

1- Prefazione

Scopo di questa sezione è di fornire al costruttore di macchine una rapida introduzione su alcune normative relative alla sicurezza macchine, chiarire alcuni principi di base e fornire alcuni esempi applicativi. Questa breve guida fa riferimento solamente agli aspetti relativi alla Sicurezza Funzionale della macchina, ovvero all'insieme delle misure atte a proteggere l'operatore dei macchinari dai rischi derivanti dal loro funzionamento. Non vengono trattati i rischi dovuti ad altre fonti di pericolo come ad esempio la presenza di energia elettrica, recipienti in pressione, atmosfere esplosive eccetera che dovranno comunque essere valutati dal costruttore dei macchinari.

Questo documento è stato preparato da Pizzato Elettrica al meglio delle proprie conoscenze, tenendo presente le normative ed interpretazioni e le tecnologie esistenti nell'anno 2011. Poiché alcune norme trattate stanno trovando in questi mesi le loro prime applicazioni reali non si può escludere che nel corso del tempo ulteriori norme o interpretazioni da parte di organismi notificati modifichino le valutazioni fornite in questo documento. Gli esempi riportati devono quindi sempre essere valutati dal cliente finale in funzione dello stato dell'arte tecnologico/normativo e non lo esimono dalle proprie responsabilità. Pizzato Elettrica non si assume nessuna responsabilità sugli esempi riportati e non esclude la possibile presenza involontaria di errori o imprecisioni nei dati forniti.

2- Progettare in sicurezza. La struttura normativa Europea.

Qualsiasi dispositivo o macchinario, per essere liberamente commercializzato all'interno dei paesi della Comunità Europea, deve soddisfare le prescrizioni delle direttive comunitarie. Esse stabiliscono i principi generali affinché i costruttori mettano in commercio prodotti che non siano pericolosi per gli operatori. L'insieme dei prodotti e dei diversi pericoli possibili è molto vasto e per questo nel corso del tempo sono state emanate diverse direttive. A titolo di esempio citiamo la direttiva bassa tensione 2006/95/EC, la direttiva sulle atmosfere esplosive 94/9/EC, la direttiva sulla compatibilità elettromagnetica 2004/108/EC, eccetera. I pericoli derivanti dal funzionamento dei macchinari sono trattati dalla Direttiva Macchine 2006/42/EC.

La conformità alle direttive viene certificata mediante l'emissione della Dichiarazione di Conformità da parte del costruttore e dall'apposizione della marcatura CE sulla macchina stessa.

Per la valutazione dei rischi che la macchina presenta e per la realizzazione dei sistemi di sicurezza atti a proteggere l'operatore da detti rischi gli enti normatori europei CEN e CENELEC hanno emanato una serie di norme che traducono in indicazioni tecniche il contenuto delle direttive. Le norme che vengono pubblicate nella Gazzetta Ufficiale dell'Unione Europea si intendono armonizzate. Il costruttore che impiega tali norme per la certificazione dei propri macchinari ha la presunzione di conformità alle direttive.

Le norme per la sicurezza macchine si suddividono in tre tipologie: A, B e C.

Norme di tipo A: Sono norme che trattano i concetti di base ed i principi di progettazione generale per la realizzazione di tutte le macchine.

Norme di tipo B: Sono norme che trattano nello specifico uno o più aspetti relativi alla sicurezza e che a loro volta si suddividono in norme di tipo:

- B1: Norme relative ad alcuni aspetti della sicurezza (ad esempio distanze di sicurezza, temperature, rumore ecc.)
- B2: Norme relative a dispositivi di sicurezza (ad esempio controlli bimanuali, dispositivi di interblocco, ripari, ecc.)

Norme di tipo C: Sono norme che trattano dettagliatamente le prescrizioni di sicurezza per particolari gruppi di macchine (es. presse idrauliche, macchine ad iniezione, ...)

Il costruttore di dispositivi o macchinari dovrà per prima cosa verificare se il proprio prodotto ricade all'interno di una norma di tipo C. In caso positivo sarà tale norma a dare le prescrizioni per la sicurezza, altrimenti faranno fede le norme di tipo B per ogni specifico aspetto o dispositivo del prodotto. In mancanza di ulteriori specifiche il costruttore seguirà i principi generali enunciati nelle norme di tipo A.

