PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5425 di Mercoledì 05 luglio 2023

Funzioni di sicurezza per le macchine: l'essenziale in breve

Un pieghevole di SUVA fornisce informazioni generali sul contenuto della norma EN ISO 13849-1 "Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza".

La Direttiva macchine stabilisce quanto segue: per evitare pericoli, gli errori hardware o software non devono compromettere la sicurezza funzionale delle macchine. La EN ISO 13849-1 concretizza questo requisito della direttiva.

Suva, l'Istituto svizzero per l'assicurazione e la prevenzione degli infortuni, ha reso disponibile un pieghevole che offre una panoramica delle funzioni di sicurezza e riassume i punti principali. Per la precisione:

- i contenuti della nuova norma, combinando in modo pratico gli elementi consolidati e quelli nuovi
- i termini
- i singoli passaggi che conducono dal rischio al livello di prestazione
- il diverso comportamento della funzione di sicurezza in caso di errore e la suddivisione nelle categorie B, 1, 2, 3 e 4

Nella sezione «Dal rischio al livello di prestazione» è presente un grafico informativo e la parte conclusiva si concentra sulla convalida. La pubblicazione fornisce un riassunto informativo dei contenuti della EN ISO 13849-1, ma non può sostituire la lettura e l'applicazione della norma.

Funzioni di sicurezza per le macchine: l'essenziale in breve

La direttiva 2006/42/CE (Direttiva macchine) prescrive che un'avaria nell'hardware o nel software del sistema di comando non crei situazioni pericolose (punto 1.2.1). Questo requisito è sancito dalla norma EN ISO 13849-1 «Sicurezza del macchinario - Parti dei sistemi di comando legate alla sicurezza». Il documento fornisce una panoramica dei contenuti essenziali di tale norma, senza peraltro sostituire la consultazione e l'applicazione della norma.

1. Metodo ben stabilito

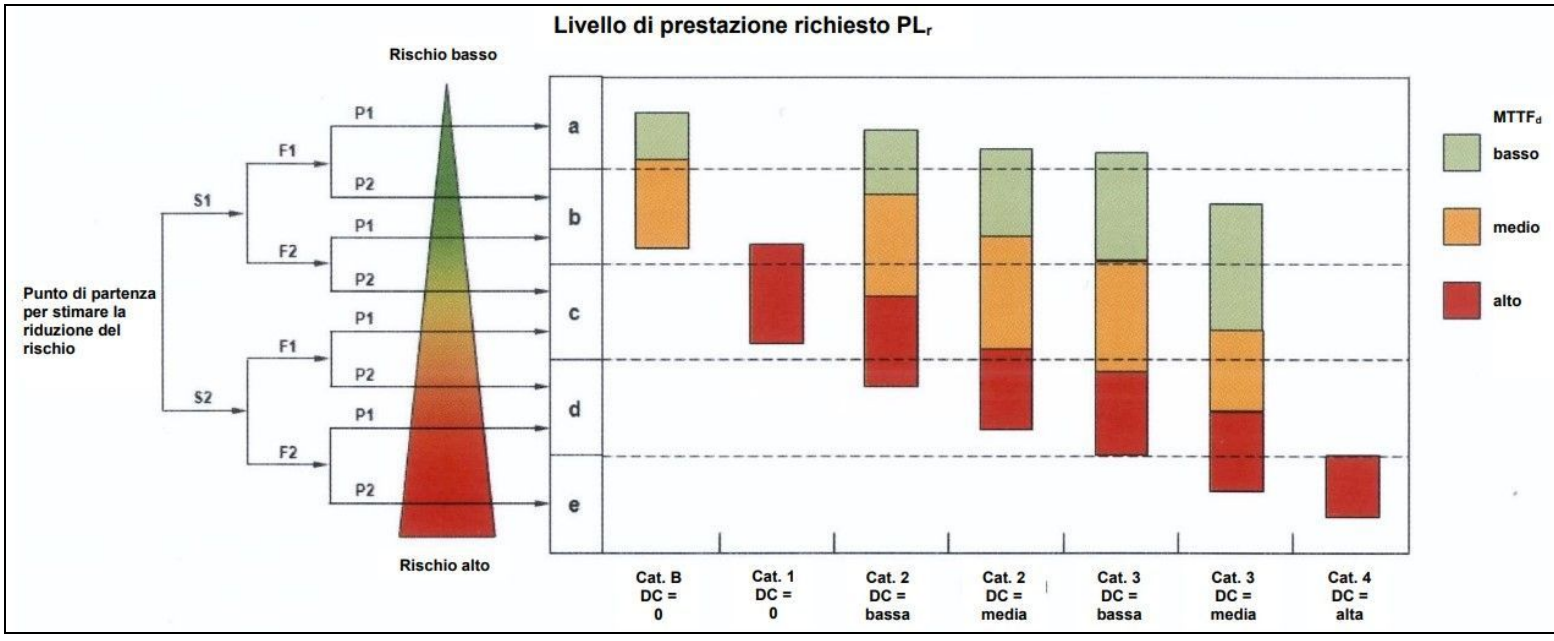
Per ogni parte del sistema di comando legata alla sicurezza o relative combinazioni occorre effettuare una determinazione del livello di prestazione (PL).
Il PL delle parti del sistema di comando legate alla sicurezza deve essere determinato mediante valutazione dei seguenti aspetti:
? architettura della funzione di sicurezza (categoria)
? affidabilità dei componenti (MTTFD)
? qualità dei test, copertura diagnostica (DC)
? guasti da causa comune (CCF)
? comportamento in condizione(i) di avaria
? software legato alla sicurezza
? misure contro guasti sistematici
? capacità di eseguire una funzione di sicurezza nelle condizioni ambientali previste
? ecc.

