametri derivati dalla ISO 12100 che tengono conto della severità del danno, della probabilità che si verifichi l'evento pericoloso, della frequenza e/o durata dell'esposizione al pericolo, della possibilità di evitare il rischio o di limitarne il danno.
Il valore di PL_r che si ottiene è legato al valore di riduzione del rischio che può essere raggiunto per mezzo della SRP/CS: maggiore è la riduzione del rischio che deve essere raggiunta dalla SRP/CS, maggiore sarà il PL_r.

1.4.1. Procedura euristica per la determinazione del livello di prestazione richiesto (PL_r)

Il metodo descritto nell'Allegato A della EN ISO 13849-1 per la stima del PL_r ha carattere informativo: è solo una guida per i progettisti e non è obbligatorio.
Per poter applicare efficacemente tale metodo di stima del PL_r è utile l'esperienza nel conoscere e trattare rischi o macchine simili.
Possono essere utilizzati altri metodi di stima studiati appositamente per macchine specifiche (ad esempio quelli che sono utilizzati nelle norme di tipo C), che potrebbero essere diversi da quello qui descritto.

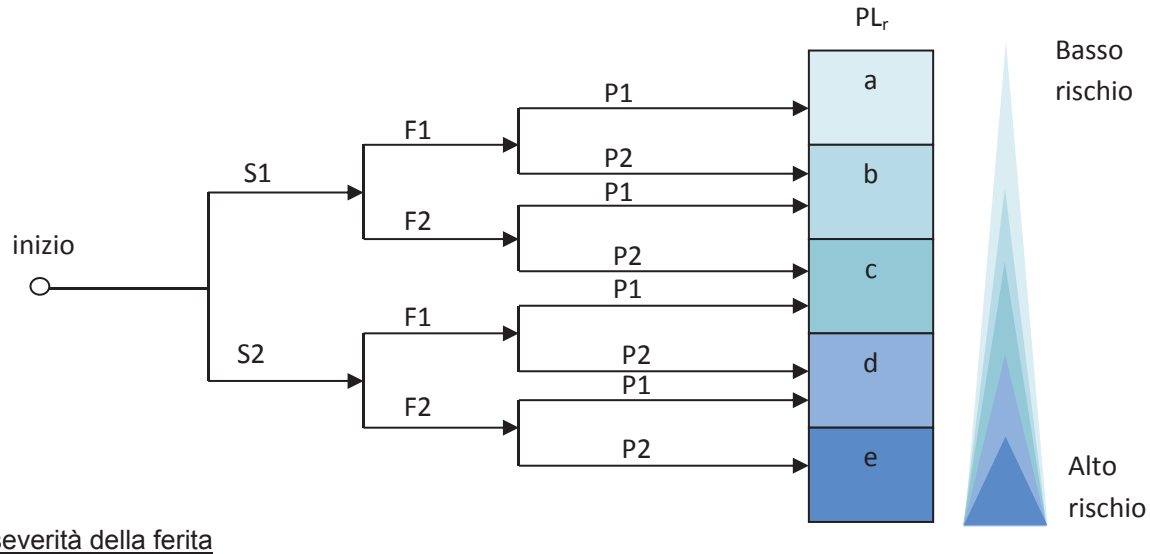
La figura 3 rappresenta la situazione prima dell'adozione della funzione di sicurezza.
Per la funzione di sicurezza considerata potrebbe essere necessario adottare preliminarmente misure per la riduzione del rischio indipendenti dal sistema di controllo (ad es. ripari) o funzioni di sicurezza addizionali, nel qual caso il punto di partenza della figura 3 comincia dopo l'adozione di tali misure.

Il metodo in oggetto assume che la probabilità di accadimento di un evento pericoloso sia del 100% (caso peggiore che può verificarsi).
Quando vi sia evidenza che la probabilità di accadimento dell'evento pericoloso non sia pari al 100% ma sia bassa, allora il PL_r che si ottiene dalla figura 3 può essere ridotto di un livello (si noti che tale eccezione deve essere basata sull'evidenza).

Nota 1: La probabilità di accadimento di un evento pericoloso dipende di solito dal comportamento umano o da un malfunzionamento delle funzioni di sicurezza. Nella maggior parte dei casi la probabilità è sconosciuta e difficile da valutare.
La stima di una tale probabilità dovrebbe essere basata sui seguenti elementi:
- le informazioni che si possiedono sull'affidabilità delle SRP/CS;
- lo storico degli incidenti che si sono verificati su macchine simili.

Nota 2: Un numero basso di incidenti non significa automaticamente che la probabilità di accadimento sia bassa, ma solo che le misure di sicurezza normalmente adottate su macchine simili sono sufficienti.

Nota 3: Le macchine da considerare simili sono le macchine:
- che presentano gli stessi rischi per la cui riduzione si stanno progettando le funzioni di sicurezza;
- che sono usate in processi lavorativi identici e con le medesime azioni da parte degli operatori;
- che applicano la stessa tecnologia che causa il pericolo.



S: severità della ferita
S1: lesione leggera (generalmente reversibile)
S2: lesione grave (generalmente irreversibile o morte)

F: frequenza e/o durata dell'esposizione al pericolo
F1: esposizione al pericolo da rara a infrequente e/o di breve durata
F2: esposizione al pericolo da frequente a continua e/o di lunga durata

P: possibilità di evitare il rischio o di limitarne il danno
P1: possibile evitare il pericolo o limitarne il danno, in condizioni specifiche
P2: scarsamente possibile evitare il pericolo o limitarne il danno

Fig. 3: Grafo per la determinazione del PL_r di una funzione di sicurezza

Il metodo descritto nella figura 3 si basa sulla stima di tre parametri:
- la severità della ferita (S) [che è solo stimata (ad es.: lacerazione, amputazione)],
- la frequenza e durata dell'esposizione al pericolo (F) e
- la possibilità di evitare il rischio o di limitarne il danno (P).

L'esperienza mostra che tali parametri possono essere combinati come nella figura 3, in modo da dare una scala di gradazione del rischio.

1.4.1.1. Severità del danno S1 e S2

Per stimare il rischio derivante dal malfunzionamento di una funzione di sicurezza è necessario capire se le lesioni che ne derivano sono leggere (generalmente reversibili) o gravi (generalmente irreversibili o mortali).
Per la corretta determinazione di S1 e S2 devono essere tenute in conto le conseguenze degli incidenti e i normali processi di guarigione (ad es.: lividi e lacerazioni senza complicazioni possono essere classificati come S1, mentre amputazioni o morte sono classificate come S2).

1.4.1.2. Frequenza e/o tempo di esposizione al pericolo F1 e F2

Il parametro F dovrebbe essere scelto valutando la frequenza e la durata dell'accesso al pericolo.
Un periodo di tempo che valga per la determinazione di F1 ed F2 non può essere specificato a priori ma dipende dall'applicazione. Comunque quando vi siano dubbi si può tener conto dei ragionamenti che seguono.
Quando la frequenza con cui è richiesta la funzione di sicurezza (che si assume essere superiore a una volta l'anno) è nota al progettista, si può utilizzare tale parametro al posto della frequenza e della durata dell'accesso al pericolo.
La durata dell'esposizione al rischio deve essere valutata sulla base del rapporto tra il tempo medio di utilizzo e il tempo totale di funzionamento della macchina.
F2 dovrebbe essere scelta se una persona è esposta al rischio frequentemente o in maniera continua. È irrilevante se a essere esposti al rischio sono una persona soltanto o persone diverse in tempi successivi (ad es. per l'uso di ascensori).
Se è necessario avvicinarsi regolarmente all'utensile di una macchina al termine di ogni ciclo di lavoro per caricare o movimentare il pezzo in lavorazione, allora dovrebbe essere scelta la frequenza F2.
Se non vi sono altre informazioni e la frequenza è più alta di una volta ogni 15 minuti, allora deve essere scelta la frequenza F2.
F1 può essere scelta se il tempo di esposizione cumulativo non supera 1/20 del tempo totale di funzionamento e la frequenza non è più alta di una volta ogni 15 minuti.

1.4.1.3. Possibilità di evitare l'evento pericoloso P1 e P2

Il parametro P è utilizzato per discriminare i casi in cui una situazione pericolosa può essere riconosciuta prima di aver causato danno ed essere evitata.
Quando si presenta la situazione pericolosa, se c'è una possibilità reale di evitare il rischio o di limitarne gli effetti, allora deve essere scelto P1, altrimenti deve essere scelto P2.
L'esposizione a un certo pericolo può essere identificata direttamente da alcune caratteristiche fisiche, oppure si può ricorrere, in casi specifici, a strumenti appositi in grado riconoscere tali caratteristiche fisiche.
Tra i fattori da considerare durante la scelta del parametro P vi sono:

- la velocità con cui il pericolo si presenta (velocemente o lentamente);
- la possibilità di evitare il pericolo (ad es.: allontanandosi);
- esperienze pratiche di sicurezza che possono essere applicate al processo lavorativo;
- l'addestramento e la capacità dell'operatore;
- la presenza o meno di supervisione durante il lavoro.

1.4.1.4. Pericoli che si sovrappongono

I pericoli devono essere identificati come pericoli specifici o situazioni pericolose, in modo che, per la quantificazione del rischio, il rischio che ogni pericolo comporta possa essere valutato separatamente.
Quando invece una serie di pericoli sono collegati, in modo tale che si presentano sempre in combinazione e simultaneamente, allora tali pericoli dovrebbero essere valutati insieme come una "*combinazione*".

1.5. Valutazione del livello di prestazione (PL) raggiunto e sua relazione con il SIL

Una volta identificate le funzioni di sicurezza del sistema di controllo, il progettista identifica le SRP/CS e valuta il livello di prestazione (PL).
Per ogni SRP/CS o combinazione di SRP/CS che realizzano una funzione di sicurezza si può stimare il PL utilizzando le seguenti informazioni:

a) Informazioni quantificabili:
   - l'$MTTF_D$ per ciascun componente (si veda il paragrafo 1.7 seguente);
   - la copertura diagnostica DC (si veda il paragrafo 1.8 seguente);
   - l'esistenza di malfunzionamenti di causa comune CCF (si veda il paragrafo 1.12 seguente);
   - la struttura del sistema (si veda il paragrafo 1.9 seguente);

b) Informazioni qualitative/non quantificabili che riguardano il comportamento della SRP/CS:
   - il comportamento della funzione di sicurezza in condizione di guasto (deve essere noto e non compromettere la riduzione del rischio raggiunta);
   - il software relativo alla sicurezza (si veda il capitolo 3 seguente);
   - i malfunzionamenti sistematici (si veda il paragrafo 1.13 seguente);
   - la capacità di continuare a realizzare la funzione di sicurezza in determinate condizioni ambientali.

Anche altri parametri possono avere una certa influenza e riguardano per esempio aspetti operativi, tasso di richiesta, tasso di prova.

Il rischio di malfunzionamenti della funzione di sicurezza può essere ridotto:
- abbassando la probabilità di guasti a livello di componente: infatti, allo scopo di ridurre la probabilità di malfunzionamento della funzione di sicurezza, si può incrementare l'affidabilità dei componenti, scegliendo componenti ben provati o applicando principi di sicurezza ben provati, in modo da minimizzare o escludere guasti critici;
- migliorando la struttura della SRP/CS: infatti, allo scopo di evitare gli effetti pericolosi di un guasto, si può ricorrere a una struttura ridondante che potrebbe servire a scoprire i malfunzionamenti e/o a fare in modo che questi non producano effetti dannosi.

Entrambe le misure possono essere adottate da sole o in combinazione.

Da quanto detto si comprende che la struttura della SRP/CS può contribuire notevolmente all'affidabilità del sistema, ad esempio è possibile, entro certi limiti, che una SRP/CS realizzata con un numero di canali ridondante (e pertanto resistente ai guasti) ma con componenti meno affidabili riesca ad avere lo stesso PL (o un PL più alto) di una SRP/CS realizzata a canale singolo con componenti altamente affidabili. Allo stesso modo l'impiego di diverse tecnologie in canali ridondanti può consentire una affidabilità maggiore.

Una volta note le informazioni quantitative e quelle qualitative, esistono metodi analitici per avere una stima degli aspetti quantificabili del PL di un sistema qualsiasi (anche se di struttura complessa), ad es. i modelli di Markov, le reti di Petri stocastiche generalizzate (GSPN) o i diagrammi a blocchi affidabilistici.

La norma EN ISO 13849-1, fornisce un metodo semplificato, basato sul modello di Markov, per rendere la valutazione degli aspetti quantificabili più semplice. Tale metodo (illustrato nel paragrafo 1.14 seguente) è basato sulla progettazione della struttura della SRP/CS in modo che sia riconducibile ad una tra cinque "architetture designate" (Categorie) che soddisfano specifici criteri di progetto e di comportamento in caso di guasto e sulla determinazione di parametri affidabilistici quantitativi che dipendono dal tipo di architettura scelto.

Per una SRP/CS progettata secondo i requisiti delle Categorie designate la probabilità media di un malfunzionamento pericoloso può essere stimata sulla base del metodo semplificato contenuto nella EN ISO 13849-1.

Per il raggiungimento degli aspetti quantitativi del PL è necessario evitare o fare in modo che i malfunzionamenti sistematici non diminuiscano il valore della riduzione del rischio, a tale scopo nella norma sono suggeriti degli accorgimenti da seguire (EN ISO 13849-1, Allegato G).

Inoltre, quando si utilizzano Categorie con più canali (Categorie 2, 3 e 4) occorre verificare che siano state adottate un numero sufficiente di misure (EN ISO 13849-1, Allegato F) per evitare che si possano presentare malfunzionamenti di modo comune (CCF).

Per ciascuna funzione di sicurezza, dopo aver stimato il PL complessivo delle SRP/CS che la realizzano, si deve confrontare tale valore con il PL_r individuato in fase di valutazione del rischio.
Per fare in modo che il valore del PL ottenuto non sia inferiore al PL_r, è necessario scegliere:

- un'architettura che permetta di raggiungere un PL adeguato, per mezzo di componenti ben provati o principi di sicurezza ben provati (Categorie B o 1), o
- un'architettura con maggiore ridonanza/copertura diagnostica per la SRP/CS (Categorie 2, 3 o 4).

Se la funzione di sicurezza è realizzata con più SRP/CS si può valutare il PL della combinazione con uno dei due metodi indicati nel paragrafo 1.10, condizione necessaria è che ciascuno dei PL delle diverse SRP/CS sia maggiore o uguale del PL_r complessivo che è stato individuato per la funzione di sicurezza.

Quando si deve realizzare una SRP/CS che devia dalle architetture delle Categorie non può essere applicato il metodo semplificato e deve essere effettuato un calcolo accurato per dimostrare il raggiungimento del livello di prestazione richiesto (PL_r).
Tuttavia, per applicazioni in cui la SRP/CS sia semplice e il livello di prestazione richiesto vada da "a" a "c", può essere sufficiente giustificare nel razionale del progetto la stima qualitativa del PL.

Nelle norme basate sulla IEC 61508, l'abilità di un sistema di controllo relativo alla sicurezza di realizzare una funzione di sicurezza è espressa in termini di SIL.
Non vi è una corrispondenza completa tra PL e SIL (si veda la tabella 1).
Il PL è utilizzabile per rischi di entità limitata (parte infatti da un intervallo di valori di probabilità oraria media di malfunzionamento pericoloso più basso dell'intervallo di valori valido per il SIL, in sostanza quello del PL "a"), mentre il SIL 4 è utilizzabile solo per rischi di entità catastrofica, come quelli che possono aversi nell'industria di processo.

Quando una funzione di sicurezza di un sistema di controllo è realizzata utilizzando una o più SRP/CS, allora ogni SRP/CS deve essere progettata utilizzando una sola norma (la EN ISO 13849-1, oppure la IEC 62061, oppure la IEC 61508), questo per evitare progettazioni inadeguate dovute a confusione dei requisiti.
Una volta progettate, ciascuna secondo un'unica norma, le SRP/CS, anche se conformi a norme diverse, possono essere integrate tra loro al fine di realizzare un'unica funzione di sicurezza.

1.6. Regole per la decomposizione a blocchi e per l'analisi del diagramma a blocchi relativo alla sicurezza

La EN ISO 13849-1 richiede una rappresentazione logica delle SRP/CS per mezzo di una decomposizione a blocchi. Tale decomposizione a blocchi è basata sulle seguenti regole:
- i blocchi rappresentano le unità della SRP/CS che servono all'esecuzione della funzione di sicurezza;
- canali diversi di una stessa funzione di sicurezza sono decomposti con blocchi diversi, in modo che se un blocco non è più in grado di funzionare, ciò non influenza l'esecuzione della funzione di sicurezza da parte dei blocchi dell'altro canale;
- ogni canale può essere decomposto in uno o più blocchi (non è necessario che vi siano almeno tre blocchi: ingresso, logica di controllo e uscita);
- ogni unità hardware della SRP/CS appartiene esattamente a un blocco, in modo da permettere di calcolare il $MTTF_D$ del blocco utilizzando i $MTTF_D$ degli elementi che formano quel blocco;
- le unità hardware usate per la diagnostica che, nel caso dovessero avere malfunzionamenti pericolosi, non hanno influenza sull'esecuzione della funzione di sicurezza da parte dei diversi canali, possono essere considerate separatamente rispetto alle unità dei diversi canali.

I blocchi ottenuti con la decomposizione a blocchi sono utilizzati per una rappresentazione logica della SRP/CS. Durante l'analisi di tale rappresentazione occorre ricordare che:
- il malfunzionamento di un blocco in una combinazione serie di blocchi può condurre al malfunzionamento del canale (infatti se una delle unità hardware del canale ha un guasto pericoloso l'intero canale potrebbe non essere più in grado di fornire la funzione di sicurezza);

- in una combinazione di canali in parallelo solo il guasto pericoloso di tutti i canali porta alla perdita della funzione di sicurezza (infatti una funzione di sicurezza eseguita in modo ridondante da più canali, continua a essere eseguita finché almeno uno dei canali continua a funzionare);
- i blocchi usati solo per la diagnostica, che non influenzano l'esecuzione della funzione di sicurezza quando hanno un guasto pericoloso, possono essere considerati separatamente dai blocchi dei canali.

1.7. Il tempo medio per un malfunzionamento pericoloso ($MTTF_D$) per un canale

Il valore del $MTTF_D$ per ciascun canale (di un sistema ridondante) può essere suddiviso in tre intervalli (si veda la tabella 2). Per ogni SRP/CS (o sottosistema) il valore massimo del $MTTF_D$ per ciascun canale è bloccato ("tagliato") a 100 anni: questo è stato previsto per creare un vincolo di struttura ed evitare che solo con l' $MTTF_D$ fosse possibile raggiungere elevati PL. Viceversa tale valore è incrementato a 2500 anni per la sola Categoria 4, in modo che sia ancora possibile raggiungere un PL pari a "e" mettendo in serie più di tre SRP/CS (o sottosistemi) di Categoria 4 con $MTTF_D$ elevato.

TABELLA 2: TEMPO MEDIO PER UN MALFUNZIONAMENTO PERICOLOSO ($MTTF_D$) PER UN CANALE

Denotazione del canale	Intervallo di valori per il canale
Basso	3 anni ≤$MTTF_D$ < 10 anni
Medio	10 anni ≤ $MTTF_D$ < 30 anni
Alto	30 anni ≤ $MTTF_D$ < 100 anni (2500 anni per la Categoria 4)
	I valori limite degli intervalli hanno un'accuratezza del 5%

La scelta del $MTTF_D$ per ciascun canale è basata sui tassi di guasto dei componenti disponibili allo stato dell'arte.
Valori di $MTTF_D$ inferiori a 3 anni non sono stati presi in considerazione, perché sono relativi a tassi di guasto superiori al 33%, ovvero se corrispondessero a componenti reali significherebbe che dopo un anno dalla messa in funzione più di un terzo di tali componenti avrebbe un malfunzionamento e dovrebbe essere sostituito.
Allo stesso modo un $MTTF_D$ per ciascun canale superiore a 100 anni (2500 anni per la Categoria 4) non è accettabile, perché significherebbe che la SRP/CS per alti rischi che utilizza quei componenti dipende solo dalla loro elevata affidabilità per realizzare la sua funzione.
Per rendere la SRP/CS resistente ai malfunzionamenti sistematici e a quelli casuali dovrebbero essere adottate altre misure, come la ridondanza e/o le prove.
Il limite di 100 anni (2500 anni per la Categoria 4) è relativo al canale nel suo insieme: i singoli componenti costituenti un canale possono avere valori più alti di $MTTF_D$.

Per stimare velocemente il $MTTF_D$ di un componente si può applicare la seguente procedura (i cui passi si succedono in ordine gerarchico):
a) il $MTTF_D$ è il valore fornito dal costruttore;
b) il $MTTF_D$ è il valore ottenuto coi metodi degli allegati C e D della EN ISO 13849-1;
c) il $MTTF_D$ è 10 anni.

1.7.1. Metodo semplificato del conteggio delle parti per la stima del $MTTF_D$ di un canale

Il metodo del conteggio delle parti serve a stimare il $MTTF_D$ di un canale.
Il metodo è basato sull'assunzione che il malfunzionamento pericoloso di un qualsiasi componente di un canale porti al malfunzionamento pericoloso di quel canale (caso peggiore).
Allo scopo di stimare il $MTTF_D$ del canale sono utilizzati i singoli $MTTF_{Di}$ degli *N* componenti di quel canale, per mezzo della seguente formula:

$$\frac{1}{\mathrm{MTTF_D}} = \sum_{i=1}^{N} \frac{1}{\mathrm{MTTF_{D}}i}$$

Tale formula è un'approssimazione che commette un errore sempre a favore della sicurezza (cioè fornisce un $MTTF_D$ più basso di quello effettivo).
Se è necessario ottenere valori più esatti, il progettista deve prendere in considerazione i modi di guasto del canale, ma ciò è più complicato.

1.7.2. Metodo per simmetrizzare il $MTTF_D$ di canali diversi

Nelle architetture designate delle Categorie 3 e 4, che hanno due canali ridondanti in parallelo, è fatta l'assunzione che il $MTTF_D$ dei due canali ridondanti sia lo stesso. Nella realtà, anche perché i due canali possono essere realizzati con tecnologie diverse, è più probabile che i due $MTTF_D$ differiscano tra loro.
Sono allora possibili due modi di procedere:
1) si prende in considerazione il $MTTF_D$ più basso tra i due (approssimazione del caso peggiore);
2) si prende in considerazione il valore del $MTTF_D$ dato dalla formula seguente:

$$\mathrm{MTTF_D} = \frac{2}{3}\left[\mathrm{MTTF_{D1}} + \mathrm{MTTF_{D2}} - \frac{1}{\frac{1}{\mathrm{MTTF_{D1}}} + \frac{1}{\mathrm{MTTF_{D2}}}}\right]$$

dove $MTTF_{D1}$ e $MTTF_{D2}$ sono i veri valori del $MTTF_D$ dei due canali ridondanti. Si ricordi che per le Categorie B, 1, 2, e 3 il $MTTF_D$ è limitato a 100 anni, mentre può arrivare fino a 2500 anni per la Categoria 4. Pertanto, prima di applicare la formula precedente, è bene effettuare la limitazione.

In pratica il secondo metodo consiste nel sostituire il sistema reale (con due $MTTF_D$ diversi in ogni canale) con un sistema fittizio con due canali dotati dello stesso identico $MTTF_D$ dato dalla formula sopra. Ciò è necessario per poter usare correttamente la figura 10 del presente documento.

1.8. Copertura diagnostica (DC)

La copertura diagnostica (DC) è definita come il rapporto tra il tasso di malfunzionamenti pericolosi rilevati e il tasso di malfunzionamenti pericolosi complessivo:

$$DC = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}}$$

dove
- λ_{DD} è il tasso di malfunzionamenti pericolosi rilevati,
- λ_{DU} è il tasso di malfunzionamenti pericolosi non rilevati,
- $\lambda_D = \lambda_{DD} + \lambda_{DU}$ è il tasso di malfunzionamenti pericolosi complessivo.

Il valore della DC può essere fatto rientrare in quattro diversi intervalli (si veda la tabella 3).

TABELLA 3: COPERTURA DIAGNOSTICA (DC)

Denotazione	Intervallo di valori
Nulla	DC<60 %
Bassa	60 % ≤DC<90 %
Media	90 % ≤ DC <99 %
Alta	99 % ≤ DC
	I valori limite degli intervalli hanno un'accuratezza del 5%

Per una stima della DC può essere usata la FMEA (*Failure Mode and Effects Analysis*) o metodi simili.
Tutti i guasti e/o i malfunzionamenti possibili devono essere considerati, tuttavia, quando si considerano le cause di malfunzionamenti di taluni componenti, è possibile escludere alcuni guasti (esclusione dei guasti: si veda in proposito il paragrafo 1.11 seguente).

Per calcoli semplificati, quando la SRP/CS consiste di più elementi o blocchi, si può considerare la DC_{avg}, definita come la media delle DC dei vari elementi o blocchi, che può essere stimata con la seguente formula:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \cdots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \cdots + \frac{1}{MTTF_{DN}}}$$

Nella sommatoria devono essere inclusi tutti i componenti della SRP/CS per cui non è possibile l'esclusione dei guasti (si veda il paragrafo 1.11 seguente). Devono essere utilizzati il $MTTF_{Di}$ e la DC_i di ogni elemento (i). La DC_{avg} della formula precedente rappresenta la media pesata delle DC_i rispetto all'inverso degli $MTTF_{Di}$ degli elementi della SRP/CS. Considerato che l'inverso dell'$MTTF_D$ di un componente rappresenta il suo tasso di guasto pericoloso, la DC_{avg} è il rapporto fra i tassi di guasto pericolosi rilevati e i tassi di guasto pericolosi complessivi per la SRP/CS. Pertanto la singola DC si riferisce al componente soggetto a diagnostica, non al dispositivo diagnostico. I componenti che non hanno rilevamento dei malfunzionamenti (e che quindi non possono essere sottoposti a diagnostica) hanno DC = 0 e contribuiscono solo al denominatore della DC_{avg}.

Nella tabella 3 la scelta degli intervalli della DC è basata sui valori 60%, 90%, 99% utilizzati anche in altre norme (ad es. IEC 61508) che fanno uso della copertura diagnostica.
Un valore di DC inferiore al 60% ha un effetto marginale sull'affidabilità del sistema in prova, per tale motivo un sistema con una tale copertura è denotato come avente "nessuna" copertura.
Viceversa un valore di DC superiore al 99% per sistemi complessi è molto arduo da raggiungere.
Nelle tabelle dalla 4.a alla 4.c è possibile trovare esempi di stime di copertura diagnostica presi dalla ISO 13849-1, Allegato E.

TABELLA 4.a: STIME DI COPERTURE DIAGNOSTICHE DI DISPOSITIVI DI INGRESSO

Misura	**DC**
Prova ciclica avviata dalla variazione dinamica del segnale d'ingresso	90%
Prova di plausibilità (uso di contatti connessi meccanicamente, normalmente chiusi e aperti)	99%
Monitoraggio incrociato degli ingressi senza prova dinamica	da 0% a 99% a seconda di quanto spesso l'applicazione produce una variazione di segnale
Monitoraggio incrociato degli ingressi con prova dinamica quando i cortocircuiti non sono rilevabili (I/O multipli)	90%
Monitoraggio incrociato degli ingressi e risultati intermedi della logica di controllo (L), e monitoraggio software (temporale e logico) del flusso del programma e rilevamento dei guasti statici e dei cortocircuiti (I/O multipli)	99%
Monitoraggio indiretto (ad es.: monitoraggio con interruttori di pressione, monitoraggio elettrico del posizionamento degli attuatori)	da 0% a 99% a seconda dell'applicazione
Monitoraggio diretto (ad es.: monitoraggio elettrico del posizionamento delle valvole di controllo, monitoraggio dei dispositivi elettromeccanici per mezzo di contatti connessi meccanicamente)	99%

TABELLA 4.a: STIME DI COPERTURE DIAGNOSTICHE DI DISPOSITIVI DI INGRESSO (PROSECUZIONE)

Misura	DC
Rilevamento dei guasti a partire dal processo	da 0% a 99% a seconda dell'applicazione (la misura da sola non è sufficiente se PL_r = "e")
Monitoraggio di alcune caratteristiche del sensore (ed es.: tempo di risposta, intervallo di variazione di parametri elettrici caratteristici, quali resistenza, capacità, ecc.)	60%

TABELLA 4.b: STIME DI COPERTURE DIAGNOSTICHE DI LOGICHE DI CONTROLLO

Misura	DC
Monitoraggio indiretto (ad es.: monitoraggio con interruttori di pressione, monitoraggio elettrico del posizionamento degli attuatori)	da 0% a 99% a seconda dell'applicazione
Monitoraggio diretto (ad es.: monitoraggio elettrico del posizionamento delle valvole di controllo, monitoraggio dei dispositivi elettromeccanici per mezzo di contatti connessi meccanicamente)	99%
Semplice monitoraggio temporale della logica di controllo (timer usato come watchdog, con i punti di trigger all'interno del programma della logica di controllo)	60%
Monitoraggio temporale e logico della logica di controllo con watchdog, il dispositivo di prova controlla la plausibilità del comportamento della logica di controllo	90%
Autotest all'avvio per individuare guasti latenti della logica di controllo (ad es.: nella memoria del programma e in quella dei dati, nelle porte di I/O, nelle interfacce)	90% (a seconda della tecnica usata per la prova)
Prova della capacità di reazione del dispositivo di monitoraggio (watchdog) da parte del canale principale, all'avvio o quando è richiesta la funzione di sicurezza o quando un segnale esterno lo richiede	90%
Principio dinamico (tutti i componenti della logica di controllo cambiano stato, ON-OFF-ON, quando è richiesta la funzione di sicurezza, ad es.: circuito di interblocco realizzato con relè)	99%
Memoria non volatile con firma di 8 bit	90%
Memoria non volatile con firma di 16 bit	99%
Memoria volatile: prova della RAM per mezzo di dati ridondanti (ad es.: flag, marker, costanti, temporizzatori e confronto incrociato di tali dati)	60%
Memoria volatile: prova della capacità di lettura e scrittura delle celle di memoria usate	60%
Memoria volatile: monitoraggio della RAM con codice di Hamming modificato o autotest della RAM (Galpat o Abraham)	99%
Processore: autotest a mezzo di software	da 60% a 90%
Processore: funzionamento per mezzo di codici	da 90% a 99%
Rilevamento dei guasti a partire dal processo	da 0% a 99% a seconda dell'applicazione (la misura da sola non è sufficiente se PL_r = "e")

TABELLA 4.c: STIME DI COPERTURE DIAGNOSTICHE DI DISPOSITIVI DI USCITA

Misura	DC
Monitoraggio delle uscite da parte di uno dei canali, senza prova dinamica	da 0% a 99% a seconda di quanto spesso l'applicazione produce una variazione di segnale
Monitoraggio incrociato delle uscite senza prova dinamica	da 0% a 99% a seconda di quanto spesso l'applicazione produce una variazione di segnale
Monitoraggio incrociato delle uscite con prova dinamica senza rilevamento dei cortocircuiti (I/O multipli)	90%
Monitoraggio incrociato delle uscite e dei risultati intermedi della logica di controllo (L) e monitoraggio software (temporale e logico) del flusso del programma e rilevamento dei guasti statici e dei cortocircuiti (I/O multipli)	99%
Ridondanza del percorso di spegnimento con monitoraggio degli attuatori per mezzo della logica di controllo e del dispositivo di prova	99%
Monitoraggio indiretto (ad es.: monitoraggio con interruttori di pressione, monitoraggio elettrico del posizionamento degli attuatori)	da 90% a 99% a seconda dell'applicazione
Rilevamento dei guasti a partire dal processo	da 0% a 99% a seconda dell'applicazione (la misura da sola non è sufficiente se PL_r = "e")
Monitoraggio diretto (ad es.: monitoraggio elettrico del posizionamento delle valvole di controllo, monitoraggio dei dispositivi elettromeccanici per mezzo di contatti azionati meccanicamente)	99%

Altre stime di coperture diagnostiche possono essere trovate nelle tabelle dell'Allegato A della IEC 61508-2.
Se la logica di controllo deve avere una DC media o alta, allora è necessario adottare almeno una delle misure consigliate per la memoria volatile, per la memoria non volatile e per il processore (la DC di ciascuna delle misure scelte deve essere almeno del 60%).
Relativamente alle tabelle precedenti, per le misure per cui è dato un intervallo di valori per la DC, il valore corretto della DC può essere determinato considerando tra tutti i guasti pericolosi quali sono quelli rilevati da quella particolare misura. In caso di dubbio conviene basarsi su una stima derivata da una FMEA.

1.9. Categorie e loro relazione col $MTTF_D$ di canale, con la DC_{avg} e con le CCF

I calcoli di PFH_D (probabilità oraria di malfunzionamento pericoloso) relativi ai diversi PL_r e le figure 3 e 10 sono basati su cinque "architetture designate", chiamate Categorie. Se un'architettura devia da quelle delle Categorie allora il suo PL deve essere giustificato con mezzi analitici (catene di Markov, alberi dei guasti o altro), al fine di mostrare che tale architettura raggiunge il livello di prestazione richiesto (PL_r).

La scelta della Categoria per una particolare SRP/CS dipende principalmente da:
- la riduzione del rischio che deve essere ottenuta con la funzione di sicurezza a cui la SRP/CS contribuisce;
- il livello di prestazione richiesto (PL_r);
- la tecnologia usata;

- il rischio che si ha in caso di guasto della SRP/CS;
- la possibilità di evitare un guasto nella SRP/CS (guasti sistematici);
- la probabilità di occorrenza di un guasto nella SRP/CS, che è funzione di alcuni parametri rilevanti, quali il tempo medio al guasto pericoloso ($MTTF_D$), la copertura diagnostica (DC) e, per le Categorie 2, 3 e 4, i guasti di modo comune (CCF).

La struttura della SRP/CS ha una grande influenza sul PL. Anche se le strutture possibili sono molte i concetti base sono spesso simili. Pertanto molte delle strutture che sono possibili nel campo delle macchine possono essere fatte rientrare in una delle Categorie.
Ogni Categoria ha una rappresentazione tipica in termini di diagramma a blocchi (architetture designate). Tali diagrammi non sono rappresentazioni circuitali, ma logiche. Per le Categorie che non hanno un unico canale ciò significa che la struttura del sistema fa in modo che vi siano dei mezzi ridondanti per assicurare che un guasto non possa portare alla perdita della funzione di sicurezza.
Le frecce nei grafici che seguono rappresentano interconnessioni logiche (funzionali e diagnostiche).

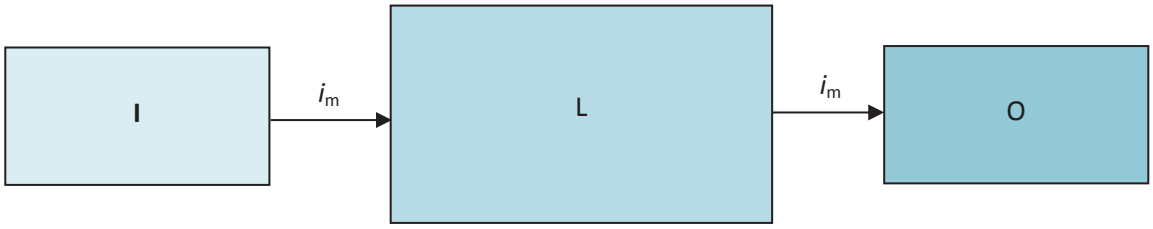
La Categoria B è quella base: un errore può portare alla perdita della funzione di sicurezza.
Nella Categoria 1 una maggiore resistenza ai guasti è ottenuta scegliendo componenti migliori.
Nelle Categorie 2, 3 e 4 prestazioni migliori sono ottenute migliorando la struttura della SRP/CS.
Nella Categoria 2 sono usate prove periodiche per verificare che la funzione di sicurezza continui a essere fornita. Nelle Categorie 3 e 4 un guasto singolo non deve portare alla perdita della funzione di sicurezza.
Nella Categoria 4, e dove ragionevolmente possibile nella Categoria 3, tale guasto deve essere rilevato. Nella Categoria 4 deve essere specificata la resistenza all'accumulo di guasti.

Il PL mostrato in figura 10 è basato sulle architetture designate e dipende dalla Categoria, dal $MTTF_D$ e dalla DC_{avg}. Per strutture con più di un canale è necessario che sia verificato che la frazione dei guasti di causa comune sia inferiore a un valore prefissato: questo nel metodo semplificato è ottenuto mediante la verifica di una checklist e il raggiungimento di un punteggio minimo. Se si usa la figura 10 per avere una stima del PL, allora si deve dimostrare che l'architettura della SRP/CS è equivalente all'architettura designata della Categoria scelta.

1.9.1. Categoria B

Per la categoria B si richiede che la SRP/CS sia, almeno, progettata, costruita, scelta, assemblata e combinata secondo quanto riportato nelle norme applicabili e siano utilizzati i principi base di sicurezza per l'applicazione specifica, in modo da resistere a:

- le sollecitazioni previste durante il funzionamento (ad es. malfunzionamenti, guasti, e loro frequenza);
- l'influenza dei materiali lavorati (ad es. sostanze corrosive, acide…;);
- altre influenze esterne rilevanti (ad es. vibrazioni, EMC, problemi dell'alimentazione).



i_m = mezzi di interconnessione
I = dispositivo di ingresso (ad es. microswitch)
L = logica (es. PLC standard)
O = dispositivo di uscita (ad es. contattore)

Fig. 4: Architettura designata per la Categoria B

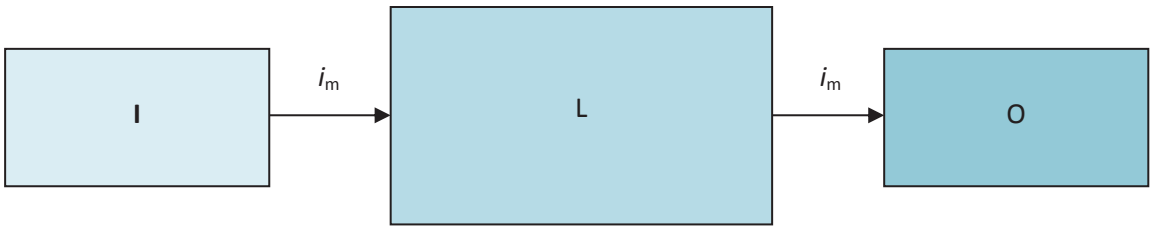
Per la Categoria B non vi è copertura diagnostica (DC_{avg} = nulla) e il $MTTF_D$ del canale può assumere i valori da “basso” a “medio”.
In tale struttura (di solito a canale singolo) le considerazioni sui CCF non hanno rilevanza.
Il massimo PL raggiungibile con tale Categoria è PL= “b”.
Se avviene un guasto ciò può portare alla perdita della funzione di sicurezza.
Per la compatibilità elettromagnetica possono essere utilizzate le norme applicabili (es. norme di prodotto specifiche se disponibili oppure almeno i requisiti per l’immunità della IEC 61000-6-2).

1.9.2. Categoria 1

Per tale struttura in aggiunta ai requisiti richiesti per la Categoria B si adottano componenti ben provati e principi di sicurezza ben provati.

Un componente ben provato per un’applicazione di sicurezza è un componente ampiamente usato in passato con risultati eccellenti in applicazioni simili oppure costruito e verificato utilizzando principi che dimostrano la sua appropriatezza e affidabilità per applicazioni di sicurezza.