NORME DI TIPO A

ad esempio:

- EN ISO 12100-1 e -2:2010 (sostituisce EN 292-1 e EN 292-2).
Concetti fondamentali, principi generali di progettazione.
- EN 61508. Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza.
- EN ISO 14121:2007: Principi per la valutazione del rischio.

NORME DI TIPO B1

ad esempio:

- EN 62061:2005 Sicurezza funzionale dei sistemi di comando e controllo elettrici, elettronici ed elettronici programmabili correlati alla sicurezza
- EN ISO 13849-1:2006 e -2:2003 Parte dei sistemi di comando legate alla sicurezza

NORME DI TIPO B2

ad esempio:

- EN 574:2008 Dispositivi di comando a due mani
- EN 13850:2006 (sostituisce EN 418:1992)
Arresto di emergenza
- EN 1088:2008 e ISO 14119 Dispositivi di interblocco dei ripari
- EN 60204-1:2006 Equipaggiamento elettrico delle macchine
- EN 60947-5-1:2009 Dispositivi di controllo elettromeccanici.

NORME DI TIPO C

ad esempio:

- EN 201:2007. Macchine per gomma e materie plastiche - Macchine a iniezione
- EN 415-1.-7:2009 Sicurezza delle macchine per imballare
- EN 692:2009 Presse meccaniche
- EN 693:2009 Presse idrauliche
- EN 848-1:2010 Sicurezza delle macchine per la lavorazione del legno - Fresatrici su un solo lato con utensile rotante - Parte 1: Fresatrici verticali monoalbero (toupie)

3 – Progettare macchine sicure. L'analisi dei rischi.

Il primo passo per la costruzione di una macchina sicura consiste nell'identificare quali sono tutti i possibili pericoli a cui sono esposti gli operatori di una macchina. L'identificazione e la classificazione dei pericoli permettono di definire il rischio per l'operatore ovvero la combinazione della probabilità che il pericolo avvenga e del tipo di danno possibile per l'operatore.

La metodologia di analisi dei rischi, della loro valutazione, di come procedere nella loro riduzione è definita dalle norme EN ISO 12100 e EN ISO 14121. Queste norme introducono un modello ciclico di analisi tale per cui, definiti degli obiettivi iniziali, l'analisi dei rischi e delle possibili soluzioni per limitare questi rischi vengono valutati ripetutamente fintantoché gli obiettivi iniziali non siano soddisfatti.

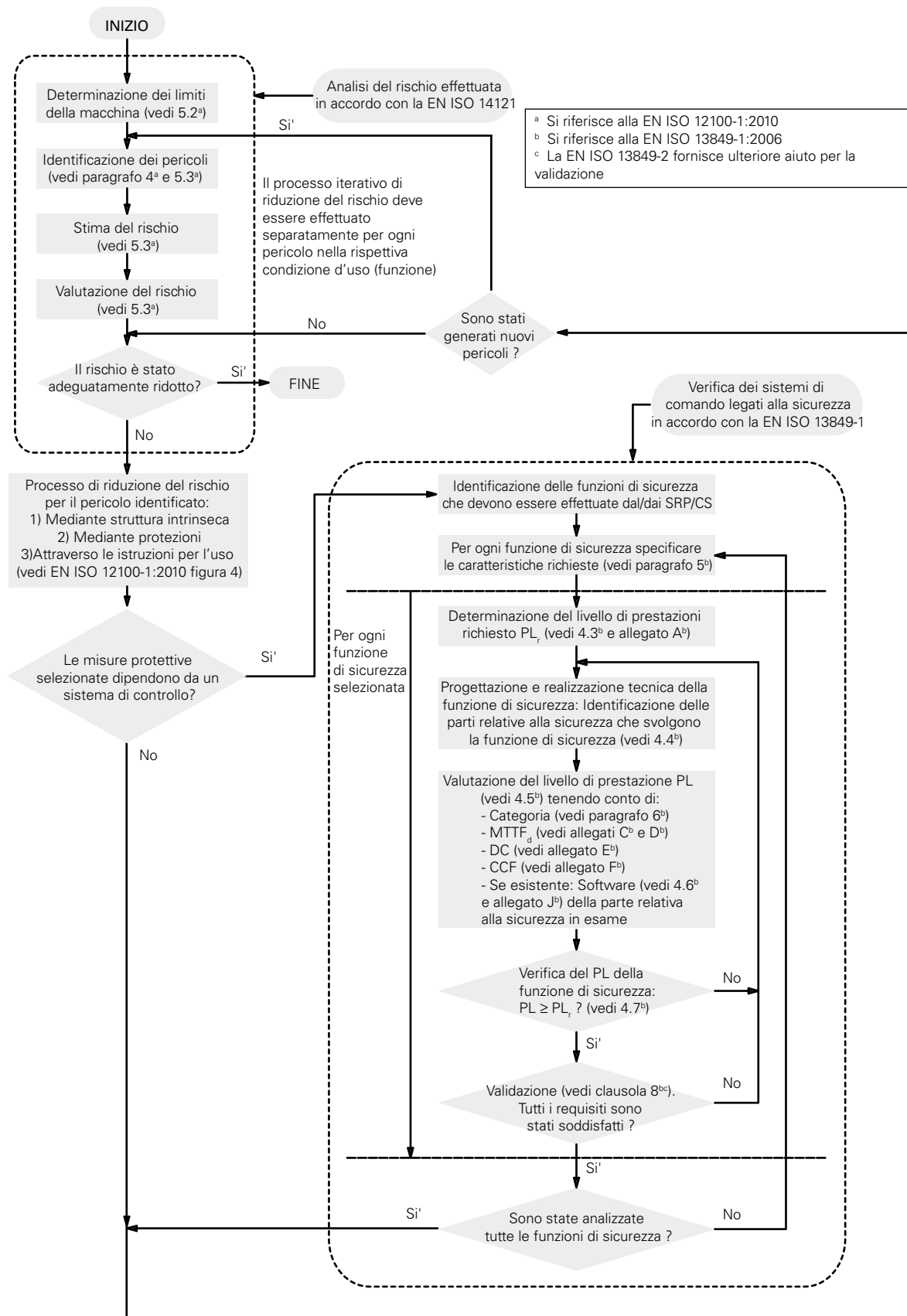
Il modello introdotto da questa coppia di norme prevede che, dopo un'analisi dei rischi secondo EN ISO 14121, si proceda alla loro riduzione/eliminazione attraverso un processo che prevede nell'ordine:

- 1) L'eliminazione dei rischi alla sorgente, mediante la struttura del sistema e l'utilizzo di principi progettuali intrinsecamente sicuri
- 2) La riduzione dei rischi attraverso sistemi di protezione e controllo
- 3) L'evidenziazione di rischi residui mediante segnalazione e l'informazione agli operatori.

Poiché ogni macchinario presenta dei pericoli e poiché non è possibile eliminare completamente tutti i possibili rischi correlati, l'obiettivo è quello

di ridurre i rischi del macchinario a livelli residuali accettabili.

Nel caso il rischio venga ridotto attraverso un sistema di controllo, entra in gioco la norma EN ISO 13849 che fornisce un modello di valutazione della bontà di tale sistema. In questo modo, dato un rischio di un determinato livello è possibile utilizzare una funzione di sicurezza di pari livello o superiore.



Nota: Questa figura è stata ottenuta dalla combinazione delle Figure 1 e 3 della EN ISO 13849-1:2006. I testi riportati sono la traduzione non ufficiale dei testi in inglese.

4 -Attuale situazione normativa (anno 2011). I perché del cambiamento, le nuove norme e qualche sovrapposizione

Le norme "tradizionali" per la sicurezza funzionale, come la EN 954-1, hanno avuto il grande merito di formalizzare alcuni principi base nell'analisi dei circuiti di sicurezza secondo principi deterministici. D'altro canto esse non trattano minimamente i dispositivi elettronici programmabili e, in generale, risentono degli anni trascorsi. Per includere i dispositivi elettronici programmabili nell'analisi dei sistemi di controllo l'approccio delle nuove norme è fondamentalmente di tipo probabilistico e in esse vengono quindi introdotte nuove variabili di tipo statistico.

La norma "madre" di tale approccio è la IEC 61508 che tratta la sicurezza dei sistemi elettronici programmabili complessi ed è una norma imponente (divisa in 8 sezioni per un totale di quasi 500 pagine) adatta a campi applicativi anche molto diversi (industria di processo, macchine industriali, impianti nucleari) tale per cui ha assunto lo status di norma di tipo A (non armonizzata). Questa norma introduce il concetto di SIL (Safety Integrity Level) ovvero un'indicazione probabilistica del rischio residuo di un sistema.

