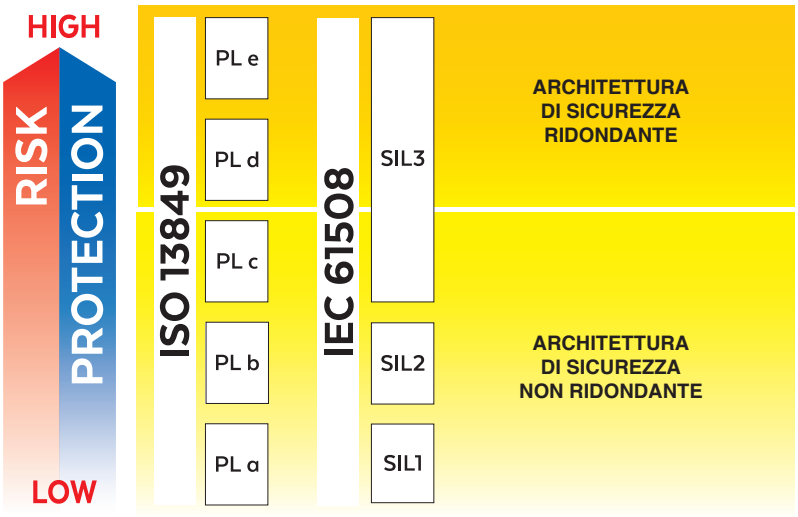
Generalità per i componenti di sicurezza

IEC 61508 Livello di integrità di sicurezza e **ISO 13849** Livello delle prestazioni - certificazione



Nell'ingegnerizzazione delle macchine moderne la sicurezza sta diventando una questione di primaria importanza per proteggere le persone da eventuali rischi causati da guasti accidentali di macchine e sistemi.

La **direttiva macchine 2006/42/CE** insieme alle norme **IEC 61508 Livello di integrità di sicurezza** (SIL, Safety Integrity Level) e **ISO 13849 Livello delle prestazioni** (PL, Performance Level) rappresenta il quadro normativo di riferimento sulla sicurezza funzionale e costituisce il fondamento dei principi generali di prevenzione in materia di sicurezza dei dispositivi e degli impianti con implicazioni per la salute.

La direttiva stabilisce i requisiti di sicurezza che il produttore di macchine deve rispettare per ottenere la certificazione e quindi per poter apporre la marcatura CE richiesta per la vendita nel mercato europeo.

La direttiva macchine 2006/42/CE sostituisce la precedente direttiva 98/37/CE ed è universalmente applicabile a macchinari, componenti di sicurezza e altri specifici equipaggiamenti.

1 NORME DI SICUREZZA

La norma **IEC 61508** e le pertinenti norme **IEC 61511** (sistemi di controllo di processo) e **IEC 62061** (sistemi di controllo delle macchine) introducono l'approccio probabilistico integrato nella sicurezza funzionale. Tali norme prescrivono i livelli di integrità di sicurezza (SIL) richiesti per l'esecuzione delle funzioni di sicurezza.

La norma **ISO 13849** prevede requisiti e indicazioni sui criteri di progettazione e integrazione dei componenti rilevanti per la sicurezza dei sistemi di controllo, compresa la progettazione di software.

Inoltre specifica il livello delle prestazioni (PL) richiesto per l'esecuzione delle funzioni di sicurezza.
PL: valore discreto che precisa la capacità dei componenti di sicurezza dei sistemi di controllo di eseguire una funzione di sicurezza in condizioni prevedibili.

I requisiti sono classificabili in cinque livelli di prestazione, dove **PL e** identifica il livello di protezione più alto.

2 CERTIFICAZIONE

Le valvole di sicurezza Atos (on-off e proporzionali) sono certificate TÜV in conformità alle norme IEC 61508, IEC 61511, IEC 62061, ISO 13849

La certificazione garantisce la conformità della valvola con le norme di sicurezza in materia e attesta il rispetto di tutti i requisiti previsti per i livelli SIL e PL della valvola in questione.