I componenti e i principi di sicurezza nuovi possono essere considerati ben provati se si dimostrano appropriati e affidabili. È importante comprendere che un componente deve essere ben provato con riferimento alla specifica applicazione per cui è destinato (un microswitch non può essere in assoluto considerato ben provato a meno che ne sia indicata la specifica applicazione ad esempio per ambienti corrosivi). In elettronica tutto ciò che è complesso cioè per il quale non è possibile definire tutti i modi di guasto non può essere considerato come ben provato.
Il $MTTF_D$ del canale deve essere “alto”.
Il massimo PL raggiungibile con la Categoria 1 è PL= “c”.
Per la Categoria 1 non vi è copertura diagnostica (DC_{avg} = nulla) e, data la struttura (a canale singolo) non si applicano le misure per ridurre i CCF.
Un guasto può comportare la perdita della funzione di sicurezza. Il valore Alto del $MTTF_D$ del canale garantisce per la Categoria 1 una affidabilità superiore a quella della Categoria B.



i_m = mezzi di interconnessione
I = dispositivo di ingresso (ad es. sensore)
L = logica
O = dispositivo di uscita (ad es. interruttore dell’azionamento)

Fig. 5: Architettura designata per la Categoria 1

1.9.3. Categoria 2

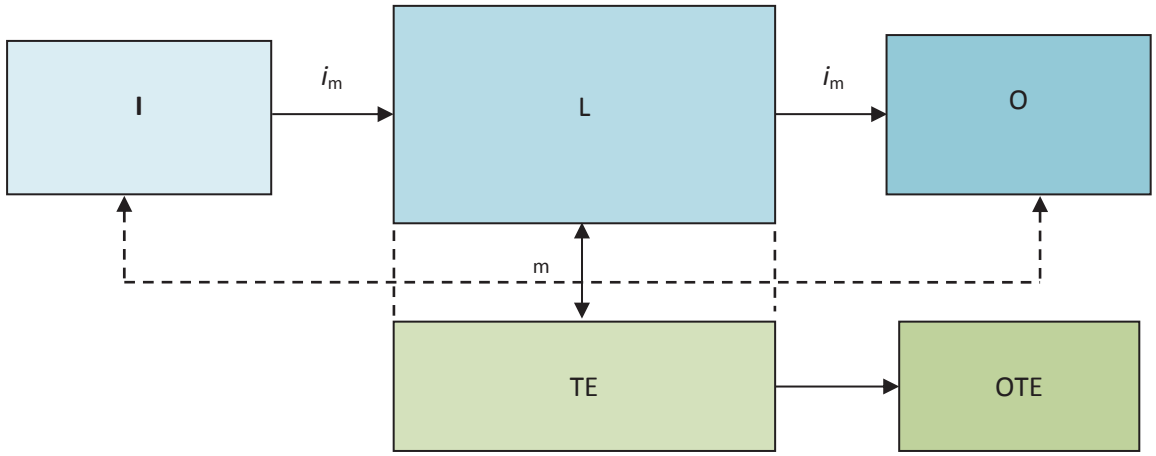
Anche per la Categoria 2 si applicano i requisiti della Categoria B con l’aggiunta dei principi di sicurezza ben provati e inoltre le funzioni di sicurezza implementate da strutture in Categoria 2 devono essere testate periodicamente e in particolare:

- all’accensione della macchina e
- prima dell’inizio di ogni situazione pericolosa (all’inizio di un nuovo ciclo, all’inizio di movimenti pericolosi, immediatamente appena sia stata richiesta la funzione di sicurezza, periodicamente in funzione della valutazione del rischio).

Il test o prova o verifica della funzione di sicurezza deve:
- permettere il funzionamento se non sono stati rilevati guasti
- generare un'uscita (OTE) che attivi appropriate azioni di controllo se è stato rilevato un guasto.

È importante sottolineare che l'uscita OTE della catena di test è necessaria affinché la categoria 2 sia correttamente eseguita.
Se PL_r="d", l'uscita (OTE) porta il sistema in uno stato sicuro che è mantenuto finché il guasto non è eliminato. Per PL_r inferiori o uguali a PL_r="c", se è fattibile, l'uscita (OTE) porta il sistema in uno stato sicuro che è mantenuto finché il guasto non è eliminato, se non è fattibile, può essere sufficiente che l'uscita (OTE) fornisca un segnale di avvertimento.

Per l'architettura designata della Categoria 2 i calcoli del $MTTF_D$ e della DC_{avg} devono tener conto solo dei blocchi del canale funzionale (I, L e O nella figura 6) e non considerare i blocchi del canale di prova (TE e OTE nella figura 6).
La copertura diagnostica DC_{avg} del canale funzionale è "bassa", "media" o "alta".
Il $MTTF_D$ del canale può variare da "basso" ad "alto" a seconda del livello di prestazione richiesto (PL_r).
Poiché sono presenti due canali, anche se uno è un canale per il test della funzione di sicurezza, si devono applicare le misure contro i CCF.



le linee tratteggiate rappresentano un rilevamento dei guasti ragionevolmente realizzabile
i_m = mezzi di interconnessione
I = dispositivo di ingresso
L = logica di controllo
O = dispositivo di uscita
m = monitoraggio
TE = dispositivo di prova
OTE = uscita del TE

Fig. 6: Architettura designata per la Categoria 2

L'esecuzione del test non deve portare a situazioni pericolose (ad es. influenzare negativamente il tempo di risposta). Il canale di test può essere separato o far parte del canale funzionale.
Il massimo PL raggiungibile con la Categoria 2 è PL="d".

Nella struttura in Categoria 2:
- il verificarsi di un guasto nell'intervallo che intercorre tra due prove può portare alla perdita della funzione di sicurezza;
- la perdita della funzione di sicurezza deve essere rilevata dalla prova.

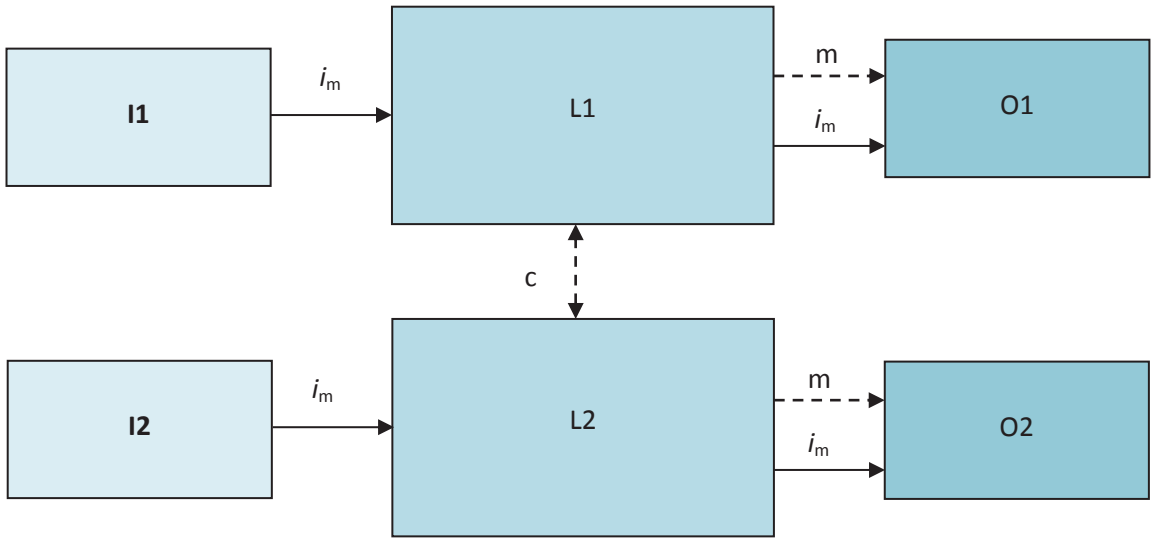
Il principio di validità della Categoria 2 è basato sul fatto che le soluzioni tecniche per essa adottate e, ad esempio, un'appropriata scelta della frequenza di prova, possono diminuire la probabilità di occorrenza delle situazioni pericolose.
La struttura di un'architettura in categoria 2 è idonea per applicazioni elettriche/elettroniche mentre per tecnologia meccanica o elettromeccanica la realizzazione è difficile se non complicata per le difficoltà di realizzare un canale di test.
Infine un'importante considerazione riguarda il vincolo fissato da osservare sul tasso di guasto per la categoria 2 nel metodo semplificato per il quale si rimanda al paragrafo dedicato (1.14).

1.9.4. Categoria 3

Per la Categoria 3 si devono applicare i requisiti per la Categoria B e in aggiunta devono essere seguiti anche i principi di sicurezza ben provati. Inoltre:

- le SRP/CS di Categoria 3 devono essere progettate in modo che un guasto singolo non porti alla perdita della funzione di sicurezza. Se è ragionevolmente praticabile il guasto singolo deve essere rilevato in occasione o prima della richiesta successiva della funzione di sicurezza.

La tecnologia utilizzata può influenzare la possibile realizzazione del rilevamento dei guasti.
La copertura diagnostica DC_{avg} complessiva della SRP/CS è "bassa" o superiore.
Il $MTTF_D$ di ciascuno dei due canali ridondanti può variare da "basso" ad "alto" a seconda del livello di prestazione richiesto (PL_r).
Si devono applicare le misure contro i CCF.



le linee tratteggiate rappresentano un rilevamento dei guasti ragionevolmente realizzabile
i_m = mezzi di interconnessione
I1, I2 = dispositivo di ingresso
L1, L2 = logica
O1, O2 = dispositivo di uscita
c = monitoraggio incrociato
m = monitoraggio

Fig. 7: Architettura designata per la Categoria 3

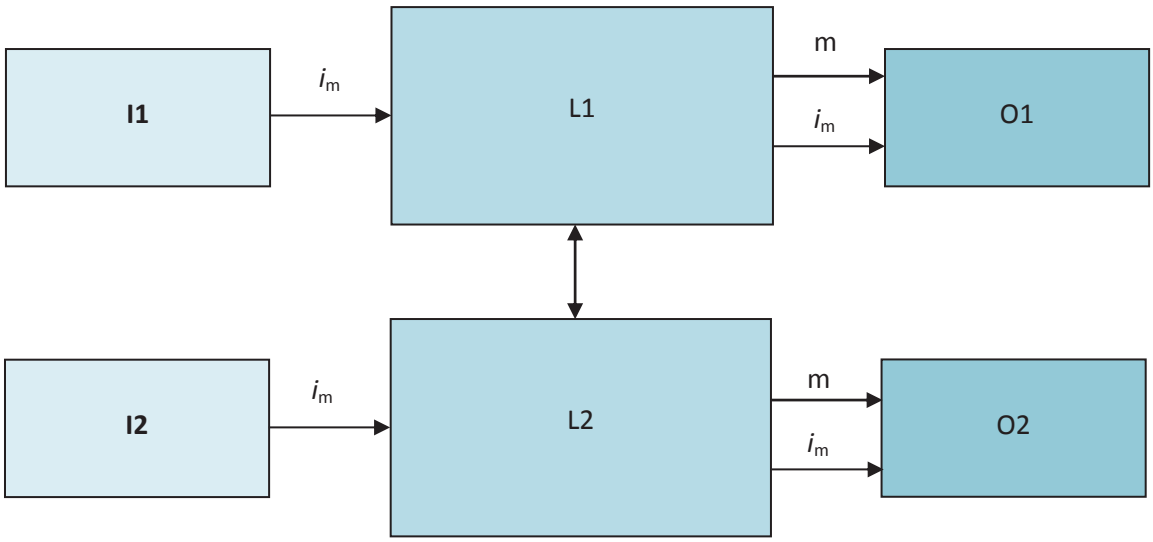
I requisiti sul rilevamento del guasto singolo non significano che tutti i guasti debbano essere rilevati. Di conseguenza l'accumularsi di guasti non rilevati può condurre a uscite non volute e a situazioni pericolose.
Il feedback che si riceve dai contatti guidati meccanicamente o dal monitoraggio di segnali di uscita ridondanti è un efficace sistema per rilevare i guasti.

La Categoria 3 è caratterizzata dai seguenti comportamenti:
- la funzione di sicurezza continua a essere realizzata anche se è avvenuto un guasto singolo;
- alcuni guasti, ma non tutti, sono rilevati;
- è possibile la perdita della funzione di sicurezza a causa dell'accumularsi di guasti non rilevati.

1.9.5. Categoria 4

Per la Categoria 4 si devono applicare i requisiti validi per la Categoria B e in aggiunta i principi di sicurezza ben provati, inoltre le SRP/CS di Categoria 4 devono essere progettate in modo che:
- un guasto singolo non porti alla perdita della funzione di sicurezza e
- il guasto singolo deve essere rilevato in occasione o prima della richiesta successiva della funzione di sicurezza, cioè immediatamente all'inizio o alla fine di ciascun ciclo di funzionamento della macchina.

Tuttavia se il rilevamento del guasto non è possibile, allora l'accumularsi di guasti non rilevati non deve condurre alla perdita della funzione di sicurezza.



le linee solide per il monitoraggio rappresentano una copertura diagnostica superiore a quella che si ha nell'architettura designata di Categoria 3
i_m = mezzi di interconnessione
I1, I2 = dispositivo di ingresso L1, L2 = logica di controllo
O1, O2 = dispositivo di uscita
c = monitoraggio incrociato
m = monitoraggio

Fig. 8: Architettura designata per la Categoria 4

La copertura diagnostica DC_{avg} complessiva della SRP/CS è "alta" e include l'accumulo di guasti.
Il $MTTF_D$ di ciascuno dei due canali ridondanti è "alto".
Si devono applicare le misure contro i CCF.

I requisiti sul rilevamento del guasto singolo non significano che tutti i guasti debbano essere rilevati. Tuttavia si presume che l'accumularsi di guasti non rilevati non conduca a situazioni pericolose, poiché, per via della DC alta, i guasti sono comunque rilevati in tempo per prevenire la perdita della funzione di sicurezza.
Il feedback che si riceve dai contatti guidati meccanicamente o dal monitoraggio di segnali di uscita ridondanti è un efficace sistema per rilevare i guasti.

Il comportamento di un sistema realizzato con la Categoria 4 è caratterizzato da:
- la funzione di sicurezza continua a essere realizzata anche se è avvenuto un guasto singolo;
- i guasti sono rilevati in tempo, in modo da prevenire la perdita della funzione di sicurezza;
- l'accumularsi di guasti non rilevati è preso in considerazione.

Le differenze tra la Categoria 4 e la Categoria 3 sono
- in Categoria 4 la copertura diagnostica DC_{avg} è superiore e
- in Categoria 4 il $MTTF_D$ di ciascun canale è di valore "alto".

In pratica, per ciò che riguarda la combinazione dei guasti, può essere sufficiente limitarsi a considerare coppie di guasti (resistenza al doppio guasto).

Entrambe le tabelle 5 e 6 riassumono le caratteristiche delle Categorie (la tabella 5 in modo più sintetico).

TABELLA 5: SOMMARIO SINTETICO DELLE CARATTERISTICHE DELLE CATEGORIE

Caratteristiche	**Categorie**				
	Caratterizzate dalla scelta dei componenti		**Caratterizzate dalla struttura**		
	B	**1**	**2**	**3**	**4**
Progettazione secondo le norme applicabili	×	×	×	×	×
Principi base di sicurezza	×	×	×	×	×
Principi di sicurezza ben provati		×	×	×	×
Componenti ben provati		×			
Rilevamento dei guasti			×	×	×
Tolleranza al guasto singolo				×	×
Considerazione dell'accumulo dei guasti					×
Adozione di misure contro i CCF			×	×	×
$MTTF_D$	da basso a medio	alto	da basso a alto	da basso a alto	alto
DC_{avg}	nulla	nulla	da bassa a media	da bassa a media	alta

TABELLA 6: SOMMARIO DELLE CARATTERISTICHE DELLE CATEGORIE

	Requisiti/comportamento/principi di sicurezza usati	$MTTF_D$	DC_{avg}	CCF
B	Le SRP/CS e/o i loro dispositivi di protezione, così come i loro componenti devono, almeno, essere progettati, costruiti, scelti, assemblati e combinati secondo quanto riportato nelle norme applicabili in modo da resistere alle sollecitazioni attese. Si devono utilizzare i principi base di sicurezza. Il verificarsi di un guasto può portare alla perdita della funzione di sicurezza. Principalmente caratterizzata dalla scelta dei componenti.	da basso a medio	nulla	No
1	Si applicano i requisiti della Categoria B. Si devono utilizzare i componenti e i principi di sicurezza ben provati. Il verificarsi di un guasto può portare alla perdita della funzione di sicurezza ma la probabilità che ciò avvenga è più bassa che per la Categoria B. Principalmente caratterizzata dalla scelta dei componenti.	alto	nulla	No
2	Si applicano i requisiti della Categoria B. Si devono utilizzare i principi di sicurezza ben provati. La funzione di sicurezza deve essere provata a intervalli di tempo stabiliti. Il verificarsi di un guasto tra due prove può portare alla perdita della funzione di sicurezza. La perdita della funzione di sicurezza è rilevata dalla prova. Principalmente caratterizzata dalla struttura.	da basso ad alto	da bassa a media	Si
3	Si applicano i requisiti della Categoria B. Si devono utilizzare i principi di sicurezza ben provati. Le SRP/CS devono essere progettate in modo che un guasto singolo non porti alla perdita della funzione di sicurezza e, se è ragionevolmente praticabile, il guasto singolo deve essere rilevato. Al verificarsi di un guasto la funzione di sicurezza continua a essere attuata. Alcuni, ma non tutti i guasti sono rilevati. L'accumularsi di guasti non rilevati può portare alla perdita della funzione di sicurezza. Principalmente caratterizzata dalla struttura.	da basso ad alto	da bassa a media	Si
4	Si applicano i requisiti della Categoria B. Si devono utilizzare i principi di sicurezza ben provati. Le SRP/CS devono essere progettate in modo che un guasto singolo non porti alla perdita della funzione di sicurezza e il guasto singolo deve essere rilevato in occasione o prima della richiesta successiva della funzione di sicurezza, tuttavia se il rilevamento del guasto non è possibile, allora l'accumularsi di guasti non rilevati non deve condurre alla perdita della funzione di sicurezza. Al verificarsi di un guasto la funzione di sicurezza continua a essere attuata. La rilevazione dei guasti riduce la probabilità di perdita della funzione di sicurezza (DC alta). I guasti sono rilevati in tempo per prevenire la perdita della funzione di sicurezza. Principalmente caratterizzata dalla struttura.	alto	alta e include l'accumulo di guasti	Si

1.10. Combinazione di SRP/CS per il raggiungimento di un PL complessivo

Una funzione di sicurezza può essere realizzata combinando tra loro più SRP/CS e ogni SRP/CS può essere considerata, in analogia con i contenuti della norma IEC 62061, un sottosistema (il sottosistema o la SRP/CS è l'oggetto a livello gerarchico più elevato nel sistema di controllo relativo alla sicurezza, un suo guasto comporta un guasto nella funzione di sicurezza). Ogni SRP/CS è realizzata per mezzo di una Categoria.
Alla combinazione delle SRP/CS può essere assegnato un PL complessivo, in tal caso è necessario validare la combinazione delle SRP/CS, verificando che soddisfi tutti i requisiti della funzione di sicurezza che deve realizzare.
La combinazione delle SRP/CS inizia nel punto dove l'ingresso relativo alla sicurezza è generato e termina all'uscita degli attuatori. La combinazione potrebbe consistere in diverse parti connesse in serie e/o in parallelo e/o in modo più complesso. Nel caso generale deve essere calcolato il PFH_D della combinazione, in modo da risalire attraverso la tabella 1 al PL raggiunto.
Nel caso più semplice e diffuso di una combinazione in serie di SRP/CS, di cui sia noto il PL di ciascuna parte, per evitare calcoli complessi, si può adottare la seguente procedura per ottenere una stima del PL complessivo della combinazione. Si assume cioè che ci si trovi nella situazione di figura 9, in cui le SRP/CS_i distinte siano N, connesse in serie, operanti per fornire la funzione di sicurezza. Il PL_i di ciascuna SRP/CS è già stato stimato.

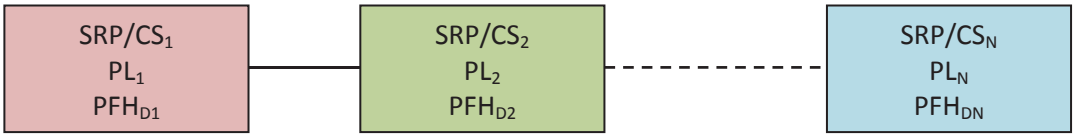


Fig. 9: Combinazione serie di SRP/CS per la realizzazione di una funzione di sicurezza

- Se i valori PFH_{Di} individuali delle SRP/CS_i sono noti, allora il PFH_D della combinazione è dato dalla somma dei PFH_{Di} individuali ($PFH_D = PFH_{D1} + PFH_{D2} + \ldots + PFH_{DN}$). Il PL della combinazione è limitato da:
  - ⇒ il più basso PL_i individuale tra quelli delle N parti SRP/CS_i coinvolte nella combinazione (tenendo conto del fatto che anche aspetti non quantificabili sono coinvolti nella determinazione del PL);
  - ⇒ il PL ottenuto dalla tabella 1, sulla base del PFH_D della combinazione.

- Se i valori PFH_{Di} individuali delle SRP/CS_i non sono noti, allora una stima del PL della combinazione, corrispondente al valore che si ha nel caso peggiore, può essere ricavata dalla tabella 7 operando nel modo seguente:
  - ⇒ prima si identifica con PL_{low} il piu basso tra i PL_i individuali;
  - ⇒ poi si identifica con $N_{low} \leq N$ il numero di SRP/CSi con $PL_i = PL_{low}$;
  - ⇒ infine si ricava il PL della combinazione dalla tabella 7.

TABELLA 7: CALCOLO DEL PL PER UNA COMBINAZIONE SERIE DI SRP/CS

PL_{low}	N_{low}	⇒	PL
a	> 3	⇒	Non permesso
	≤ 3	⇒	a
b	> 2	⇒	a
	≤ 2	⇒	b
c	> 2	⇒	b
	≤ 2	⇒	c
d	> 3	⇒	c
	≤ 3	⇒	d
e	> 3	⇒	d
	≤ 3	⇒	e

La tabella 7 è stata calcolata sulla base dei valori mediani degli intervalli di PFH_D validi per ciascun PL.

1.11. Guasti da considerare e guasti da escludere

Sulla base della Categoria scelta, le SRP/CS devono essere progettate in modo da raggiungere il livello di prestazione richiesto (PL_r). Durante la progettazione deve essere valutata la resistenza ai guasti. Per portare a termine tale valutazione è necessario capire quali sono i guasti da considerare e se alcuni di questi possano essere esclusi a priori.

La EN ISO 13849-2 fornisce, per ogni tecnologia, una lista di guasti e malfunzionamenti da prendere in considerazione. La lista non è esaustiva e se necessario possono essere considerati guasti ulteriori. In pratica, per ogni SRP/CS conviene costruire una lista dedicata, ottenuta sulla base dei guasti indicati nella EN ISO 13849-2 e dei guasti possibili derivati dal progetto.
Per i componenti non menzionati nella EN ISO 13849-2, è necessario condurre una FMEA per stabilire quali siano i guasti da considerare.
In generale si possono utilizzare i seguenti criteri per realizzare la lista dei guasti da considerare:

- se, come conseguenza di un guasto, altri componenti si guastano, il primo guasto e tutti quelli da esso derivati devono essere considerati come un guasto singolo;
- due o più guasti separati che hanno una causa comune devono essere considerati come un guasto singolo (CCF);
- il verificarsi simultaneo di due o più guasti le cui cause siano separate è altamente improbabile e, pertanto, non deve essere considerato.

In talune applicazioni è possibile assumere a priori che alcuni guasti non si possano presentare. Informazioni dettagliate su quali guasti escludere sono presenti nella ISO 13849-2. L'esclusione di alcuni guasti è un compromesso tra i requisiti di sicurezza e la possibilità teorica che un guasto si verifichi.
L'esclusione dei guasti è basata su:

- la scarsa probabilità tecnica che hanno alcuni guasti di verificarsi;
- l'esperienza tecnica generalmente accettata, indipendentemente dall'applicazione considerata;
- i requisiti tecnici dell'applicazione e dei rischi specifici.

L'esclusione dei guasti deve essere giustificata dettagliatamente nella documentazione tecnica.

Le locuzioni "ben provato" ed "esclusione dei guasti" si riferiscono a concetti che non devono essere confusi: un componente ben provato, di solito, è stato già usato in una certa applicazione con risultati eccellenti (la qualifica di ben provato dipende come già detto dall'applicazione), invece perché sia possibile escludere i guasti di un altro componente potrebbe essere necessario dover adottare misure aggiuntive, che dovrebbero essere applicate per tutta la vita del componente.

1.12. Stima dei malfunzionamenti di causa comune (CCF)

Nell'Allegato D della IEC 61508-6 sono contenute alcune procedure per la scelta delle misure contro i malfunzionamenti di causa comune (CCF). Una procedura è applicabile ai sensori e agli attuatori e una è applicabile alla logica di controllo. Non tutte le misure contenute in tali procedure sono applicabili alle macchine.
Nell'Allegato F della EN ISO 13849-1 sono riportate quelle che hanno più importanza per le macchine.
Per quanto riguarda tale Allegato, in esso è descritto un metodo euristico ("basato su un giudizio ingegneristico") per valutare se si è adottato un numero sufficiente di misure contro i CCF. Se così è, allora si può presumere che il valore della frazione residua dei guasti di modo comune sia minore o uguale al 2%.

Ogni componente della SRP/CS deve essere considerato nell'applicazione del metodo.
La tabella 8 contiene una lista di misure contro i CCF e i valori a esse associati. A ogni misura contenuta nella lista può essere associato solo il valore riportato o il valore zero (se una misura è solo parzialmente adottata, il valore a essa associato è zero). Se alla fine si ottiene un valore complessivo pari a 65 o superiore, allora le misure adottate sono sufficienti per ritenere che la frazione di CCF residua sia minore o uguale al 2%, viceversa se il valore complessivo è inferiore a 65 è necessario adottare ulteriori misure.

TABELLA 8: QUANTIFICAZIONE DELLE MISURE CONTRO I MALFUNZIONAMENTI DI CAUSA COMUNE (CCF)

	Misure contro i CCF	**Valore**
1	**Separazione/segregazione**	
	Separazione fisica tra i percorsi dei segnali, ad esempio: – separazione nel percorso dei cavi/tubature; – rilevamento di cortocircuiti o circuiti aperti nei cavi con test dinamici; – sufficienti distanze in aria e superficiali sulle schede dei circuiti stampati.	15
2	**Diversità**	
	Sono utilizzati differenti tecnologie/progetti o principi fisici, ad esempio: – attivazione della funzione di sicurezza diversa per ogni canale (ad es.: elettronica o elettronica programmabile su uno ed elettromeccanica sull'altro); – misurazione analogica e digitale delle variabili (ad es.: distanze, pressioni, temperature) – componenti di costruttori diversi.	20
3	**Progetto/applicazione/esperienza**	
3.1	Protezione contro sovratensioni, sovracorrenti, sovrapressioni, sovratemperature, ecc.	15
3.2	Uso di componenti ben provati.	5
4	**Valutazione/analisi**	
	Per ogni SRP/CS è condotta una FMEA i cui risultati sono utilizzati per evitare CCF nel progetto.	5
5	**Competenza/addestramento**	
	Addestramento dei progettisti per comprendere le cause e le conseguenze dei CCF.	5
6	**Misure contro le influenze ambientali**	
6.1	Protezione dei sistemi elettrici/elettronici dalla contaminazione (polvere, liquidi, sporco) e dai disturbi elettromagnetici, secondo quanto riportato nelle norme applicabili. Conformità ai requisiti del costruttore per la purezza del fluido da pressurizzare (filtri del fluido, misure per impedire l'ingresso dello sporco e per lo spurgo dei gas), per i sistemi a fluido. Per i sistemi misti (a fluido ed elettrici) entrambi i criteri devono essere considerati.	25
6.2	Requisiti per l'immunità ad altre influenze ambientali (temperature, urti, vibrazioni, umidità), secondo quanto riportato nelle norme applicabili.	10
	Totale massimo raggiungibile	**100**

Totale raggiunto	**Valutazione delle misure contro i CCF**[a]
65 o superiore	Misure sufficienti (la frazione di CCF della SRP/CS è minore o uguale al 2%)
inferiore a 65	Misure insufficienti: ne devono essere scelte di ulteriori

[a]Quando le misure riportate sopra non sono pertinenti, i punti indicati possono essere considerati nel calcolo totale

1.13. Guasti sistematici

La EN ISO 13849-2 consiglia una serie di misure contro i guasti sistematici basate sui principi di sicurezza di base e su quelli ben provati.

Le seguenti misure sono consigliate per limitare gli effetti dei guasti sistematici:
- uso della de-energizzazione: la SRP/CS dovrebbe essere progettata in modo che alla perdita dell'alimentazione la macchina raggiunga o mantenga uno stato sicuro;
- uso di misure per controllare gli effetti delle sovratensioni (che potrebbero portare al superamento delle tensioni di rottura degli isolamenti o a malfunzionamenti) e delle variazioni di tensione (incluse le tensioni più basse): il comportamento della SRP/CS in risposta a tali sollecitazioni dovrebbe essere predeterminato, in modo che la SRP/CS possa far raggiungere o mantenere alla macchina uno stato sicuro;
- uso di misure per controllare o evitare gli effetti dell'ambiente fisico (temperatura, umidità, acqua, vibrazioni, polvere, sostanze corrosive, interferenze elettromagnetiche): il comportamento della SRP/CS in risposta agli effetti dell'ambiente fisico dovrebbe essere predeterminato, in modo che la SRP/CS possa far raggiungere o mantenere alla macchina uno stato sicuro;
- uso del monitoraggio delle sequenze di programma, con software della SRP/CS aggiuntivo per rilevare difetti nelle sequenze di programma: una sequenza di programma difettosa si ha quando gli elementi individuali di un programma (moduli software, sottoprogrammi o comandi) sono eseguiti in sequenza errata o in un intervallo di tempo errato o quando il clock del processore è guasto;
- uso di misure per controllare gli effetti degli errori o altri effetti che nascono durante qualsiasi processo di comunicazione dei dati**.**

In aggiunta, una o più delle seguenti misure sono consigliate per limitare gli effetti dei guasti sistematici, in base alla complessità della SRP/CS e al valore del suo PL:
- rilevamento dei guasti con prove automatiche;
- hardware ridondante per i test;
- diversità dell'hardware;
- funzionamento in "modo positivo";
- contatti ad azione guidata (*mechanically linked*);
- apertura ad azione diretta;
- modo di guasto orientato;
- sovradimensionamento con fattore opportuno, ove il costruttore possa dimostrare che ciò migliori l'affidabilità (in tal caso è consigliabile utilizzare un fattore di almeno 1,5).

Si consigliano le seguenti misure per evitare i guasti sistematici:
- uso di materiali idonei e di una fabbricazione adeguata: scelta dei materiali, dei metodi di fabbricazione e di trattamento, in relazione ad esempio alle sollecitazioni, alla durabilità, all'elasticità, all'attrito, all'invecchiamento, alla corrosione, alla temperatura, alla conducibilità, alla rigidità dielettrica;
- uso di un corretto dimensionamento e di una forma adatta: in relazione ad esempio alle sollecitazioni, agli sforzi, alla fatica, alla temperatura, alla ruvidezza delle superfici, alla fabbricazione;
- scelta, combinazione, assemblaggio e installazione dei componenti in modo appropriato, incluso il cablaggio, il percorso dei cavi e le interconnessioni: applicazione delle norme appropriate e delle note del costruttore (fogli di informazione, istruzioni di installazione, specifiche tecniche e applicazione di buone pratiche ingegneristiche[1]);
- compatibilità: uso di componenti con caratteristiche operative compatibili;
- tenuta specifica alle condizioni ambientali: progettazione delle SRP/CS in modo che la macchina possa operare in tutte le situazioni ambientali in cui è destinata a essere utilizzata e in ogni condizione avversa prevedibile (ad es.: temperatura, umidità, vibrazioni, interferenze elettromagnetiche);

[1] I componenti come le valvole idrauliche o pneumatiche possono dover essere azionati ciclicamente, al fine di evitare la probabilità di bloccaggio o per scongiurare incrementi inaccettabili del tempo di azionamento (per tali componenti è necessario che il progettista preveda l'effettuazione di prove periodiche).

- uso di componenti progettati secondo norme appropriate[2], con modi di guasto ben determinati: lo scopo è di ridurre il rischio di guasti non rilevati grazie all'uso di componenti con caratteristiche specificate.

In aggiunta, una o più delle seguenti misure sono consigliate per evitare i guasti sistematici, in base alla complessità della SRP/CS e al valore del suo PL:
- revisione della progettazione hardware (ad es.: per ispezione o walk-through): lo scopo è di rivelare, con la revisione e l'analisi, possibili discrepanze tra quanto specificato e quanto realizzato;
- uso di strumenti per la progettazione computer-aided con capacità di simulazione o di analisi: lo scopo è di eseguire la procedura di progettazione in modo sistematico e di includere in essa i componenti e gli elementi già disponibili e provati che sono già inclusi all'interno dello strumento per la progettazione computer-aided che si sta usando;
- uso di simulazioni: lo scopo è quello di eseguire un'ispezione sistematica e completa della SRP/CS sia in termini di prestazione sia per il corretto dimensionamento dei suoi componenti**.**

Anche durante l'integrazione della SRP/CS potrebbero aver luogo guasti sistematici.
Le seguenti misure sono consigliate durante l'integrazione della SRP/CS:
- prove di funzionamento;
- gestione della progettazione (project management);
- documentazione.

In aggiunta, per evitare guasti sistematici durante l'integrazione è consigliabile condurre prove come se il sistema fosse una black-box, in base alla complessità della SRP/CS e al valore del suo PL.

1.14. Metodo semplificato per la stima del PL

Le architetture scelte devono essere rappresentate con un diagramma a blocchi e fatte rientrare in una tra le architetture designate delle Categorie.
Le Categorie servono a fornire una rappresentazione logica della struttura del sistema, l'effettiva realizzazione tecnica e il diagramma circuitale del sistema possono differire notevolmente da tale rappresentazione.
Le architetture scelte per le Categorie iniziano dal punto dove iniziano i segnali relativi alla sicurezza e terminano all'uscita degli attuatori. Tali architetture possono essere utilizzate anche per rappresentare una sottoparte che ha in ingresso dei segnali e genera in uscita altri segnali relativi alla sicurezza.

Per le architetture designate delle Categorie è possibile costruire il grafico della figura 10 seguente, basato sui valori di PFH_D della tabella K.1 della EN ISO 13849-1. Tale grafico è stato ottenuto applicando il Metodo di Markov e così pure i valori indicati nella tabella K.1. Per tale motivo se si applica il metodo semplificato qui descritto non è possibile derogare dalle architetture designate.
Per ottenere tale grafico sono state fatte le seguenti assunzioni:
- Tempo di missione = 20 anni;
- tassi di malfunzionamento costanti all'interno del tempo di missione;
- per la Categoria 2:
  - ⇒ tasso di richiesta della funzione di sicurezza ≤ (1/100) × tasso di test,
  - ⇒ oppure tasso di richiesta ≤ (1/25) × tasso di test, allora i valori del PFH_D della Categoria 2 della tabella K.1 della EN ISO 13849-1 devono essere degradati moltiplicandoli per 1,1 ed essere utilizzati come stima nel caso peggiore,

[2] Ad es.: l'Allegato F della norma IEC 61508-2, specifica tecniche e misure per evitare i guasti sistematici durante la progettazione di ASIC (application-specific integrated circuits), di FPGA (field programmable gate arrays) e di PLD (programmable logic devices).

⇒ oppure la prova è eseguita immediatamente quando si ha la richiesta della funzione di sicurezza e il tempo complessivo per scoprire il guasto e portare la macchina in una condizione non pericolosa è inferiore al tempo necessario al raggiungimento del pericolo;

– per la Categoria 2 il $MTTF_D$ del canale di prova è maggiore della metà del $MTTF_D$ del canale funzionale;
– calcoli dei valori di PFH_D basati sui seguenti valori di DC_{avg}: DC_{avg} = bassa (DC_{avg} = 60%); DC_{avg} = media (DC_{avg} = 90%); DC_{avg} = alta (DC_{avg} = 99%).

La figura 10 permette di disporre di un metodo semplificato per la stima del PL. Tale metodo è basato sui citati valori di PFH_D, ottenuti con calcoli analitici (Markov) effettuati sulle architetture designate delle Categorie al variare del $MTTF_D$ e per al più due livelli di DC_{avg}. Nella tabella K.1 della EN ISO 13849-1 sono forniti tali valori di PFH_D e i relativi PL ottenibili, che poi sono stati utilizzati per costruire la Figura 10.
Tale figura può essere usata per scegliere la Categoria di una data applicazione, a partire da una stima qualitativa del $MTTF_D$ di ciascun canale, della DC_{avg} e del PL_r.
Viceversa se si è già scelta la Categoria, a partire da una stima qualitativa del $MTTF_D$ di ciascun canale e della DC_{avg} è possibile avere una stima del PL raggiunto dalla SRP/CS (se un'area copre più valori di PL, allora il valore di PL da considerare è dato dalla tabella 9, valori più precisi possono essere ottenuti utilizzando la tabella K.1 della EN ISO 13849-1).

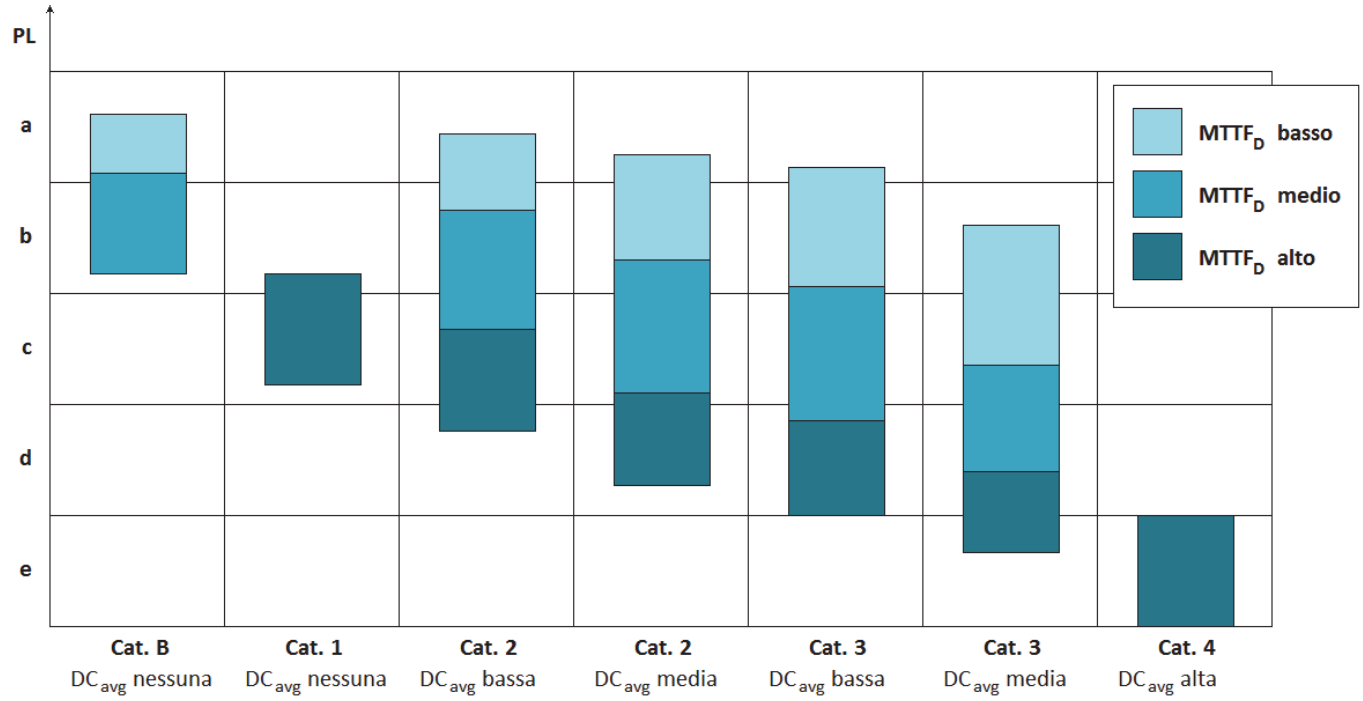


Fig. 10: Relazione tra Categoria, DC_{avg}, $MTTF_D$ di ciascun canale e PL

TABELLA 9: PROCEDURA SEMPLIFICATA PER CALCOLARE IL PL RAGGIUNTO DA UNA SRP/CS

Categoria	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**nulla**	**nulla**	**bassa**	**media**	**bassa**	**media**	**alta**
$MTTF_D$ basso	a	–	a	b	b	c	–
$MTTF_D$ medio	b	–	b	c	c	d	–
$MTTF_D$ alto	–	c	c	d	d	d	e

Se per alcuni parametri non è possibile avere a disposizione valori quantitativi, allora dovrebbero essere scelti i valori relativi al caso peggiore.
Se il sistema è composto da più SRP/CS, allora il PFH_D complessivo può essere stimato con le regole di composizione del PFH_D (si veda in proposito il paragrafo 1.10).