La norma consente di adottare un metodo semplificato basato sulla definizione di cinque architetture designate, le quali soddisfano specifici criteri di progettazione e il comportamento in condizione di avaria.
Sulla base dei primi tre parametri sopra elencati e con l'aiuto della norma EN ISO 13849-1, figura 5, il metodo semplificato consente di determinare il PL.
Il vantaggio: l'utente ha la possibilità di riprendere l'architettura designata o di svilupparne una propria. In quest'ultimo caso, tuttavia, l'utente deve eseguire complessi calcoli matematici, non supportati da questa norma.

2. Definizioni

PL	Performance Level, livello di prestazione
	Livello discreto utilizzato per specificare la capacità delle parti dei sistemi di comando legate alla sicurezza di eseguire una funzione di sicurezza in condizioni prevedibili.
$MTTF_D$	Mean time to dangerous failure
	Previsione del tempo medio al guasto pericoloso (appendici C, D)
DC	Diagnostic coverage
	Copertura diagnostica (appendice E)
CCF	Common cause failure
	Guasto da causa comune (appendice F)

3. Dal rischio al livello di prestazione



clicca sull'immagine per ingrandirla

Fonte: figura A.1 e figura 5 tratte dalla norma EN ISO 13849-1

Legenda:

S	**Gravità della lesione**
S1	Leggera (lesione normalmente reversibile)
S2	Grave (lesione normalmente irreversibile) o morte
F	**Frequenza e/o esposizione al pericolo**
F1	Da rara a infrequente e/o tempo di esposizione breve
F2	Da frequente a continua e/o tempo di esposizione lungo
P	**Possibilità di evitare il pericolo o limitare il danno**
P1	Possibile in condizioni specifiche
P2	Scarsamente possibile

$MTTF_D$	**Tempo medio al guasto pericoloso**
basso	3 anni ≤ $MTTF_D$ < 10 anni
medio	10 anni ≤ $MTTF_D$ < 30 anni
alto	30 anni ≤ $MTTF_D$ ≤ 100 anni