La certificazione conferma che il produttore può utilizzare a tal fine i dati seguenti per l'intero sistema:

- il processo di progettazione utilizzato dal produttore della valvola per evitare guasti
- le tecniche e le misure utilizzate nella progettazione per controllare i guasti
- i metodi utilizzati per definire le tolleranze ai guasti meccanici
- i metodi utilizzati per misurare le frazioni dei guasti sicuri
- i metodi utilizzati per misurare le probabilità del guasto

⚠ **L'utilizzo di prodotti non certificati comporta per il produttore della macchina la responsabilità di convalidare che tutti i criteri sopra riportati sono stati applicati nel rispetto delle norme vigenti in materia.**

Senza la certificazione della valvola il produttore della macchina è tenuto alternativamente a:

- raccogliere dal produttore della valvola tutti i dati sull'affidabilità necessari a valutare il livello di sicurezza dell'intero sistema
- considerare il caso peggiore in merito al livello di sicurezza (es. assegnare alle valvole il livello di sicurezza più basso **PL a** o **SIL 1** nella valutazione della sicurezza del sistema)

3 VALUTAZIONE DEL RISCHIO

Il primo passo per stabilire la necessaria riduzione del rischio è la valutazione del rischio.
Tale valutazione consiste nella procedura prevista per l'individuazione dei rischi della macchina che richiedono la mitigazione per mezzo di sistemi di controllo della macchina (es. barriere laser, valvole di intercettazione, dispositivi di consenso, ecc.). Ciascuno di tali sistemi di controllo costituiscono una funzione di sicurezza.
A questo punto occorre definire le funzioni di sicurezza e attuarle attraverso la progettazione della macchina (vedere 3.1).

⚠ **Il produttore della macchina è responsabile del rispetto di tutti i requisiti di sicurezza e della redazione del documento di valutazione dei rischi che garantisca la gestione di tutti i possibili pericoli della macchina.**

3.1 Produttore della macchina

La denominazione “produttori della macchina” designa i produttori OEM, gli utenti finali che fabbricano macchinari per esigenze proprie o chiunque esegua “modifiche significative” quali:

- modifica del funzionamento della macchina
- modifica dell’ambito di applicazione della macchina
- modifica dell’attrezzatura
- modifica delle prestazioni della macchina

Se la modifica di uno di tali parametri comporta la variazione dell’uso previsto oppure la modifica del sistema di sicurezza o dei relativi componenti, la modifica apportata alla macchina deve essere considerata come “significativa”.
Esempio:

Aggiunta di un collegamento pneumatico per pistola ad aria compressa = modifica NON significativa

Aggiunta di accumulatore idraulico per aumentare la velocità e migliorare il tempo di ciclo della macchina = modifica significativa

4 PARTI CORRELATE ALLA SICUREZZA

Si tratta di parti dei sistemi di controllo della macchina adibite a funzioni di sicurezza, consentendo al sistema di raggiungere o mantenere condizioni di funzionamento sicure.
Tali parti sono costituite da hardware o software e da componenti indipendenti o integrati del sistema di controllo della macchina.
Le parti correlate alla sicurezza integrano la catena completa della funzione di sicurezza svolta da unità di controllo, valvole, sensori e attuatori.

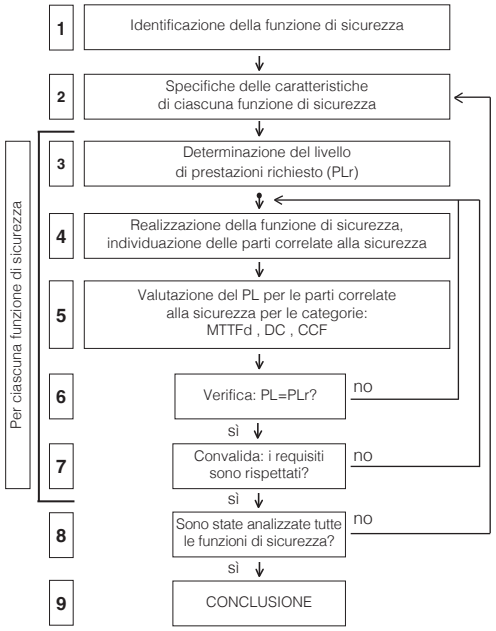
①	②	③	④
SENSORI	LOGICA	VALVOLA	DIAGNOSI DELLA VALVOLA
Rileva situazioni pericolose	Controlla le operazioni della macchina e attiva le procedure di sicurezza in situazioni pericolose	Comanda l’attuatore ed evita movimenti pericolosi	Monitora il corretto funzionamento della valvola

5 ANALISI DI SICUREZZA

Il secondo passo dopo l’individuazione del rischio è l’analisi di sicurezza.
Il processo per la progettazione delle parti correlate alla sicurezza dei sistemi di controllo è di tipo iterativo.