1.14.1. Stima del PL della parte di uscita di una SRP/CS sulla base della Categoria

Se, per parti di uscita di SRP/CS costituite da componenti meccanici, idraulici o pneumatici (o loro combinazioni), non sono disponibili informazioni sull'affidabilità relativa a una data applicazione, il fabbricante della macchina può ancora ottenere una stima del PL senza avere informazioni sul $MTTF_D$, utilizzando la tabella 10.

In tale tabella il PL è funzione della Categoria, della DC_{avg} e delle misure contro le CCF.
La tabella mostra la relazione (desunta dalla figura 10) tra il PL raggiungibile e la Categoria della parte di uscita della SRP/CS.

- Il PL "a" o "b" può essere ottenuto facendo ricorso alla Categoria B.
- Il PL "c" può essere ottenuto facendo ricorso alla Categoria 1 o alla Categoria 2, se sono utilizzati componenti ben provati e principi di sicurezza ben provati. È stata introdotta per le Categorie 2, 3 e 4 la possibilità di utilizzare in alternativa ai componenti ben provati (*well tried*) i componenti provati in uso (*proven in use*). Un componente può essere definito provato in uso qualora abbia una funzionalità (applicazione) specifica e determinata ed esista un'evidenza documentata che dimostri che la probabilità di ogni guasto sistematico pericoloso sia sufficientemente bassa da garantire che il livello di integrità della sicurezza richiesto per la funzione di sicurezza sia garantito. L'evidenza di cui sopra deve basarsi sull'analisi dell'esperienza operativa di una configurazione specifica del componente accompagnata da analisi e prove, il tutto chiaramente documentato. Si sottolinea che il concetto di componente provato in uso proviene dalla norma IEC 61508 e quindi è specifico di componenti elettrici/elettronici.
  Inoltre quando si utilizza una Categoria 1 per realizzare una funzione di sicurezza con un PL "c", il valore del T_{10D} dei componenti relativi alla sicurezza può essere determinato sulla base di dati del tipo provato in uso forniti dal costruttore della macchina.
  Il $MTTF_D$ del canale di prova della Categoria 2 deve essere almeno di 10 anni.
- Il PL "d" può essere ottenuto facendo ricorso alla Categoria 3, se sono utilizzati componenti ben provati e principi di sicurezza ben provati.
- Il PL "e" può essere ottenuto facendo ricorso alla Categoria 4, se sono utilizzati componenti ben provati e principi di sicurezza ben provati.

Nella realizzazione della funzione di sicurezza rispettivamente con le Categorie 2, 3 e 4 devono essere messe in atto misure per eliminare o controllare le CCF e deve essere adottata una copertura diagnostica sufficiente (DC_{avg} bassa o media per le Categorie 2 e 3 e DC_{avg} alta per la Categoria 4). In tal caso la DC_{avg} è calcolata come media aritmetica dei valori di DC dei singoli componenti del canale funzionale.

TABELLA 10: PL E PFH_D COME STIMA DEL CASO PEGGIORE SULLA BASE DELLA CATEGORIA, DELLA DC_{avg} E DELL'USO DI COMPONENTI BEN PROVATI

	PFH_D [1/h]	Cat. B	Cat. 1	Cat. 2	Cat. 3	Cat. 4
PL a	2×10^{-5}	●	O	O	O	O
PL b	5×10^{-6}	●	O	O	O	O
PL c	$1{,}7\times10^{-6}$	–	●**	●*	O	O
PL d	$2{,}9\times10^{-7}$	–	–	–	●*	O
PL e	$4{,}7\times10^{-8}$	–	–	–	–	●*
●	L'uso della Categoria indicata è raccomandato					
O	L'uso della Categoria indicata è opzionale					
–	L'uso della Categoria indicata non è permesso					
*	Devono essere usati componenti provati in uso (*proven in use*) o ben provati (dichiarati dal fabbricante del componente adatti per la particolare applicazione) e principi di sicurezza ben provati.					
**	Devono essere utilizzati componenti ben provati e principi di sicurezza ben provati. Per i componenti relativi alla sicurezza che non sono monitorati durante il processo, il valore del T_{10D} può essere determinato sulla base di dati del tipo provato in uso forniti dal costruttore della macchina					

1.15. Aspetti di ergonomia

L'interfaccia tra gli operatori e la SCP/CS deve essere progettata in modo che nessun essere umano possa risultare in pericolo durante l'uso previsto della macchina e l'uso errato ragionevolmente prevedibile.
I principi dell'ergonomia devono essere utilizzati per fare in modo che la macchina e il sistema di controllo, incluse le parti relative alla sicurezza, siano semplici da usare e l'operatore non sia tentato di bypassare le funzioni di sicurezza. Nella ISO 12100 sono contenuti i requisiti di sicurezza per il rispetto dei principi dell'ergonomia nel settore delle macchine.

1.16. Manutenzione

La manutenzione (preventiva e/o correttiva) è necessaria affinché le prestazioni delle SRP/CS si conservino nel tempo. L'allontanamento dalle prestazioni specificate può condurre, col tempo, a un deterioramento della sicurezza o a situazioni pericolose. Le informazioni per l'uso devono contenere anche informazioni per la manutenzione delle SRP/CS (incluse indicazioni sulle verifiche periodiche).
I principi da seguire per la preparazione di tali informazioni sono contenute nella ISO 12100.

1.17. Documentazione tecnica

Quando si progetta una SRP/CS, almeno i seguenti aspetti devono essere documentati:
- quale funzione di sicurezza è realizzata con la SRP/CS;
- le caratteristiche di tale funzione di sicurezza;
- i punti esatti di inizio e di fine della SRP/CS;
- le condizioni ambientali;
- il livello di prestazione (PL);
- la Categoria o le Categorie scelte;
- i parametri di rilievo per l'affidabilità ($MTTF_D$, DC, CCF e tempo di missione);
- le misure adottate contro i malfunzionamenti sistematici;
- la tecnologia o le tecnologie adottate;
- tutti i guasti considerati ai fini della sicurezza;
- le giustificazioni delle esclusioni dei guasti;
- il razionale del progetto;
- la documentazione del software;
- le misure contro gli usi errati ragionevolmente prevedibili.

Tale documentazione, di solito, non è distribuita all'utilizzatore della macchina.

1.18. Informazioni per l'uso

All'utilizzatore, invece, devono essere fornite tutte le informazioni importanti per l'uso sicuro della SRP/CS.

Tali informazioni includono, non esaustivamente, le seguenti:
- i limiti delle SRP/CS e i guasti che sono stati esclusi;
- i limiti delle SRP/CS e dei guasti esclusi che comportano azioni da parte dell'utilizzatore (ad es.: modifiche, manutenzioni e riparazioni) al fine di mantenere la Categoria scelta o la prestazione di sicurezza o la giustificazione per l'esclusione dei guasti;
- gli effetti delle deviazioni dalle prestazioni specificate per le funzioni di sicurezza;
- una chiara descrizione delle interfacce delle SRP/CS e dei dispositivi di protezione;
- il tempo di risposta;

- i limiti di funzionamento (incluse le condizioni ambientali);
- indicazioni e allarmi;
- muting e sospensione della funzione di sicurezza;
- i modi del sistema di controlli;
- la manutenzione;
- le liste di controllo per la manutenzione;
- l'accessibilità delle parti interne per la sostituzione;
- i mezzi per eseguire test semplici e sicuri per la ricerca dei guasti;
- le informazioni che spiegano per quali applicazioni rilevanti utilizzare la Categoria a cui si è fatto riferimento;
- la verifica degli intervalli di prova, quando è necessario.

Devono essere fornite informazioni sulle Categorie e sui livelli di prestazione delle SRP/CS indicando la data dell'edizione di riferimento della EN ISO 13849-1, la Categoria (B, 1, 2, 3, o 4), il livello di prestazione ("a", "b", "c", "d", "e").

2. Valori di $MTTF_D$ per componenti singoli

Sono possibili diversi metodi per calcolare il $MTTF_D$ di un componente. A volte tali metodi possono dipendere dal tipo di componente. L'Allegato C della norma EN ISO 13849-1 riporta una serie di tali metodi.

2.1. Metodo di buona pratica ingegneristica

Il $MTTF_D$ o il B_{10D} possono essere stimati sulla base dei valori che si trovano nella tabella 11 se i seguenti criteri sono soddisfatti:

a) i componenti sono stati prodotti seguendo i principi di sicurezza di base e quelli ben provati in accordo con la EN ISO 13849-2 (elencati nella seconda colonna della tabella 11) o le norme applicabili per componenti (elencate nella terza colonna della tabella 11); il criterio costruttivo applicato può essere inserito nel data sheet del componente;
b) il costruttore del componente specifica le applicazioni appropriate e le condizioni di funzionamento del componente;
c) il progetto della SRP/CS soddisfa i principi di sicurezza base e quelli ben provati in accordo con la EN ISO 13849-2 per l'applicazione e il funzionamento del componente.

2.2. Componenti idraulici

Il $MTTF_D$ di un componente idraulico può essere stimato pari a 150 anni, se i seguenti criteri sono soddisfatti:

a) i componenti idraulici sono stati prodotti seguendo i principi di sicurezza base e quelli ben provati in accordo con le tabelle C.1 e C.2 della EN ISO 13849-2 per il progetto dei componenti idraulici (il criterio costruttivo applicato può essere inserito nel data sheet del componente);
b) il costruttore del componente specifica le applicazioni appropriate e le condizioni di funzionamento del componente; il progettista della SRP/CS fornisce le informazioni che gli competono per ciò che riguarda l'applicazione dei principi di sicurezza base e di quelli ben provati in accordo con le tabelle C.1 e C.2 della EN ISO 13849-2 per l'applicazione e il funzionamento del componente.

Se i precedenti criteri sono soddisfatti il $MTTF_D$ del componente idraulico può essere stimato pari a 150 anni. Se il numero medio di operazioni l'anno (n_{op}) è inferiore a 1 000 000, allora il $MTTF_D$ può essere stimato di valore superiore a 150 anni, secondo le indicazioni della tabella 11.
Ma se almeno uno dei due criteri a) o b) precedenti non è soddisfatto allora il valore più corretto per la stima del $MTTF_D$ deve essere fornito dal costruttore. Anche per i componenti idraulici si può far uso della formula che lega il B_{10D} al $MTTF_D$ del paragrafo 2.3.1 relativa ai componenti pneumatici, meccanici ed elettromeccanici.

2.3. $MTTF_D$ dei componenti pneumatici, meccanici ed elettromeccanici

Per i componenti pneumatici, meccanici ed elettromeccanici (valvole pneumatiche, relè, contattori, interruttori di posizione, dispositivi a camme per gli interruttori di posizione, ecc.) può risultare difficile stimare il valore di $MTTF_D$. La maggior parte delle volte il costruttore fornisce solo il numero di cicli in corrispondenza dei quali il 10% dei componenti presenta dei guasti pericolosi (B_{10D}) essendo tali componenti soggetti a usura e non a guasto casuale. Nel paragrafo 2.3.1 seguente è riportato un semplice metodo che consente di stimare il valore di $MTTF_D$ utilizzando il B_{10D} o il tempo di vita del componente T_{10D}.

TABELLA 11: NORME INTERNAZIONALI CHE TRATTANO IL $MTTF_D$ O IL B_{10D} DEI COMPONENTI

	Principi di sicurezza base e ben provati secondo la EN ISO 13849-2	**Norme di interesse**	**Tipici $MTTF_D$ (anni) Tipici B_{10D} (cicli)**
Componenti meccanici	Tabelle A.1 e A.2	–	$MTTF_D$ = 150
Componenti idraulici con $n_{op} \geq 1\,000\,000$	Tabelle C.1 e C.2	ISO 4413	$MTTF_D$ = 150
Componenti idraulici con $500\,000 \leq n_{op} < 1\,000\,000$	Tabelle C.1 e C.2	ISO 4413	$MTTF_D$ = 300
Componenti idraulici con $250\,000 \leq n_{op} < 500\,000$	Tabelle C.1 e C.2	ISO 4413	$MTTF_D$ = 600
Componenti idraulici con con $n_{op} < 250\,000$	Tabelle C.1 e C.2	ISO 4413	$MTTF_D$ = 1200
Componenti pneumatici	Tabelle B.1 e B.2	ISO 4414	B_{10D} = 20 000 000
Relè e interruttori di manovra con carico piccolo	Tabelle D.1 e D.2	EN 50205 IEC 61810 IEC60947	B_{10D} = 20 000 000
Relè e interruttori di manovra con carico nominale	Tabelle D.1 e D.2	EN 50205 IEC 61810 IEC 60947	B_{10D} = 400 000
Interruttori di prossimità con carico piccolo	Tabelle D.1 e D.2	IEC 60947 ISO 14119	B_{10D} = 20 000 000
Interruttori di prossimità con carico nominale	Tabelle D.1 e D.2	IEC 60947 ISO 14119	B_{10D} = 400 000
Contattori con carico piccolo	Tabelle D.1 e D.2	IEC 60947	B_{10D} = 20 000 000
Contattori con carico nominale	Tabelle D.1 e D.2	IEC 60947	B_{10D} = 1 300 000 (B_{10D}= 2 × B_{10})
Interruttori di posizione [a]	Tabelle D.1 e D.2	IEC 60947 ISO 14119	B_{10D} = 20 000 000
Interruttori di posizione [a] (con attuatori separati, bloccaggio dei ripari	Tabelle D.1 e D.2	IEC 60947 ISO 14119	B_{10D} = 2 000 000
Arresto di emergenza [a]	Tabelle D.1 e D.2	IEC 60947 ISO 13850	B_{10D} = 100 000
Pulsanti [a]	Tabelle D.1 e D.2	IEC 60947	B_{10D} = 100 000

Il B_{10D} è stimato essere pari a due volte il B_{10} (50% di guasti pericolosi) se non si hanno altre informazioni.

I termini “carico ridotto” e “carico nominale” sono riferiti ai principi di sicurezza descritti nella EN ISO 13849-2 (ad es.: al sovradimensionamento della corrente nominale), ad esempio “carico ridotto” significa il 20% del carico nominale.

Gli stop di emergenza (IEC 60947-5-5 e ISO 13850) e i pulsanti (IEC 60947-5-8) possono essere considerati sottosistemi di Categoria 1 o di Categoria 3 o 4 a seconda del numero di contatti elettrici in uscita e della rilevazione dei guasti messa in atto nella SRP/CS. Ogni contatto (inclusi gli attuatori meccanici) può essere considerato come un canale con un valore di B_{10D}. Per i dispositivi (switch, pulsanti) di abilitazione (enabling) (IEC 60947-5-8) ciò significa che la sospensione della funzione si ottiene premendo o rilasciando lo stesso. In alcuni casi il costruttore della macchina può applicare l’esclusione dei guasti in accordo con la tabella D.8 della EN ISO 13849-2, in base alla specifica applicazione e alle condizioni ambientali.

[a] Se è possibile l’esclusione dei guasti per l’adozione del principio di azione diretta

Il valore di $MTTF_D$ di un componente pneumatico, meccanico ed elettromeccanico può essere stimato col metodo descritto in 2.3.1, se i seguenti criteri sono soddisfatti:

a) i componenti sono stati prodotti seguendo i principi di sicurezza base in accordo con le tabelle A.1, B.1 o D.1 della EN ISO 13849-2 per il progetto di tali componenti (il criterio costruttivo applicato può essere inserito nel data sheet del componente);
b) i componenti per le Categorie 1, 2, 3 o 4 sono stati realizzati seguendo i principi di sicurezza ben provati secondo le tabelle A.2, B.2 o D.2 della EN ISO 13849-2 il criterio costruttivo applicato può essere inserito nel data sheet del componente);
c) il costruttore del componente specifica le applicazioni appropriate e le condizioni di funzionamento del componente; il progettista della SRP/CS fornisce le informazioni che gli competono per ciò che riguarda l'applicazione dei principi di sicurezza base in accordo con le tabelle B.1 o D.1 della EN ISO 13849-2 per l'applicazione e il funzionamento del componente; per le Categorie 1, 2, 3 o 4, l'utilizzatore deve essere informato delle sue responsabilità nel soddisfacimento dei principi di sicurezza ben provati in accordo con le tabelle B.2 o D.2 della ISO 13849-2 per l'applicazione e il funzionamento del componente.

2.3.1. Calcolo del $MTTF_D$ di un componente dal B_{10}

Il numero di cicli in corrispondenza dei quali il 10% dei componenti presenta dei guasti pericolosi (B_{10D}) dovrebbe essere stimato dal costruttore, sulla base delle prove contenute nelle norme applicabili. I guasti pericolosi del componente devono essere identificati a partire da tutti i guasti possibili dello stesso.
Se durante le prove non tutti i componenti si sono guastati pericolosamente, allora deve essere condotta un'analisi dello stato dei componenti che tenga conto anche dei componenti che non presentano guasti pericolosi.
Se il valore B_{10D} non è dato esplicitamente (dal costruttore del componente) ma è fornito solo il numero di cicli in corrispondenza dei quali il 10% dei componenti presenta un guasto qualsiasi (B_{10}), allora, sono necessarie ulteriori informazioni per risalire al valore di B_{10D}. Nella EN ISO 13849-1, in mancanza di FMEA è fatta l'assunzione che la frazione dei guasti pericolosi sia il 50% del totale. Ciò significa che il numero di cicli al termine dei quali il 10% dei componenti presenterà un guasto pericoloso è il doppio del numero di quelli relativi al B_{10}. Pertanto, la norma EN ISO 13849-1 propone $B_{10D} = 2 \times B_{10}$ come valore raccomandato per tale parametro.

Il valore del $MTTF_D$ può essere determinato grazie ai due parametri B_{10D} e n_{op}, quest'ultimo individua il numero medio di operazioni l'anno effettuate dal componente. La relazione da utilizzare è la seguente:

$$\mathrm{MTTF_D} = \frac{B_{10\mathrm{D}}}{0{,}1 \times n_{\mathrm{op}}}$$

dove

n_{op} = numero medio di operazioni l'anno effettuate da un componente, con $n_{\mathrm{op}} = \frac{d_{\mathrm{op}} \times h_{\mathrm{op}} \times 3600}{t_{\mathrm{cycle}}}$,

d_{op} = numero medio di giorni di lavoro per anno,
h_{op} = durata media di una giornata di lavoro, in ore al giorno,
t_{cycle} = tempo medio tra l'inizio di due cicli di lavoro successivi di un componente, in secondi per ciclo.

Alla formula data per il calcolo del $MTTF_D$ si arriva ragionando nel modo seguente. Il tempo operativo di un componente è limitato dal valore di T_{10D}, il tempo medio in corrispondenza del quale il 10% di tali componenti presenta un guasto pericoloso. Tale tempo è legato al numero di cicli B_{10D} dalla seguente formula:

$$T_{10\mathrm{D}} = \frac{B_{10\mathrm{D}}}{n_{\mathrm{op}}}$$

La EN ISO 13849-1 assume, in prima approssimazione, che la funzione di distribuzione dei guasti sia di tipo esponenziale, ovvero:

$$F(t) = 1 - \mathrm{e}^{(-\lambda_D t)}$$

dove λ_D è il tasso di guasto.
Nel caso in cui si sostituiscano in tale espressione i seguenti valori: $t = T_{10D}$ e $F(T_{10D})$=10%, e si espliciti il tasso di guasto λ_D, si trova che questo può essere approssimato con la seguente relazione:

$$\lambda_D = -\frac{\ln 0{,}9}{T_{10D}} \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 \times n_{op}}{B_{10D}}$$

Nel caso di distribuzioni di tipo esponenziale è possibile dimostrare che $MTTF_D = 1/\lambda_D$ e quindi si ottiene la formula per il calcolo del valore di $MTTF_D$ in funzione del B_{10D} e di n_{op} presentata in precedenza (si consiglia di esprimere i valori dei parametri delle formule con le unità di misura corrette, per evitare errori).

2.4. $MTTF_D$ dei componenti elettrici

La EN ISO 13849-1 fornisce una serie di tipici valori medi per il $MTTF_D$ di componenti elettronici, estratti dal database delle SN 29500. I valori riportati sono di tipo generico. Se il progettista della SRP/CS ha a disposizione altri dati specifici e affidabili per un dato componente, è altamente raccomandabile che usi tali dati al posto di quelli generici.
I valori forniti nelle tabelle da 12 a 17 si assumono validi alla temperatura di 40°C, per componenti sottoposti a corrente e tensione nominali.
Nelle tabelle sono riportate la colonna dei valori del MTTF e quella dei valori del $MTTF_D$. Questo perché nelle SN 29500 sono riportati i valori di MTTF validi per tutti i possibili malfunzionamenti, senza fare distinzioni per quelli pericolosi. Infatti, non tutti i malfunzionamenti sono malfunzionamenti pericolosi.
La pericolosità o meno dipende dall'applicazione del componente.
Un modo per determinare il tipico $MTTF_D$ di un componente è quello di condurre una FMEA.
Non potendo condurre una FMEA è stato assunto che solo il 50% dei malfunzionamenti fosse pericoloso, ciò significa che nella colonna del $MTTF_D$ è stato preso il doppio del valore presente nella colonna del MTTF, e nell'ultima colonna (relativa alle osservazioni) si è voluto ricordare che i valori sono relativi a una frazione del 50% di malfunzionamenti pericolosi.

2.4.1. Semiconduttori

TABELLA 12: TRANSISTORI (USATI COME INTERRUTTORI)

Transistor	Esempio	MTTF (anni)	$MTTF_D$ (anni)	Malfunzionamenti pericolosi
Bipolare	TO18, TO92, SOT23	38052	76104	50%
Bipolare bassa potenza	TO5, TO39	5708	11416	50%
Bipolare alta potenza	TO3, TO220, D-Pack	1903	3806	50%
FET	Junction MOS	22831	45662	50%
MOS alta potenza	TO3, TO220, D-Pack	1903	3806	50%

TABELLA 13: DIODI, SEMICONDUTTORI DI POTENZA E CIRCUITI INTEGRATI

Diodo	Esempio	MTTF (anni)	$MTTF_D$ (anni)	Malfunzionamenti pericolosi
Per usi generali	–	114155	228311	50%
Soppressore	–	16308	32616	50%
Zener P_{tot} < 1 W	–	114155	228311	50%
Raddrizzatore	–	57078	114155	50%
Ponte raddrizzatore	–	11415	22831	50%
Tiristore	–	2283	4566	50%
Triac, Diac	–	1522	3044	50%
Circuiti integrati (programmabili e non)	Utilizzare i dati del costruttore			50%

2.4.2. Componenti passivi

TABELLA 14: CAPACITÀ

Capacità	Esempio	MTTF (anni)	$MTTF_D$ (anni)	Malfunzionamenti pericolosi
Standard senza potenza	KS, KP, KC, KT, MKT, MKC, MKP, MKU, MP, MKV	57078	114155	50%
Ceramica	–	22831	45662	50%
Elettrolitico di alluminio	Elettrolita non solido	22831	45662	50%
Elettrolitico di alluminio	Elettrolita solido	38052	76104	50%
Elettrolitico di tantalio	Elettrolita non solido	11415	22831	50%
Elettrolitico di tantalio	Elettrolita solido	114155	228311	50%

TABELLA 15: RESISTENZE

Resistenza	Esempio	MTTF (anni)	$MTTF_D$ (anni)	Malfunzionamenti pericolosi
A film di carbone	–	114155	228311	50%
A film metallico	–	570776	1141552	50%
A metallo-ossido e a filo	–	22831	45662	50%
Variabile	–	3805	7618	50%

TABELLA 16: INDUTTORI

Induttore	Esempio	MTTF (anni)	$MTTF_D$ (anni)	Malfunzionamenti pericolosi
Per applicazioni MC	–	38052	76104	50%
Induttori e trasformatori per bassa frequenza	–	22831	45662	50%
Trasformatori per alimentatori, trasformatori switched mode	–	11415	22831	50%

TABELLA 17: OPTO-ACCOPPIATORI

Opto-accoppiatore	Esempio	MTTF (anni)	$MTTF_D$ (anni)	Malfunzionamenti pericolosi
Stadio di uscita con transistor bipolare	SFH 610	7610	15220	50%
Stadio di uscita a FET	LH 1056	2854	5708	50%

3. I requisiti di sicurezza del software secondo la EN ISO 13849-1

3.1. Introduzione

Il software di sicurezza di una SRP/CS costituisce, per la tipologia dei requisiti previsti e le misure contro i guasti sistematici, uno degli aspetti qualitativi del PL. La EN ISO 13849-1 tratta l'argomento indicando:

- il ciclo di vita del software (il cosiddetto "V-model");
- i requisiti per il software di sistema (Embedded software "SRESW");
- i requisiti per il software applicativo (Application software "SRASW");
- i requisiti per la parametrizzazione tramite software.

A causa della trattazione molto concisa e particolarmente specialistica, questa parte della norma risulta non sufficientemente completa e non facilmente applicabile da parte dell'utente. Comunque, non era intenzione del normatore approfondire l'argomento in maniera dettagliata, in quanto una trattazione approfondita era già contenuta nella IEC 61508, tuttavia il richiamo ha lo scopo di calare i requisiti base anche all'interno della struttura della EN ISO 13849-1. Ciò è stato ritenuto necessario perché la IEC 61508 tratta il software in maniera specifica nella parte 3 e in maniera diffusa nelle altre parti, per cui, senza il richiamo, sarebbero stati necessari una lettura e uno studio globale della IEC 61508 per avere una visione completa ed esaustiva dell'argomento.
I requisiti per il software contenuti nella EN ISO 13849-1 dipendono strettamente dal PL richiesto.

3.2. Il ciclo di vita del software

Lo scopo principale da perseguire durante la stesura del software è quello di realizzare un prodotto che sia leggibile, comprensibile, testabile e manutenibile. Il V-model semplificato (figura 11), concepito per questo obiettivo, presenta sette fasi. I risultati di uscita di ciascuna fase sono utilizzati come ingressi dalle fasi successive. Il ramo a sinistra rappresenta le fasi di progettazione, mentre il ramo a destra rappresenta le fasi di prova (test).

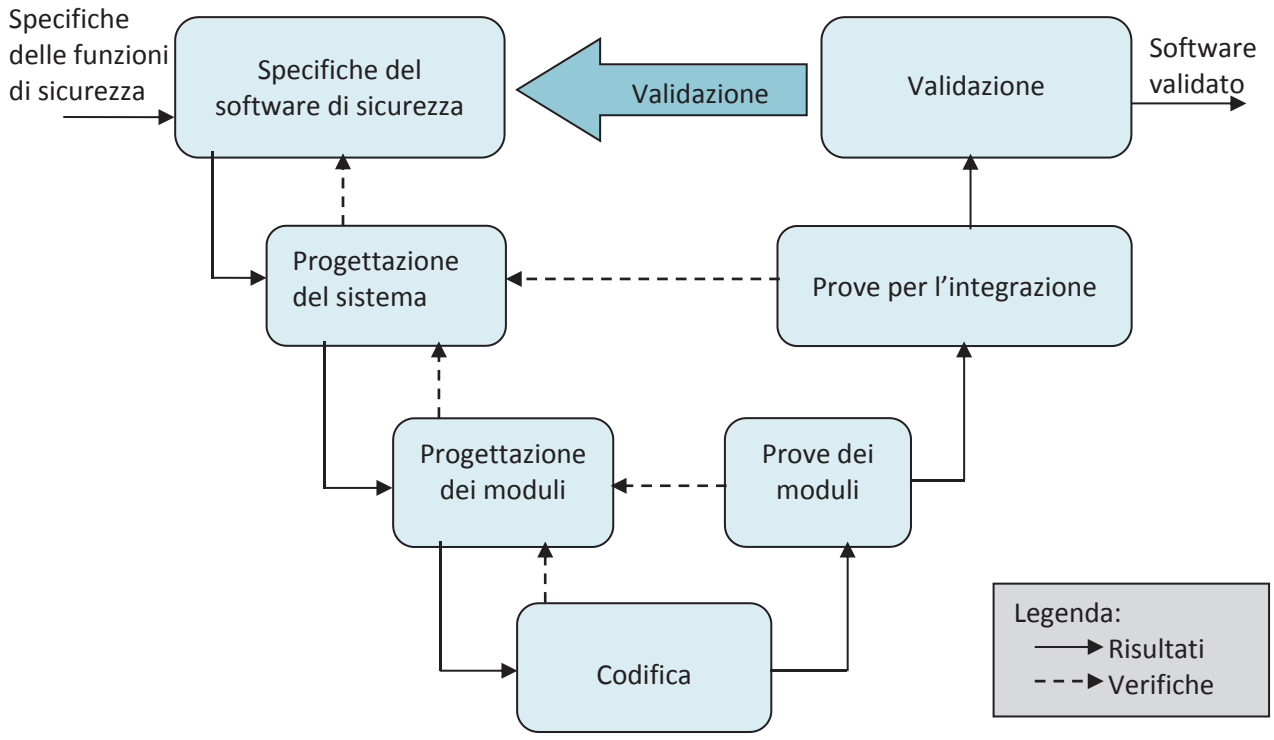


Fig. 11: V-model (semplificato) del ciclo di vita del software

Ogni fase deve terminare con un documento formale approvato dalla struttura che ha realizzato il progetto.
Nella tabella 18 sono indicati alcuni documenti da produrre durante l'applicazione del V-model.
I rami tratteggiati rappresentano verifiche eseguite dalla fase che emette la freccia sulla fase che la riceve (ad esempio durante la fase delle prove dei moduli si esegue contestualmente una verifica di quanto è stato fatto durante la fase di progettazione dei moduli stessi e durante la fase delle prove per l'integrazione si esegue contestualmente una verifica di quanto è stato fatto durante la fase di progettazione del sistema, inoltre durante ogni fase di progettazione si esegue una verifica sul soddisfacimento delle specifiche del modulo precedente).
La freccia spessa è una speciale verifica volta ad accertare che il software realizzato (attraverso le fasi colorate in celeste) verifichi le specifiche del software di sicurezza (derivate dalle specifiche delle funzioni di sicurezza).
Il software necessario all'esecuzione di ciascuna funzione di sicurezza è scomposto in parti (costituite da un programma che esegue blocchi funzionali) che servono al funzionamento dei singoli moduli.

TAB. 18 – LISTA NON ESAUSTIVA DI DOCUMENTI RELATIVI AL V-MODEL

Documenti
Specifiche delle funzioni di sicurezza;
Schema della macchina o dell'insieme;
Progetto del sistema di controllo (funzioni, modi operativi);
Specifiche del software di sicurezza,
Schema circuitale (hardware – Figura 12);
Lista dei segnali di Input e Output;
Indicazioni guida per il codice;
Architettura del programma di sicurezza;
Architettura del programma non di sicurezza,
Architettura dei moduli del programma (funzioni, segnali, indirizzi),
Schema del programma;
Codice;
Protocollo di verifica;
Protocollo di revisione del codice;
Protocollo di validazione del software.

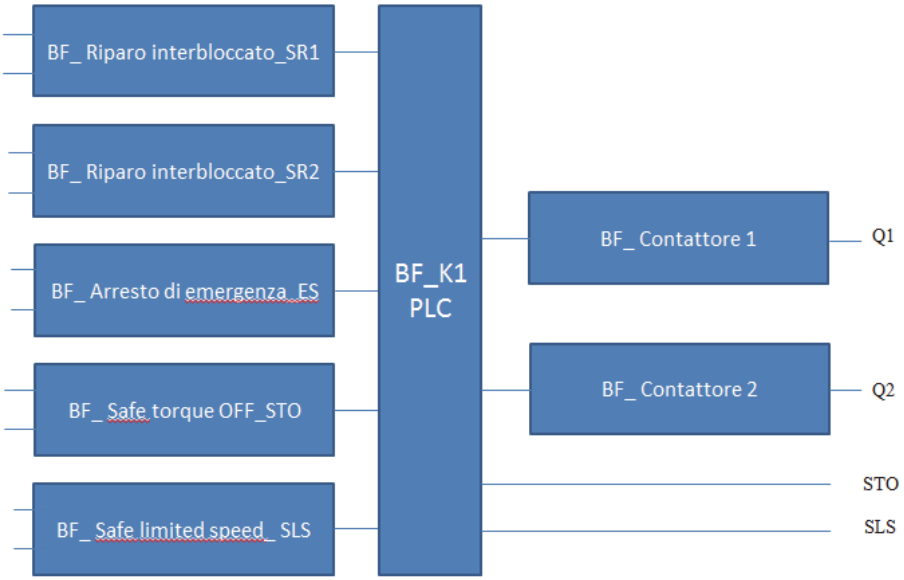


Fig. 12: Esempio di schema circuitale

3.3. Regole di programmazione

Un software per applicazioni di sicurezza deve seguire regole che lo rendano univocamente identificabile e tracciabile, in modo da evitare errori e malfunzionamenti.
Ai fini dell'identificazione e della tracciabilità devono essere definiti:
- l'autore;
- la versione;
- la data;
- l'ultimo accesso effettuato per modifiche.

Le regole per la stesura del software si differenziano a livello di:
- struttura del programma;
- scelta delle variabili;
- blocchi funzionali.

3.3.1. Struttura del programma
Il software deve essere sequenziale, coerente e comprensibile.
A tale scopo sono di seguito indicate alcune regole da seguire:
- i blocchi di funzione devono essere di dimensioni ridotte;
- il programma deve essere suddiviso in sezioni o parti in modo da separare gli ingressi, l'elaborazione/processo dei dati, le uscite;
- ogni blocco deve essere descritto e commentato;
- la programmazione deve essere "strutturata";
- le aree di memoria utilizzate devono essere specificate e descritte;
- le variabili devono essere identificate nel tipo e univoche.

3.3.2. Le variabili del programma
Le variabili devono essere gestite in modo da non compromettere la funzionalità del programma.
Alcuni criteri di utilizzazione sono i seguenti:
- far apparire solo una volta nel programma l'ON e l'OFF di un segnale di uscita (output);
- usare simboli espliciti per individuare le variabili;
- gestire da una sola posizione nel programma l'aggiornamento delle variabili.

Altri criteri di questo tipo che rendono univoche e definite le scelte, evitando rimandi e loop, consentono di dare al programma linearità, sequenzialità, chiarezza e leggibilità e al tempo stesso di evitare errori e malfunzionamenti.

3.3.3. I blocchi funzionali
Sul mercato sono disponibili blocchi funzionali validati e certificati dal fabbricante per diverse esigenze [ad esempio STO (safe torque off), SS1 (safe stop 1), SS2 (safe stop 2), SLS (safe limited speed)].
Utilizzare blocchi funzionali certificati da un fabbricante è certamente utile, occorre però accertarsi che le condizioni operative corrispondano a quelle indicate dal fabbricante.
In particolare, alcune regole di cui si suggerisce l'applicazione sono:
- utilizzare blocchi di dimensioni ridotte in termini di ingresso e uscita, ad esempio al massimo 8 ingressi booleani, 2 numerici e una sola uscita;
- limitare a 10 le variabili numeriche e a 20 quelle booleane;
- le variabili numeriche e booleane devono essere inizializzate prima di essere usate per la prima volta;
- le variabili globali non devono essere modificate dai blocchi funzionali;
- evitare incongruenze nei blocchi in cui sono contenute le definizioni delle variabili;
- identificare i guasti nei blocchi, definire con commenti quelli rilevati e lo stato del blocco (il ripristino o l'azzeramento del blocco devono essere commentati).

3.4. Il software di sistema (SRESW - *safety-related embedded software*)

Il software di sistema (SRESW) è quella parte del software di un sistema elettronico programmabile relativo al funzionamento del dispositivo elettronico stesso e ai servizi da esso forniti. Costituisce parte integrante del sistema fornito dal fabbricante e l'utilizzatore non vi ha alcun accesso.
La EN ISO 13849-1 distingue le misure da applicare al software di sistema in misure di base comuni (tabella 19.a), da applicare fino a PL_r = "d", e in misure addizionali per PL_r = "c" e PL_r = "d" (tabella 19.b).
Per PL_r = "e" occorre applicare la norma IEC 61508 parte 3ª, paragrafo 7 a meno che non si applichi per il software dei due canali (categoria 3 e 4) il criterio della diversità nella definizione delle specifiche, nella progettazione e nella codifica, nel qual caso sono sufficienti le misure addizionali di cui sopra (fig. 13). Ciò perché l'applicazione del criterio della diversità fa presumere una riduzione della probabilità di guasti sistematici, che consente, in fase di verifica o validazione, di applicare solo una revisione della struttura del software invece del controllo di ogni linea del codice.

TAB. 19.a: MISURE DI BASE PER IL SRESW

Misure di base (per PL_r = "a", PL_r = "b", PL_r = "c", PL_r = "d")
Ciclo di vita del software (V-model), con verifiche e validazione;
Documentazione: specifiche e progetto;
Progetto e codifica modulare e strutturata;
Controllo dei guasti sistematici;
Verifica di corretta implementazione, se il software è usato per il controllo dei guasti hardware;
Prove funzionali, ad es."black box testing";
Dopo eventuali modifiche, rielaborazione delle fasi del V-model applicabili.

TAB. 19.b: MISURE ADDIZIONALI PER IL SRESW

Misure di addizionali (per PL_r = "c", PL_r = "d")
Sistema di gestione del progetto e della qualità confrontabile con IEC 61508 o ISO 9001;
Documentazione di tutte le attività rilevanti durante il ciclo del software;
Gestione della configurazione per identificare tutte le caratteristiche e i documenti della versione;
Specifica strutturata con requisiti di sicurezza e progetto;
Impiego di linguaggi e tool idonei di cui si abbia competenza nell'uso;
Programmazione modulare e strutturata, separazione dal software non di sicurezza, dimensioni limitate dei moduli con interfacce completamente definite, uso di progettazione e codifica standard;
Verifica del codice (tramite "walk-through" o revisione con analisi del flusso);
Prove funzionali estese, ad es. "grey box testing", prove di prestazione o simulazioni;
Dopo eventuali modifiche, analisi dell'impatto e rielaborazione delle fasi del V-model applicabili.

L'Amendment del 2016 della norma EN ISO 13849-1 tratta il caso di componenti per i quali non siano rispettati i requisiti richiesti per il SRESW, quali per esempio PLC, inverter, sensori non espressamente destinati ad applicazioni di sicurezza.
Per tali componenti è consentito l'uso se (figura 14):

- la SRP/CS ha un PL_r = "a" o un PL_r = "b" e la sua struttura è in Categoria B, 2 o 3
- la SRP/CS ha un PL_r = "c" o un PL_r = "d" e può usare più componenti per i due canali nelle Categorie 2 o 3. I componenti dei due canali devono utilizzare tecnologie diverse.

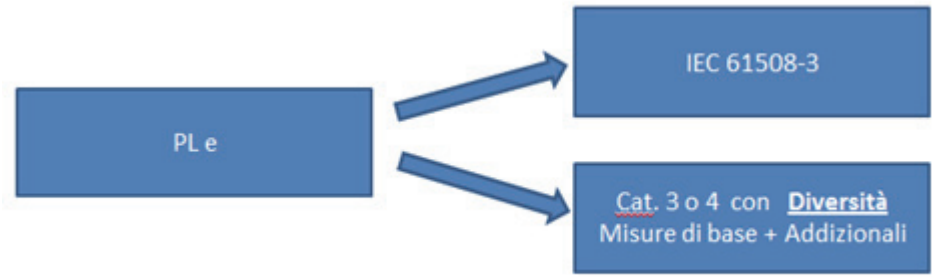


Fig. 13: Misure per SRESW in PL = "e"

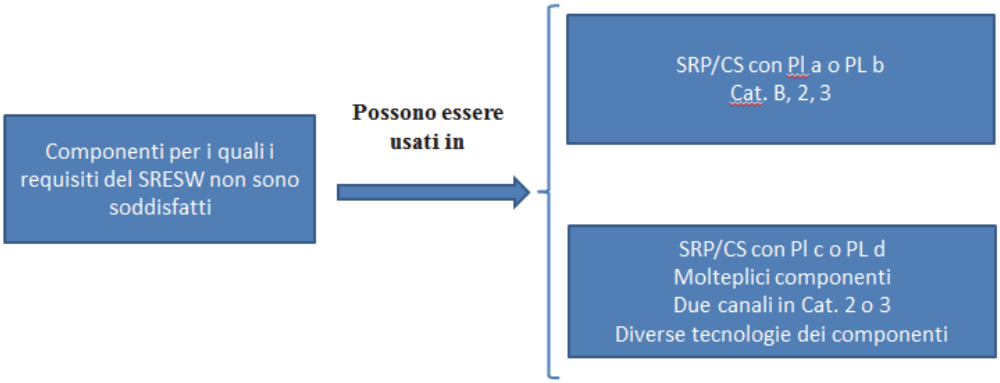


Fig. 14: Impiego di componenti non di sicurezza

3.5. Il software applicativo (SRASW - *Safety-Related Application Software)*

Il software applicativo SRAWS è quella parte del software di un sistema elettronico programmabile che riguarda le funzioni che assolvono un compito specifico relativo alla sicurezza della macchina.
Il software applicativo può essere scritto con linguaggi LVL (*low variability languages*) oppure FVL (*full variability languages*). I linguaggi LVL sono tipicamente utilizzati dai PLC e offrono la possibilità di utilizzare librerie di funzioni predefinite per realizzare le specifiche dei requisiti di sicurezza.
Alcuni esempi di LVL (ad es. *function block diagram, ladder logic*) sono definiti nella norma IEC 61131-3.
I linguaggi FVL permettono di realizzare una vasta tipologia di funzioni e applicazioni, [tipici esempi sono: l'Assembler (basso livello) ma anche il C ed il C++ (medio livello)]. Nel settore delle macchine i linguaggi FVL si trovano nel software di sistema e più raramente nel software applicativo.
Nel caso si utilizzi un linguaggio FVL per il software applicativo allora si applicano gli stessi requisiti indicati per il software di sistema (vedi paragrafo precedente) con la possibilità di soddisfare PL da "a" fino a "e".
La EN ISO 13849-1 distingue le misure da applicare al software applicativo in misure di base comuni (tabella 20.a), da applicare fino a PL_r = "e", e in misure addizionali per PL_r = "c", PL_r = "d" e PL_r = "e" (tabella 20.b).
Le misure addizionali sono in parte richieste in parte raccomandate e dovrebbero essere applicate con efficacia crescente al crescere del PL richiesto.
Non è chiaro come tale efficacia crescente vada gestita, sarebbe ragionevole che ciò sia indicato nella norma stessa quando propone o raccomanda per un certo PL una misura piuttosto che un'altra.