Dalla IEC 61508 deriva la EN 62061, in particolare per quanto riguarda la sicurezza dei sistemi con elettronica complessa o comunque programmabile nei macchinari industriali. I concetti introdotti ne permettono comunque l'applicazione in generale a qualsiasi sistema di controllo con tecnologia di tipo elettrico, elettronico ed elettronico programmabile (sono esclusi i sistemi con tecnologie non elettriche).

La EN ISO 13849, sviluppata dal CEN sotto l'egida dell'ISO, deriva anch'essa da questo approccio probabilistico ma cerca di fare in modo che il costruttore avvezzo ai concetti della EN 954-1 possa transitare in modo meno traumatico ai nuovi concetti. La norma si applica ai sistemi elettromeccanici, idraulici, elettronici "non complessi" ed alcuni sistemi elettronici programmabili con strutture predefinite. La EN ISO 13849 è una norma di tipo B1, introduce il concetto di PL (Performance Level) ovvero, come per il SIL, un'indicazione probabilistica del rischio residuo di un macchinario. In questa norma viene indicata una correlazione tra SIL e PL, vengono usati concetti (come DC e CCF) mutuati dalla IEC 61508 e viene stabilito un riferimento con le categorie di sicurezza della EN 954-1.

Nel campo della sicurezza funzionale, per la sicurezza dei circuiti di controllo, sono quindi attualmente in vigore tre norme (anno 2011):

- EN 954-1:1996. E' una norma di tipo B1, che ha introdotto il concetto delle Categorie di Sicurezza, ormai prossima alla scadenza. L'attuale EN 954-1:1996 rimarrà in vigore fino a Dicembre 2011 data in cui verrà ufficialmente sostituita dalla EN ISO 13849. Per la diffusione che ha avuto negli anni passati tale norma rimarrà comunque a lungo un riferimento tecnico.
- EN ISO 13849:2006. Norma di tipo B1 che utilizza il concetto di PL
- EN 62061:2005. Norma di tipo B1 che utilizza il concetto di SIL.

PL EN ISO 13849-1	a	b	c	d	e	
SIL EN 62061 - IEC 61508	-	1	2	3	(4)	
PFHd	10 ⁻⁴	10 ⁻⁵	3x10 ⁻⁶	10 ⁻⁶	10 ⁻⁷	10 ⁻⁸
Un guasto pericoloso ogni n° anni	~1	~10	~40	~100	~1000	~10000

Le due norme EN 62061 ed EN 13849 hanno quindi una discreta sovrapposizione per quanto riguarda il campo applicativo e per parecchi aspetti si assomigliano tanto è vero che esiste un legame preciso tra i due diversi nomi simbolo (SIL e PL) che indicano il risultato dell'analisi secondo le due norme.

Le raccomandazioni sull'ambito di applicabilità delle due norme è riportato nella tabella 1 della EN 13849 e come si può vedere per ampie tipologie di prodotti entrambe le norme sono applicabili.

Tabella 1 – Applicazioni raccomandate della IEC 62061 e EN ISO 13849-1

Tecnologia utilizzata dalla parte del sistema di comando legata alla sicurezza	EN ISO 13849-1	IEC 62061
A Non elettrica, ad esempio idraulica	X	Non trattata
B Elettromeccanica, ad esempio relè e/o elettronica non complessa	Limitatamente alle architetture designate ^a e fino a PL=e	Tutte le architetture e fino a SIL 3
C Elettronica complessa, ad esempio programmabile	Limitatamente alle architetture designate ^a e fino a PL=d	Tutte le architetture e fino a SIL 3
D A combinata con B	Limitatamente alle architetture designate ^a e fino a PL=e	X ^c
E C combinata con B	Limitatamente alle architetture designate (vedi nota 1) e fino a PL=d	Tutte le architetture e fino a SIL 3
F C combinata con A oppure C combinata con A e B	X ^b	X ^c

X indica che la riga è trattata dalla norma internazionale indicata nell'intestazione della colonna

a. Le architetture designate sono definite al punto 6.2 (della EN ISO 13849-1) per fornire un approccio semplificato alla quantificazione del livello di prestazioni

b. Per elettronica complessa: si usino le architetture designate in accordo con questa parte della EN ISO 13849-1 e fino a PL=d o qualsiasi architettura in accordo con la IEC 62061

c. Per tecnologie non elettriche si usino le parti come sottosistemi in accordo con questa parte della EN ISO 13849-1

Nota. La presente tabella è la traduzione non ufficiale in italiano della tabella 1 presente nella versione in Inglese nella norma EN ISO 13849-1:2006

La scelta della norma da utilizzare è del costruttore, in funzione della tecnologia utilizzata. Riteniamo che la EN 13849 con il suo approccio mediato e con il riutilizzo di concetti già noti al mercato sia una norma di più semplice applicazione.