Lo schema riportato a lato è quello di cui alla norma EN ISO 13849-1:

- Il primo passo consiste nell’identificazione delle funzioni di sicurezza.
- Qualsiasi caratteristica di ogni funzione di sicurezza deve essere descritta e documentata.
- È necessario stabilire il livello di prestazioni richiesto (Plr, Performance Level required) da ciascuna funzione di sicurezza. La norma ISO13849-1 utilizza un percorso come quello mostrato nella sezione 5.1.
- Il produttore della macchina deve adibire un sistema alla protezione dell’operatore, assegnando un livello di prestazioni (PL) pari o superiore al livello di prestazioni richiesto (PLr). Per stabilire il livello di prestazioni (PL) occorre tenere in considerazione i seguenti parametri:
  - MTTFd, affidabilità del sistema di sicurezza – vedere la sezione 5.2
  - DC, capacità di rilevare Fault – vedere la sezione 5.3
  - CCF, vulnerabilità del sistema ai guasti – vedere la sezione 5.4
  - categorie di architettura del sistema di sicurezza – vedere la sezione 6

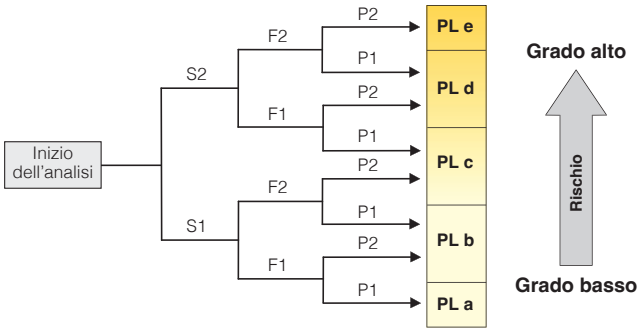


5.1 Livello di prestazioni richiesto - PLr

La determinazione del PLr per la norma ISO 13849-1 avviene attraverso l'analisi dei seguenti parametri:

- Gravità del danno:
  S1 = danno lieve
  S2 = danno grave
- Frequenza e durata dell'esposizione al pericolo:
  F1 = rara
  F2 = frequente
- Possibilità di evitare il pericolo o limitare il danno:
  P1 = possibile
  P2 = raramente possibile

Ciascuno dei cinque livelli di prestazione corrisponde a un'ulteriore scala di parametri, basata sulla probabilità di un guasto pericoloso all'ora.



Livello delle prestazioni	Probabilità media di guasti pericolosi all'ora, h-1
PL e	da ≥ 10^{-8} a < 10^{-7}
PL d	da ≥ 10^{-7} a < 10^{-6}
PL c	da ≥ 10^{-6} a < 3 x 10^{-6}
PL b	da ≥ 3 x 10^{-6} a < 10^{-5}
PL a	da ≥ 10^{-5} a < 10^{-4}

5.2 Tempo medio di guasto pericoloso - MTTFd

Il raggiungimento di un livello PL o SIL specifico si basa sull'affidabilità del sistema.
L'affidabilità viene quantificata dal tempo medio di guasto pericoloso (MTTFd, Mean Time to Failure dangerous) misurata in ore.

Il MTTFd è stabilito sulla base dei dati forniti dal produttore del componente.

5.2 Copertura diagnostica - DC

La copertura diagnostica (DC, Diagnostic Coverage) è la misura dell'efficacia di individuazione dei guasti potenzialmente pericolosi da parte del sistema di monitoraggio.

La norma EN ISO 13849-1 indica i criteri per stabilire la copertura diagnostica (DC).

La copertura diagnostica è definita come misura dell'efficacia della procedura di diagnosi: è determinata dal rapporto tra il tasso di guasto corrispondente ai guasti pericolosi rilevati e il tasso di guasto corrispondente ai guasti pericolosi totali;

DC = 0% non sono rilevati guasti pericolosi

DC ≅ 100% la maggior parte dei guasti pericolosi sono rilevati (è impossibile raggiungere DC = 100% poiché le procedure diagnostiche non sono considerate completamente affidabili)

Categorie di copertura diagnostica:

Categoria	Intervallo
Assente	DC < 60%
Grado basso	60% ≤ DC < 90%
Media	90% ≤ DC < 99%
Grado alto	DC ≥ 99%

5.3 Guasto di causa comune - CCF

Il valore CCF (Common Cause Failure) è il parametro di valutazione delle misure da adottare contro guasti provocati da cause comuni.
Si tratta di guasti riguardanti due o più canali di sistemi ridondanti che si verificano contemporaneamente in conseguenza di una singla causa comune.
Il verificarsi di un guasto contemporaneo su entrambi i canali per la stessa causa compromette la ridondanza.
La norma EN ISO 13849-1 assegna al valore CCF un punteggio che viene utilizzato per stabilire il livello delle prestazioni (PL).