TAB. 20.a: MISURE DI BASE PER IL SRASW

Misure di base (per PL_r = “a”, PL_r = “b”, PL_r = “c”, PL_r = ”d”, PL_r = “e”)
Ciclo di vita del software con verifiche e validazione;
Documentazione: specifiche e progetto;
Progetto e codifica modulare e strutturata;
Prove funzionali;
Dopo eventuali modifiche, rielaborazione delle fasi del V-model applicabili.

TAB. 20.b: MISURE ADDIZIONALI PER IL SRASW

Misure di addizionali (per PL_r = “c”, PL_r = ”d”, PL_r = “e”)
Revisione delle specifiche del software di sicurezza, da rendere disponibili a chiunque fa parte del gruppo di lavoro incaricato del ciclo di vita del software. Le specifiche devono contenere: a) le funzioni di sicurezza col PL_r e i modi operativi associati; b) i criteri di prestazione, ad es. i tempi di reazione; c) l’architettura hardware con i segnali d’interfaccia; d) la rilevazione e il controllo dei guasti.
Scelta di tool idonei: a) devono rilevare situazioni che possono causare guasti sistematici, effettuando verifiche anche durante la compilazione e non solo durante il funzionamento della macchina; b) devono sostenere le strutture del linguaggio e le linee guida della codifica o almeno guidare o supervisionare l’utente; c) se il PL_r = “e” è raggiunto con un unico componente e il suo tool, allora il tool deve essere conforme alla norma tecnica pertinente; se sono usati due diversi componenti con tool diversi, allora è sufficiente la competenza nell’uso
Scelta di librerie idonee: a) Se ragionevolmente possibile scegliere blocchi di funzione (FB) validati, ad es. librerie di software di sicurezza provenienti dal fornitore del tool (altamente raccomandate per PL_r = “e”) o librerie per applicazioni specifiche conformi alla ISO 13849-1.
Scelta di linguaggi idonei: a) Si raccomanda caldamente di usare un sottoinsieme del linguaggio LVL (*function block diagram, ladder logic*) idoneo per la programmazione modulare
La progettazione del software dovrebbe consistere di: a) metodi semi-formali per controllo dati e flusso, es. diagramma di stato o flow chart del programma; b) programmazione modulare e strutturata (con librerie di blocchi di funzione validati); c) blocchi di funzione di dimensioni ridotte; d) esecuzione del codice, in ogni blocco funzionale, con un solo punto di ingresso e uno solo d’uscita; e) architettura del programma a tre livelli: ingresso dei dati, elaborazione, uscita; f) assegnazione dell’uscita di sicurezza in una sola posizione nel programma; g) utilizzo di tecniche per rilevare i guasti e per portare il sistema in uno stato sicuro durante l’ingresso dei dati, l’elaborazione, l’uscita (programmazione difensiva).
Quando il software SRAWS si trova combinato col software NON SRASW in un componente: a) software SRAWS e NON SRAWS devono essere codificati in blocchi funzionali diversi con collegamenti dati ben definiti; b) dati relativi alla sicurezza non devono essere combinati con quelli non di sicurezza.
Codifica del software: a) Il codice deve essere leggibile, comprensibile, testabile (ad es. usare variabili simboliche); b) devono essere usate linee guida accettate e giustificate per la codifica; c) dovrebbero essere usate le verifiche per l’integrità dei dati e i test di plausibilità disponibili nell’application layer (programmazione difensiva); d) il codice dovrebbe essere testato con simulazioni; e) per i PL_r =”d” o PL_r = “e” dovrebbero essere condotte verifiche con il controllo e l’analisi del flusso di dati.

TAB. 20.b: MISURE ADDIZIONALI PER IL SRASW (PROSECUZIONE)

Misure di addizionali (per PL_r = “c”, PL_r = ”d”, PL_r = “e”)
Testing: a) condurre “black box testing” della funzionalità e delle prestazioni (ad es. “timing performance”); b) per i PL_r =”d” o PL_r = “e” sono raccomandati dei test di esecuzione con valori limite dei parametri; c) raccomandata di pianificare i test includendo i criteri per la completezza e i tool da utilizzare; d) l’effettuazione di test di I/O garantisce che il SRASW usi correttamente i segnali relativi alla sicurezza.
Documentazione: a) tutte le attività di vita e le modifiche del software devono essere documentate; b) la documentazione deve essere completa, disponibile, leggibile e comprensibile; c) la documentazione del codice deve contenere l’intestazione dei moduli con le informazioni legali, la descrizione del funzionamento del modulo e le informazioni di I/O, la versione del programma e delle librerie usate, commenti e spiegazioni in quantità sufficiente.
Verifiche (ad es. revisioni, ispezioni): a) sono necessarie solo per il software scritto appositamente per una data applicazione e non per le librerie certificate.
Gestione della configurazione: a) devono essere definite procedure opportune per l’identificazione e l’archiviazione della documentazione per ogni versione del software SRASW.
Modifiche: a) dopo eventuali modifiche effettuare analisi dell’impatto sul soddisfacimento delle specifiche e rielaborazione delle fasi del V-model applicabili; b) controllo dei diritti di accesso; c) documentazione storica delle modifiche.

Le misure addizionali possono essere messe in atto con efficienza crescente con il PL_r (efficienza bassa se il PL_r = “c”, efficienza media se il PL_r = “d”, efficienza alta se il PL_r = “e”).

3.6. La parametrizzazione tramite software

La parametrizzazione serve a configurare e gestire le funzioni e i parametri caratteristici dei diversi dispositivi, come sensori e attuatori, nonché a variare la risposta della SRP/CS a seconda di valori preimpostati.
La parametrizzazione tramite software rientra tra gli aspetti di sicurezza della SRP/CS, e come tale deve essere inclusa nella specifica dei requisiti di sicurezza del software.
Tale parametrizzazione può essere effettuata impiegando tool software dedicati messi a disposizione dal fornitore della SRP/CS che soddisfano i requisiti della EN ISO 13849-1 (in particolare hanno un nome, una versione e prevengono modifiche non autorizzate ad es. tramite password).
Per fare in modo che sia mantenuta l’integrità dei dati utilizzati per la parametrizzazione, devono essere applicate le misure della tabella 21.

TAB. 21: MISURE PER L’INTEGRITÀ DEI DATI PARAMETRIZZATI TRAMITE SOFTWARE

Misure per l’integrità dei dati parametrizzati tramite software
Controllo degli intervalli di ingresso validi;
Controllo della corruzione dei dati prima della trasmissione;
Controllo degli effetti degli errori dovuti al processo di trasmissione dei parametri;
Controllo degli effetti della trasmissione incompleta dei parametri;
Controllo degli effetti dei guasti hardware e degli errori software del tool usato per la parametrizzazione.

È possibile utilizzare una procedura alternativa per stabilire i valori dei parametri di sicurezza. Tale procedura prevede la conferma dei parametri in ingresso alla SRP/CS per mezzo di:

- ritrasmissione dei parametri modificati al tool di parametrizzazione, oppure
- altri mezzi opportuni per confermare l'integrità dei parametri;
- conferma a posteriori, da parte di una persona addestrata, per mezzo di un tool di parametrizzazione.

L'ultima possibilità è utile quando la parametrizzazione è stata effettuata con dispositivi non specificamente dedicati allo scopo (e quindi non dotati di tool di controllo), ma ad es. con normali personal computer, e quindi un controllo, dopo l'inserimento dei parametri e prima delle operazioni della macchina, per verificare che tutto sia in ordine, è utile per la sicurezza.

I moduli software usati per la codifica/decodifica all'interno del processo di trasmissione/ritrasmissione e i moduli software usati per la visualizzazione dei parametri di sicurezza devono, come minimo, usare la diversità (nei blocchi funzionali), per evitare errori sistematici.
La documentazione della parametrizzazione tramite software deve indicare i dati usati (ad es. i valori predefiniti dei parametri), le informazioni necessarie per identificare i valori dei parametri che la SRP/CS sta usando, la persona che ha effettuato la parametrizzazione, la data di tale parametrizzazione e le altre informazioni importanti.

Le attività di verifica riportate in tabella 22 devono essere applicate alla parametrizzazione tramite software.

TAB. 22: VERIFICHE DA APPLICARE ALLA PARAMETRIZZAZIONE TRAMITE SOFTWARE

Verifiche da applicare alla parametrizzazione tramite software
Verifica della corretta impostazione dei parametri di sicurezza (valori minimo, massimo e valore tipico);
Verifica del fatto che è attuato il controllo della plausibilità dei parametri di sicurezza, ad es. utilizzando valori non validi;
Verifica del fatto che le modifiche non autorizzate dei parametri sono prevenute;
Verifica del fatto che i dati e i segnali di sicurezza sono generati e usati in modo tale che eventuali guasti non possano portare alla perdita della funzione di sicurezza (ciò è utile quando la parametrizzazione è stata effettuata con dispositivi non specificamente dedicati allo scopo).

4. Le principali innovazioni introdotte dall'Amendment del 2015

4.1. Introduzione

Nel 2015 è terminato il processo di Amendment che ha portato all'edizione del 2015 della norma EN ISO 13849-1. L'Amendment mira a migliorare la chiarezza e a semplificare l'applicazione della norma stessa. Per tale motivo i cambiamenti significativi sono pochi, mentre le correzioni e i miglioramenti minori sono più numerosi.
Nei Capitoli 1, 2 e 3 del presente documento le innovazioni e i cambiamenti sono stati già inseriti, tuttavia il presente capitolo ha lo scopo di sottolineare e rendere evidenti quelli più importanti.
I cambiamenti sono stati tutti ispirati dalla necessità di chiarire problemi sorti dall'applicazione della norma a casi reali. Non è necessario rivalutare le SRP/CS già realizzate con la norma nell'edizione precedente all'Amendment.

4.2. Cambiamenti nell'introduzione della EN ISO 13849-1

La tabella 1 dell'introduzione della EN ISO 13849-1 che indicava quando utilizzare la IEC 62061 e quando la EN ISO 13849-1 è stata sostituita con un rinvio al rapporto tecnico ISO/TR 23849 che descrive in dettaglio le differenze e quanto invece in comune tra le due norme.

4.3. Cambiamenti nello scopo della EN ISO 13849-1

È chiarito che la EN ISO 13849-1 si applica solo alle SRP/CS che hanno un'alta frequenza di domanda (*high demand mode*) o sono costruite per un uso continuo (*continuous mode*), cioè alle SRP/CS per le quali il modo di funzionamento è tale per cui la frequenza della richiesta di eseguire la funzione di sicurezza è almeno superiore a una volta l'anno.

4.4. Cambiamenti nelle definizioni della EN ISO 13849-1

È stata introdotta la sigla (PFH_D) per indicare la probabilità oraria media di guasti pericolosi (unità di misura è [1/h]). Inoltre, tutte le volte che compariva il pedice "d", è stato sostituito dal pedice "D".

4.5. Cambiamenti nella Sezione 4 della EN ISO 13849-1 relativi ai valori dei parametri

I sottosistemi della SRP/CS possono essere progettati utilizzando altri standard, grazie alla corrispondenza tra SIL e PL basata sui valori di probabilità oraria media di malfunzionamento pericoloso. Però ogni SRP/CS deve essere progettata utilizzando una sola norma (la EN ISO 13849-1, oppure la IEC 62061, oppure la IEC 61508), per evitare progettazioni inadeguate dovute a confusione dei requisiti. Una volta progettate, le SRP/CS, anche conformi a norme diverse, possono essere integrate tra loro al fine di realizzare un'unica funzione di sicurezza (come è spiegato nel paragrafo 6.3 della norma e anche nella ISO/TR 23849).

Per la Categoria 4 il limite del $MTTF_D$ per ciascun canale è stato portato a 2500 anni. Il limite superiore a 100 anni del $MTTF_D$ (che comunque continua a valere per le altre Categorie) è stato imposto per fare in modo che l'affidabilità di una SRP/CS non dipenda solo dall'affidabilità dei suoi componenti: per rendere la SRP/CS resistente ai malfunzionamenti sistematici e a quelli casuali dovrebbero essere adottate altre misure come la ridondanza e la copertura diagnostica elevata. Il limite di 100 anni (2500 anni per la Categoria 4) è relativo al canale nel suo insieme: i singoli componenti costituenti un canale possono avere valori più alti di $MTTF_D$. Inoltre, un limite più alto per la Categoria 4 permette, per tale Categoria, di avere un numero più alto di sottosistemi prima che il PL complessivo scenda da "e" a "d".

Alcuni cambiamenti riguardano in particolare le assunzioni alla base della Categoria 2:
- per la Categoria 2,
  - ⇒ tasso di richiesta ≤ (1/100) × tasso di test,
  - ⇒ oppure tasso di richiesta ≤ (1/25) × tasso di test, allora i valori del PFH_D della Categoria 2 della tabella K.1 della EN ISO 13849-1 moltiplicati per 1,1 possono essere utilizzati come stima nel caso peggiore,
  - ⇒ oppure la prova può essere eseguita immediatamente quando si ha la richiesta della funzione di sicurezza se il tempo complessivo per scoprire il guasto e portare la macchina in una condizione non pericolosa è inferiore al tempo necessario al raggiungimento del pericolo;
- per la Categoria 2 il $MTTF_D$ del canale di prova è maggiore della metà del $MTTF_D$ del canale funzionale;
- i calcoli dei valori di PFH_D della tabella K.1 della EN ISO 13849-1 sono basati sui seguenti valori di DC_{avg}: DC_{avg} = bassa (calcoli fatti con DC_{avg} = 60%); DC_{avg} = media (calcoli fatti con DC_{avg} = 90%); DC_{avg} = alta (calcoli fatti con DC_{avg} = 99%).

4.6. Introduzione nella Sezione 4 della EN ISO 13849-1 di una procedura semplificata per la stima del PL della parte di uscita di una SRP/CS

Se, per parti di uscita di SRP/CS costituite da componenti meccanici, idraulici o pneumatici (o loro combinazioni), non sono disponibili informazioni sull'affidabilità relativa a una data applicazione, il fabbricante della macchina può ancora ottenere una stima degli aspetti quantificabili del PL della parte di uscita senza avere informazioni sul $MTTF_D$, utilizzando una procedura semplificata che permette di ricavare il PL in funzione della Categoria, della DC_{avg} e delle misure contro le CCF.
Il metodo assume che, oltre ai principi di sicurezza ben provati, siano usati componenti ben provati, detti "well tried", (per le Categorie 1, 2, 3 e 4) o componenti provati in uso, detti "proven in use" (per le categorie 2, 3 e 4), dichiarati tali per la particolare applicazione dal costruttore del componente stesso.
I componenti provati in uso (*proven in use*) non erano nominati nella norma prima dell'introduzione di tale metodo e non devono essere confusi con i componenti ben provati. Sono componenti per cui deve valere una dimostrazione, basata sull'analisi dell'esperienza di funzionamento di un elemento in configurazione specifica, che la probabilità di guasti sistematici pericolosi sia bassa a sufficienza, in modo che ogni funzione di sicurezza che usa quell'elemento raggiunga il livello di prestazione richiesto (PL_r).

Il metodo è basato sulla tabella 10 del capitolo 1 del presente documento (a cui si rimanda) e mostra la relazione tra il PL raggiungibile e la Categoria della parte di uscita, in particolare:
- Il PL "a" o "b" può essere ottenuto facendo ricorso alla Categoria B.
- Il PL "c" può essere ottenuto facendo ricorso alla Categoria 1 o alla Categoria 2, se sono utilizzati componenti ben provati e principi di sicurezza ben provati. Per la Categoria 2 possono essere usati anche componenti provati in uso invece di componenti ben provati.
  Quando si utilizza una Categoria 1 per realizzare una funzione di sicurezza con un PL "c", il valore del T_{10D} dei componenti relativi alla sicurezza può essere determinato sulla base di dati del tipo "proven in use" forniti dal fabbricante della macchina.
  Il $MTTF_D$ del canale di prova della Categoria 2 deve essere almeno di 10 anni.
- Il PL "d" può essere ottenuto facendo ricorso alla Categoria 3, se sono utilizzati componenti ben provati o provati in uso e principi di sicurezza ben provati.
- Il PL "e" può essere ottenuto facendo ricorso alla Categoria 4, se sono utilizzati componenti ben provati o provati in uso e principi di sicurezza ben provati.

Nella realizzazione della funzione di sicurezza rispettivamente con le Categorie 2, 3 e 4 devono essere messe in atto misure per eliminare o controllare le CCF e deve essere adottata una copertura diagnostica sufficiente (DC_{avg} bassa o media per le Categorie 2 e 3 e DC_{avg} alta per la

Categoria 4). In tal caso la DC_{avg} è calcolata come media aritmetica dei valori di DC dei singoli componenti del canale funzionale.

4.7. Requisiti relativi al software di Sistema (SRESW) quando sono utilizzati componenti standard

Per la realizzazione di una SRP/CS possono essere utilizzati componenti standard (ad es.: PLC, convertitori di frequenza, sensori) dotati di un proprio software di sistema.
I requisiti richiesti dalla EN ISO 13849-1 per il software di sistema non sono di solito confermati dai costruttori di componenti standard. A causa di ciò gli integratori hanno avuto nel passato difficoltà nell'uso di simili componenti.
Pertanto è stata aggiunta una semplificazione che dispensa dalla dimostrazione del soddisfacimento dei requisiti per il software di sistema se vale almeno una delle seguenti condizioni:

- la SRP/CS è limitata a PL = "a" o PL = "b" e usa Categorie B, 2 o 3.
- la SRP/CS è limitata a PL = "c" o PL = "d" e può usare più componenti per i due canali nelle Categorie 2 o 3. I componenti dei due canali devono utilizzare tecnologie diverse (la ragione risiede nel fatto che ciò abbassa la probabilità di un malfunzionamento pericoloso a causa di un errore nel software di sistema).

4.8. Cambiamenti nella Sezione 5 della EN ISO 13849-1 riguardanti le funzioni di sicurezza

Nel paragrafo iniziale della sezione, relativo all'identificazione delle funzioni di sicurezza, è stata data enfasi al fatto che debba essere posta attenzione al comportamento della macchina in situazioni particolari, ad esempio: quando vi sia la perdita della potenza. In tali casi la SRP/CS deve continuare a fornire la funzione di sicurezza o inviare segnali ad altre parti in grado di portare e mantenere la macchina in uno stato sicuro.
In alcune applicazioni potrebbe essere necessario duplicare le funzioni di sicurezza: una per quando la potenza è disponibile e una per quando non lo è (tipico è il caso di assi che non devono permettere l'abbassamento di bracci per azione della gravità bensì mantenere il carico in posizione anche quando non è disponibile la potenza; in tal caso si può ricorrere a un dispositivo opportuno, ad es. un freno meccanico).

4.9. Cambiamenti nella Sezione 6 della EN ISO 13849-1 riguardanti le Categorie

In precedenza quando una SRP/CS in Categoria 2 non poteva portare la macchina in uno stato sicuro dopo aver rilevato un guasto, era permesso che fosse dato solo un avvertimento del pericolo (ad es.: in caso di saldatura dei contatti del dispositivo di interruzione).
Ora è stato chiarito in quali casi è permesso solo un avvertimento:

- Se PL_r="d", l'uscita (OTE) deve portare il sistema in uno stato sicuro che è mantenuto finché il guasto non è eliminato (non è possibile avere solo un avvertimento)
- Per PL_r inferiori o uguali a PL_r="c", se è praticabile, l'uscita (OTE) porta il sistema in uno stato sicuro che è mantenuto finché il guasto non è eliminato, se non è praticabile (ad es. nel caso di saldatura dei contatti del dispositivo di interruzione), può essere sufficiente che l'uscita (OTE) fornisca un segnale di avvertimento.

4.10. Cambiamenti nella Sezione 6 della EN ISO 13849-1 riguardanti la combinazione di SRP/CS

Molti costruttori forniscono il valore PFH_D delle SRP/CS (*encapsulated subsystems*) da loro prodotte, insieme al PL (o al SIL), pertanto è possibile applicare la procedura semplificata descritta

nella norma per calcolare il PL di una combinazione in serie di SRP/CS, utilizzata per realizzare una funzione di sicurezza, tenendo conto:

- della limitazione a causa di aspetti non quantificabili: il PL della combinazione vale al più quanto il più piccolo PL degli elementi della combinazione;
- della limitazione a causa di aspetti quantificabili: il PL della combinazione vale al più quanto il PL che si ottiene sommando i PFH_D degli elementi della combinazione

Il metodo semplificato basato sulla tabella contenuta nel paragrafo 6.3 della EN ISO 13849-1 (si veda anche la tab. 7 del Capitolo 1 del presente documento) richiede solo la conoscenza del PL di ogni singola SRP/CS.

4.11. Cambiamenti nell'Allegato A della EN ISO 13849-1 riguardanti la determinazione del PL_r

Diversi cambiamenti hanno interessato l'Allegato A. Innanzi tutto è stato sottolineato il suo carattere informativo e non obbligatorio (fatto che, del resto, vale anche per gli altri allegati della norma).
Per tale motivo e per il fatto che possono esistere procedure diverse da quella descritta nell'allegato A, potrebbero esistere norme di tipo C che deviano dal metodo dell'Allegato A.

È stato chiarito come valutare una frequenza e/o un tempo di esposizione al pericolo:

- se non vi sono altre informazioni e la frequenza è più alta di una volta ogni 15 minuti, allora deve essere scelta la frequenza F2;
- F1 può essere scelta se il tempo di esposizione cumulativo non supera 1/20 del tempo totale di funzionamento e la frequenza non è più alta di una volta ogni 15 minuti.

La probabilità di accadimento di un evento pericoloso e la possibilità di evitarlo sono state raccolte in un unico parametro (P). Quando vi è evidenza che la probabilità di accadimento dell'evento pericoloso sia bassa, allora il PL_r che si ottiene dalla figura A.1 può essere ridotto di un livello (naturalmente se PL_r = "a", allora il PL_r non può essere ridotto a un livello inferiore).
Nella ISO 12100 il parametro P è diviso in due parametri: uno per la probabilità di accadimento di un evento pericoloso, detto "O", e uno per la possibilità di evitarlo, detto "P".
La probabilità di accadimento di un evento pericoloso dipende o dal comportamento umano o da un malfunzionamento. Nella maggior parte dei casi la probabilità è sconosciuta e difficile da valutare. La stima di una tale probabilità dovrebbe essere basata sulle informazioni sull'affidabilità e sullo storico degli incidenti che si sono verificati su macchine simili. Però un numero basso di incidenti non significa automaticamente che la probabilità di accadimento sia bassa, ma solo che le misure di sicurezza normalmente adottate su macchine simili sono sufficienti.
Pertanto non si deve commettere l'errore di giudicare la probabilità di accadimento di un dato evento pericoloso inferiore a quanto sia in realtà.

È stato introdotto anche il paragrafo A.3 per suggerire come dovrebbero essere trattati i pericoli che si sovrappongono. I pericoli devono essere identificati come pericoli specifici o situazioni pericolose, in modo che, per la quantificazione, il rischio che ogni pericolo comporta possa essere valutato separatamente. Come conseguenza la parte di uscita della SRP/CS aziona l'attuatore che serve a ridurre solo quel pericolo specifico.
Quando invece una serie di pericoli sono collegati, in modo tale che si presentano sempre in combinazione e simultaneamente (ad esempio un robot per saldatura espone l'operatore continuamente sia al pericolo di urto che a quello di bruciature), allora tali pericoli dovrebbero essere valutati insieme come una "*combinazione*", cioè un unico pericolo.

4.12. Cambiamenti negli Allegati C e D della EN ISO 13849-1 riguardanti la stima del valore del $MTTF_D$

Nella tabella C.1 sono stati fatti i seguenti cambiamenti:

- Per i component idraulici possono essere adottati valori più alti di $MTTF_D$ in funzione del numero medio di operazioni l'anno n_{op}. Il valore di 150 anni (1 000 000 $\leq n_{op}$) può essere raddoppiato a 300 anni se 500 000 $\leq n_{op}$ <1 000 000 e così via fino a 600 anni (250 000 $\leq n_{op}$ < 500 000) o 1200 anni (n_{op} < 250 000).
- Il valore di B_{10D} per contattori sotto carico nominale è stato ridotto a B_{10D} = 1 300 000 cicli (poiché nella norma di prodotto IEC 60947-4-1 la proporzione di guasti pericolosi è assunta essere il 74% del totale).
- L'arresto di emergenza è stato sintetizzato in una sola riga. I dispositivi di arresto di emergenza (conformi a IEC 60947-5-5 and ISO 13850) e quelli di consenso/abilitazione (conformi a IEC 60947-5-8 possono essere considerati sottosistemi di Categoria 1 o di Categoria 3 o 4 a seconda del numero di contatti elettrici in uscita e della rilevazione dei guasti messa in atto nella SRP/CS. Ogni contatto (inclusi gli attuatori meccanici) può essere considerato come un canale con un valore di B_{10D} = 100 000 cicli. Per i dispositivi di consenso/abilitazione (IEC 60947-5-8) ciò significa che la funzione può essere ottenuta spingendo o rilasciando il pulsante. In alcuni casi il costruttore della macchina può applicare l'esclusione dei guasti in accordo con la tabella D.8 della EN ISO 13849-2, in base alla specifica applicazione e alle condizioni ambientali.
- È stata tolta la colonna del caso peggiore nelle tabelle da C.2 a C.7, poiché è considerato più aderente alla realtà servirsi nei calcoli dei dati forniti dal costruttore, al posto dei dati ottenibili da tali colonne.

4.13. Cambiamenti nell'Allegato E della EN ISO 13849-1 riguardanti la copertura diagnostica

Due misure sono state cancellate dalla parte della tabella E.1 relativa alle stime valide per i dispositivi di uscita, perché non rilevanti nella pratica:

- Percorso ridondante di Shut-off senza monitoraggio degli attuatori (DC = 0%)
- Percorso ridondante di Shut-off con monitoraggio di uno degli attuatori da parte della logica di controllo o del dispositivo di prova (la DC deve essere stimata individualmente per ogni percorso di shut-off, l'analisi della combinazione non è appropriata).

Alcune misure prevedono un intervallo del DC che si estende da 0 % a 99 % perché il corretto valore deve essere determinato dopo aver individuato (eventualmente effettuando una FMEA) tutti i malfunzionamenti pericolosi e determinato quali possono essere rilevati.

La misura relativa al "rilevamento dei guasti a partire dal processo" merita di essere chiarita in dettaglio:

- per la stima della DC nell'intervallo da 0% a 99%, tutti i malfunzionamenti pericolosi rilevati tramite il processo devono essere identificati;
- la misura può essere adottata per la copertura diagnostica solo se i malfunzionamenti pericolosi possono essere effettivamente rilevati dall'osservazione e dal corretto svolgersi del processo, pertanto se vi sono componenti nel percorso della funzione di sicurezza che sono attivati solo quando è richiesta la funzione di sicurezza, allora per tali componenti non è possibile assumere che i malfunzionamenti pericolosi possano essere rilevati a partire dal processo.

4.14. Cambiamenti nell'Allegato F della EN ISO 13849-1 riguardanti le misure contro le CCF

È stata migliorata la chiarezza in alcuni punti.

5. La norma EN ISO 13849-2

5.1. Validazione

La validazione serve a dimostrare che la combinazione delle SRP/CS scelte per realizzare la funzione di sicurezza verifichi tutti i requisiti necessari della EN ISO 13849-1.
La validazione di una SRP/CS è disciplinata dalla parte 2 della norma EN ISO 13849 che contiene la metodologia, i criteri e gli strumenti per verificare se sono soddisfatti i requisiti specifici di sicurezza per la corretta progettazione indicati nella parte 1 della norma stessa.
Gli oggetti presi in esame durante il processo di validazione sono:
- **la funzione di sicurezza** implementata nella SRP/CS;
- **il PL** della SRP/CS;
- **la Categoria** realizzata (struttura logica) per la SRP/CS.

Gli strumenti impiegati nel processo di validazione consistono in procedure di **analisi** e in **test**.
La norma EN ISO 13849-2 si compone di 12 capitoli dei quali i primi tre sono introduttivi e informativi mentre dal quarto in poi viene descritto il processo di validazione con i relativi criteri.
Si aggiungono 6 Allegati di cui i primi 4 (da A a D) riguardano:
- **i principi base di sicurezza** (*Basic Safety Principles*);
- **i principi di sicurezza ben provati** (*Well Tried Safety Principles*);
- **i componenti ben provati** (*Well Tried Components*);
- **i guasti e l'esclusione dei guasti** (*Faults and Fault Exclusions*).

Questi argomenti sono trattati separatamente per tecnologia meccanica, pneumatica, idraulica ed elettrica.

Gli altri allegati hanno la seguente struttura:
L'Allegato E riporta un esempio che non copre tutto il processo di validazione ma si dedica all'esame del comportamento del sistema nei confronti dei possibili guasti e della copertura diagnostica (DC) basandosi sull'applicazione della FMEA (e dell'Allegato E della parte 1 della norma). Tale tipo di valutazione risulta essere una delle parti più importanti e impegnative dell'esame della SRP/CS.

Infine la norma si chiude con il classico Allegato ZA che riguarda i riferimenti alla Direttiva Macchine 2006/42/CE

5.2. Il processo di validazione

Il processo di validazione si articola in una serie di fasi come indicato in fig. 15, in parte anche contestuali alla progettazione stessa della SRP/CS, che prevedono la stesura di un **piano** operativo e gestionale, un'**analisi** documentale e tecnica nella quale se necessario possono essere effettuati test, **l'esame della funzione di sicurezza in caso di guasto** (per le Categorie 2, 3 e 4), la **registrazione** dei risultati. Nel processo di validazione tutte le funzioni di sicurezza della SRP/CS devono essere prese in considerazione.

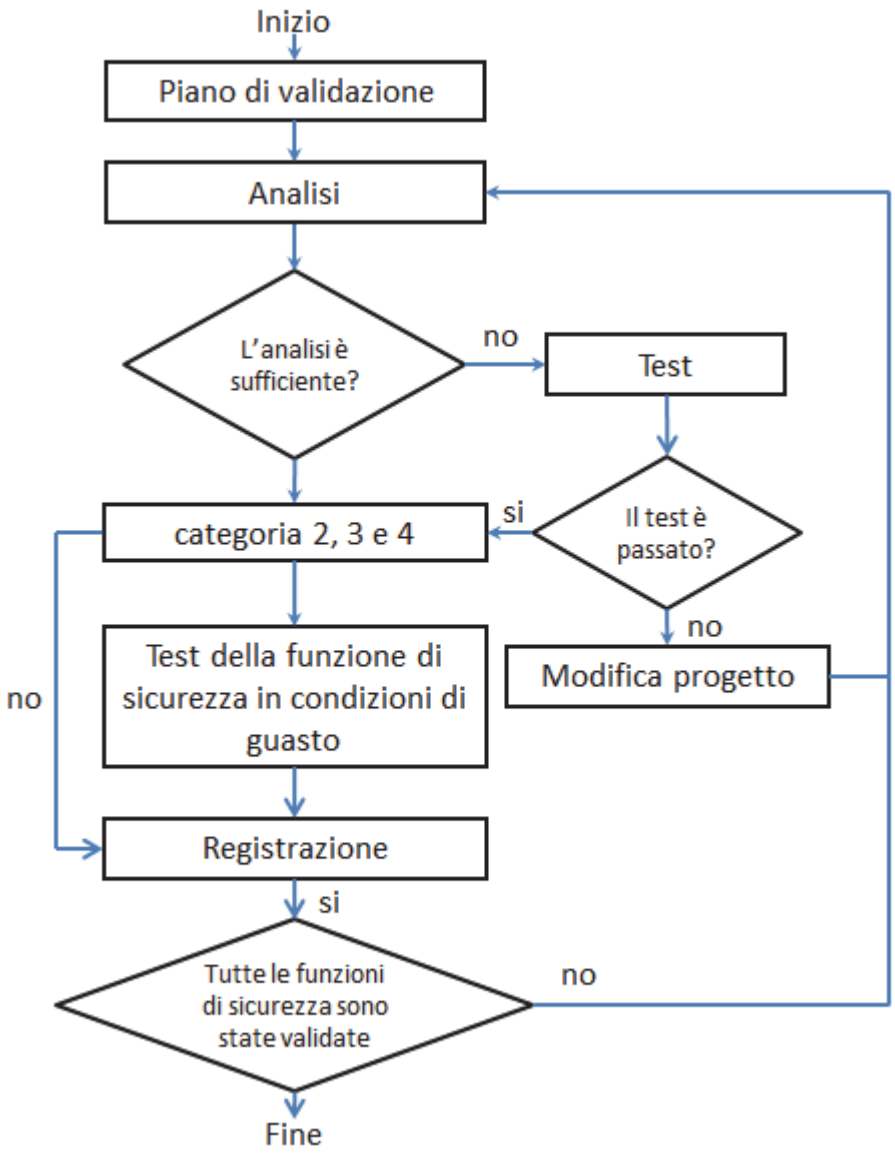


Fig. 15: Processo di validazione

5.2.1. Il piano di validazione

Il piano di validazione (vedi fig. 16) formalizza l'iter procedurale, gli strumenti, la documentazione, l'analisi, i test, le condizioni ambientali, le norme di riferimento, le persone responsabili per la validazione.

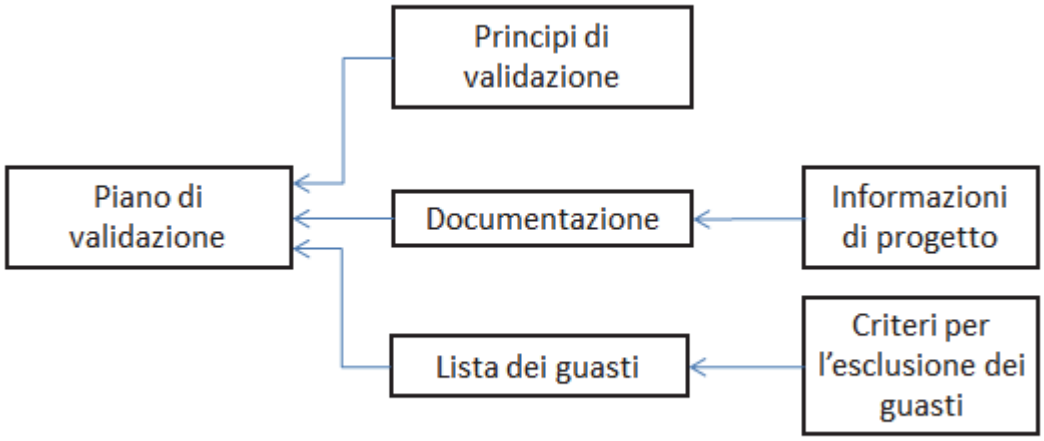


Fig. 16: Piano di validazione

5.2.1.1. I principi di validazione

Nella stesura del piano di validazione occorre tener conto dei principi di validazione che devono guidare chi effettua l'esame della SRP/CS e che richiedono di:

- rispettare le caratteristiche imposte per la funzione di sicurezza controllandone la corretta e ben specificata definizione;
- rispettare i requisiti previsti per il PL, in particolare quelli relativi alla Categoria scelta per l'architettura, all'applicazione delle misure per controllare ed evitare i guasti sistematici, al software di sicurezza, alla capacità di svolgere correttamente la funzione di sicurezza nelle condizioni ambientali di funzionamento previste;
- rispettare i requisiti di ergonomia che consentono all'operatore della macchina di agire sulle interfacce della stessa in maniera conforme alle condizioni di sicurezza previste in modo da evitare eventuali e/o prevedibili manomissioni;
- far effettuare la validazione a una persona non coinvolta nel progetto che non necessariamente deve essere di terza parte, ma è sufficiente che disponga di una adeguata indipendenza.

La necessità di effettuare dei test dipende fondamentalmente dal bisogno di avere risposte che l'analisi non può dare e questo dipende per esempio dalla tecnologia impiegata (es. complessa oppure necessità di integrazione della SRP/CS in un sistema di controllo con test prima e dopo l'implementazione) e dalle condizioni di utilizzo che possono comportare situazioni non note o prevedibili con sicurezza.
Per i sistemi ridondanti a due canali (Categoria 2, 3 e 4) è necessario effettuare test in condizioni di guasto per verificare che non si perda la funzione di sicurezza a seguito di una avaria singola.

5.2.1.2. La documentazione

La documentazione da raccogliere nel piano di validazione è relativa a tutte le informazioni di supporto indispensabili per il processo e necessarie per effettuare l'analisi e i test.
Si tratta di dati specifici di progetto, disegni, diagrammi a blocchi e funzionali, certificazioni, descrizioni funzionali di circuiti e componenti, sequenze temporali d'intervento dei dispositivi e dei segnali, valori nominali e tolleranze per i componenti, condizioni operative limite di stress, influenze dal processo (materiali, sostanze, temperature ecc.) e istruzioni per l'uso.
Inoltre deve essere raccolta la documentazione relativa al software di sicurezza comprensiva di certificazioni e/o di evidenze relative al raggiungimento del PL richiesto e dei test effettuati per confermarlo.
È necessaria infine la documentazione relativa all'ottenimento del PL in termini di PFH_D comprensiva della valutazione dei parametri connessi $MTTF_D$, DC_{avg}, CCF e della Categoria

impiegata. Per completare la valutazione del PL occorre verificare la documentazione relativa alle misure contro i guasti sistematici.
Nel caso più SRP/CS vengano assemblate per realizzare la funzione di sicurezza occorre reperire le informazioni relative alla determinazione del PL della combinazione.
Poiché i requisiti che una SRP/CS deve soddisfare dipendono pesantemente dal tipo di architettura impiegata per la sua realizzazione la norma EN ISO 13849-2 indica, in funzione della Categoria, la tipologia di documentazione richiesta (tab. 23).