Nota: L'ente per la prevenzione e sicurezza tedesca IFA ha introdotto nel 2008 un report (BGIA Report 2/2008) sulla applicazione della EN 13849 dove viene dichiarato che le raccomandazioni ed i limiti sull'applicazione della 13849 devono considerarsi obsolete e che quindi anche nei casi di elettronica programmabile (casi C ed E nella tabella superiore) il limite si può considerare PL_e.

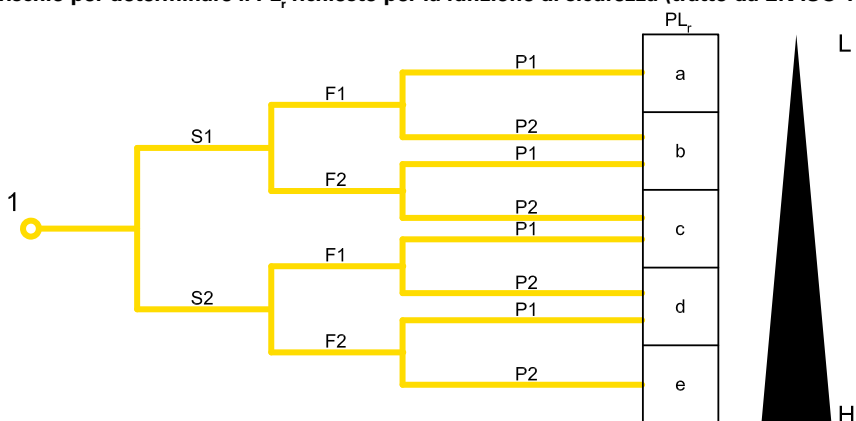
5- La norma EN ISO 13849 ed i nuovi parametri: PL, MTTFd, DC, CCF

La norma EN ISO 13849 fornisce al costruttore un metodo iterativo per valutare se i rischi di una macchina possano essere limitati ad un livello residuo accettabile mediante l'impiego di adeguate funzioni di sicurezza. Il metodo adottato prevede, per ogni rischio, un ciclo di ipotesi-analisi-validazione alla fine del quale si deve poter dimostrare che ogni funzione di sicurezza prescelta è adeguata al relativo rischio in esame.

Il primo passo consiste quindi nella valutazione del livello di prestazione richiesto da ogni funzione di sicurezza. Come per la EN 954-1 anche la EN ISO 13849 utilizza un grafico per l'analisi del rischio di una funzione di una macchina (figura A.1) determinando, in funzione del rischio, anziché una categoria di sicurezza richiesta, un livello di prestazione richiesto o PL_r (Required Performance Level) per la funzione di sicurezza che andrà a proteggere quella parte di macchina.

Il costruttore del macchinario, partendo dal punto 1 del grafico e rispondendo alle domande S, F e P identificherà il PL_r per la funzione di sicurezza in esame. Dovrà poi realizzare un sistema per proteggere l'operatore della macchina che abbia un livello di prestazione PL uguale o migliore di quello richiesto.

Grafico del rischio per determinare il PL_r richiesto per la funzione di sicurezza (tratto da EN ISO 13849-1, figura A.1)



Chiavi di lettura

- 1** Punto di partenza per la valutazione del contributo alla riduzione del rischio dato dalle funzioni di sicurezza
L Basso contributo alla riduzione del rischio
H Alto contributo alla riduzione del rischio
PL_r Livello di prestazioni richiesto

Parametri di rischio

- S** Gravità del danno
S1 leggero (danno normalmente reversibile)
S2 serio (danno normalmente irreversibile o morte)
F Frequenza e/o esposizione al rischio
F1 da rara a poco frequente e/o con breve tempo di esposizione
F2 da frequente a continua e/o con lungo tempo di esposizione
P Possibilità di evitare il rischio o di limitare il danno
P1 possibile in certe condizioni
P2 scarsamente possibile

Nota: Potrebbe essere interessante per un costruttore di macchine non dover ripetere l'analisi dei rischi della macchina ma tentare di riutilizzare quanto già svolto con l'analisi dei rischi della EN 954-1.