Per assegnare tale punteggio la norma EN ISO13849-1 stabilisce una checklist di sette importanti contromisure:

1. I percorsi dei segnali di canali differenti sono fisicamente separati (punteggio = 15 punti)
2. Diversità nella tecnologia, nella progettazione o nei principi fisici dei canali (punteggio = 20 punti)
3. Protezione contro possibili sovraccarichi (15 punti) e utilizzo di componenti sperimentati [ovvero ampiamente utilizzati o prodotti o verificati in analoghe applicazioni di sicurezza (punteggio = 5 punti)]
4. Analisi delle modalità e delle conseguenze dei guasti durante lo sviluppo per l'identificazione di potenziali guasti di causa comune (punteggio = 5 punti)
5. Formazione del personale di progettazione/assistenza con riferimento ai CCF e nelle relative misure per evitarli (punteggio = 5 punti)
6. Protezione contro guasti comuni causati da contaminazione (filtrazione dei fluidi) e interferenza elettromagnetica di parti elettriche (punteggio = 25 punti)
7. Protezione contro guasti di causa comune causati da condizioni ambientali sfavorevoli (punteggio = 10 punti)

Per categorie di architettura 2, 3 e 4 è richiesto un punteggio minimo di 65 punti (vedere la sezione 6).

Nota: Il CCF dipende sempre dal sistema e dal tipo di applicazione.

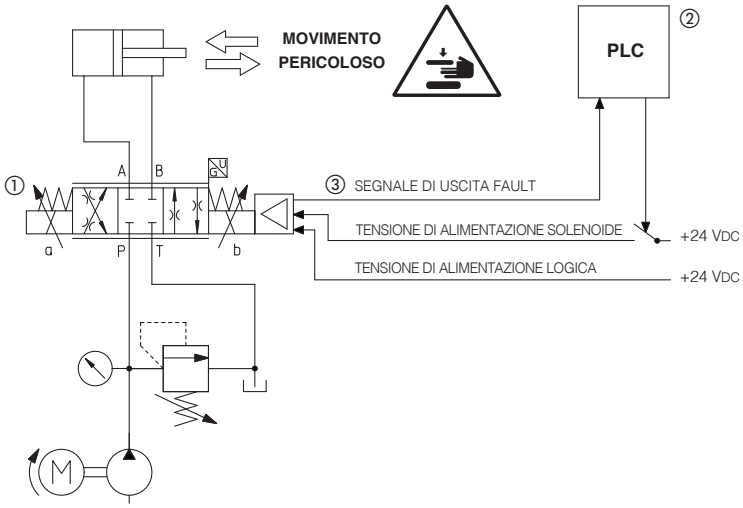
6 CATEGORIE DI ARCHITETTURA

I livelli SIL e PL dipendono non solo dalle caratteristiche del singolo componente ma anche dall'architettura del sistema idraulico e dalla diagnosi dei segnali.
Le categorie di architettura consentono di stabilire la probabilità di un guasto e il PL delle parti correlate alla sicurezza in un sistema di controllo in relazione alla loro resistenza ai guasti e al conseguente comportamento in condizioni di fault
Sono previste cinque categorie di architettura, identificate come: **B, 1, 2, 3, 4**
A un numero più elevato corrispondono una maggiore complessità del sistema di sicurezza e un maggior livello di prestazioni (PL).

6.1 Categorie di architettura B e 1

Nelle categorie B e 1, la resistenza ai guasti si ottiene principalmente attraverso la selezione dei componenti corretti. Si tratta di architetture non ridondanti, pertanto il verificarsi del guasto compromettere la funzione di sicurezza.
La categoria 1 offre una resistenza superiore alla categoria B grazie all'utilizzo di componenti e principi specifici che sono considerati sperimentati e collaudati in un sistema di sicurezza.

Esempio di categoria di architettura 1



Funzione di sicurezza = evitare il pericoloso movimento del cilindro in una determinata fase del ciclo oppure in emergenza

La funzione di sicurezza si ottiene disabilitando la corrente fornita ai solenoidi della valvola proporzionale di sicurezza, in modo che il cursore sia condotto dalle molle in posizione di riposto con ricoprimento positivo.