TAB. 23: DOCUMENTAZIONE RICHIESTA PER LA VALIDAZIONE

Documentazione richiesta	Categoria				
	B	1	2	3	4
Principi base di sicurezza	X	X	X	X	X
Principi di sicurezza di ben provati	X	X	X	X	X
Componenti ben provati	–	X	–	–	–
$MTTF_D$ per canale	X	X	X	X	X
DC_{avg}	–	–	X	X	X
CCF e relative misure da adottare	–	–	X	X	X
Intervalli di verifica (check), se indicato	–	–	X	X	X
Guasti da rilevare e metodo usato	–	–	X	X	X
Misure diagnostiche e reazione al guasto	–	–	X	X	X
Guasti singoli esclusi	–	–	–	X	X
Test della funzione di sicurezza a idonei intervalli	–	–	X	–	–
Come la funzione di sicurezza viene mantenuta in caso di singolo guasto	–	–	–	X	X
Come la funzione di sicurezza viene mantenuta in caso di più guasti	–	–	–	–	X
Misure contro i guasti sistematici	X	X	X	X	X
Misure contro i guasti del software	X	–	X	X	X
Stress operativi attesi	X	X	X	X	X
Influenze relative ai materiali di processo	X	X	X	X	X
Prestazioni a seguito delle influenze ambientali	X	X	X	X	X

5.2.1.3. I guasti

Un passo importante nella progettazione, e tanto più nella validazione, consiste nell'individuazione di una lista di guasti prevedibili, strumento propedeutico per caratterizzare il comportamento al guasto della SRP/CS.
La norma distingue una lista di guasti generici ricavabile dalle tabelle presenti negli Allegati da A a D, per i componenti nelle diverse tecnologie che possono esserne interessati, correlata da quei guasti che invece possono essere esclusi nelle condizioni ambientali e operative di funzionamento.
Deve esser preparata una lista di guasti specifica per prodotto, nel caso si renda necessario, che può essere anche basata sulla lista generica. In tal caso essa deve contenere i guasti della lista generica, quelli in essa non compresi e quelli che possono essere esclusi.
In via eccezionale, se sono disponibili sufficienti motivazioni, e solo in tal caso, possono essere esclusi anche altri guasti per i quali la lista generica non permetterebbe l'esclusione.

5.2.3. Analisi

Nella fase di analisi vengono esaminati criticamente gli elementi, che caratterizzano la SRP/CS, riportati nello schema di figura 17, determinati nella fase di progettazione, per verificarne la rispondenza ai requisiti indicati nella norma EN ISO 13849-1.

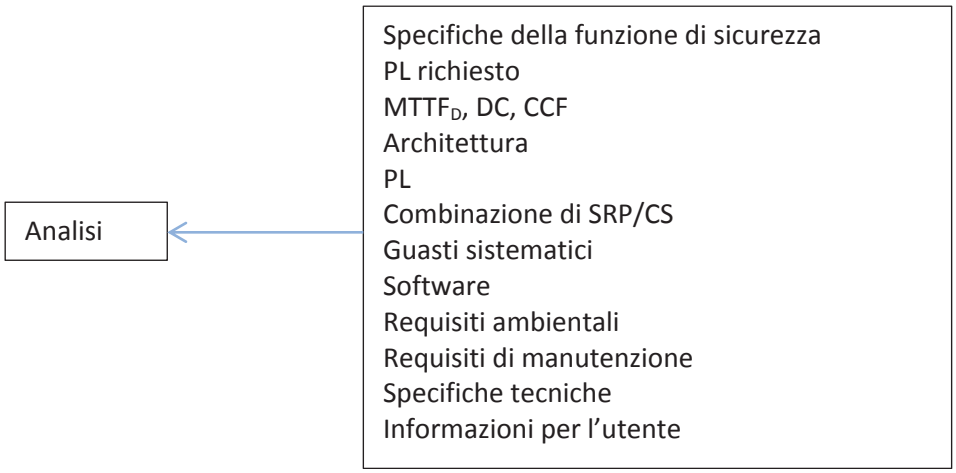


Fig. 17: Struttura del processo di analisi

Vengono quindi presi in considerazione la funzione di sicurezza, i parametri affidabilistici (scelta e calcolo), la struttura (Categoria), la valutazione del rischio e la scelta del livello di prestazione (PL_r), gli argomenti qualitativi (guasti sistematici, esperienza nell'uso dei componenti, fattori ambientali ed ergonomici, ecc.).
Le tecniche che possono essere utilizzate variano in funzione dell'elemento in esame e dell'obiettivo da raggiungere. Si tratta di procedimenti che seguono modelli logici e quindi possono essere di tipo deduttivo o induttivo. Il procedimento deduttivo parte dal generale cioè da un guasto sul sistema (detto anche evento top, nessun evento lo succede ma tutti lo precedono) per individuare gli eventi/guasti sui componenti che lo hanno generato. Metodi di questo tipo sono l'albero dei guasti (FTA) e l'albero degli eventi (ETA). Il procedimento induttivo parte invece dal particolare cioè dal guasto sui componenti per arrivare al guasto sul sistema. Metodi di questo tipo sono l'analisi dei modi e degli effetti dei guasti (FMEA) e l'analisi dei modi, degli effetti e della criticità dei guasti (FMECA).
In particolare l'analisi si deve concentrare sull'esame dei diagrammi circuitali per verificare che i requisiti di sicurezza contro il manifestarsi dei guasti pericolosi siano soddisfatti.

5.2.4. Test

La validazione per test non è obbligatoria ma si applica quando l'analisi non è decisiva per completare la validazione e quando si vogliono individuare funzionamenti anomali o provare situazioni anomale come gli effetti dell'uso scorretto ragionevolmente prevedibile.
In tal caso si rendono necessarie procedure di iniezione di guasti sia nei circuiti che nei componenti per testarne il comportamento. Possono essere utilizzati modelli hardware o software e possono essere considerati guasti del singolo sottosistema.
Particolare attenzione, nella fase di iniezione del guasto o di simulazione dello stesso, va posta per la sequenza temporale di intervento (tempo critico) in modo da rispettare il più possibile le reali condizioni in cui il guasto stesso si manifesta.
I test devono essere pianificati e registrati indicando le modalità di svolgimento i criteri di valutazione, il conduttore e le condizioni ambientali.
I test vengono effettuati applicando diverse combinazioni di segnali di input preferibilmente direttamente al sistema di controllo e alla macchina per esempio effettuando l'accensione, l'avvio, il cambio di velocità o direzione, l'arresto e il riavvio.
I principali requisiti che i campioni da sottoporre a test devono soddisfare sono:

- un singolo campione della produzione viene sottoposto a test;
- le SRP/CS non possono essere modificate durante il test;
- si può fare un test solo su una parte della SRP/CS, qualora un test integrale possa danneggiarla ma è necessario che il test parziale sia sufficientemente esaustivo;
- se durante un test un componente cambia le sue proprietà e questo causa un comportamento della SRP/CS che non soddisfa più i requisiti richiesti, il campione in prova deve essere sostituito.

5.3. Oggetti della validazione

La validazione, tenuto conto degli oggetti/elementi che compongono la funzione di sicurezza si suddivide in:
- validazione delle specifiche della funzione di sicurezza;
- validazione della funzione di sicurezza;
- validazione delle Categorie;
- validazione di $MTTF_D$, DC_{avg} e CCF;
- validazione delle misure contro i guasti sistematici;
- validazione del software di sicurezza;
- validazione del PL;
- validazione della combinazione di SRP/CS;
- validazione dei requisiti ambientali;
- validazione dei requisiti per la manutenzione;
- validazione della documentazione tecnica e delle informazioni per l'uso.

5.3.1. Validazione delle specifiche della funzione di sicurezza

Questa fase ha lo scopo di garantire la coerenza e la completezza delle specifiche indicate per la funzione di sicurezza.
Si tratta di verificare che la funzione di sicurezza sia definita e descritta in maniera corretta e completa e che il PL richiesto sia ben giustificato, considerando l'uso previsto della macchina, i modi di funzionamento, i tempi di ciclo e di risposta (della funzione).
È inoltre importante che sia verificato che la funzione di sicurezza garantisca il comportamento voluto della macchina al manifestarsi di un guasto pericoloso.

5.3.2. Validazione della funzione di sicurezza

Una volta che le specifiche di sicurezza sono state validate occorre validare la funzione stessa cioè verificare che operi correttamente secondo quanto indicato.
Bisogna controllare che:
- la corretta funzione di sicurezza sia stata implementata;
- la realizzazione della funzione di sicurezza corrisponda al progetto;
- tutti i modi di funzionamento siano stati considerati;
- la corretta elaborazione da parte della logica dei segnali di ingresso, in modo che i segnali di uscita siano orientati verso uno stato sicuro.

A tal scopo si possono applicare:
- tecniche di simulazione;
- analisi degli schemi funzionali, controllo del programma software;
- controllo dei componenti hardware e software e verifica di corrispondenza documentale (dati di targa, costruttore, versione, ecc.);
- test funzionale della funzione di sicurezza provando i vari modi di funzionamento, verificando che i parametri rientrino negli intervalli previsti, eventualmente effettuando test di sovraccarico;
- combinazione di segnali di input per verificare situazioni anomale;
- controllo dell'ergonomia delle interfacce con l'operatore.

5.4. Validazione delle Categorie

Per validare la Categoria occorre controllare che le specifiche per essa indicate nella EN ISO 13849-1 siano rispettate.
In questo contesto, come già evidenziato, i test possono essere utilizzati per verificare il comportamento in caso di guasto e in particolare che la reazione del sistema sia quella prevista.
Ad esempio per la Categoria 4 è importante verificare che il guasto sia rivelato prima o durante la richiesta della funzione di sicurezza ma se questo non avviene l'accumulo di guasti non deve portare alla perdita della funzione di sicurezza.

5.4.1. Validazione dei valori di DC

Devono essere controllati i valori di DC assegnati alle funzioni sulla base delle prove, dei monitoraggi e delle misure diagnostiche per i componenti e i blocchi che costituiscono l'architettura della Categoria scelta. Il progettista deve aver giustificato correttamente le proprie scelte. La verifica, che anche in questo caso può essere efficacemente condotta con test, deve dimostrare, che i valori assegnati siano credibili e ben fondati.
In particolare occorre analizzare il comportamento al guasto per verificare la capacità della funzione diagnostica di rilevare il guasto stesso.
Sembra opportuno ricordare che l'Allegato E della norma EN ISO 13849-1 indica dei valori di riferimento di DC per misure diagnostiche applicabili a blocchi di input, output e logici, alcuni dei quali però, dipendendo purtroppo dalla specifica applicazione, sono compresi in un ampio intervallo di variabilità, che lascia al progettista l'onere della scelta e l'obbligo di una corretta giustificazione.
Ovviamente la validazione comprende anche la verifica del calcolo del DC_{avg} per l'intera SRP/CS.

5.4.2. Validazione dei valori di $MTTF_D$

I valori di $MTTF_D$ sia dei singoli componenti che dei canali, compreso il calcolo e l'eventuale simmetrizzazione, devono essere verificati. Questo può essere fatto controllando la corrispondenza con i dati forniti dai costruttori, la plausibilità con le indicazioni fornite nell'Allegato C della EN ISO 13849-1 e i calcoli effettuati secondo l'Allegato D della EN ISO 13849-1.
Allo stesso modo devono essere verificati i valori di B_{10D} per i componenti soggetti a usura e i valori correlati della vita utile T_{10D} e del numero medio di operazioni annuali n_{op}, quest'ultimo fondamentale per il calcolo del corrispondente valore di $MTTF_D$.
Si evidenzia che la scelta del valore di $MTTF_D$ o B_{10D} dipende pesantemente dalle condizioni di utilizzo per il componente, a volte determinate dalla Categoria scelta per la SRP/CS. Ad esempio un contattore principale, per poter essere considerato componente "ben provato" e quindi utilizzato per Categoria 1, deve soddisfare i seguenti requisiti (tab. D.3, EN ISO 13849-2):

- essere conforme alla norma IEC 60947-5-1;
- altre influenze devono essere state considerate, per esempio vibrazioni;
- i guasti sono evitati con metodi adeguati, per esempio sovradimensionamento;
- la corrente di carico è limitata dalla protezione termica;
- i circuiti sono protetti da un dispositivo contro il sovraccarico.

In particolare sono esempi di operazioni di sovradimensionamento:

- la riduzione della corrente che attraversa i contatti a un valore inferiore alla metà del valore di targa;
- la riduzione della frequenza di commutazione del componente a un valore inferiore alla metà del valore di targa;
- la riduzione del numero totale di operazioni a un valore non superiore al 10% della durabilità del componente elettrico.

Si scelga per esempio di sovradimensionare un contattore, in termini di durabilità, che abbia un B_{10D} pari a 1300000 cicli, un tempo di missione (*mission time*) di 20 anni e un numero di operazioni per anno pari a 65000 cicli/anno (1300000/20).
Per sovradimensionarlo occorrerà tagliare a 1/10 tale valore, che diventa n_{op}= 6500, fortemente ridotto rispetto al valore originario, per renderlo idoneo all'applicazione in una Categoria 1.
L'$MTTF_D$ del componente sarà pari a $B_{10D}/(n_{op} \times 0{,}1)$ = 2000 anni: si avrà quindi un valore molto elevato (per una più bassa probabilità di guasto) a discapito del numero di operazioni annue effettuabili, per garantirne la durabilità.

5.4.3. Validazione delle misure contro il CCF

Le misure contro i guasti di causa comune sono organizzate in gruppi omogenei nell'Allegato F della norma ISO EN 13849-1. A ogni misura applicata corrisponde un punteggio e quando il totale raggiunto è uguale o superiore a 65 i requisiti contro il CCF si ritengono soddisfatti.
Per verificare che le misure siano state correttamente applicate occorre effettuare un esame documentale e funzionale dei circuiti ed eventualmente effettuare test.

5.4.4. Validazione del PL

Questa fase consiste nel verificare che la determinazione del PL sia stata correttamente effettuata e che il valore individuato sia almeno uguale al PL_r determinato a valle del processo di riduzione del rischio.
Con il già noto algoritmo grafico, riportato in fig. 10, si può verificare la corrispondenza del PL in funzione della Categoria della SRP/CS e dei parametri $MTTF_D$ e DC_{avg} e successivamente controllare che

$$PL \geq PL_r$$

Oltre agli aspetti quantitativi del PL (PFH_D, probabilità di guasto hardware pericoloso) occorre verificare anche quelli qualitativi relativi al software di sicurezza e alle misure contro i guasti sistematici.

5.4.5. Validazione delle misure contro i guasti sistematici

I guasti sistematici possono essere ridotti e controllati attraverso una gestione efficace della sicurezza funzionale (gestione della qualità), utilizzando funzioni diagnostiche, sfruttando i criteri di ridondanza e diversità o utilizzando tecnologie intrinsecamente sicure.
La validazione delle misure contro i guasti sistematici può effettuarsi attraverso:

- analisi documentale;
- rispetto dei principi di base e ben provati;
- diversità hardware;
- analisi dei guasti;
- test con iniezione di guasti;
- Verifica della comunicazione dei dati (ispezione e test);
- Applicazione di un sistema di gestione della qualità nella fabbricazione.

5.4.6. Validazione del software di sicurezza

Il software si compone di uno o più moduli (es. interblocco ripari), cioè unità di progettazione che contengono programmi e strutture dati realizzati in codice.
La base della procedura di validazione (fig. 18) sono le specifiche definite per il software che costituiscono l'input per il piano di validazione o per il cosiddetto protocollo di validazione.
Nella fase di analisi viene esaminata la documentazione di base (es. specifiche hardware, specifiche ingressi/uscite, linee guida per il codice, test per l'integrazione e test statici e dinamici del codice effettuati in fase di verifica, ecc.). È molto importante verificare il rispetto di tutte le fasi previste dal V-Model (fig. 11)

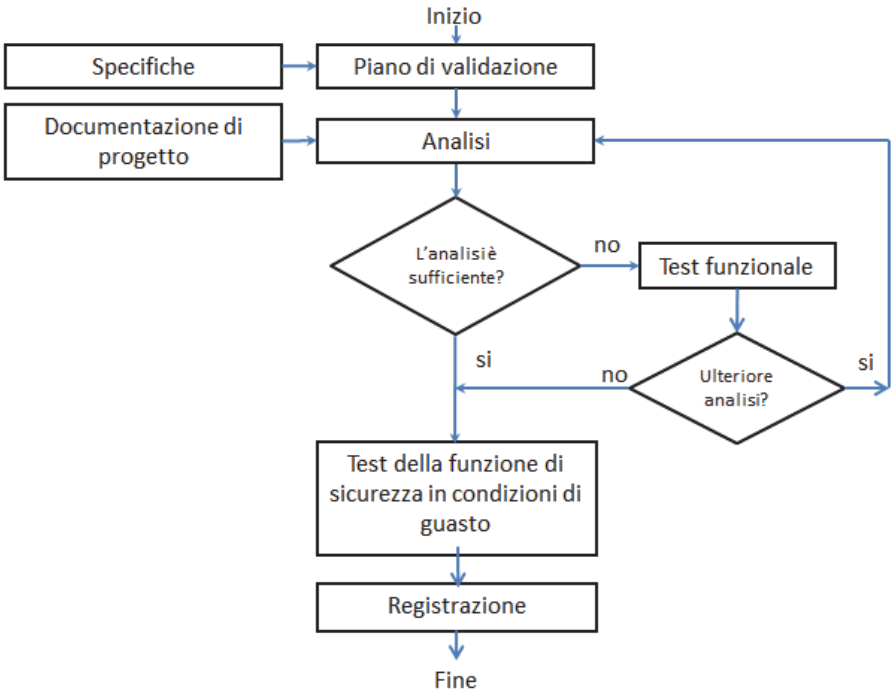


Fig. 18: Processo di validazione del software

La documentazione necessaria per effettuare la validazione del software è la seguente:
- le specifiche delle funzioni di sicurezza;
- specifiche hardware, specifiche ingressi/uscite;
- individuazione dei “tools” utilizzati (es. librerie, software di parametrizzazione, ecc.);
- descrizione dei moduli con versione, autore, data;
- i criteri di qualità impiegati per la realizzazione ed eventuali linee guida;
- prove e test di integrazione dei moduli nonché analisi statica e dinamica del codice;
- documentazione per misure, metodi e test per prevenire i guasti.

5.4.7. Validazione della combinazione di SRP/CS

Qualora una funzione di sicurezza venga realizzata mediante più SRP/CS o sottosistemi (fig. 19) occorre effettuare la validazione della combinazione, controllando:
- la documentazione che descrive la funzione di sicurezza;
- la verifica del calcolo del PL totale;
- l’esame delle caratteristiche di interfaccia tra i sottosistemi quali per esempio potenza, voltaggio, temperatura pressione, input dei dati;
- i guasti che possono riguardare la combinazione e l’integrazione fra i sottosistemi;
- per i sistemi ridondanti il comportamento al guasto dovuto alla combinazione/integrazione.

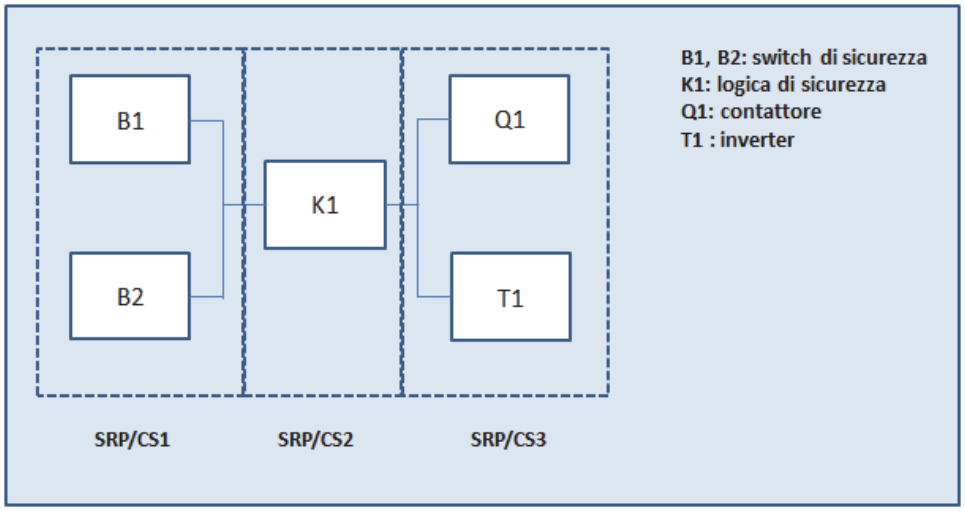


Fig. 19: Combinazione di SRP/CS

5.4.8. Validazione dei requisiti per le condizioni ambientali

La verifica delle condizioni ambientali e dei requisiti connessi, imposti per strutture e componenti, è importante per il corretto funzionamento e per la prevenzione del guasto. Alcuni componenti, per esempio, garantiscono le prestazioni in termini di affidabilità soltanto nelle specifiche condizioni ambientali in cui è previsto il loro uso. Le principali condizioni da verificare riguardano:
- sollecitazioni dovute a shock, vibrazioni, ingresso di inquinanti;
- sollecitazioni meccaniche;
- potenza e corrente di alimentazione;
- condizioni climatiche;
- immunità elettromagnetica EMC.

5.4.9. Validazione dei requisiti per la manutenzione

La validazione dei requisiti richiesti per la manutenzione viene effettuata sulle istruzioni per l’utilizzatore dove occorre controllare:

- la completezza delle istruzioni, che devono essere comprensibili e contenere indicazioni sugli strumenti da impiegare, le procedure da effettuare, la frequenza dei controlli e dei test, la durata dei componenti soggetti a usura (T_{10D});
- la necessità di affidare alcune operazioni a personale addestrato;
- la presenza di strumenti diagnostici per rilevare il guasto e riparare il sistema;
- l'indicazione e la presenza di misure per evitare errori nella manutenzione e modifiche pericolose mediante, per esempio, password.

5.4.10. Validazione della documentazione tecnica e delle istruzioni per l'uso

La documentazione tecnica e il manuale d'uso devono essere chiari e leggibili e contenere le seguenti informazioni previste dalla norma EN ISO 13849-1:

- la destinazione d'uso;
- il PL e la Categoria;
- i limiti funzionali e operativi della SRP/CS;
- modi di funzionamento e controllo;
- condizioni di sospensione delle funzioni di sicurezza (*muting, blanking*);
- le caratteristiche delle interfacce;
- allarmi e display;
- le condizioni corrette di assemblaggio e installazione comprese indicazioni per la parametrizzazione software e la programmazione;
- indicazioni per la manutenzione e le scadenze per il cambio dei componenti soggetti a usura.

5.5. Strumenti per la validazione: gli Allegati della EN ISO 13849-2

Gli Allegati da A a D della norma EN ISO 13849-2 forniscono, rispettivamente per tecnologia meccanica, pneumatica, idraulica ed elettrica, i seguenti strumenti necessari (oltre che per la progettazione) per la validazione:

- principi base di sicurezza;
- principi di sicurezza ben provati;
- componenti ben provati (non disponibili per tecnologia pneumatica e idraulica);
- guasti da considerare e la possibilità di escluderli in determinate condizioni.

Per la parte elettrica per esempio queste informazioni sono contenute nell'Allegato D e sono organizzate in tabelle con commenti.

5.5.1. I principi di sicurezza di base

I principi base di sicurezza sono principi generali di progettazione, di scelta di materiali e di procedure di produzione, assemblaggio, installazione, funzionamento e protezione, considerati fondamentali dalla normativa e dalla corretta pratica ingegneristica. La tabella 24 che segue è un estratto dei principi base di sicurezza per i sistemi elettrici.

TAB. 24: ALCUNI PRINCIPI BASE DI SICUREZZA

Principi base di sicurezza	Note
Uso di materiali idonei e di una fabbricazione adeguata	Scelta dei materiali, dei metodi di fabbricazione e di trattamento, in relazione ad esempio agli sforzi, alla durabilità, all'elasticità, all'attrito, all'invecchiamento, alla corrosione, alla temperatura, alla conducibilità, alla rigidità dielettrica.
Uso di un corretto dimensionamento e di una forma adatta	In relazione ad esempio agli sforzi, alle deformazioni, alla fatica, alla ruvidezza delle superfici, alle tolleranze, alla fabbricazione
Connessione al conduttore di protezione	Un lato del circuito di controllo, un terminale di ogni dispositivo a funzionamento elettromagnetico o un terminale di un qualsiasi altro dispositivo elettrico è connesso al conduttore di protezione.
Monitoraggio dell'isolamento	Uso di un dispositivo di monitoraggio dell'isolamento che segnala un guasto a terra o interrompe il circuito dopo un guasto a terra
Protezione contro l'avvio inatteso	Previene l'avvio inatteso per esempio dopo il ripristino dell'alimentazione
Uso della de-energizzazione	Lo stato sicuro è ottenuto de-energizzando tutti i dispositivi necessari per esempio usando contatti normalmente chiusi (NC) per gli ingressi (pulsanti e interruttori di posizione) e contatti normalmente aperti (NO) per i relè. Possono esistere eccezioni, nel caso, ad esempio, in cui la perdita di energia possa creare un pericolo addizionale. Possono essere necessarie funzioni di ritardo per raggiungere uno stato sicuro.

5.5.2. I principi di sicurezza ben provati

I principi di sicurezza ben provati sono criteri di scelta di soluzioni tecniche progettuali per sistemi e componenti ritenuti idonei e affidabili per applicazioni di sicurezza, ampiamente utilizzati con risultati positivi, provenienti dalla normativa o raccomandati dallo stato dell'arte.
La tabella 25 che segue è un estratto dei principi di sicurezza ben provati per i sistemi elettrici.

TAB. 25: ALCUNI PRINCIPI DI SICUREZZA DI BEN PROVATI

Principi di sicurezza ben provati	Note
Contatti positivi ad azione guidata (*mechanically linked*)	Uso dei contatti positivi ad azione guidata per, ad esempio, funzioni di monitoraggio in Categoria 2, 3, 4 (fig. 20)
Evitare i guasti dei cavi	Usare cavi con lo schermo collegato al conduttore di protezione ogni volta che è necessario un cavo separato; per cavi piatti collegare un conduttore a terra tra ciascun conduttore di segnale.
Distanza di separazione	Usare una distanza sufficiente tra terminali, componenti e cablaggi per evitare interferenze indesiderate
Limitazione dell'energia	Uso di capacità per fornire una quantità limitata di energia, per esempio in applicazioni a tempo
Azionamento diretto (positivo)	L'azione è trasmessa direttamente dalla forma dell'attuatore senza l'interposizione di elementi elastici come una molla tra attuatore e contatti (fig. 21)
Sovra-dimensionamento	Sottodimensionare l'uso di un componente quando è impiegato nei circuiti di sicurezza per esempio: – riducendo la corrente negli interruttori al di sotto della metà del valore di targa del componente; – riducendo la frequenza di intervento degli interruttori al di sotto della metà del valore di targa del componente; – riducendo il numero totale dei cicli di intervento degli interruttori a non più del 10% di quelli corrispondenti alla durabilità media del componente.

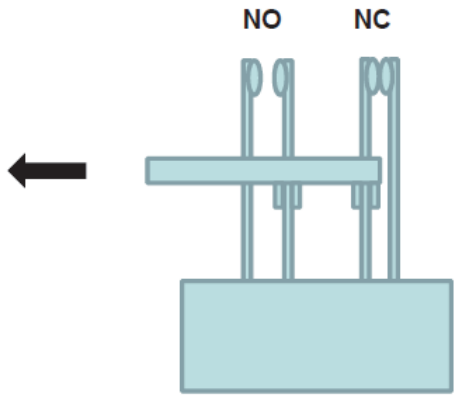


Fig. 20: Contatti ad azione guidata

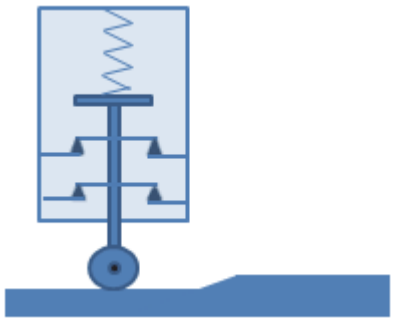


Fig. 21: Contatti duplicati NC ad azione diretta

5.5.3. I componenti ben provati

I componenti di sicurezza ben provati detti anche "well tried components" sono previsti di regola solo in Categoria 1 dove la scelta del componente affidabile, per questa struttura monocanale, è essenziale per garantire il livello di prestazione richiesto, in termini di guasto per ora del sistema. Un componente è ben provato se:

- è stato ampiamente utilizzato in passato con risultati positivi;
- è realizzato in modo da essere idoneo e affidabile per applicazioni di sicurezza.

I componenti e i principi di sicurezza sviluppati di recente possono essere considerati equivalenti a quelli "ben provati" se soddisfano l'ultima delle condizioni sopra indicate, cioè se la loro costruzione è effettuata secondo principi che ne garantiscano un'elevata affidabilità.

La tabella 26 che segue è un estratto di componenti ben provati per sistemi elettrici.
Componenti che non possono essere considerati ben provati sono i PLC, i microprocessori, i circuiti integrati.

TAB. 26: ALCUNI COMPONENTI DI SICUREZZA DI BEN PROVATI

Componenti ben provati	Note
Interruttori con apertura ad azione diretta: – pulsanti, – interruttori di posizione; – selettori a camma	Conformi a IEC 60947-5-1 Allegato K
Dispositivi di emergenza	Conformi a ISO 13850, IEC 60947-5-5
Contattore principale	È considerato ben provato solo se: – sono state considerate le altre influenze, es. vibrazioni, inquinamento, temperatura; – il guasto viene evitato con idonee misure, ad esempio il sovradimensionamento; – la corrente di carico è limitata dalla protezione termica – i circuiti sono protetti contro il sovraccarico. Non è possibile l'esclusione dei guasti
Contattore ausiliario	È considerato ben provato solo se: – sono state considerate le altre influenze, es. vibrazioni, inquinamento, temperatura; – energizzazione ad azione positiva; – il guasto viene evitato con idonee misure, ad esempio il sovradimensionamento; – la corrente è limitata da protezioni (fusibili o interruttori) per evitare la saldatura dei contatti; – i contatti sono guidati ad azione positiva se usati per monitoraggio. Non è possibile l'esclusione dei guasti Norme di riferimento: EN 50205, IEC 60947-5-1, IEC 60947-4-1, Allegato F

È molto importante sottolineare che quanto detto per i componenti ben provati deve essere valido per l'applicazione specifica nella quale il componente è utilizzato: ad esempio un microinterruttore di sicurezza, per essere utilizzato in processi o ambienti corrosivi come componente ben provato, deve essere garantito come idoneo e altamente affidabile in questa situazione specifica e non soltanto in generale, per qualsiasi applicazione.
Questa è una delle ragioni per cui, per alcune tecnologie come quella pneumatica e idraulica, vi è una grande difficoltà nel trovare componenti ben provati certificati come tali dai costruttori, i quali non vogliono garantire le prestazioni di componenti per tipologie di utilizzo che possono essere molteplici e che possono richiedere una sperimentazione specifica.
L'Amendment del 2015 della norma EN ISO 13849-1, ha cercato di superare tale ostacolo, per la parte di uscita "output" di una SRP/CS, assegnando al costruttore del componente ben provato il compito di indicarne l'idoneità all'uso.

5.5.4. Guasti ed esclusione dei guasti

La tabella 27 che segue è un estratto della lista dei guasti e delle possibili esclusioni, nonché delle condizioni per applicarle, per componenti e sistemi elettrici. Le liste dei guasti non sono certamente esaustive e, per componenti non in elenco, possono essere ricavate con una FMEA, mentre le eventuali esclusioni di guasti, devono essere dettagliatamente motivate nella documentazione tecnica.

Se più guasti derivano da un solo guasto, la loro combinazione si considera un solo guasto e così pure nel caso di guasti di causa comune (CCF).
L'esclusione di un guasto si basa sulla probabilità che questo avvenga, sull'esperienza tecnica, sulle caratteristiche dell'applicazione e del rischio specifico.

TAB. 27: ESCLUSIONE DI ALCUNI GUASTI

Guasti	Esclusioni dei guasti	Note
Tutti i contatti sono energizzati quando la bobina è de-energizzata	Nessuna	—
Cortocircuito fra contatti adiacenti isolati fra loro	I cortocircuiti possono essere esclusi per interruttori conformi a IEC 60947-5-1	Parti conduttive che diventano mobili non dovrebbero poter cortocircuitare l'isolamento intermedio
I contatti di interruttori non aprono	Esclusione per contatti conformi a IEC 60947-5-1, Allegato K	—
Chiusura simultanea di contatti normalmente aperti (NO) e normalmente chiusi (NC)	La chiusura simultanea dei contatti può essere esclusa per contatti ad azione guidata (*mechanically linked*) (IEC 60947-5-1, Allegato L)	—
Per componenti elettronici programmabili: segnale 0 o 1 statico a tutti gli ingressi e uscite singolarmente o simultaneamente	Nessuna	—

6. I principi di sicurezza riportati nella EN ISO 13849-2

6.1. Principi di sicurezza per i sistemi meccanici

Quando si usano componenti meccanici occorre fare riferimento ai principi del presente paragrafo. L'istante preciso in cui avviene il guasto potrebbe essere critico.

TAB. 28.a: TABELLA A.1, EN ISO 13849-2 – PRINCIPI BASE DI SICUREZZA PER I SISTEMI MECCANICI

Principi base di sicurezza	Osservazioni
Uso di materiali idonei e di una fabbricazione adeguata	Scelta dei materiali, dei metodi di fabbricazione e di trattamento, in relazione ad esempio agli sforzi, alla durabilità, all'elasticità, all'attrito, all'invecchiamento, alla corrosione, alla temperatura.
Uso di un corretto dimensionamento e di una forma adatta	In relazione ad esempio agli sforzi, alle deformazioni, alla fatica, alla ruvidezza delle superfici, alle tolleranze, al bloccaggio, alla fabbricazione.
Scelta, combinazione, assemblaggio e installazione dei componenti/sistemi in modo appropriato	Applicazione delle note del costruttore, ad es.: fogli di informazione, istruzioni di installazione, specifiche tecniche e applicazione della buona pratica ingegneristica in componenti/sistemi simili.
Uso della de-energizzazione	Se si toglie energia la macchina si porta in uno stato sicuro. Si veda l'azione primaria per l'arresto nella ISO 12100, 6.2.11.3. Per iniziare un movimento deve essere fornita energia. Si veda l'azione primaria per l'avviamento nella ISO 12100, 6.2.11.3. Si devono considerare modi diversi, ad esempio: modo di funzionamento, modo di manutenzione. Il presente principio non deve essere seguito se la mancanza di energia può creare un rischio, ad es.: rilascio di un pezzo in lavorazione a causa del venir meno della forza di serraggio.
Fissaggio adeguato	Per il serraggio con viti si devono applicare le note del costruttore. Il sovraccarico può essere evitato utilizzando una tecnologia che permetta l'applicazione della corretta coppia di serraggio.
Limitazione della generazione e/o della trasmissione di forza e di parametri simili	Esempi sono le spine di rottura, la piastra di rottura e il limitatore di coppia. Il presente principio non deve essere seguito se l'integrità dei componenti è essenziale per mantenere il livello di controllo richiesto.
Campi limitati per i parametri ambientali	Esempi sono la temperatura, l'umidità e l'inquinamento nel luogo di installazione (si consiglia di consultare le note del costruttore e il paragrafo 10 della EN ISO 13849-2, o il punto 2.5.5 del capitolo 4 del presente documento).
Limitazione della velocità e di parametri simili	Considerare, ad esempio, la velocità, l'accelerazione o la decelerazione richieste dall'applicazione.
Tempo di reazione adeguato	Considerare, ad esempio, la fatica della molla, l'attrito, la lubrificazione, la temperatura, l'inerzia durante l'accelerazione o la decelerazione, la combinazione delle tolleranze.
Protezione contro le partenze non volute	Considerare le partenze non volute causate dall'accumulo di energia o dal ripristino dell'alimentazione nei diversi modi (modo di funzionamento, modo di manutenzione). Possono essere necessarie apparecchiature speciali per il rilascio dell'energia accumulata. Applicazioni speciali (ed es.: accumulo di energia per dispositivi di bloccaggio e per assicurare una posizione) devono essere considerate a parte.

TAB. 28.b: TABELLA A.1, EN ISO 13849-2 – PRINCIPI BASE DI SICUREZZA PER I SISTEMI MECCANICI (PROSECUZ.)

Principi base di sicurezza	Osservazioni
Semplificazione	Evitare componenti non necessari nei sistemi relativi alla sicurezza.
Separazione	Separazione delle funzioni di sicurezza dalle altre funzioni.
Lubrificazione adeguata	Considerare la necessità di dispositivi di lubrificazione, di informazioni sui lubrificanti e sugli intervalli di lubrificazione.
Adeguata prevenzione dell'ingresso di liquidi e polveri	Considerare il grado di protezione IP (si veda la IEC 60529).

TAB. 29.a: TABELLA A.2, EN ISO 13849-2 – PRINCIPI DI SICUREZZA BEN PROVATI, PER I SISTEMI MECCANICI

Principi di sicurezza ben provati	Osservazioni
Uso di materiali attentamente scelti e di fabbricazione adeguata	Scelta dei materiali adatti, dei metodi di fabbricazione e di trattamento adeguati in relazione all'applicazione.
Uso di componenti con modo di guasto orientato	Il modo di guasto predominante di un componente è conosciuto ed è sempre lo stesso (si veda la ISO 12100, 6.2.12.3).
Sovradimensionamento/fattori di sicurezza	I fattori di sicurezza sono suggeriti dalle norme o dall'esperienza nelle applicazioni di sicurezza.
Posizione sicura	La parte mobile di un componente è mantenuta in una delle posizioni di sicurezza da mezzi meccanici (l'attrito da solo non è sufficiente). È richiesta una forza per muoverla da tale posiz.
Forza per lo spegnimento aumentata	Uno stato sicuro può essere ottenuto con una forza per lo spegnimento aumentata rispetto alla forza per l'accensione.
Scelta, combinazione, assemblaggio e installazione dei componenti in modo appropriato in relazione all'applicazione	—
Scelta appropriata del fissaggio in relazione all'applicazione	Evitare di fare affidamento solo sull'attrito.
Azione meccanica positiva	Per ottenere un'azione meccanica positiva, l'azione è trasmessa direttamente dalla forma dell'attuatore (ad esempio un albero apre direttamente il contatto di un interruttore elettrico, senza l'interposizione di una molla (si veda la ISO 12100, 6.2.5).
Uso di molle ben provate (le specifiche tecniche delle molle d'acciaio e altre applicazioni speciali si trovano nella ISO 4960)	Una molla ben provata richiede: – scelta dei materiali adatti, dei metodi di fabbricazione (precondizionamento e cicli di prova prima dell'uso) e di trattamento (ad es.: laminazione, pallinatura) adeguati, – guida sufficiente della molla, – sufficiente fattore di sicurezza per lo sforzo da fatica (in modo da avere una probabilità più alta del fatto che non possano intervenire rotture). Molle a spirale di compressione ben provate possono essere progettate con i seguenti accorgimenti: – scelta dei materiali adatti, dei metodi di fabbricazione (precondizionamento e cicli di prova prima dell'uso) e di trattamento (ad es.: laminazione, pallinatura) adeguati, – guida sufficiente della molla, – spazio tra le spire < diametro del filo se la molla è scarica, – mantenimento di una forza sufficiente anche dopo una o più rotture, in modo che queste non determinino una condizione pericolosa.

TAB. 29.b: TABELLA A.2, EN ISO 13849-2 – PRINCIPI DI SICUREZZA BEN PROVATI, PER I SISTEMI MECCANICI (PROSEC.)

Principi di sicurezza ben provati	Osservazioni
Parti multiple (ridondanti)	Ridurre l'effetto di un guasto utilizzando più parti che agiscono in parallelo (ad es.: il guasto di una molla tra più molle in parallelo non porta a una condizione pericolosa).
Campi limitati per le forze e per parametri simili	Determinare i limiti necessari in base all'esperienza e all'applicazione. Esempi sono le spine di rottura, la piastra di rottura e il limitatore di coppia. Il presente principio non deve essere seguito se l'integrità dei componenti è essenziale per mantenere il livello di controllo richiesto.
Campi limitati della velocità e di parametri simili	Determinare i limiti necessari in base all'esperienza e all'applicazione. Esempi sono il regolatore centrifugo, il monitoraggio della velocità e gli spostamenti limitati.
Campi limitati per i parametri ambientali	Determinare i limiti necessari. Esempi sono la temperature, l'umidità e l'inquinamento nel luogo di installazione (si consiglia di consultare le note del costruttore e il paragrafo 10 della EN ISO 13849-2, o il punto 2.5.5 del capitolo 4 del presente documento).
Campo limitato per il tempo di reazione, isteresi limitata	Determinare i limiti necessari. Considerare, ad esempio, la fatica della molla, l'attrito, la lubrificazione, la temperatura, l'inerzia durante l'accelerazione o la decelerazione, la combinazione delle tolleranze.

6.2. Principi di sicurezza per i sistemi pneumatici

Quando si usano componenti pneumatici occorre fare riferimento ai principi del presente paragrafo. Se i componenti sono anche elettrici occorre fare riferimento anche ai principi del paragrafo 6.4. Alcuni componenti potrebbero rientrare nell'applicazione della Direttiva PED o della Direttiva TPED. L'istante preciso in cui avviene il guasto potrebbe essere critico.