DC	**Copertura diagnostica**
nessuna	DC < 60 %
bassa	60 % ≤ DC < 90 %
media	90 % ≤ DC < 99 %
alta	99 % ≤ DC

I seguenti passi portano dal rischio al livello di prestazione per ogni singola funzione di sicurezza:
1. In primo luogo bisogna determinare quale livello di prestazione è necessario per la relativa funzione di sicurezza (PLr, livello di prestazione richiesto). Il PLr viene determinato in base alla valutazione dei rischi e ai requisiti della norma di tipo C o ? se non disponibile ? mediante il diagramma riportato qui sopra (per i parametri S, F e P vedi legenda della figura in alto).
2. In una fase successiva si progetta la parte del sistema di comando legata alla sicurezza (SRP/CS) che applica la funzione di sicurezza.
3. Per la progettazione delle parti del sistema di comando legate alla sicurezza sono necessari i parametri dei componenti (MTTFd), della copertura diagnostica (DC) e la categoria. Con questi dati e con il diagramma riportato sopra è possibile determinare il PL conseguito. Si presuppone che tutti gli altri requisiti importanti (misure contro i CCF, requisiti di software ecc.) siano soddisfatti.

4. Il PL conseguito con la progettazione deve essere altrettanto affidabile del PLrichiesto (PL > PLr).

4. Qual è il significato di queste categorie?

Le categorie descrivono come interviene la funzione di sicurezza in caso di avaria e le modalità di rilevamento. Le categorie si suddividono in B, 1, 2, 3 e 4.

Categoria B
I componenti sono fabbricati in conformità alle norme pertinenti (principi di sicurezza di base) e resistono alle sollecitazioni previste.
Avaria: possibile perdita della funzione di sicurezza
ilevamento avarie:nessuno (DC = 0)

Categoria 1
Si devono applicare i requisiti della categoria B.
Si devono utilizzare componenti e principi di sicurezza ben provati.
Avaria: possibile perdita della funzione di sicurezza, ma meno probabile rispetto alla categoria B
Rilevamento avarie:nessuno (DC = 0)
Categoria 2
Si devono applicare i requisiti della categoria B.
Test di avviamento e test periodico della funzione di sicurezza, si devono utilizzare principi di sicurezza ben provati.
Avaria: possibile perdita della funzione di sicurezza tra i controlli
Rilevamento avarie:per ogni controllo (DC = da bassa a media)

Categoria 3
Si devono applicare i requisiti della categoria B e utilizzare principi di sicurezza ben provati.
Una singola avaria non porta alla perdita della funzione di sicurezza, ogniqualvolta sia ragionevolmente fattibile.
Avaria: nessuna perdita della funzione di sicurezza
Rilevamento avarie:buono ma incompleto (DC = da bassa a media)

Categoria 4
Si devono applicare i requisiti della categoria B e utilizzare principi di sicurezza ben provati.
Una singola avaria non porta alla perdita della funzione di sicurezza, un accumulo di avarie non rilevate non deve portare alla perdita della funzione di sicurezza.
Avaria: nessuna perdita della funzione di sicurezza
Rilevamento avarie:molto buono (DC = alta)

5. Non dimenticare la validazione!

La norma EN ISO 13849-2 stabilisce la procedura e le condizioni in base alle quali è possibile validare una funzione di sicurezza, il livello di prestazione conseguito e la relativa categoria.
Per le categorie 2, 3, e 4 la validazione della funzione di sicurezza deve comprendere anche un test con adeguata iniezione di guasti.

SUVA - Funzioni di sicurezza per le macchine: l'essenziale in breve. Informazioni generali sul contenuto della norma EN ISO 13849-1 (pdf)

N.B.: Se alcuni riferimenti legislativi e alcune indicazioni contenute nei documenti di Suva riguardano la realtà elvetica, i suggerimenti indicati e le informazioni riportate sono comunque utili per migliorare la valutazione e la riduzione dei rischi correlati all'utilizzo delle macchine.