Attraverso il continuo monitoraggio della posizione del cursore della valvola, il PLC della macchina verifica l'effettiva sussistenza della "condizione sicura".

⚠ **La funzione di sicurezza non viene eseguita in caso di guasto della valvola ①**
Tolleranza ai guasti meccanici (HFT) = 0

① Valvola proporzionale digitale con doppia tensione di alimentazione - opzione /U (ovvero DHZO-TES-SN-NP-07*-L5 **/U**)

② PLC macchina che supervisiona la funzione di sicurezza

③ Segnale di uscita Fault utilizzato per la diagnostica di sicurezza

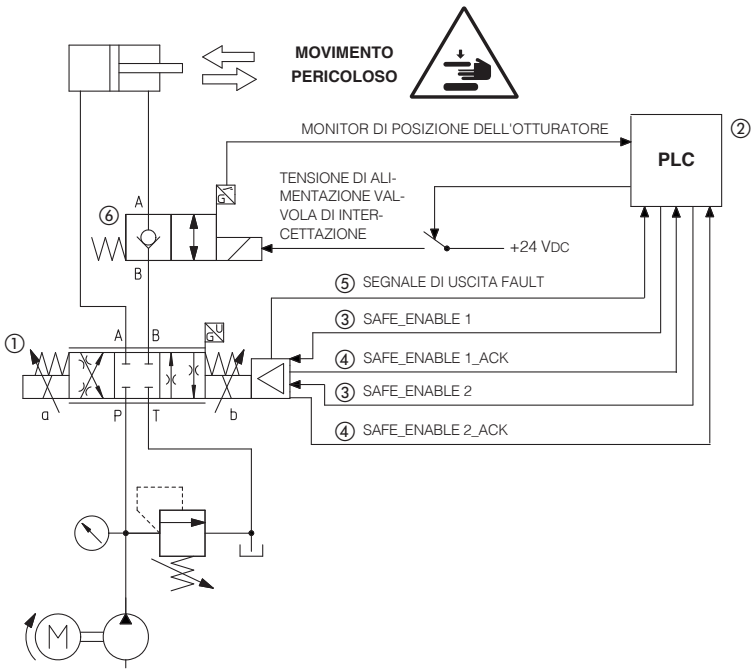
6.2 Architettura - categoria 2

Nella categoria 2 sono compresi tutti i requisiti dell'architettura B e 1. Inoltre, il sistema viene monitorato per intercettare i guasti che compromettono la funzione di sicurezza.
Tali segnali monitor sono inviati a intervalli regolari, ad es. all'avviamento o prima della successiva richiesta della funzione di sicurezza.
Attraverso l'adeguata selezione degli intervalli di prova, si ottiene la riduzione del rischio appropriata.

6.3 Categorie di architettura 3 e 4

Nelle categorie 3 e 4, il verificarsi di un guasto singolo non comporta la compromissione della funzione di sicurezza.
Nella categoria 4 il rilevamento di tali guasti avviene automaticamente.
L'accumulo di guasti non porta alla perdita della funzione di sicurezza.

Esempio di categoria di architettura 4



Funzione di sicurezza = evitare il pericoloso movimento del cilindro in una determinata fase del ciclo oppure in emergenza

In questo esempio alle valvole proporzionali di sicurezza è stata aggiunta una valvola di intercettazione con interruttore di posizione otturatore per garantire una **architettura di sicurezza ridondante**.

La funzione di sicurezza si ottiene disabilitando la corrente fornita ai solenoidi della valvola proporzionale e della valvola di intercettazione di sicurezza, in modo che il cursore sia condotto dalle molle in posizione di riposto con ricoprimento positivo.

La condizione di sicurezza è confermata da:

- stato SAFE_ENABLE_ACK = 24 VDC
- segnali monitor di posizione otturatore nella valvola di intercettazione

⚠ **La funzione di sicurezza viene eseguita anche in caso di guasto di una valvola, ① o ⑥**
Tolleranza ai guasti meccanici (HFT) = 1

① Valvola proporzionale digitale - opzione /K (ovvero DHZO-TES-SN-NP-07*-L5 **/K**)

② PLC macchina che supervisiona la funzione di sicurezza

③ Segnali utilizzati per abilitare/disabilitare la corrente fornita alle elettrovalvole

④ Segnali di conferma dello stato di sicurezza della valvola

⑤ Segnale di uscita Fault utilizzato per la diagnostica di sicurezza

⑥ Valvola di intercettazione di sicurezza con segnale monitor di posizione otturatore (ovvero JO-DL **/FV**)