TAB. 30.a: TABELLA B.1, EN ISO 13849-2 – PRINCIPI BASE DI SICUREZZA PER I SISTEMI PNEUMATICI

Principi base di sicurezza	Osservazioni
Uso di materiali idonei e di una fabbricazione adeguata	Scelta dei materiali, dei metodi di fabbricazione e di trattamento, in relazione ad esempio agli sforzi, alla durabilità, all'elasticità, all'attrito, all'invecchiamento, alla corrosione, alla temperatura.
Uso di un corretto dimensionamento e di una forma adatta	In relazione ad esempio agli sforzi, alle deformazioni, alla fatica, alla ruvidezza delle superfici, alle tolleranze, al bloccaggio, alla fabbricazione.
Scelta, combinazione, assemblaggio e installazione dei componenti/sistemi in modo appropriato	Applicazione delle note del costruttore, ad es.: fogli di informazione, istruzioni di installazione, specifiche tecniche e applicazione della buona pratica ingegneristica in componenti/sistemi simili.
Uso della de-energizzazione	Se si toglie energia la macchina si porta in uno stato sicuro. Si veda l'azione primaria per l'arresto nella ISO 12100, 6.2.11.3. Per iniziare un movimento deve essere fornita energia. Si veda l'azione primaria per l'avviamento nella ISO 12100, 6.2.11.3. Si devono considerare modi diversi, ad esempio: modo di funzionamento, modo di manutenzione. Il presente principio non deve essere usato in alcune applicazioni, ad es. se la perdita di pressione pneumatica può creare un rischio aggiuntivo.

TAB. 30.b: TABELLA B.1, EN ISO 13849-2 – PRINCIPI BASE DI SICUREZZA PER I SISTEMI PNEUMATICI (PROSECUZ.)

Principi base di sicurezza	Osservazioni
Fissaggio adeguato	Per il serraggio con viti, raccordi, colla, anelli di fissaggio si devono applicare le note del costruttore. Il sovraccarico può essere evitato utilizzando una tecnologia che permetta l'applicazione della corretta coppia di serraggio.
Limitazione della pressione	Esempi sono le valvole a pressione massima, le valvole per regolare la pressione, le valvole di controllo.
Limitazione/riduzione della velocità	Un esempio è la limitazione della velocità di un pistone con una valvola limitatrice di portata o una valvola a farfalla.
Sufficiente prevenzione della contaminazione del fluido	Considerare il filtraggio e la separazione delle particelle solide o dell'acqua dal fluido.
Campo adeguato dei tempi di commutazione	Considerare, ad es. la lunghezza dei tubi, la pressione, la capacità di sfiato, la forza, la fatica della molla, l'attrito, la lubrificazione, la temperatura, l'inerzia durante l'accelerazione o la decelerazione, la combinazione delle tolleranze.
Resistenza alle condizioni ambientali	Progettare l'apparecchiatura in modo che possa lavorare nelle condizioni ambientali attese e in quelle avverse prevedibili, per quanto riguarda ad es. la temperatura, l'umidità, le vibrazioni e l'inquinamento (si consiglia di consultare le note del costruttore e il paragrafo 10 della EN ISO 13849-2, o il punto 2.5.5 del capitolo 4 del presente documento).
Protezione contro le partenze non volute	Considerare le partenze non volute causate dall'accumulo di energia o dal ripristino dell'alimentazione nei diversi modi (modo di funzionamento, modo di manutenzione). Possono essere necessarie apparecchiature speciali per il rilascio dell'energia accumulata (si veda la ISO 14118, 5.3.1.3). Applicazioni speciali (ed es.: accumulo di energia per dispositivi di bloccaggio e per assicurare una posizione) devono essere considerate a parte.
Semplificazione	Evitare componenti non necessari nei sistemi relativi alla sicurezza.
Campo di temperatura adeguato	Da considerare per tutto il sistema
Separazione	Separazione delle funzioni di sicurezza dalle altre funzioni (ad es. separazione logica).

TAB. 31.a: TABELLA B.2, EN ISO 13849-2 – PRINCIPI DI SICUREZZA BEN PROVATI, PER I SISTEMI PNEUMATICI

Principi di sicurezza ben provati	Osservazioni
Sovradimensionamento/fattori di sicurezza	I fattori di sicurezza sono suggeriti dalle norme o dall'esperienza nelle applicazioni di sicurezza.
Posizione sicura	La parte mobile di un componente è mantenuta in una delle posizioni di sicurezza da mezzi meccanici (l'attrito da solo non è sufficiente). È richiesta una forza per muoverla da tale posizione.
Forza per la posizione di arresto aumentata	Una soluzione è che il rapporto di area per muovere lo stantuffo di una valvola in una posizione sicura (posizione di arresto) sia significativamente più grande di quello per muoverlo in una posizione di avviamento (fattore di sicurezza).
Valvola chiusa dalla pressione di carico	Sono generalmente le valvole di fondo, ad esempio le valvole a fungo, le valvole a sfera. Considerare come applicare la pressione di carico per mantenere la valvola chiusa anche se, ad esempio, la molla che la chiude si rompe.

TAB. 31.b: TABELLA B.2, EN ISO 13849-2 – PRINCIPI DI SICUREZZA BEN PROVATI, PER I SISTEMI PNEUMATICI (PROSEC.)

Principi di sicurezza ben provati	Osservazioni
Azione meccanica positiva	L'azione meccanica positiva è usata per le parti mobili dei componenti pneumatici. Si veda anche la voce corrispondente nella tab. A.2
Parti multiple (ridondanti)	Si veda la voce corrispondente nella tabella A.2.
Uso di molle ben provate	Si veda la voce corrispondente nella tabella A.2.
Limitazione/riduzione della velocità mediante resistenza a un flusso definito	Esempi sono orifizi fissi e valvole a farfalla fisse.
Limitazione/riduzione della forza	Può essere ottenuta con una valvola a pressione massima ben provata che è, ad esempio, equipaggiata con una molla ben provata, correttamente dimensionata e selezionata.
Campo appropriato delle condizioni di funzionamento	Dovrebbe essere considerata la limitazione delle condizioni di funzionamento (ad es. l'intervallo della pressione, l'intervallo della portata, l'intervallo della temperatura).
Adeguata prevenzione della contaminazione del fluido	Considerare la necessità di un migliore filtraggio e una migliore separazione delle particelle solide o dell'acqua dal fluido.
Sufficiente sovrapposizione positiva nelle valvole a stantuffo	La sovrapposizione positiva assicura la funzione di arresto e impedisce movimenti non ammessi.
Isteresi limitata	Ad esempio un incremento dell'attrito o una combinazione delle tolleranze influenzano l'isteresi.

6.3. Principi di sicurezza per i sistemi idraulici

Quando si usano componenti idraulici occorre fare riferimento ai principi del presente paragrafo.
Se i componenti sono anche elettrici occorre fare riferimento anche ai principi del paragrafo 6.4.
Alcuni componenti potrebbero rientrare nell'applicazione della Direttiva PED o della Direttiva TPED.
Bolle d'aria e cavitazione nei fluidi idraulica devono essere evitate perché possono creare pericoli aggiuntivi (ad es. movimenti non voluti).
L'istante preciso in cui avviene il guasto potrebbe essere critico.

TAB. 32.a: TABELLA C.1, EN ISO 13849-2 – PRINCIPI BASE DI SICUREZZA PER I SISTEMI IDRAULICI

Principi base di sicurezza	Osservazioni
Uso di materiali idonei e di una fabbricazione adeguata	Scelta dei materiali, dei metodi di fabbricazione e di trattamento, in relazione ad esempio agli sforzi, alla durabilità, all'elasticità, all'attrito, all'invecchiamento, alla corrosione, alla temperatura, ai fluidi idraulici.
Uso di un corretto dimensionamento e di una forma adatta	In relazione ad esempio agli sforzi, alle deformazioni, alla fatica, alla ruvidezza delle superfici, alle tolleranze, al bloccaggio, alla fabbricazione.
Scelta, combinazione, assemblaggio e installazione dei componenti/sistemi in modo appropriato	Applicazione delle note del costruttore, ad es.: fogli di informazione, istruzioni di installazione, specifiche tecniche e applicazione della buona pratica ingegneristica in componenti/sistemi simili.
Uso della de-energizzazione	Se si toglie energia la macchina si porta in uno stato sicuro. Si veda l'azione primaria per l'arresto nella ISO 12100, 6.2.11.3. Per iniziare un movimento deve essere fornita energia. Si veda l'azione primaria per l'avviamento nella ISO 12100, 6.2.11.3. Si devono considerare modi diversi, ad esempio: modo di funzionamento, modo di manutenzione. Il presente principio non deve essere usato in alcune applicazioni, ad es. se la perdita di pressione idraulica può creare un rischio aggiuntivo.

TAB. 32.b: TABELLA C.1, EN ISO 13849-2 – PRINCIPI BASE DI SICUREZZA PER I SISTEMI IDRAULICI (PROSECUZIONE)

Principi base di sicurezza	Osservazioni
Fissaggio adeguato	Per il serraggio con viti, raccordi, colla, anelli di fissaggio si devono applicare le note del costruttore. Il sovraccarico può essere evitato utilizzando una tecnologia che permetta l'applicazione della corretta coppia di serraggio.
Limitazione della pressione	Esempi sono le valvole a pressione massima, le valvole per regolare la pressione, le valvole di controllo.
Limitazione/riduzione della velocità	Un esempio è la limitazione della velocità di un pistone con una valvola limitatrice di portata o una valvola a farfalla.
Sufficiente prevenzione della contaminazione del fluido	Considerare il filtraggio e la separazione delle particelle solide o dell'acqua dal fluido e la necessità della manutenzione del filtro.
Campo adeguato dei tempi di commutazione	Considerare, ad es. la lunghezza dei tubi, la pressione, la capacità di sfiato, la fatica della molla, l'attrito, la lubrificazione, la temperatura/viscosità, l'inerzia durante l'accelerazione o la decelerazione, la combinazione delle tolleranze.
Resistenza alle condizioni ambientali	Progettare l'apparecchiatura in modo che possa lavorare nelle condizioni ambientali attese e in quelle averse prevedibili, per quanto riguarda ad es. la temperatura, l'umidità, le vibrazioni e l'inquinamento (si consiglia di consultare le note del costruttore e il paragrafo 10 della EN ISO 13849-2, o il punto 2.5.5 del capitolo 4 del presente documento).
Protezione contro le partenze non volute	Considerare le partenze non volute causate dall'accumulo di energia o dal ripristino dell'alimentazione nei diversi modi (modo di funzionamento, modo di manutenzione). Possono essere necessarie apparecchiature speciali per il rilascio dell'energia accumulata. Applicazioni speciali (ed es.: accumulo di energia per dispositivi di bloccaggio e per assicurare una posizione) devono essere considerate a parte.
Semplificazione	Evitare componenti non necessari nei sistemi relativi alla sicurezza.
Campo di temperatura adeguato	Da considerare per tutto il sistema
Separazione	Separazione delle funzioni di sicurezza dalle altre funzioni.

TAB. 33.a: TABELLA C.2, EN ISO 13849-2 – PRINCIPI DI SICUREZZA BEN PROVATI, PER I SISTEMI IDRAULICI

Principi di sicurezza ben provati	Osservazioni
Sovradimensionamento/fattori di sicurezza	I fattori di sicurezza sono suggeriti dalle norme o dall'esperienza nelle applicazioni di sicurezza.
Posizione sicura	La parte mobile di un componente è mantenuta in una delle posizioni di sicurezza da mezzi meccanici (l'attrito da solo non è sufficiente). È richiesta una forza per muoverla da tale posizione.
Forza per la posizione di arresto aumentata	Una soluzione è che il rapporto di area per muovere lo stantuffo di una valvola in una posizione sicura (posizione di arresto) sia significativamente più grande di quello per muoverlo in una posizione di avviamento (fattore di sicurezza).
Valvola chiusa dalla pressione di carico	Sono generalmente le valvole di fondo, e le valvole a cartuccia. Considerare come applicare la pressione di carico per mantenere la valvola chiusa anche se, ad esempio, la molla che la chiude si rompe.

TAB. 33.b: TABELLA C.2, EN ISO 13849-2 – PRINCIPI DI SICUREZZA BEN PROVATI, PER I SISTEMI IDRAULICA (PROSEC.)

Principi di sicurezza ben provati	Osservazioni
Azione meccanica positiva	L'azione meccanica positiva è usata per le parti mobili dei componenti idraulici. Si veda anche la voce corrispondente nella tabella A.2.
Parti multiple (ridondanti)	Si veda la voce corrispondente nella tabella A.2.
Uso di molle ben provate	Si veda la voce corrispondente nella tabella A.2.
Limitazione/riduzione della velocità mediante resistenza a un flusso definito	Esempi sono orifizi fissi e valvole a farfalla fisse.
Limitazione/riduzione della forza	Può essere ottenuta con una valvola a pressione massima ben provata che è, ad esempio, equipaggiata con una molla ben provata, correttamente dimensionata e selezionata.
Campo appropriato delle condizioni di funzionamento	Dovrebbe essere considerata la limitazione delle condizioni di funzionamento (ad es. l'intervallo della pressione, l'intervallo della portata, l'intervallo della temperatura).
Monitoraggio delle condizioni del fluido	Considerare la necessità di un migliore filtraggio e una migliore separazione delle particelle solide o dell'acqua dal fluido. Considerare anche le condizioni chimiche/fisiche del fluido. Considerare un indicatore della necessità di manutenzione del filtro.
Sufficiente sovrapposizione positiva nelle valvole a stantuffo	La sovrapposizione positiva assicura la funzione di arresto e impedisce movimenti non ammessi.
Isteresi limitata	Ad esempio un incremento dell'attrito o una combinazione delle tolleranze influenzano l'isteresi.

6.4. Principi di sicurezza per i sistemi elettrici

Quando si usano componenti elettrici (anche in congiunzione con altre tecnologie) occorre fare riferimento ai principi del presente paragrafo.
Le condizioni ambientali della IEC 60204-1 si applicano al processo di validazione. Se sono specificate altre condizioni ambientali se ne deve tener conto.
L'istante preciso in cui avviene il guasto potrebbe essere critico.

TAB. 34.a: TABELLA D.1, EN ISO 13849-2 – PRINCIPI BASE DI SICUREZZA PER I SISTEMI ELETTRICI

Principi base di sicurezza	Osservazioni
Uso di materiali idonei e di una fabbricazione adeguata	Scelta dei materiali, dei metodi di fabbricazione e di trattamento, in relazione ad esempio agli sforzi, alla durabilità, all'elasticità, all'attrito, all'invecchiamento, alla corrosione, alla temperatura, alla conducibilità, alla rigidità dielettrica.
Uso di un corretto dimensionamento e di una forma adatta	In relazione ad esempio agli sforzi, alle deformazioni, alla fatica, alla ruvidezza delle superfici, alle tolleranze, alla fabbricazione.
Scelta, combinazione, assemblaggio e installazione dei componenti/sistemi in modo appropriato	Applicazione delle note del costruttore, ad es.: fogli di informazione, istruzioni di installazione, specifiche tecniche e applicazione della buona pratica ingegneristica in componenti/sistemi simili.
Connessione al conduttore di protezione	Un lato del circuito di controllo, un terminale di ogni dispositivo a funzionamento elettromagnetico o un terminale di un qualsiasi altro dispositivo elettrico è connesso al conduttore di protezione (IEC 60204-1, 9.4.3.1).
Monitoraggio dell'isolamento	Uso di un dispositivo di monitoraggio dell'isolamento che segnala un guasto a terra o interrompe il circuito dopo un guasto a terra (IEC 60204-1, 6.3.3)

TAB. 34.b: TABELLA D.1, EN ISO 13849-2 – PRINCIPI BASE DI SICUREZZA PER I SISTEMI ELETTRICI (PROSECUZIONE)

Principi base di sicurezza	Osservazioni
Uso della de-energizzazione	Lo stato sicuro è ottenuto de-energizzando tutti i dispositivi necessari per esempio usando contatti normalmente chiusi (NC) per gli ingressi (pulsanti e interruttori di posizione) e contatti normalmente aperti (NO) per i relè. Possono esistere eccezioni, nel caso, ad esempio, in cui la perdita di energia possa creare un pericolo addizionale. Possono essere necessarie funzioni di ritardo per raggiungere uno stato sicuro (IEC 60204-1, 9.2.2).
Soppressione dei transitori	Uso di un dispositivo di soppressione (filtro RC, diodo, varistore) in parallelo al carico, ma non in parallelo ai contatti. Un diodo aumenta il tempo per lo spegnimento.
Riduzione del tempo di risposta	Minimizzare il ritardo per disalimentare i componenti che commutano.
Compatibilità	Utilizzare componenti compatibili con le tensioni e le correnti usate.
Resistenza alle condizioni ambientali	Progettare l'apparecchiatura in modo che possa lavorare nelle condizioni ambientali attese e in quelle averse prevedibili, per quanto riguarda ad es. la temperatura, l'umidità, le vibrazioni e le interferenze elettromagnetiche (EMI) (si consiglia di consultare il paragrafo 10 della EN ISO 13849-2, o il punto 2.5.5 del capitolo 4 del presente documento).
Assicurare il fissaggio dei dispositivi di ingresso	Assicurare i dispositivi di ingresso (ad es. interruttori di interblocco, interruttori di posizione, finecorsa, interruttori di prossimità) in modo che la posizione, l'allineamento e la tolleranza di commutazione siano mantenute in tutte le condizioni attese (ad es. vibrazioni, normale usura, penetrazione di corpi estranei, temperatura) (ISO 14119, Clausola 5)
Protezione contro l'avvio inatteso	Prevenire l'avvio inatteso per esempio dopo aver ripristinato l'alimentazione (ISO 12100, 6.2.11.4, ISO 14118, IEC 60204-1)
Protezione del circuito di controllo	Il circuito di controllo dovrebbe essere protetto secondo quanto richiesto dalla IEC 60204-1, 7.2 e 9.1.1.
Azionamento sequenziale dei circuiti di contatti seriali di segnali ridondanti	Per evitare malfunzionamenti di modo comune a causa della saldatura di entrambi i contatti, l'accensione e lo spegnimento non avvengono simultaneamente, cosicché uno dei contatti commuta sempre senza corrente.

TAB. 35.a: TABELLA D.2, EN ISO 13849-2 – PRINCIPI DI SICUREZZA BEN PROVATI, PER I SISTEMI ELETTRICI

Principi di sicurezza ben provati	Osservazioni
Contatti positivi ad azione guidata (*mechanically linked*)	Uso dei contatti positivi ad azione guidata per, ad esempio, funzioni di monitoraggio in Categoria 2, 3, 4 (EN 50205, IEC 60947-4-1, Allegato F, IEC 60947-5-1, Allegato L)
Evitare i guasti dei cavi	Per evitare cortocircuiti tra due conduttori adiacenti: – usare cavi con lo schermo collegato al conduttore di protezione ogni volta che è necessario un cavo separato; – per cavi piatti collegare un conduttore a terra tra ciascun conduttore di segnale.
Distanza di separazione	Usare una distanza sufficiente tra terminali, componenti e cablaggi per evitare interferenze indesiderate
Limitazione dell'energia	Uso di capacità per fornire una quantità limitata di energia, per esempio in applicazioni a tempo

TAB. 35.b: TABELLA D.2, EN ISO 13849-2 – PRINCIPI DI SICUREZZA BEN PROVATI, PER I SISTEMI ELETTRICI (PROSEC.)

Principi di sicurezza ben provati	**Osservazioni**
Limitazione dei parametri elettrici	Limitazione della tensione, della corrente, dell'energia o della frequenza per limitare i movimenti (ad es.: limitazione della coppia, comando ad azione mantenuta con spostamento/tempo limitato, velocità ridotta, per evitare uno stato non sicuro)
Evitare stati non definiti	Evitare stati non definiti nel sistema di controllo. Progettare e realizzare il sistema di controllo in modo che, durante il normale funzionamento e tutte le condizioni operative attese e suoi stati (cioè le uscite) possano essere previsti.
Azionamento diretto (positivo)	L'azione è trasmessa direttamente dalla forma dell'attuatore (e non dalla forza) senza l'interposizione di elementi elastici come una molla tra attuatore e contatti (ISO 14119, 5.1, ISO 12100, 6.2.5)
Orientazione del modo di guasto	Se possibile, il dispositivo/circuito deve guastarsi andando in uno stato sicuro o in una condizione sicura.
Modo di guasto orientato	Se possibile, dovrebbero essere usati componenti o sistemi con modo di guasto orientato (ISO 12100, 6.2.12.3).
Sovra-dimensionamento	Sottodimensionare l'uso di un componente quando è impiegato nei circuiti di sicurezza per esempio: – riducendo la corrente negli interruttori al di sotto della metà del valore di targa del componente; – riducendo la frequenza di intervento degli interruttori al di sotto della metà del valore di targa del componente; – riducendo il numero totale dei cicli di intervento degli interruttori a non più del 10% di quelli corrispondenti alla durabilità media del componente.
Minimizzare la possibilità di guasti	Separare le funzioni di sicurezza dalle altre funzioni
Bilanciamento tra complessità e semplificazione	Il bilanciamento dovrebbe essere fatto tra – la complessità per raggiungere un controllo migliore e – la semplificazione per avere una migliore affidabilità.

7. Dispositivi di interblocco

7.1. Generalità sui dispositivi di interblocco

I dispositivi di interblocco di un riparo di una macchina sono costituiti da un interruttore di posizione e dall'attuatore che aziona tale interruttore alla chiusura del riparo.
Sono suddivisi dalla norma ISO 14119 nelle seguenti 4 tipologie:
- Tipo 1: elettromeccanico, con attuatore non codificato (ad es.: cerniera, camma o altro);
- Tipo 2: elettromeccanico, con attuatore codificato (ad es.: chiave, linguetta codificata o altro);
- Tipo 3: elettronico, azionato senza contatto, con attuatore non codificato (con funzionamento dell'attuatore di tipo: induttivo, magnetico, capacitivo, ultrasonico, ottico);
- Tipo 4: elettronico, azionato senza contatto, con attuatore codificato (con funzionamento dell'attuatore di tipo: magnetico, RFID, ottico).

I livelli di codifica possono essere:
- basso (da 1 a 9 variazioni possibili),
- medio (da 10 a 1000 variazioni possibili), oppure
- alto (più di 1000 variazioni possibili).

La norma ISO 14119 fornisce le misure di base per la progettazione e l'utilizzo dei dispositivi di interblocco, nonché contro l'elusione. Richiede, inoltre, l'individuazione delle motivazioni che spingono all'elusione, per eliminarla o minimizzarla. Qualora questo non fosse possibile è previsto l'impiego di misure addizionali, obbligatorie e raccomandate contro l'elusione, in funzione del tipo di interblocco e, per quelli dei Tipi 2 e 4, del livello di codifica (tab. 3, ISO 14119).

Le misure di base riguardano:
- il montaggio e il fissaggio degli interruttori (affidabile, sicuro, con l'uso di un utensile);
- il montaggio e il fissaggio degli attuatori (affidabile, sicuro, con l'uso di un utensile);
- i modi di attuazione (azione ad apertura diretta per i Tipi 1 e 2, requisiti della norma IEC 60947-5-3 per i Tipi 3 e 4 se usati singolarmente);
- la capacità di sopportare gli sforzi richiesti.

Le misure addizionali riguardano invece:
- la prevenzione dell'accesso agli elementi dell'interblocco;
- la prevenzione della sostituzione dell'attuatore con oggetti facilmente reperibili;
- la prevenzione dello smontaggio e dello spostamento degli elementi dell'interblocco utilizzando sistemi di fissaggio permanente;
- l'impiego del monitoraggio dello stato (es. verifica di una corretta successione di stati), di test ciclici della protezione, di verifiche di plausibilità con un secondo interblocco.

I Tipi 3 o 4 possono essere utilizzati in modalità singola solo se impiegano sensori di prossimità che soddisfano oltre alla norma ISO 14119 anche la norma IEC 60947-5-3 (ISO 14119, par. 5.4).
Il livello di prestazione (PL) che si può raggiungere per i dispositivi di interblocco dipende:
- dal tipo di interblocco e dalla tecnologia impiegata;
- dalla presenza di una logica di controllo per effettuare la diagnostica;
- dal tipo di collegamento utilizzato;
- dall'esclusione dei guasti.

La funzione di interblocco può essere integrata da quella di bloccaggio del riparo che in tal caso deve essere monitorabile (nella posizione inserita).
Occorre precisare, come si vedrà in dettaglio nel prossimo capitolo, che per una connessione in serie di dispositivi di interblocco si può verificare il mascheramento di un guasto su uno di essi, causato dall'apertura e dal successivo ripristino di un secondo dispositivo di interblocco, che con

tale operazione resetta l'unità logica, nascondendo il primo guasto, con la conseguenza di un probabile accumulo successivo di guasti pericolosi non rilevati.
Inoltre la connessione in serie può portare al degrado della copertura diagnostica ammissibile fino al 60% oppure addirittura a 0.

7.2. Dispositivi di interblocco di Tipo 1 e di Tipo 2

I dispositivi di interblocco dei Tipi 1 e 2 (figg. 22 e 23) possono essere usati singolarmente solo se attuati con azione meccanica diretta e con azione di apertura diretta dei contatti.

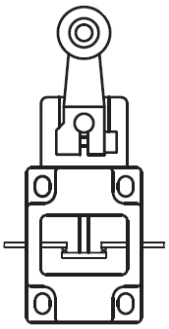


Fig. 22: Interblocco di Tipo 1 (ISO 14119)

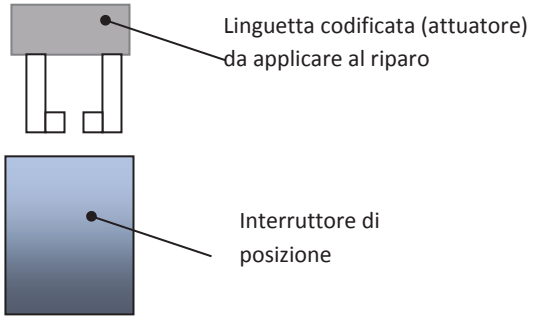


Fig. 23: Interblocco di Tipo 2

Interruttori ad azione meccanica non diretta possono essere utilizzati soltanto in combinazione con interruttori ad azione meccanica diretta e apertura diretta dei contatti (principio della diversità): tale combinazione permette anche di evitare il verificarsi di eventuali guasti di causa comune (fig. 24).

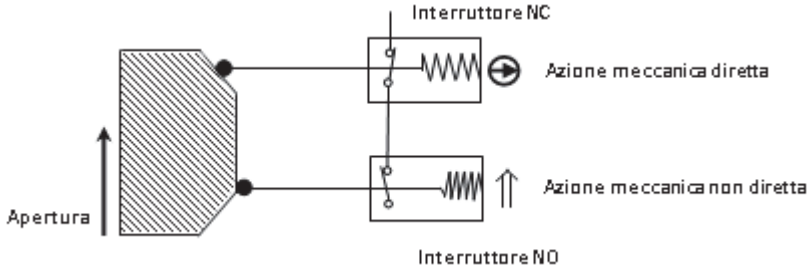


Fig. 24: Interruttore ad azione meccanica diretta in combinazione serie
con un interruttore ad azione meccanica non diretta

L'azione meccanica diretta è il movimento di un componente meccanico che deriva inevitabilmente dal movimento di un altro componente meccanico. Tale movimento può avvenire per contatto diretto o tramite elementi rigidi (ISO 14119).

L'azione di apertura positiva (come in fig. 25, indicata anche simbolicamente da una freccia all'interno di un cerchio ⊖ in fig. 24) rappresenta l'apertura di un contatto come risultato diretto di un movimento specifico dell'attuatore dell'interruttore attraverso componenti non elastici (ad es. camma rotante o lineare, fissata sul riparo, che agisce sull'interruttore) (IEC 60947-5-1, All. K).

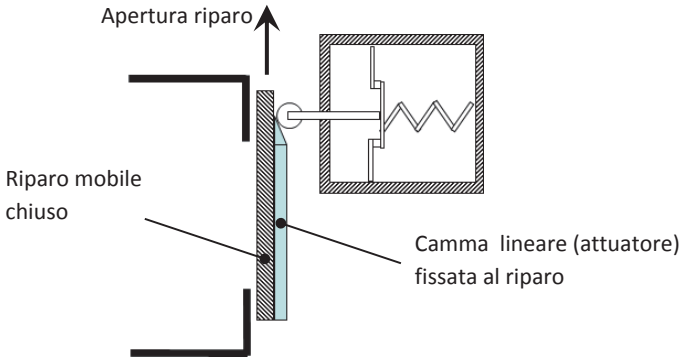


Fig. 25: Interruttore ad azione meccanica diretta ed azione di apertura positiva

Nella situazione della figura 24, a partire dall'apertura o chiusura degli interruttori, utilizzando una logica di controllo, è possibile effettuare un test di plausibilità che evidenzi gli eventuali guasti.

A titolo esemplificativo e non esaustivo, è possibile assumere i seguenti valori, reperibili sui cataloghi dei costruttori, per il Tipo 1 ad azione diretta: B_{10D} pari a 20 000 000 di cicli per il contatto NC ed a 1 000 000 di cicli per il contatto NO (con un carico ohmico del 10% sul contatto). Per il Tipo 2, a linguetta codificata (azione diretta), è possibile assumere i seguenti valori: B_{10D} pari a 2 000 000 di cicli per il contatto NC e a 1 000 000 di cicli per il contatto NO (con un carico ohmico del 10% sul contatto).

Un interruttore di posizione dei Tipi 1 o 2 ad azione diretta, conforme alla norma IEC 60947-5-1, All. K, può essere considerato "ben provato" (prospetto D.3 della norma EN ISO 13849-2), di conseguenza con esso, in una struttura di Categoria 1, può essere raggiunto un PL pari a "c".

L'esclusione dei guasti elettrici è possibile secondo le indicazioni del prospetto D.8 della norma ISO 13849-2 (in base alla conformità ai requisiti della norma IEC 60947-5-1, All. K), mentre l'esclusione dei guasti relativi al cablaggio è possibile secondo le indicazioni del prospetto D.4 della stessa norma (ad es. separazione dei conduttori).
È inoltre possibile l'esclusione dei guasti meccanici (corrosione, usura, rottura, allentamento) secondo le indicazioni del prospetto A.4 della norma EN ISO 13849-2. L'esclusione dei guasti meccanici dipende dall'applicazione in cui l'interruttore è utilizzato, per tale motivo può essere valutata solo dal costruttore della macchina. A tale scopo occorre tener conto degli sforzi meccanici cui saranno sottoposti l'interruttore e l'attuatore, inclusi quelli derivanti dai gioghi di montaggio, dal peso dei ripari e dalle condizioni di utilizzo (vibrazioni, forza applicata dagli operatori, altri stress).
L'esclusione dei guasti elettrici e/o meccanici è necessario che sia documentata. L'esclusione non è possibile per strutture per cui è richiesto PL pari a "e".

Sfruttando il principio dell'esclusione dei guasti meccanici, quando la copertura diagnostica è almeno pari al 60% (DC "bassa"), è possibile realizzare una struttura in Categoria 3, utilizzando come elemento di input un solo dispositivo con più contatti. In tal modo è possibile raggiungere un PL pari a "c" o , nei casi migliori, pari a "d", se la copertura diagnostica è sufficientemente alta. Particolare attenzione va fatta nella valutazione della copertura diagnostica quando più sensori sono collegati in serie per realizzare funzioni di sicurezza diverse e per i quali è possibile il mascheramento: infatti nel collegamento in serie non tutti i guasti possono essere rilevati e la copertura diagnostica può essere facilmente inferiore al 60% e quindi nulla.

Con l'adozione di due dispositivi fisici (principio della diversità) è invece possibile raggiungere valori di PL pari a "e", verificando che $MTTF_D$ e DC_{avg} raggiungano livelli medi o alti.

La copertura diagnostica è ottenuta collegando tali dispositivi a una unità di controllo. Quest'ultima permette anche di rilevare:
- dispersioni verso terra;
- rottura dei conduttori;
- anomalie della tensione di alimentazione;
- cortocircuiti.

Il montaggio deve garantire:
- la stabilità del dispositivo sul riparo (fissaggio sicuro con attrezzi specifici) e quella del riparo stesso;
- l'intervento dell'attuatore senza stress meccanici;
- la massima velocità d'intervento;
- l'idoneità delle condizioni ambientali (per umidità, temperatura, radiazioni, polveri, pulizia).

7.3. Dispositivi di interblocco di Tipo 3

I dispositivi di interblocco di Tipo 3 possono essere utilizzati soltanto se la valutazione del rischio dimostra che non sono neutralizzabili in modo ragionevolmente prevedibile manualmente o con l'uso di strumenti facilmente reperibili (come giraviti, chiavi, pinze o altro) o a disposizione, in quanto necessari per l'impiego della macchina (ISO 14119 par. 7.1 lettera a).
Dopo aver effettuato tale valutazione, individuando gli eventuali motivi che possono spingere all'elusione, se non è possibile eliminarli o minimizzarli, allora è necessario adottare le misure addizionali.
La norma ISO 14119 richiede di adottare almeno una delle seguenti misure addizionali per interblocchi di Tipo 3:
- montaggio fuori portata di mano;
- ostruzione fisica/schermo;
- montaggio in posizione nascosta;
- monitoraggio dello stato o test ciclico;
- fissaggio permanente dell'interruttore di posizione e dell'attuatore.

Per maggior sicurezza è raccomandato di utilizzare un secondo interblocco, che abbia, ad esempio, un diverso sistema di attuazione, con il quale verificare la plausibilità.
Ovviamente possono essere utilizzati sistemi aggiuntivi a seguito della valutazione del rischio.

7.4. Dispositivi di interblocco del Tipo 4

I dispositivi di interblocco di Tipo 4 sono basati su tecnologie elettriche ed elettroniche e utilizzano sensori magnetici, o a radiofrequenza (RFID), o ottici, quindi con azionamento senza contatto.
I sensori magnetici sono idonei ad ambienti sporchi (possono essere facilmente puliti), con difficoltà di allineamento dei ripari. Un valore di B_{10D} indicativo reperibile sui cataloghi si aggira intorno ai 2 000 000 di cicli.
I sensori RFID prevengono la manipolazione, resistono agli urti e alle vibrazioni e permettono elevate tolleranze di allineamento. Sono messi in commercio come sottosistemi (come le barriere luminose, hanno 2 uscite a semiconduttore OSSD) con PFH_D molto bassi (ad esempio tra 10^{-9} e 10^{-11} 1/h).

Tutti i tipi di sensori permettono di raggiungere valori di PL pari a "e" e sono utilizzabili in categoria 4. Devono essere collegati a una unità di controllo per le valutazioni diagnostiche. Alcuni hanno sistemi di test integrati.

7.5. Test dinamico sui connettori

Un modo per scoprire possibili guasti sui circuiti dei dispositivi di interblocco è quello di ricorrere ai test dinamici.
Con riferimento alla disposizione circuitale illustrata in figura 26, un test dinamico permette di rilevare eventuali cortocircuiti oppure interruzioni sui conduttori di collegamento al modulo di sicurezza degli interruttori di posizione SQ1 e SQ2.

Una volta rilevato il guasto il modulo di sicurezza K comanda la diseccittazione delle bobine.

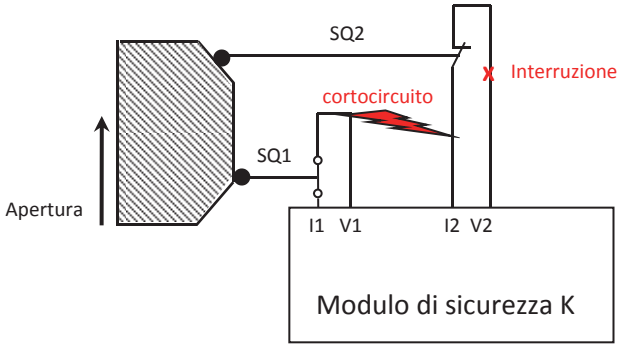


Fig. 26: Test dinamico sui connettori di SQ1 ed SQ2

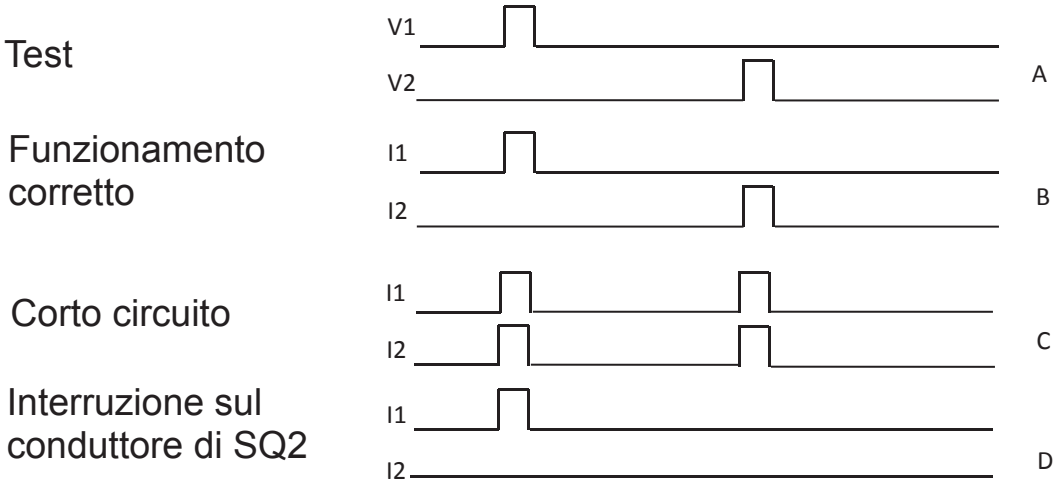


Fig. 27: Test dinamico sui connettori di SQ1 ed SQ2 (A,B,C,D)

Il test consiste nell'invio, a opportuni istanti di tempo (con sfasamento e frequenza stabiliti) di un impulso di tensione agli ingressi V1 e V2 dei due interruttori (fig. 27 A).
In caso di funzionamento corretto, negli stessi istanti di tempo (i ritardi sono trascurabili), dovranno aversi impulsi di tensione corrispondenti sui morsetti I1 e I2 (fig. 27 B).
Viceversa in caso di corto circuito fra i due cablaggi a ogni impulso di tensione su ciascun cavo corrisponderà un impulso di tensione su ambedue i morsetti I1 e I2 (fig. 27 C).
Infine, in caso di interruzione di una connessione, sul morsetto corrispondente (I2 nel caso delle figg. 26 e 27) non si rileverà alcuna tensione (fig. 27 D).

8. Mascheramento dei guasti

8.1. Il problema del mascheramento dei guasti

Il problema del mascheramento dei guasti, nel caso di utilizzo di dispositivi di interblocco connessi con gli interruttori in serie, è trattato all'interno del Technical Report ISO/TR 24119.

In tale documento il mascheramento è definito come "il ripristino involontario o l'impedimento della rilevazione di guasti in una SRP/CS a seguito dell'intervento di parti della SRP/CS sulle quali non è presente un guasto".

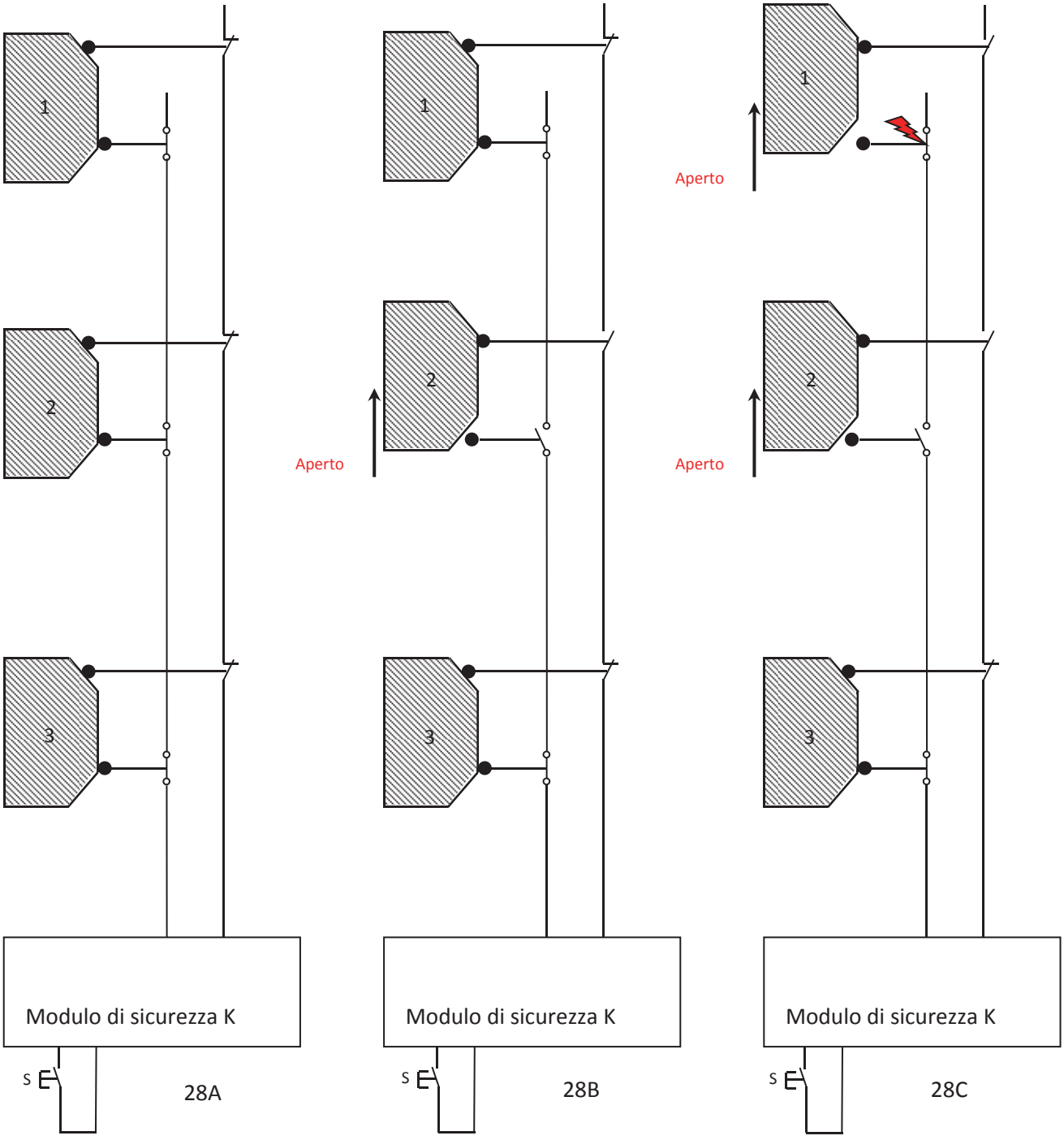
Il fenomeno si manifesta su strutture ridondanti, nel caso di dispositivi con contatti senza potenziale (puliti) connessi in serie, come avviene nel caso di più interblocchi (ad esempio per porte, cancelli o altro), collegati in ingresso a una unica logica di sicurezza, la quale svolge funzioni di diagnostica.

Sebbene in tali applicazioni un guasto singolo non porti, nella maggior parte dei casi, alla perdita della funzione di sicurezza e venga rilevato, in pratica, a volte, possono aversi dei problemi.
Infatti, è possibile che più ripari siano aperti in successione o allo stesso tempo (ad es. durante operazioni di manutenzione o durante il normale funzionamento).
A causa della connessione in serie dei contatti, guasti nel loro cablaggio, che normalmente sono rilevati dall'unità logica, possono essere mascherati dal funzionamento di uno o più di altri interblocchi connessi in serie.
Come conseguenza, è possibile che la macchina continui a operare anche se è presente un guasto nella SRP/CS.
L'accumulo di simili guasti può portare a situazioni pericolose.

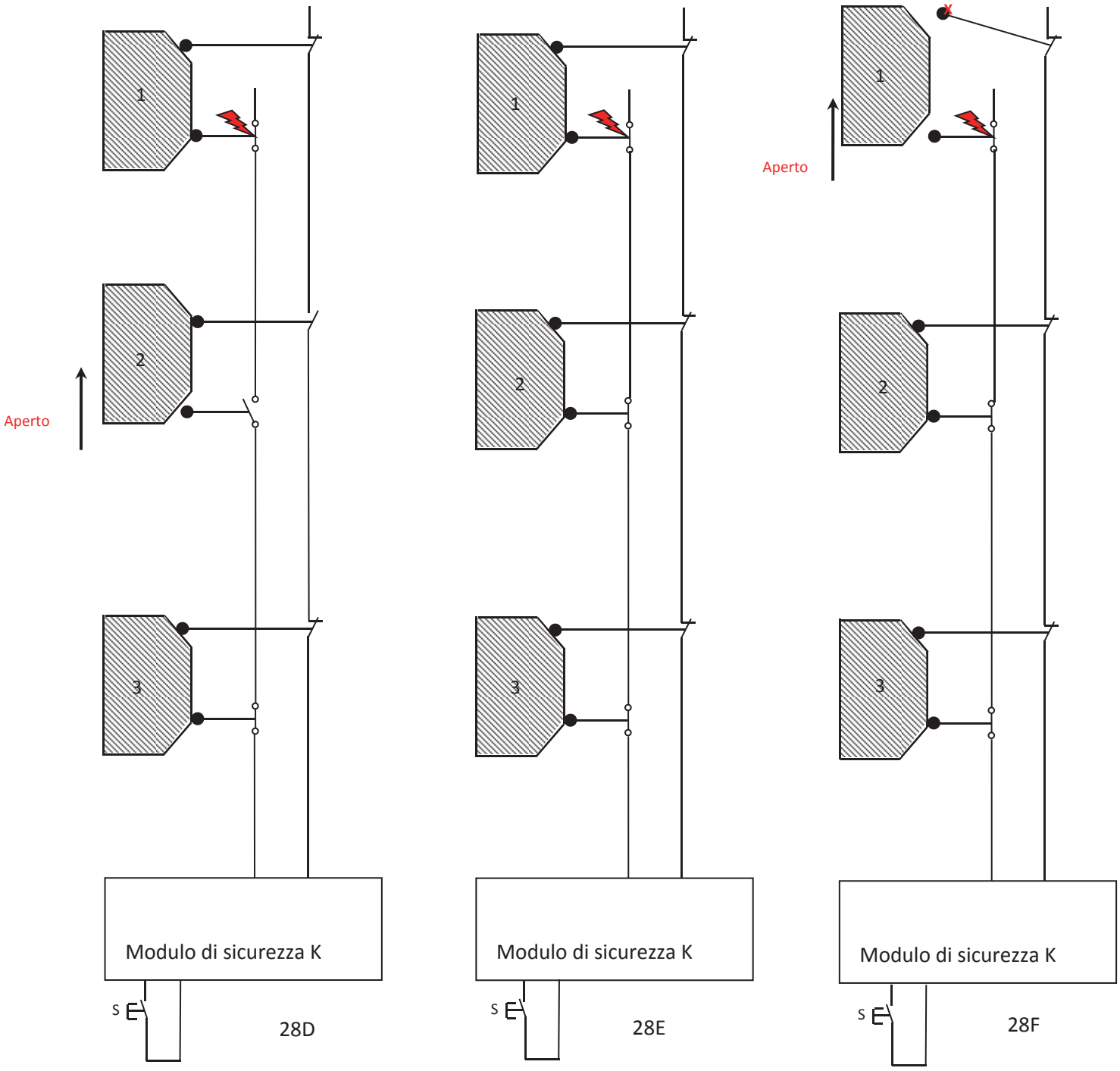
Il Technical Report ISO/TR 24119 descrive, a titolo di esempio, tre possibili casi di mascheramento del guasto:
1) mascheramento del guasto diretto
2) ripristino involontario del guasto
3) guasto su cavo con ripristino involontario

8.2. Mascheramento del guasto diretto

Nel primo dei tre possibili casi di mascheramento riportati dal Technical Report ISO/TR 24119 si considera una sequenza di ripari interbloccati ciascuno con due sensori uno NO e l'altro NC (fig. 28A). I contatti NO sono collegati in serie su un canale e quelli NC in serie su di un altro canale parallelo.
Se si apre il secondo riparo, l'operazione, correttamente, comporta l'apertura di entrambi i contatti sui due canali (fig. 28B). Se, poi, si apre il primo riparo e se il contatto NO sul primo canale resta incollato (fig. 28C), allora la logica di sicurezza non è in grado di riconoscere il guasto, perché le risultano entrambi i canali aperti. Supponendo che il primo riparo sia richiuso, il guasto resta mascherato (fig. 28D). Alla chiusura del secondo riparo ne risulterà un sistema con un guasto non rilevato sul primo canale pronto ad avviarsi (fig. 28E). Un successivo guasto sul contatto NC del primo interblocco (fig. 28F), in occasione di una nuova apertura del primo riparo, causerà una situazione di pericolo per il mancato arresto della macchina (entrambi i contatti di sicurezza interessati dal doppio guasto restano chiusi).



Figg. 28A, 28B, 28C: Mascheramento diretto del guasto



Figg. 28D, 28E, 28F: Mascheramento diretto del guasto

8.3. Ripristino involontario del guasto

Nel secondo dei tre possibili casi di mascheramento riportati dal Technical Report ISO/TR 24119 si considera un reset involontario del guasto. In particolare, se il primo riparo viene aperto e richiuso con il contatto NO incollato, allora il guasto può essere rilevato dal modulo di sicurezza all'avvio successivo, che non sarà permesso. Però se avviene la successiva apertura e chiusura del secondo riparo, questo annulla (reset) la segnalazione del guasto aprendo e chiudendo il canale con il guasto. Se si esegue tale reset della funzione di sicurezza senza risolvere il primo guasto, un secondo guasto sul primo riparo causerà una situazione di pericolo per il mancato arresto della macchina (entrambi i contatti di sicurezza interessati dal doppio guasto resteranno chiusi).

8.4. Guasto su cavo con ripristino involontario

Anche nel terzo dei tre possibili casi di mascheramento riportati dal Technical Report ISO/TR 24119 si considera un reset involontario del guasto. Se si ha un cortocircuito sul cavo di un contatto del primo riparo, che viene aperto e richiuso, e subito dopo avviene l'apertura e chiusura del secondo riparo questo maschera il guasto allo stesso modo dei casi precedenti. È evidente quindi che in tale condizione un secondo guasto sul primo interblocco non causerà l'arresto della macchina dopo l'apertura del relativo riparo.

8.5. Suggerimenti per aumentare la resistenza al mascheramento del guasto

Il Technical Report ISO/TR 24119 suggerisce, per aumentare la resistenza al mascheramento del guasto, di usare metodi diagnostici differenti, di migliorare il cablaggio e di adottare la ridondanza dei dispositivi con tipi diversi di interblocco per permettere l'esclusione dei guasti.

Considerato che l'accumulo dei guasti porta a un degrado della copertura diagnostica (e questo limita automaticamente il massimo PL raggiungibile a PL "d" e la massima DC a "media"), il documento suggerisce due metodi per valutare la massima DC raggiungibile, uno semplificato, l'altro più dettagliato che deve essere applicato quando con il primo non si riesce a ottenere il livello di DC desiderato.

Nel metodo semplificato la massima copertura diagnostica raggiungibile si determina con la tab. 36 seguente.

TAB. 36: DC_{max} – METODO SEMPLIFICATO PER LA VALUTAZIONE DELLA MASSIMA COPERTURA DIAGNOSTICA

numero di ripari mobili aperti di frequente [a), b)]	Numero di ripari mobili addizionali [c)]	DC massima [d)]
0	da 2 a 4	media
	da 5 a 30	bassa
	> 30	nulla
1	1	media
	da 2 a 4	bassa
	≥5	nulla
> 1	≥0	nulla

a) Se la frequenza è più alta di 1/h.
b) Se il numero di operatori in grado di aprire ripari separati è maggiore di 1, allora il numero di ripari mobili aperti di frequente deve essere aumentato di 1.
c) Il numero di ripari mobili addizionali può essere ridotto di 1 se la distanza minima tra i ripari è maggiore di 5 m oppure se nessuno dei ripari addizionali è direttamente raggiungibile.
d) In ogni caso se è prevedibile il mascheramento del guasto (cioè se i ripari mobili possono essere aperti contemporaneamente come parte del funzionamento o per manutenzione), allora la DC deve essere considerata nulla.

Nel metodo più dettagliato sono presi in considerazione:
- il numero di dispositivi di interblocco collegati in serie;
- la frequenza di apertura dei ripari;
- la distanza tra i ripari interessati;
- l'accessibilità dei ripari;
- il numero di operatori coinvolti.

TAB. 37: DC_{max} – METODO PIÙ DETTAGLIATO: LIVELLO DELLA PROBABILITÀ DI MASCHERAMENTO

numero di ripari mobili aperti di frequente [a), b)]	Numero di ripari mobili addizionali [c)]	Livello della probabilità di mascheramento (FM) [d)]
0	da 2 a 4	1
	da 5 a 30	2
	> 30	3
1	1	1
	da 2 a 4	2
	≥5	3
> 1	≥0	3

a) Se la frequenza è più alta di 1/h.
b) Se il numero di operatori in grado di aprire ripari separati è maggiore di 1, allora il numero di ripari mobili aperti di frequente deve essere aumentato di 1.
c) Il numero di ripari mobili addizionali può essere ridotto di 1 se la distanza minima tra i ripari è maggiore di 5 m oppure se nessuno dei ripari addizionali è direttamente raggiungibile.
d) In ogni caso se è prevedibile il mascheramento del guasto (cioè se i ripari mobili possono essere aperti contemporaneamente come parte del funzionamento o per manutenzione), allora il livello della probabilità di mascheramento (FM) è 3.

Il metodo più dettagliato parte dal livello della probabilità di mascheramento (FM), aggiungendo vincoli su:
- il tipo di cablaggio (a stella, ramificato, ad anello);
- l'impiego di configurazione a interruttore singolo o ridondante;
- la tecnica diagnostica per il segnale (stessa polarità, polarità inversa, segnali dinamici).

Inoltre è fatta distinzione per l'impiego di cavi multipolari protetti o non protetti con o senza cavo a tensione positiva. La copertura diagnostica si ricava dalle tabelle 38, 39 e 40.

TAB. 38: MASSIMA DC RAGGIUNGIBILE DA CAVI MULTIPOLARI NON PROTETTI SENZA CONDUTTORE A TENSIONE POSITIVA (+U)

Numero di interruttori ad apertura positiva	cablaggio	Valutazione del segnale	Massima DC raggiungibile		
			FM=3	FM=2	FM=1
Disposizione singola	Ramificato/A stella	Stessa polarità (+U/+U)	nulla	bassa	media
		Polarità inversa (+U/GND)	nulla	bassa	media
		Segnali dinamici	nulla	bassa	media
	Ad anello	Stessa polarità (+U/+U)	nulla	bassa	media
		Polarità inversa (+U/GND)	nulla	bassa	media
		Segnali dinamici	media	media	media
Disposizione ridondante	Ramificato/A stella	Stessa polarità (+U/+U)	nulla	bassa	media
		Polarità inversa (+U/GND)	nulla	bassa	media
		Segnali dinamici	nulla	bassa	media
	Ad anello	Stessa polarità (+U/+U)	media	media	media
		Polarità inversa (+U/GND)	nulla	bassa	media
		Segnali dinamici	media	media	media

TAB. 39: MASSIMA DC RAGGIUNGIBILE DA CAVI MULTIPOLARI NON PROTETTI CON CONDUTTORE A TENSIONE POSITIVA (+U)

Numero di interruttori ad apertura positiva	cablaggio	Valutazione del segnale	Massima DC raggiungibile		
			FM=3	FM=2	FM=1
Disposizione singola	Ramificato/A stella	Stessa polarità (+U/+U)	nulla	bassa	media
		Polarità inversa (+U/GND)	nulla	bassa	media
		Segnali dinamici	bassa	media	media
	Ad anello	Stessa polarità (+U/+U)	nulla	bassa	media
		Polarità inversa (+U/GND)	nulla	bassa	media
		Segnali dinamici	media	media	media
Disposizione ridondante	Ramificato/A stella	Stessa polarità (+U/+U)	nulla	bassa	media
		Polarità inversa (+U/GND)	nulla	bassa	media
		Segnali dinamici	bassa	media	media
	Ad anello	Stessa polarità (+U/+U)	nulla	bassa	media
		Polarità inversa (+U/GND)	nulla	bassa	media
		Segnali dinamici	media	media	media

TAB. 40: MASSIMA DC RAGGIUNGIBILE DA CAVI MULTIPOLARI PROTETTI CON O SENZA CONDUTTORE A TENSIONE POSITIVA (+U)

Numero di interruttori ad apertura positiva	cablaggio	Valutazione del segnale	Massima DC raggiungibile		
			FM=3	FM=2	FM=1
Disposizione singola	Ramificato/A stella	Stessa polarità (+U/+U)	media	media	media
		Polarità inversa (+U/GND)	nulla	bassa	media
		Segnali dinamici	media	media	media
	Ad anello	Stessa polarità (+U/+U)	media	media	media
		Polarità inversa (+U/GND)	nulla	bassa	media
		Segnali dinamici	media	media	media
Disposizione ridondante	Ramificato/A stella	Stessa polarità (+U/+U)	media	media	media
		Polarità inversa (+U/GND)	nulla	bassa	media
		Segnali dinamici	media	media	media
	Ad anello	Stessa polarità (+U/+U)	media	media	media
		Polarità inversa (+U/GND)	nulla	bassa	media
		Segnali dinamici	media	media	media

In ogni caso se è prevedibile il mascheramento del guasto (cioè se i ripari mobili possono essere aperti allo stesso tempo come parte del funzionamento o per manutenzione), allora la DC deve essere considerata nulla.

È possibile, a ogni modo, evitare il mascheramento utilizzando contatti addizionali e misure diagnostiche adeguate oppure ripiegando su ingressi individuali per ogni interblocco oppure ancora usando dispositivi con diagnostica incorporata: i costruttori forniscono sul mercato soluzioni sofisticate per diverse esigenze e applicazioni.

9. Esempi

9.1. Esempio 1

Un riparo interbloccato, situato sulla parte superiore di una pialla a spessore per legno, per la protezione contro l'accesso all'organo di taglio e al meccanismo per l'alimentazione del pezzo da lavorare, può essere realizzato in Categoria 1.
Per realizzare la relativa SRP/CS in Categoria 1 è essenziale il ricorso a componenti "ben provati", insieme all'adozione dei principi di sicurezza base e di quelli ben provati.
Per la sicurezza si sottolinea l'importanza dell'individuazione corretta delle condizioni sotto le quali un componente possa essere definito "ben provato".
La pialla a spessore per legno (fig. 29) è una macchina progettata per tagliare e rendere piana la superficie superiore di un pezzo da lavorare.
Il pezzo da lavorare è supportato su una tavola poggia-pezzo che può essere sollevata verso l'utensile. L'utensile è realizzato con un cilindro metallico sul quale sono calettate delle lame che asportano il materiale. L'utensile e le parti in movimento per l'alimentazione del pezzo si trovano sotto il riparo superiore (fig. 30).

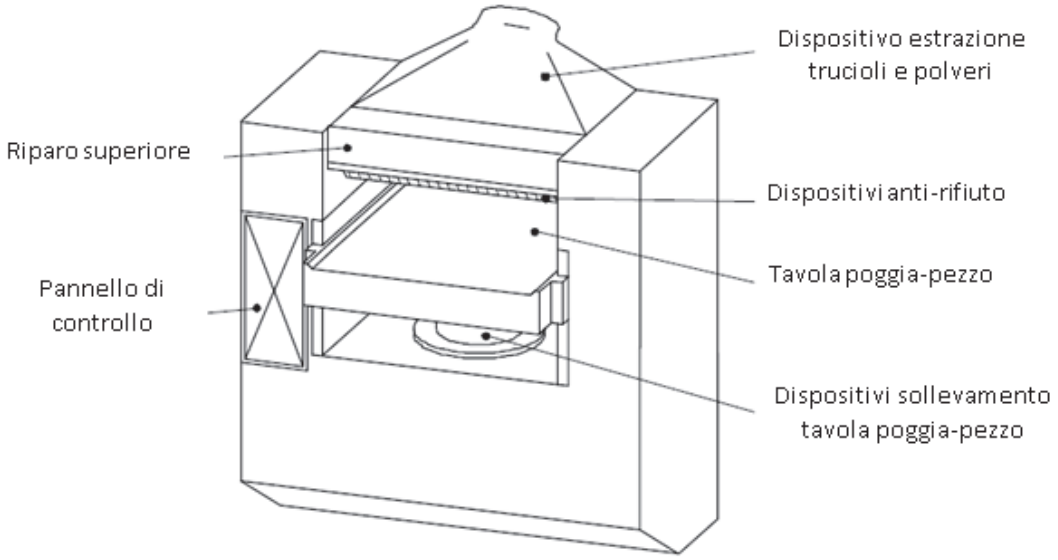


Fig. 29: Pialla a spessore per legno

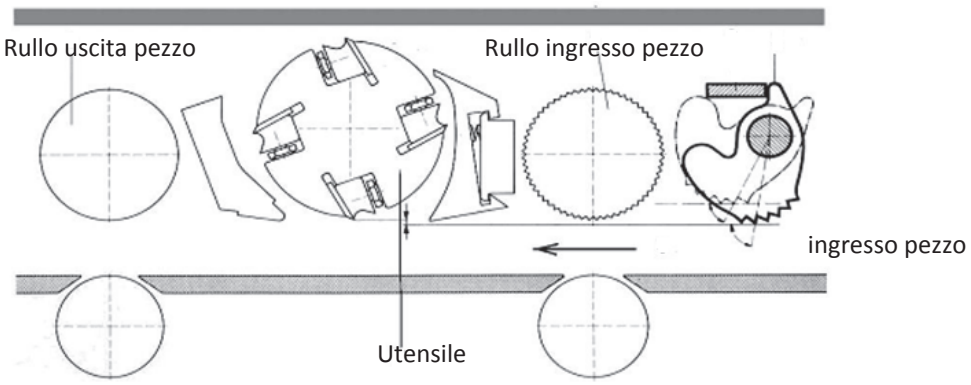


Fig. 30: Vista in sezione verticale sotto il riparo superiore

La descrizione della macchina, del suo funzionamento e dei suoi limiti, relativamente alle parti di interesse per la funzione di sicurezza, è funzionale alla definizione di quest'ultima.

- Definizione della funzione di sicurezza: interblocco del riparo superiore della macchina con l'alimentazione di potenza del motore.
- Descrizione funzionale: l'apertura del riparo mobile superiore della pialla a spessore causa l'attuazione del microinterruttore di interblocco che apre il contattore del motore, che rimane senza potenza. In tal modo si previene o si arresta il movimento dell'utensile e l'alimentazione del pezzo. Il tempo di arresto non supera il valore massimo di 10 secondi richiesto dalla norma EN 860:2007+A2:2012.

Per questa funzione di sicurezza di interblocco del riparo è richiesto un PL = "c" dalla norma EN 860:2012 (5.3.7.1).

Le caratteristiche scelte per il progetto della SRP/CS sono le seguenti:
- PL_r = "c";
- architettura a canale singolo in Categoria 1;
- applicazione dei principi di sicurezza di base e "ben provati";
- utilizzo di componenti "ben provati".

Lo schema circuitale e il diagramma a blocchi della SRP/CS da realizzare sono riportati in fig. 31, dove SQ1 è il microinterruttore di interblocco (NC) e KM11 è il contattore.

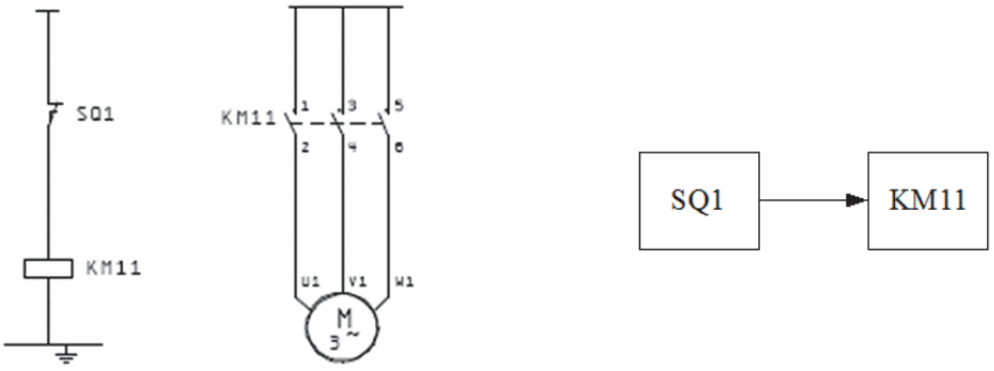


Fig. 31: Schema circuitale e diagramma a blocchi

L'interruttore di sicurezza SQ1 con cui si realizza il dispositivo d'ingresso è uno switch ad attuatore separato con contatti normalmente chiusi (NC) ad apertura diretta, dichiarato dal costruttore conforme alla norma IEC 60947-5-1, Allegato K, che quindi può essere considerato "ben provato" secondo il prospetto D.3 della norma EN ISO 13849-2 (Validazione).
Per l'interruttore di sicurezza SQ1 si può assumere un B_{10D} = 2 000 000 (tab. 11). È necessario che siano soddisfatti i principi di sicurezza di base e i principi ben provati applicabili, secondo i prospetti D1 e D2 della norma EN ISO 13849-2 (Validazione), in particolare:

• Principi di sicurezza di base (prospetto D1 della norma EN ISO 13849-2):
- selezione di materiali idonei all'applicazione;
- dimensionamento corretto e montaggio sicuro e stabile sulla parte fissa e sul riparo mobile (evitare giochi, vibrazioni);
- contatti NC;
- l'attuatore deve inserirsi e disinserirsi facilmente e correttamente senza urti, attriti, sforzi;
- l'attuatore separato deve essere fissato in maniera inamovibile sul riparo (in modo da non essere manomesso);

- l'inserimento deve essere rapido in modo da non allungare il tempo di intervento;
- il dispositivo deve essere idoneo all'applicazione (condizioni ambientali, temperatura, pressione, vibrazioni, radiazioni, liquidi corrosivi, gas corrosivi o altro che potrebbe limitare le prestazioni richieste).

• Principi di sicurezza ben provati (prospetto D2 della norma EN ISO 13849-2):
- modo positivo di azionamento;
- sovradimensionamento;
- prevenzione dei guasti sui cavi (es. cavi schermati, connessione equipotenziale di terra, cablaggio lontano da urti e influenze ambientali).

Supponendo d_{op}=220 (giorni/anno), h_{op}= 8 (ore), t_{cycle}= 8 (ore) si ottiene:
- n_{op}= (220×8×3600)/ (3600×8)=220 cicli/anno;
- T_{10D}= B_{10D}/n_{op}= 2 000 000/220=9091 anni;
- $MTTF_D$=T_{10D}/0,1=90910 anni (alto).

Il tempo di servizio (durata di utilizzo) è 20 anni.

Il contattore KM11 scelto è della Categoria AC-3, per AC o DC, conforme alla norma IEC 60947-4-1, che in condizioni di carico nominale e se sono soddisfatti i principi di sicurezza di base e ben provati (prospetti D1 e D2 della norma EN ISO 13849-2) si assume abbia B_{10D} = 1 300 000 (tab. 11).

Per poter utilizzare tale contattore in un'architettura in Categoria 1 occorre che sia "ben provato", cioè che soddisfi le condizioni addizionali del prospetto D.3 della norma EN ISO 13849-2 che richiedono:
- la protezione contro altre influenze quali, vibrazioni, temperatura, polveri, acidi;
- l'impiego di metodi ben provati (tab. D.2 della norma EN ISO 13849-2) per evitare guasti, quali il sovradimensionamento (es. riduzione della corrente di carico al 50% del valore nominale);
- la limitazione della corrente di carico con una protezione termica;
- la protezione dal sovraccarico.

Supponendo d_{op}=220 (giorni/anno), h_{op}= 8 (ore), t_{cycle}= 1 (ore) si ottiene:
- n_{op}= (220×8×3600)/ (3600×1)=1760 cicli/anno;
- T_{10D}= B_{10D}/n_{op}= 1 300 000/1760=739 anni;
- $MTTF_D$=T_{10D}/0,1=7390 anni (alto).

Il valore di $MTTF_D$ del canale (par. D.1) è pari a 6834 anni che deve essere tagliato a 100 anni.
Dalla tabella K (fig. 32) si ricava per l'architettura in Categoria 1 un PL= "c" per un PFH_D = 1,14×10^{-6}.

$MTTF_d$ for each channel years	Cat. B PL DC_{avg} = none	Cat. 1 PL DC_{avg} = none	Cat. 2 PL DC_{avg} = low	Cat. 2 PL DC_{avg} = medium	Cat. 3 PL DC_{avg} = low	Cat. 3 PL DC_{avg} = medium	Cat. 4 PL DC_{avg} = high
15	$7,61 \times 10^{-6}$ b		$4,53 \times 10^{-6}$ b	$3,01 \times 10^{-6}$ b	$1,82 \times 10^{-6}$ c	$7,44 \times 10^{-7}$ d	
16	$7,13 \times 10^{-6}$ b		$4,21 \times 10^{-6}$ b	$2,77 \times 10^{-6}$ c	$1,67 \times 10^{-6}$ c	$6,76 \times 10^{-7}$ d	
18	$6,34 \times 10^{-6}$ b		$3,68 \times 10^{-6}$ b	$2,37 \times 10^{-6}$ c	$1,41 \times 10^{-6}$ c	$5,67 \times 10^{-7}$ d	
20	$5,71 \times 10^{-6}$ b		$3,26 \times 10^{-6}$ b	$2,06 \times 10^{-6}$ c	$1,22 \times 10^{-6}$ c	$4,85 \times 10^{-7}$ d	
22	$5,19 \times 10^{-6}$ b		$2,93 \times 10^{-6}$ c	$1,82 \times 10^{-6}$ c	$1,07 \times 10^{-6}$ c	$4,21 \times 10^{-7}$ d	
24	$4,76 \times 10^{-6}$ b		$2,65 \times 10^{-6}$ c	$1,62 \times 10^{-6}$ c	$9,47 \times 10^{-7}$ d	$3,70 \times 10^{-7}$ d	
27	$4,23 \times 10^{-6}$ b		$2,32 \times 10^{-6}$ c	$1,39 \times 10^{-6}$ c	$8,04 \times 10^{-7}$ d	$3,10 \times 10^{-7}$ d	
30		$3,80 \times 10^{-6}$ b	$2,06 \times 10^{-6}$ c	$1,21 \times 10^{-6}$ c	$6,94 \times 10^{-7}$ d	$2,65 \times 10^{-7}$ d	$9,54 \times 10^{-8}$ e
33		$3,46 \times 10^{-6}$ b	$1,85 \times 10^{-6}$ c	$1,06 \times 10^{-6}$ c	$5,94 \times 10^{-7}$ d	$2,30 \times 10^{-7}$ d	$8,57 \times 10^{-8}$ e
36		$3,17 \times 10^{-6}$ b	$1,67 \times 10^{-6}$ c	$9,39 \times 10^{-7}$ d	$5,16 \times 10^{-7}$ d	$2,01 \times 10^{-7}$ d	$7,77 \times 10^{-8}$ e
39		$2,93 \times 10^{-6}$ c	$1,53 \times 10^{-6}$ c	$8,40 \times 10^{-7}$ d	$4,53 \times 10^{-7}$ d	$1,78 \times 10^{-7}$ d	$7,11 \times 10^{-8}$ e
43		$2,65 \times 10^{-6}$ c	$1,37 \times 10^{-6}$ c	$7,34 \times 10^{-7}$ d	$3,87 \times 10^{-7}$ d	$1,54 \times 10^{-7}$ d	$6,37 \times 10^{-8}$ e
47		$2,43 \times 10^{-6}$ c	$1,24 \times 10^{-6}$ c	$6,49 \times 10^{-7}$ d	$3,35 \times 10^{-7}$ d	$1,34 \times 10^{-7}$ d	$5,76 \times 10^{-8}$ e
51		$2,24 \times 10^{-6}$ c	$1,13 \times 10^{-6}$ c	$5,80 \times 10^{-7}$ d	$2,93 \times 10^{-7}$ d	$1,19 \times 10^{-7}$ d	$5,26 \times 10^{-8}$ e
56		$2,04 \times 10^{-6}$ c	$1,02 \times 10^{-6}$ c	$5,10 \times 10^{-7}$ d	$2,52 \times 10^{-7}$ d	$1,03 \times 10^{-7}$ d	$4,73 \times 10^{-8}$ e
62		$1,84 \times 10^{-6}$ c	$9,06 \times 10^{-7}$ d	$4,43 \times 10^{-7}$ d	$2,13 \times 10^{-7}$ d	$8,84 \times 10^{-8}$ e	$4,22 \times 10^{-8}$ e
68		$1,68 \times 10^{-6}$ c	$8,17 \times 10^{-7}$ d	$3,90 \times 10^{-7}$ d	$1,84 \times 10^{-7}$ d	$7,68 \times 10^{-8}$ e	$3,80 \times 10^{-8}$ e
75		$1,52 \times 10^{-6}$ c	$7,31 \times 10^{-7}$ d	$3,40 \times 10^{-7}$ d	$1,57 \times 10^{-7}$ d	$6,62 \times 10^{-8}$ e	$3,41 \times 10^{-8}$ e
82		$1,39 \times 10^{-6}$ c	$6,61 \times 10^{-7}$ d	$3,01 \times 10^{-7}$ d	$1,35 \times 10^{-7}$ d	$5,79 \times 10^{-8}$ e	$3,08 \times 10^{-8}$ e
91		$1,25 \times 10^{-6}$ c	$5,88 \times 10^{-7}$ d	$2,61 \times 10^{-7}$ d	$1,14 \times 10^{-7}$ d	$4,94 \times 10^{-8}$ e	$2,74 \times 10^{-8}$ e
100		$1,14 \times 10^{-6}$ c	$5,28 \times 10^{-7}$ d	$2,29 \times 10^{-7}$ d	$1,01 \times 10^{-7}$ d	$4,29 \times 10^{-8}$ e	$2,47 \times 10^{-8}$ e

Fig. 32: PFH_D (1/h) – ISO 13849-1, estratto tabella K.1

9.2. Esempio 2

Per mostrare il processo di validazione, in particolare per quanto riguarda la copertura diagnostica e il CCF, si può considerare come esempio una funzione di arresto di un motore tramite interblocco.

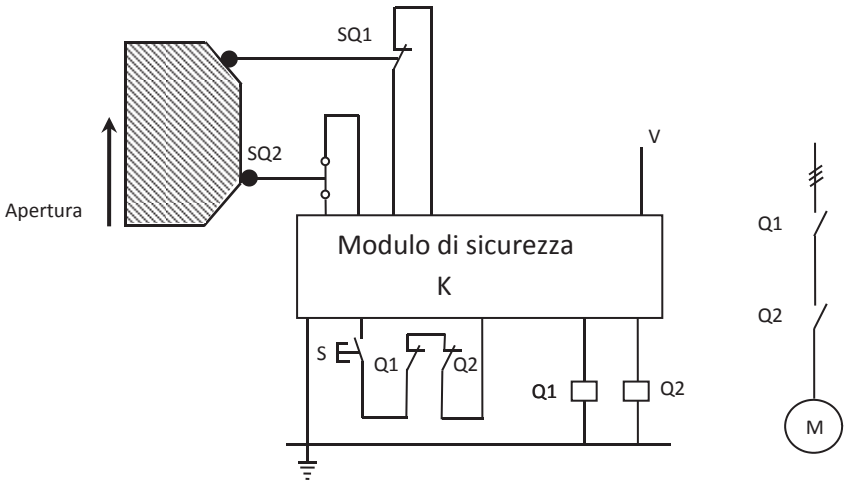


Fig. 33: Schema circuitale

- Definizione della funzione di sicurezza: funzione di arresto del motore tramite l'interblocco di un riparo mobile per prevenire l'accesso a una zona pericolosa.
- Descrizione funzionale: l'apertura del riparo mobile superiore causa l'apertura dell'interruttore SQ1 (NC) ad azione positiva e l'apertura dell'interruttore SQ2 tramite il contatto NO. Entrambi i contattori Q1 e Q2 pilotati rispettivamente dalle omonime bobine aprono il circuito di potenza e tolgono energia al motore.

Il progetto, basato sulla richiesta di un PL_r "e", è caratterizzato dai seguenti dati e risultati:
- architettura in Categoria 4;
- schema circuitale mostrato in fig. 33 e diagramma a blocchi mostrato in fig. 34.

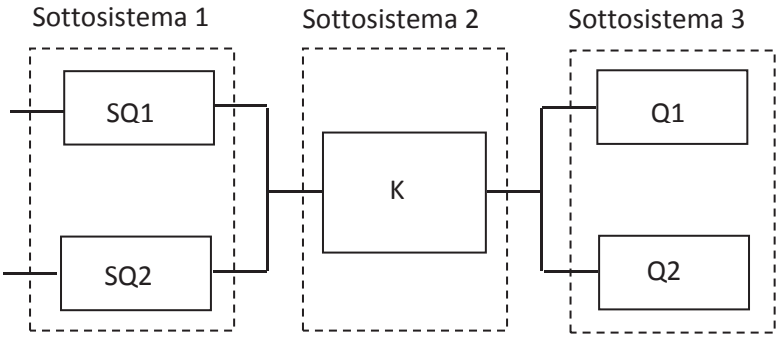


Fig. 34: Diagramma a blocchi

La funzione di sicurezza è composta da tre sottosistemi: il primo è costituito dai sensori, il secondo dal modulo di sicurezza e il terzo dai contattori.

- B_{10D} SQ1: 20 000 000 ridotto a 2 000 000;
- B_{10D} SQ2: 1 000 000 (con il 10% di carico ohmico sul contatto);
- $MTTF_D$ SQ1: 631 anni; T_{10D}=63 anni;
- $MTTF_D$ SQ2: 316 anni ; T_{10D}= 32 anni (d=220 g; h=24 ore; t=600 s);
- La simmetrizzazione (par. D.2) fornisce un valore di $MTTF_D$ pari a 491 anni per i due canali del sottosistema 1 (si ricorda che nella Categoria 4 il taglio $MTTF_D$ si ha per valori superiori a 2500 anni);
- modulo di sicurezza K: Categoria 4, PFH_D= 3×10^{-8}, DC Alta, T_{10D} > 20 anni;
- B_{10D} Q1/Q2: 1 300 000;
- $MTTF_D$ Q1 e $MTTF_D$ Q2: 410 anni ciascuno (d=220 g; h=24 ore; t=600 s) e T_{10D}=41 anni;
- La simmetrizzazione (par. D.2) fornisce un valore di $MTTF_D$ pari a 410 anni per i due canali del sottosistema 3 (si ricorda che nella Categoria 4 il taglio $MTTF_D$ si ha per valori superiori a 2500 anni);
- PFH_D sottosistema 1 (SQ1 ed SQ2): $4{,}7\times10^{-9}$ (interpolato dalla tabella K.1 della ISO 13849-1); PL “e”;
- PFH_D sottosistema 2 (K): 3×10^{-8}; PL “e”;
- PFH_D sottosistema 3 (Q1 ed Q2): $5{,}7\times10^{-9}$ (interpolato dalla tabella K.1 della ISO 13849-1); PL “e”;
- PFH_D della funzione di sicurezza : 4×10^{-8}; PL “e”;
- CCF: punteggio > 65 (Separazione, protezione contro sovra-correnti e sovratensioni, altre influenze, condizioni ambientali, competenza progettisti).

Il diagramma a blocchi poteva anche essere diversamente realizzato, con risultati simili, ponendo in un unico sottosistema interruttori e contattori come mostrato in fig. 35.

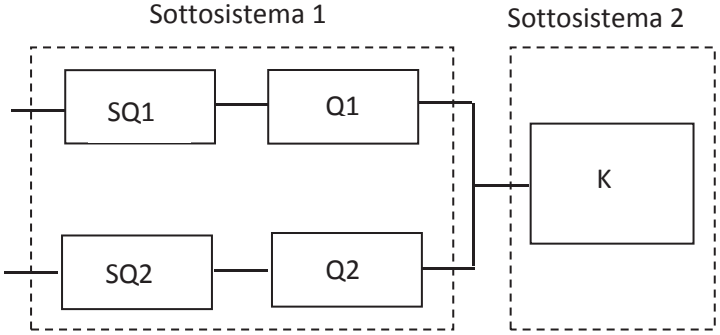


Fig. 35: Diagramma a blocchi alternativo a quello di fig. 34

La validazione può essere fatta sulla base dei ragionamenti che seguono.

I valori dei parametri del rischio, corrispondenti a una gravità del danno alta (S2), a una esposizione al pericolo (F2) prolungata, che supera 1/20 del tempo operativo, e a un danno difficilmente evitabile (P2), giustificano la scelta del livello di prestazione PL_r pari a "e".

L'architettura della SRP/CSF, rappresentata dallo schema circuitale di fig. 35 e dal diagramma a blocchi di fig. 36, è ridondante, con due canali in ingresso (elettromeccanici), un modulo di sicurezza configurabile (mediante software), due canali di uscita e una funzione diagnostica (1oo2D). Il singolo guasto non porta alla perdita della funzione di sicurezza.

Dall'esame della documentazione tecnica e delle condizioni di utilizzo, risulta che sono rispettate le norme tecniche applicabili e i principi base di sicurezza nonché i principi ben provati. In particolare, sono presenti le protezioni contro i contatti diretti e indiretti, le sovratensioni, le cadute di tensione, le sovracorrenti, i guasti a terra e i guasti dell'isolamento.

Le bobine dei contattori Q1 e Q2 sono protette da diodi contro effetti EMC.
Dall'esame della documentazione tecnica il modulo di sicurezza è certificato e dichiarato dal costruttore in Categoria 4 e PL "e" con PFH_D pari a 3×10^{-8}.

Il software di configurazione è messo a disposizione dal costruttore, ha un nome, una versione e le modifiche non autorizzate sono evitate tramite password; sono utilizzate misure per garantire la consistenza dei dati (controllo sugli ingressi).
I sensori hanno ingressi separati sul modulo di sicurezza e sono da questo monitorati utilizzando un criterio di plausibilità che permette una copertura diagnostica alta, del 99%, e il controllo è effettuato ogni volta che il dispositivo cambia stato.

L'interruttore SQ1 (NC) è del tipo ad apertura diretta, ad azionamento positivo, conforme alla norma IEC 60947-5-1 All. K e può essere considerato "ben provato" (tab. D.3 della norma ISO 13849-2). L'interruttore SQ2 (NO) non è ad azionamento positivo.

La documentazione tecnica allegata conferma le caratteristiche tecniche indicate.

Il montaggio è stato effettuato correttamente, rispettando la stabilità del riparo, garantendo l'azionamento dell'attuatore, annullando gli stress meccanici, con un fissaggio solido e controllando l'assenza di influssi esterni negativi (ad es. vibrazioni).
Per quanto riguarda il cablaggio, il modulo di controllo permette di rilevare la rottura dei conduttori, eventuali dispersioni verso terra, cortocircuiti e consente di monitorare la tensione di alimentazione.
La saldatura di un contatto o un guasto del cablaggio su un interruttore di posizione è rilevata dall'unità di controllo tramite una verifica di plausibilità fra gli interruttori.

I cavi sono installati con percorsi separati e in modo da evitare problemi EMC.

Il valore di $MTTF_D$ della SRP/CS costituita dagli interruttori di posizione è alto e la sua valutazione è correttamente riportata nella documentazione allegata.

Il singolo guasto è rilevato al momento della richiesta della funzione di sicurezza o prima della stessa e la sua funzionalità è sempre garantita. La copertura diagnostica è alta. Le misure contro i CCF sono applicate e sono sufficienti (punteggio superiore a 65).

L'accumulo di più di due guasti può portare alla perdita della funzione di sicurezza.
Il sottosistema 1 è validato in termini di PL "e" e Categoria 4 dichiarata.

Il sottosistema 2 è certificato come PL "e" e Categoria 4 con il relativo PFH_D documentato.

I contattori Q1 e Q2 costituiscono il sottosistema 3 e per l'individuazione dei possibili guasti può essere effettuata una FMEA i cui risultati sono riportati nella tab. 41 seguente.

TAB. 41: FMEA PER I GUASTI DEI CONTATTORI Q1 E Q2

Guasto possibile	Verifica
Il contatto Q1 o Q2 non si rilascia	Il guasto è rilevato in avvio dal PLC (test di start up).
Il contatto Q1 o Q2 non si chiude	Il guasto non è pericoloso perché il motore non parte, tale guasto si rileva dal processo.
Circuito aperto sui contatti ausiliari Q1 o Q2	Il guasto è rilevato dal modulo K.
Chiusura non contemporanea di Q1 e Q2	Il guasto non è rilevato, non è pericoloso finché Q1 e Q2 sono integri. È possibile l'esclusione del guasto poiché i collegamenti e i cablaggi sono isolati.

Considerata l'analisi effettuata e considerato il monitoraggio diretto, effettuato dal modulo K al momento dell'avvio, la copertura diagnostica per la SRP/CS costituita dai contattori può essere considerata alta (99%) come dichiarato. Ne segue che anche per il sottosistema 3 il singolo guasto è rilevato al momento della richiesta della funzione di sicurezza o prima della stessa e la sua funzionalità è sempre garantita.
Il valore di $MTTF_D$ del sottosistema 3 è alto, la sua valutazione è correttamente riportata nella documentazione allegata.
Le misure contro i CCF sono applicate e sono sufficienti (punteggio superiore a 65).
L'accumulo di più di due guasti può portare alla perdita della funzione di sicurezza.
Il sottosistema 3 è validato in termini di PL "e" e Categoria 4 dichiarata.

La funzione di sicurezza risulta dalla combinazione dei tre sottosistemi descritti, tutti con PL "e".
Il PL risultante è determinato dalla somma dei rispettivi PFH_D.
Poiché il risultato è un PFH_D pari a $4 \times 10^{-8} < 10^{-7}$, la combinazione è un'architettura con PL "e" in Categoria 4.

9.3. Esempio 3

Secondo le indicazioni della norma EN 691-1, paragrafo 5.2.1.12, (oppure della norma ISO 19085-1, paragrafo 5.2.5), è possibile l'applicazione di un'architettura in Categoria 2 per realizzare una funzione di frenatura su macchine da legno, con tecnologia elettrica di PL pari a "b".
Si è scelto un esempio di questo tipo per mostrare come la normativa di tipo C impieghi la EN ISO 13849-1, cercando di risolvere problemi applicativi in funzione dello stato dell'arte e della valutazione del rischio.

- Definizione della funzione di sicurezza: funzione di frenatura del motore tramite azionamento di un inverter che riduce linearmente a zero (rampa decrescente) la corrente negli avvolgimenti del motore.
- Descrizione funzionale: l'azionamento del pulsante di arresto normale o di emergenza provoca l'invio da parte dell'unità di controllo (PLC) del segnale di frenata all'inverter. Quest'ultimo avvia la frenatura (rampa di discesa) fino a ridurre a zero la corrente del motore e conseguentemente la sua velocità in un tempo non superiore a 10 secondi. Un sensore di velocità zero controlla il raggiungimento della completa frenatura mentre il rispetto dei 10 secondi è verificato dall'unità di controllo. L'unità di controllo (PLC) è integrata con un watchdog che verifica la regolarità dell'esecuzione nel tempo del programma.

Occorre precisare che la normativa sulle macchine da legno separa la funzione di arresto dalla funzione di frenatura, pertanto in quest'ultima devono essere considerati solo gli elementi che

concorrono a ridurre a zero la velocità e ovviamente la relativa parte diagnostica e di test della funzione. Inoltre in considerazione della valutazione dei rischi effettuata e dello stato dell'arte per le macchine da legno, la normativa in questione richiede un'architettura in Categoria 2, ma permette di non rispettare il requisito previsto nella norma EN ISO 13849-1 per la frequenza del test.

Le caratteristiche di progetto della SRP/CS considerata sono le seguenti:
- PL_r = "b";
- architettura a doppio canale con canale funzionale e canale di test corrispondente ad un'architettura in Categoria 2 ove però, secondo la norma armonizzata applicabile, non è necessario rispettare il requisito che impone che la frequenza di test sia pari a 100 volte il tasso di richiesta della funzione di sicurezza;
- applicazione dei principi di sicurezza base e di quelli ben provati.

La SRP/CS da realizzare ha lo schema circuitale di fig. 36 e il diagramma a blocchi di fig. 37.
PLC è l'unità di controllo con watchdog integrato, T è l'inverter, G è il sensore di velocità zero, OTE è l'uscita del canale di test che a seguito di un'avaria esercita un'azione di controllo (in questo caso realizzata da un'interfaccia uomo macchina).

Il pulsante di STOP azionato per arrestare il motore non è considerato far parte della funzione di sicurezza. Ad ogni modo, per tale pulsante si può adottare un pulsante ad azione diretta (positiva) conforme alla norma IEC 60947-5-1, All. K, che può essere considerato "ben provato". Un tale pulsante, per cui possano essere esclusi sia i guasti elettrici che quelli meccanici, non è rilevante ai fini della funzione di sicurezza in oggetto.

Il canale funzionale è costituito dal PLC e dall'inverter mentre il canale di test è costituito dal watchdog (TE integrato nel PLC, ma in grado di svolgere funzione autonoma), dal sensore di velocità zero (G) e dal dispositivo di interfaccia di allarme (OTE).

Il PLC utilizzato è un componente ordinario, conforme alla norma IEC 61131-2, il cui corretto svolgimento del programma nel tempo è controllato da un watchdog. Un problema di tensione di alimentazione, una anomalia nel clock, un arresto del programma oppure un blocco del PLC si traducono in un segnale di arresto sull'inverter che inizia la procedura di frenamento. Il PLC effettua test interni per verificare le aree di memoria ma alcuni guasti non possono essere rilevati. A seguito di quanto considerato si assume una copertura diagnostica del 60% con un $MTTF_D$ dichiarato dal costruttore pari a 30 anni.
Si ricorda che, a seguito del processo di Amendment nell'edizione 2015 della norma EN ISO 13849-1, per SRP/CS con PL "b" e Categoria 2 è possibile utilizzare componenti ordinari, come il PLC in questione: per il software embedded (SRESW) di tali componenti non è necessario rispettare i requisiti di sicurezza previsti.

L'inverter T è un componente ordinario che è monitorato indirettamente tramite il sensore di velocità zero e il processo stesso, per una copertura diagnostica stimata del 90% in applicazione delle indicazioni dell'All. E. Il valore di $MTTF_D$ a esso attribuito dal costruttore è di 20 anni.

Per quanto riguarda il canale di test si hanno per i suoi componenti i seguenti valori di $MTTF_D$:
- watchdog (PLC): 30 anni;
- sensore di velocità zero: 150 anni;
- unità OTE: 30 anni, conforme alla norma IEC 61131-2.

Le misure adottate contro i CCF sono sufficienti, raggiungendo un punteggio pari a 65, e sono: separazione (15), protezione contro la sovratensione (15), protezione per le condizioni ambientali (25+10).

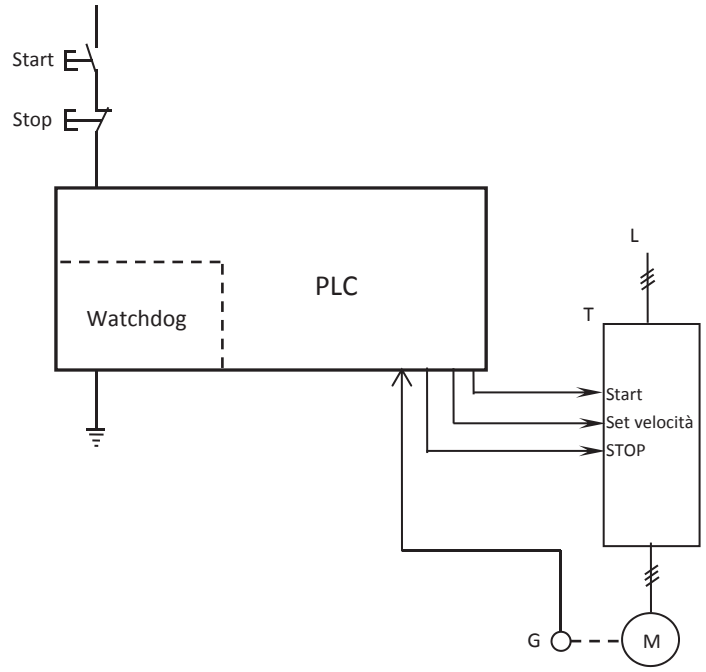


Fig. 36: Schema circuitale

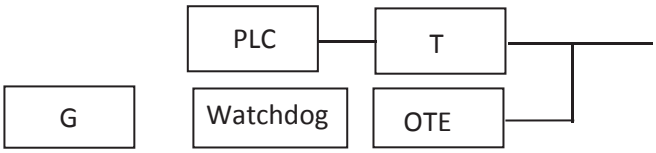


Fig. 37: Diagramma a blocchi

Il sottosistema costituito dal PLC e dall'inverter (canale funzionale) ha un $MTTF_D$ pari a 12 anni (medio), una DC del 60%. Il canale di test ha un $MTTF_D$ pari a 14 anni (medio), superiore alla metà del valore del canale funzionale. Il PFH_D è pari a $5{,}84\times10^{-6}$ e corrisponde a un PL "b" (fig. 38). L'architettura della funzione di sicurezza è una Categoria 2, la funzione è verificata a istanti di tempo idonei, anche se non corrispondenti a 100 volte il tasso di richiesta. Un guasto tra due test può portare alla perdita della funzione di sicurezza che è rilevata dal test immediatamente successivo.

Table K.1 — Numerical representation of Figure 5

	Average probability of a dangerous failure per hour (1/h) and corresponding performance level (PL)															
$MTTF_d$ for each channel years	Cat. B DC_{avg} = none	PL	Cat. 1 DC_{avg} = none	PL	Cat. 2 DC_{avg} = low	PL	Cat. 2 DC_{avg} = medium	PL	Cat. 3 DC_{avg} = low	PL	Cat. 3 DC_{avg} = medium	PL	Cat. 4 DC_{avg} = high	PL
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	a	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	a	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-6}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-6}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		

Fig. 38: PFH_D (1/h) - ISO 13849-1, estratto tabella K.1

9.4. Esempio 4

Per il controllo della sovra-velocità degli assi o dei mandrini di una macchina (SLS) è possibile l'applicazione di un'architettura in Categoria 3.

- Definizione della funzione di sicurezza: il superamento della velocità massima stabilita per un asse o un mandrino provoca l'arresto sicuro controllato (SS1) del sistema di azionamento (drive) della macchina.
- Descrizione funzionale: due sensori di velocità diversi G1 e G2, ciascuno su un canale separato, rilevano la velocità di rotazione dell'asse o del mandrino mentre l'unità di controllo (PLC) la confronta con il valore impostato sul drive (T). Quest'ultimo è un componente di sicurezza che implementa la funzione di STOP (SS1) per l'arresto controllato e di pulse-blocking (STO), che si attiva con ritardo rispetto alla funzione di STOP, disabilitando la funzione di inverter e portando a un arresto incontrollato accettato in fase di valutazione del rischio (possibilità di evitare il pericolo da parte dell'operatore e accesso alla zona pericolosa ritardato da misure deterrenti/ostacoli). Quando la velocità supera di un valore predeterminato la velocità massima impostata, il PLC invia un segnale al drive T nell'ingresso STOP e attiva la funzione di arresto sicuro controllato che previene anche l'avvio inatteso. Successivamente come già descritto si attiva la funzione di pulse blocking (STO) che disabilita l'inverter.

Le caratteristiche di progetto della funzione di sicurezza considerata sono le seguenti:
- PL_r = "d" (da valutazione del rischio con metodo del risk graph (S=S2, F=F2, P=P1));
- architettura a doppio canale con diagnostica (1oo2D) e tolleranza singola al guasto;
- applicazione dei principi di sicurezza base e di quelli ben provati.

La SRP/CS da realizzare ha lo schema circuitale di fig. 39 e il diagramma a blocchi di fig. 40.

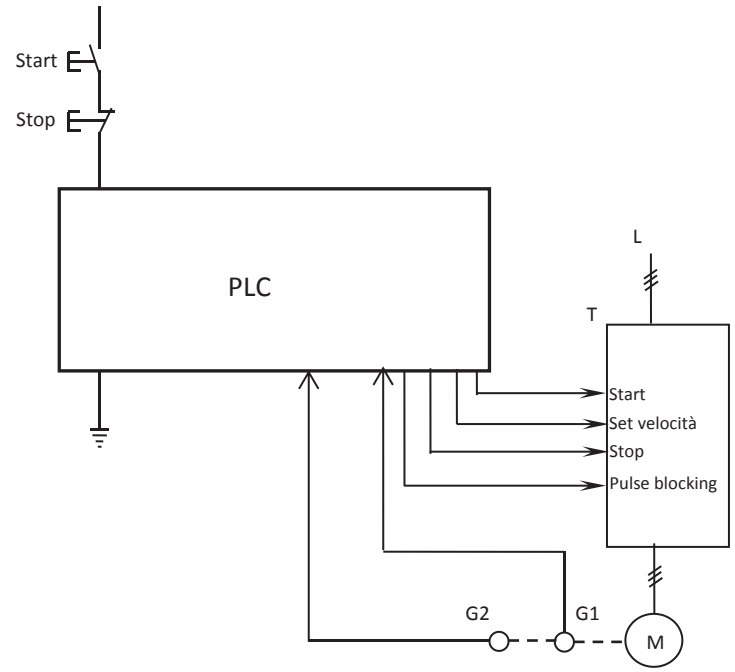


Fig. 39: Schema circuitale

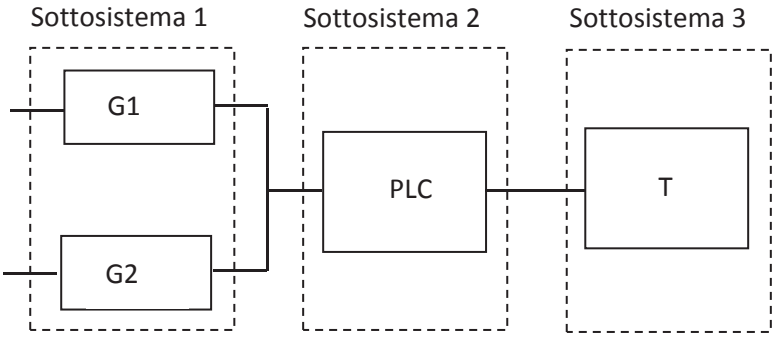


Fig. 40: Diagramma a blocchi

I pulsanti di avvio e arresto non sono ovviamente rilevanti per la funzione.

Il primo canale funzionale è costituito dal sensore G1, da una unità di controllo PLC per applicazioni di sicurezza e dal driver T collegato sull'ingresso STOP. Il secondo canale è costituito dal sensore G2, dal PLC e dal driver T collegato all'ingresso del *pulse blocking* (STO).
La funzione è realizzata con 3 sottosistemi, il primo costituito dai sensori, il secondo dal PLC, il terzo dal driver.

Il PLC è un componente di sicurezza, conforme alle norme IEC 61131-6.
Il driver T è anch'esso un componente di sicurezza certificato per Categoria 3 e PL "d".

I dati per il calcolo della probabilità di guasto PFH_D della funzione di sicurezza sono i seguenti:
- il valore di $MTTF_D$ per G1 e G2 è di 100 anni; la diagnostica è effettuata dal PLC che confronta in maniera dinamica i valori dei due sensori, la DC è pari al 90%; da tali valori si ricava un PFH_D pari a $4{,}29\times10^{-8}$ corrispondente a un PL "e";
- il PLC è dichiarato idoneo ad applicazioni in PL "d" e per strutture in Categoria 3 con un PFH_D pari a $3{,}2\times10^{-7}$;
- il driver T ha un PFH_D dichiarato pari a $3{,}2\times10^{-7}$.

Le misure adottate contro i CCF sono sufficienti, raggiungendo un punteggio pari a 65, e sono: separazione (15), protezione contro la sovratensione (15), protezione per le condizioni ambientali (25+10).
Per quanto riguarda l'architettura, la copertura diagnostica DC evidenzia che non tutti i guasti possono essere rilevati e che l'accumulo porta alla perdita della funzione di sicurezza.
Con la combinazione dei tre sottosistemi si ottiene un PFH_D totale pari a $6{,}8\times10^{-7}$, corrispondente a un PL pari a "d".

9.5. Esempio 5

Per la protezione contro l'accesso a una zona pericolosa è possibile utilizzare una barriera luminosa (ESPE).

- Definizione della funzione di sicurezza: l'attraversamento della barriera luminosa provoca l'interruzione dell'alimentazione del motore della macchina.
- Descrizione funzionale: una barriera luminosa (B) di Tipo 2 protegge contro l'accesso a una zona pericolosa di una macchina operatrice durante la fase di caricamento materiali. L'attraversamento di tale barriera da parte di un operatore produce un segnale che viene inviato al modulo di sicurezza K il quale provoca l'apertura del contattore Q sulla linea di alimentazione del motore.

Le caratteristiche di progetto della funzione di sicurezza considerata sono le seguenti:
- PL_r = "c" (da valutazione del rischio con metodo del risk graph (S=S2, F=F1, P=P1));
- combinazione di 3 sottosistemi con strutture rispettivamente in Categoria 2, 4 ed 1: barriera, modulo logico, contattore.

La SRP/CS da realizzare ha lo schema circuitale di fig. 41 e il diagramma a blocchi di fig. 42.
La barriera di Tipo 2 può raggiungere al massimo un PL "c" e ha un'architettura in Categoria 2.

La barriera luminosa ha un ingresso per controllo EDM (*external device monitoring*) e autotest interno ed è certificata di Tipo 2, idonea per applicazioni fino a PL "c" con PFH_D pari a 2×10^{-8}.

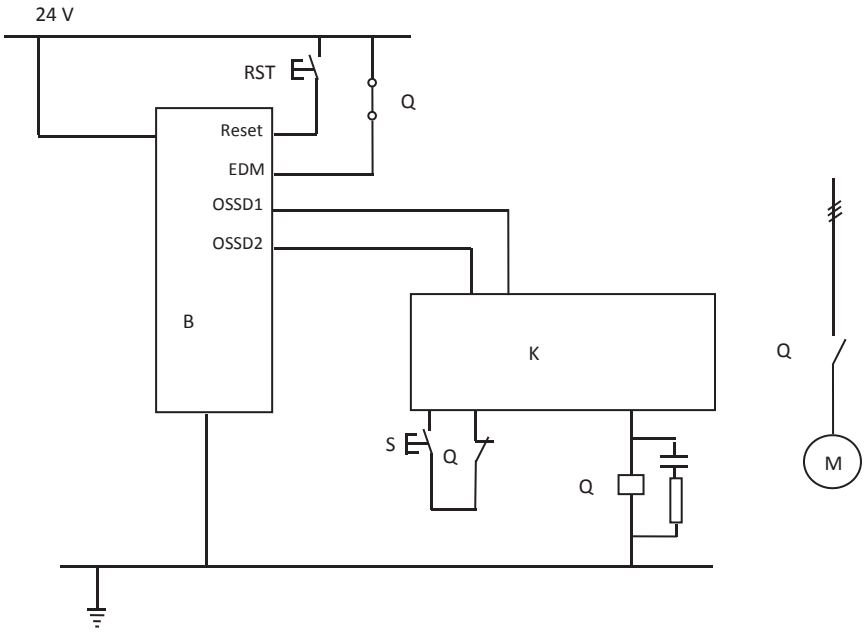


Fig. 41: Schema circuitale

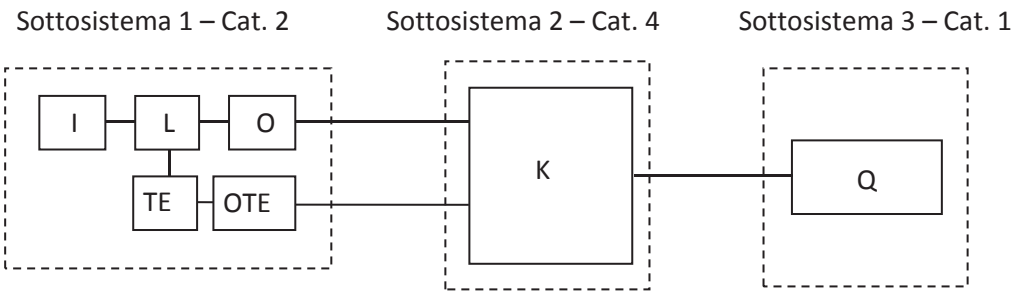


Fig. 42: Diagramma a blocchi

L'output del test effettuato dalla barriera è inviato al modulo K di sicurezza. Quest'ultimo è un'unità di controllo certificata per applicazioni fino a PL "e" in Categoria 4 con PFH_D pari a 3×10^{-8}.

Il contattore Q è dello stesso tipo utilizzato per l'esempio 1, cioè di Categoria AC-3, per AC o DC, conforme alla norma IEC 60947-4-1, che in condizioni di carico nominale e se sono soddisfatti i principi di sicurezza base e quelli ben provati (prospetti D1 e D2 della norma ISO 13849-2) ha un B_{10D} = 1 300 000 (tab. 11).
Il contattore è anche monitorato a ogni avvio della macchina e il suo stato tramite l'ingresso EDM viene riportato alla barriera luminosa. Tale monitoraggio non è richiesto dalla categoria 1, si tratta quindi di una ridondanza.

Per poter utilizzare tale contattore in un'architettura in Categoria 1 occorre che sia "ben provato" cioè che soddisfi le condizioni addizionali del prospetto D.3 della norma ISO 13849-2 che richiedono:
- la protezione contro altre influenze quali, vibrazioni, temperatura, polveri, acidi;
- l'impiego di metodi ben provati (prospetto D.2 della ISO 13849-2) per evitare guasti quali il sovradimensionamento (es. riduzione della corrente di carico al 50% del valore nominale);
- la limitazione della corrente di carico con una protezione termica;
- la protezione dal sovraccarico.

Supponendo d_{op}=220 (giorni/anno), h_{op}= 8 (ore), t_{cycle}= 1 (ore) si ottiene:
- n_{op}= (220×8×3600)/ (3600×1)=1760 cicli/anno;
- T_{10D}= B_{10D}/n_{op}= 1 300 000/1760=739 anni;
- $MTTF_D$=T_{10D}/0,1=7390 anni (alto).

Con tali valori si ottiene per il sottosistema 3 un PL "c" con un PFH_D pari $1{,}14\times10^{-6}$.
Dalla combinazione dei tre sottosistemi risulta un PL "c" (il più basso fra i PL dei sottosistemi assemblati) e un PFH_D pari a $1{,}19\times10^{-6}$.

10. Glossario

Parte di un sistema di controllo relativa alla sicurezza (*safety-related part of a control system* – SRP/CS): parte di un sistema di controllo che risponde a segnali di ingresso relativi alla sicurezza e genera segnali di uscita relativi alla sicurezza. Tale parte inizia nel punto dove l'ingresso relativo alla sicurezza è generato e termina all'uscita degli attuatori. Anche i sistemi di monitoraggio utilizzati per la diagnostica sono considerati SRP/CS.

Categoria: classificazione di SRP/CS rispetto alla loro resistenza ai guasti e al loro comportamento in conseguenza di un guasto. Una Categoria è caratterizzata da una struttura particolare delle parti che realizzano la SRP/CS, dalla capacità di riconoscere i guasti e dalla sua affidabilità.

Avaria (fault): stato di un dispositivo caratterizzato dall'impossibilità di portare a termine la funzione richiesta, esclusa l'impossibilità dovuta a manutenzione preventiva o ad altre azioni pianificate o dovuta alla mancanza di risorse esterne. Un guasto è spesso il risultato di un malfunzionamento del dispositivo stesso, ma può esistere senza che vi sia prima il malfunzionamento. I guasti qui considerati sono naturalmente guasti casuali.

Guasto (*failure*): fine della capacità di un dispositivo di portare a termine la funzione richiesta. Dopo un malfunzionamento il dispositivo ha un guasto. Il malfunzionamento è da intendersi come un evento, in modo da distinguerlo dal guasto che invece è uno stato. Il concetto non si applica al software. Malfunzionamenti che riguardano solo la disponibilità del processo da controllare non rientrano nello scopo della EN ISO 13849-1.

Guasti pericolosi (*dangerous failures*): malfunzionamenti che hanno la capacità di mettere la SRP/CS in uno stato pericoloso o tale che possa farne fallire il funzionamento. L'architettura del sistema può influenzare tale capacità, infatti nei sistemi ridondanti un malfunzionamento pericoloso dell'hardware è probabile che non conduca a uno stato di perdita della funzione da realizzare.

Guasti di causa comune (*common cause failure* – CCF): malfunzionamenti di dispositivi diversi dovuti a un evento singolo quando tali malfunzionamenti non sono conseguenza uno dell'altro.

Guasto sistematico (*systematic failure*): malfunzionamento dovuto a una causa deterministica che può essere eliminato modificando il progetto, o il processo produttivo, o le procedure di lavoro, o la documentazione o altri fattori rilevanti. La manutenzione correttiva senza modifiche di solito non elimina la causa del malfunzionamento. Un malfunzionamento sistematico può essere indotto simulandone la causa. Esempi di cause di malfunzionamenti sistematici includono l'errore umano durante la specifica dei requisiti di sicurezza, durante la progettazione, la realizzazione, l'installazione e l'uso dell'hardware, durante la progettazione e la realizzazione del software.

Danno (*harm*): ferita o peggioramento della salute.

Pericolo (*hazard*): potenziale sorgente di danno. Il pericolo può essere classificato in base alla sua origine (ad es. meccanico, elettrico) o in base al possibile danno (ad es. di elettrocuzione, di taglio, di incendio). I pericoli considerati dalla EN ISO 13849-1 possono essere presenti in modo permanente durante l'uso previsto della macchina (parti in movimento pericolose, arco elettrico durante la saldatura, emissione di rumore, alta temperatura) o possono apparire inaspettatamente (esplosione, scontro come conseguenza di un'accensione non voluta/inattesa, lancio come conseguenza di una rottura, caduta come conseguenza di accelerazione/decelerazione).

Situazione pericolosa: circostanza durante la quale una persona è esposta a un pericolo. L'esposizione può potenzialmente portare a un danno immediato o dopo un lungo periodo di tempo.

Rischio (*risk*): combinazione della probabilità di accadimento di un danno e della severità di quel danno.

Rischio residuo: rischio rimanente dopo l'adozione di misure protettive.

Valutazione del rischio (*risk assessment*): processo complessivo comprendente l'analisi del rischio e la stima del rischio.

Analisi del rischio (*risk analysis*): combinazione delle specifiche dei limiti della macchina, dell'identificazione dei pericoli e della stima del rischio.

Ponderazione del rischio (*risk evaluation*): giudizio, sulla base dell'analisi del rischio, sul raggiungimento o meno degli obiettivi di riduzione del rischio.

Uso previsto della macchina: uso della macchina in accordo con le informazioni fornite nelle istruzioni per l'uso.

Uso scorretto ragionevolmente prevedibile: uso della macchina in modo non inteso dal progettista, ma che può essere previsto in base al comportamento umano.

Funzione di sicurezza: funzione della macchina il cui guasto può provocare un aumento immediato del rischio.

Sistema elettronico programmabile (*programmable electronic system* – PES): sistema per il controllo, la protezione o il monitoraggio che dipende per il suo funzionamento da uno o più dispositivi elettronici programmabili. Include tutti gli elementi del sistema, come gli alimentatori, i sensori e altri dispositivi di ingresso, i contattori e altri dispositivi di uscita.

Livello di prestazione (*performance level* – PL): livello discreto utilizzato per specificare la capacità della parte del sistema di controllo relativa alla sicurezza di eseguire la funzione di sicurezza in condizioni determinate.

Livello di prestazione richiesto (*required performance level* – PL_r): livello di prestazione che deve essere realizzato in modo da ottenere, per una data funzione di sicurezza, la richiesta riduzione del rischio.

Tempo medio per un guasto pericoloso (*mean time to dangerous failure* – $MTTF_D$): valore atteso del tempo medio per avere un malfunzionamento pericoloso.

Copertura diagnostica (*diagnostic coverage* – DC): misura dell'efficacia della diagnostica determinata come rapporto tra il tasso di malfunzionamenti pericolosi rilevati e il tasso di malfunzionamenti pericolosi complessivo. La copertura diagnostica potrebbe esistere per una parte del sistema relativo alla sicurezza (ad es. per i sensori e/o per la logica di controllo e/o per gli elementi di uscita).

Misura di protezione: misura utilizzata per ridurre il rischio. Tra quelle messe in atto dal progettista vi sono: progettazione a sicurezza intrinseca, uso di ripari (*safeguards*) e misure di protezione complementari, istruzioni per l'uso. Tra quelle messe in atto dall'utilizzatore vi sono: organizzazione (procedure di sicurezza, supervisione, sistemi di consenso per le operazioni), fornitura e messa in opera di ripari addizionali, dispositivi di protezione personali, addestramento.

Tempo di missione (*mission time* – T_M): periodo di tempo che copre l'uso previsto di una SRP/CS.

Frequenza di domanda alta o continua (*high demand or continuous mode*): modo di funzionamento in cui la frequenza della richiesta di eseguire la funzione di sicurezza della SRP/CS è superiore ad

una volta l'anno oppure in cui la funzione di controllo relativa alla sicurezza mantiene la macchina in un stato sicuro come parte del normale funzionamento.

Tasso di prova (*test rate* – r_t): frequenza delle prove eseguite automaticamente per rilevare guasti in una SRP/CS, inverso del valore dell'intervallo di prova diagnostica (*diagnostic test interval*).

Tasso di richiesta (*demand rate* – r_d): frequenza della richiesta di eseguire la funzione di sicurezza della SRP/CS.

Tasso di riparazione (*repair rate* – r_r): inverso del valore del periodo di tempo tra la rilevazione di un malfunzionamento pericoloso (a seguito di una prova durante il funzionamento o di un malfunzionamento del sistema) e l'istante di ripartenza delle operazioni dopo la riparazione o la sostituzione del sistema/componente. Il tempo di riparazione non include il tempo necessario per la rilevazione del malfunzionamento.

B_{10}: numero di cicli in corrispondenza dei quali il 10% dei componenti uguali presenta dei guasti. Se si prendono in considerazione i soli guasti pericolosi il parametro è indicato con B_{10D}.

T_{10}: è il tempo medio della vita di un componente in corrispondenza del quale il 10% dei componenti a lui uguali presenta un guasto. Se si prendono in considerazione i soli guasti pericolosi il parametro è indicato con T_{10D}.

Sistema di controllo della macchina: sistema che risponde a segnali di ingresso provenienti dagli elementi di parti della macchina, dall'operatore, da dispositivi di controllo esterni o da una qualsiasi combinazione di questi e che genera segnali di uscita che fanno agire la macchina nella maniera desiderata. Tale sistema può utilizzare qualsiasi tecnologia o combinazione di tecnologie differenti.

Livello di integrità di sicurezza (*safety integrity level* – SIL): livello discreto (tra quattro possibili) per specificare i requisiti di integrità di sicurezza della funzione di sicurezza che deve essere realizzata con un sistema di sicurezza elettrico/elettronico programmabile.

Provato in uso (*proven in use*): dimostrazione, basata sull'analisi dell'esperienza di funzionamento di un elemento in configurazione specifica, che la probabilità di guasti sistematici pericolosi sia bassa a sufficienza in modo che ogni funzione di sicurezza che usa quell'elemento raggiunga il livello di prestazione richiesto (PL_r).

Componente ben provato: componente per un'applicazione di sicurezza che è stato:
a) ampiamente usato in passato con risultati eccellenti in applicazioni simili oppure
b) costruito e verificato utilizzando principi che dimostrano la sua appropriatezza ed affidabilità per applicazioni di sicurezza.

I componenti sviluppati da poco possono essere considerati equivalenti a quelli ben provati se soddisfano la seconda condizione. La decisione di accettare un particolare componente come ben provato dipende dall'applicazione. Componenti elettronici complessi non possono essere considerati come ben provati.

Principio base di sicurezza: principio di sicurezza che è alla base della progettazione di una data funzione di sicurezza per l'applicazione di interesse.

Principio di sicurezza ben provato: principio di sicurezza che è stato:
c) ampiamente usato in passato con risultati eccellenti in applicazioni simili oppure
d) costruito e verificato dimostrando la sua appropriatezza e affidabilità per applicazioni di sicurezza.

Monitoraggio (*monitoring*): funzione di sicurezza che assicura che una data misura di protezione sia messa in atto se la capacità di un componente o di un elemento a eseguire la sua funzione è

diminuita o se le condizioni del processo sono cambiate in modo tale che si è avuta una diminuzione del valore della riduzione del rischio.

Linguaggio a variabilità limitata (*limited variability language* – LVL): tipo di linguaggio che ha la capacità di combinare funzioni di libreria, studiate per specifiche applicazioni, per realizzare specifici requisiti di sicurezza (esempi tipici: ladder logic, function block diagram).

Linguaggio a variabilità completa (*full variability language* – FVL): tipo di linguaggio che ha la capacità di realizzare una gran varietà di funzioni ed applicazioni (esempi: C++, Assembler). Nel settore delle macchine i linguaggi FVL si trovano nel software di sistema e più raramente nel software applicativo.

Software applicativo (*application software*): software specifico per una data applicazione, realizzato dal fabbricante della macchina, che di solito contiene sequenze logiche, limiti ed espressioni per controllare gli ingressi, le uscite, i calcoli e le decisioni necessari per soddisfare i requisiti della SRP/CS.

Software di sistema (*embedded software – firmware – system software*): software che è parte del Sistema fornito dal fabbricante del sistema di controllo, che non è accessibile per essere modificato dall'utilizzatore della macchina. Di solito è scritto in un linguaggio FVL.

Azione meccanica diretta: movimento di un componente meccanico che deriva inevitabilmente dal movimento di un altro componente meccanico, per contatto diretto o tramite elementi rigidi (ISO 14119).

Azione di apertura positiva: apertura di un contatto come risultato diretto di un movimento specifico dell'attuatore dell'interruttore attraverso componenti non elastici (ad es. camma rotante o lineare, fissata sul riparo, che agisce sull'interruttore) (IEC 60947-5-1, All. K).

11. Riferimenti

[1] Decreto legislativo 27 gennaio 2010, n. 17, “Attuazione della direttiva 2006/42/CE, relativa alle macchine e che modifica la direttiva 95/16/CE relativa agli ascensori”. (GU n. 41 del 19-2-2010)

[2] Decreto legislativo del 9 Aprile 2008 n. 81 e successive modificazioni e integrazioni “Attuazione dell’articolo 1 della legge 3 agosto 2007 n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro”

[3] G. L. Amicucci, F. Pera, *Le norme per i sistemi di controllo delle macchine*, “Costozero”, n. 10, dicembre 2012, pp. 46-47, Ed. del Mediterraneo

[4] F. Pera, G. L. Amicucci, *Indagine sull’adozione delle norme per i sistemi di comando delle macchine*, Unione e Certificazione n. 10, novembre/dicembre 2013

[5] EN ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction

[6] EN ISO 13849-1:2015, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design

[7] EN ISO 13849-1:2006 FDAM 1:2015, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design, Amendment 1

[8] EN ISO 13849-2:2012, Safety of machinery — Safety-related parts of control systems — Part 2: Validation

[9] ISO/TR 22100-2:2013, Safety of machinery — Relationship with ISO 12100 — Part 2: How ISO 12100 relates to ISO 13849-1

[10] ISO/TR 23849:2010, Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery

[11] EN IEC 62061:2005, Safety of machinery — Functional safety of safety–related electrical, electronic and programmable electronic control systems"

[12] EN IEC 61508:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems

[13] EN IEC 60204-1:2016, Safety of machinery — Electrical equipment of machines — Part 1: General requirements

[14] EN ISO 13850:2015, Safety of machinery — Emergency stop — Principles for design

[15] ISO 13854:1996, Safety of machinery — Minimum gaps to avoid crushing of parts of the human body

[16] EN ISO 13855:2010, Safety of machinery — Positioning of safeguards with respect to the approach speeds of parts of the human body

[17] EN ISO 13856:2013 (all parts), Safety of machinery — Pressure-sensitive protective devices

[18] EN ISO 13857:2008, Safety of machinery — Safety distances to prevent hazard zones being reached by upper and lower limbs

[19] ISO 14118:2000, Safety of machinery — Prevention of unexpected start-up

[20] EN ISO 14119:2013, Safety of machinery — Interlocking devices associated with guards — Principles for design and selection

[21] EN ISO 14120:2015, Safety of machinery — Guards — General requirements for the design and construction of fixed and movable guards

[22] ISO/TR 14121:2013, Safety of machinery — Principles of risk assessment

[23] EN ISO 14122:2016 (all parts), Safety of machinery — Permanent means of access to machinery

[24] IEC 61496-1, Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests

[25] ISO/TR 24119:2015, Safety of machinery — Evaluation of fault masking serial connection of guard interlocking devices with potential free contacts

[26] BGIA, Report 2/2008e

[27] IFA, Sistema Cookbook 1 – 6