Questo in generale non è possibile poiché con la nuova norma è variato il grafico del rischio (vedi figura precedente) e quindi a parità di rischio possono essere cambiate i livelli di funzione di sicurezza richiesta. L'ente tedesco BGIA nel report 2008/2 sulla EN ISO 13849 suggerisce che, adottando un approccio del tipo "caso peggiore", si possa adottare una conversione come nella tabella che segue. Per ulteriori informazioni si faccia riferimento al testo in questione.

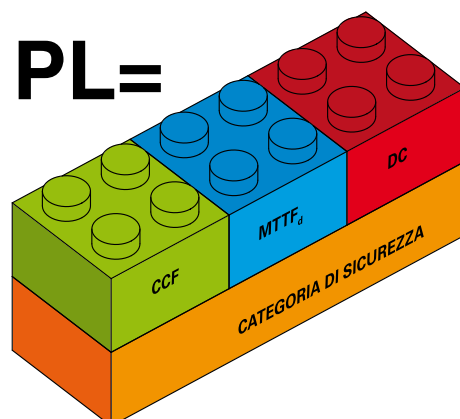
Categoria richiesta dalla EN 954-1:1996	Performance Level richiesto (PL _r) e Categoria richiesta secondo EN ISO 13849-1:2006
B	→ b
1	→ c
2	→ d, Categoria 2
3	→ d, Categoria 3
4	→ e, Categoria 4

I PL sono classificati in cinque livelli, da PL_a a PL_e al crescere del rischio ed ognuno di essi identifica un ambito numerico di probabilità media di guasto pericoloso per ora. Ad esempio PL_d indica che la probabilità media di guasti pericolosi per ora è compresa tra 1×10^{-6} e 1×10^{-7} ovvero all'incirca 1 guasto pericoloso mediamente ogni 100-1000 anni.

PL	Probabilità media di guasti pericolosi per ora PFH _d (1/h)	
a	$\geq 10^{-5}$	$< 10^{-4}$
b	$\geq 3 \times 10^{-6}$	$< 10^{-5}$
c	$\geq 10^{-6}$	$< 3 \times 10^{-6}$
d	$\geq 10^{-7}$	$< 10^{-6}$
e	$\geq 10^{-8}$	$< 10^{-7}$

Per la valutazione del PL di un sistema di controllo servono più parametri ovvero:

1. La Categoria di sicurezza del sistema che a sua volta deriva dall'architettura (struttura) del sistema di controllo e dal suo comportamento in caso di guasto
2. MTTF_d dei componenti
3. DC o Copertura Diagnostica del sistema.
4. CCF o Guasti di causa comune del sistema.



Categoria di Sicurezza.

La stragrande maggioranza dei circuiti di controllo normalmente utilizzati sono rappresentabili mediante una struttura a blocchi logici di tipo:

- Input o ingresso di segnali
- Logic o logica di elaborazione dei segnali
- Output o uscita del segnale di controllo

tra di loro variamente interconnessi a seconda della struttura del circuito di controllo.

La EN ISO 13849 ammette cinque diverse strutture circuitali di base definendole Architetture Designate del sistema. Le architetture combinate con le richieste di comportamento al guasto del sistema e con dei valori minimi di $MTTF_d$, DC e CCF indicano la Categoria di Sicurezza del sistema di controllo come riportato nella tabella che segue. Le Categorie di Sicurezza della EN ISO 13849-1 quindi non sono equivalenti bensì estendono il concetto di Categoria di Sicurezza introdotta nella precedente EN 954-1.

Categoria	Elenco dei requisiti	Comportamento del sistema	Principi per la sicurezza	$MTTF_d$ di ogni canale	DC_{avg}	CCF
B	<p>Le parti rilevanti per la sicurezza dei sistemi di controllo e/o le loro attrezzature di protezione, nonché le loro componenti devono essere progettate, costruite, selezionate e combinate in ottemperanza alle norme pertinenti in modo da poter resistere agli influssi previsti. Devono essere usati principi base di sicurezza.</p> <p>Architettura: </p>	Il verificarsi di un errore può portare alla perdita della funzione di sicurezza.	Caratterizzato principalmente dalla selezione dei componenti	Basso o Medio	Nulla	Non rilevante
1	<p>Si applicano i requisiti della categoria B. Devono essere usati dei componenti ben provati e dei principi di sicurezza ben provati.</p> <p>Architettura: </p>	Il verificarsi di un errore può portare alla perdita della funzione di sicurezza però la probabilità del verificarsi di un errore è inferiore a quello della categoria B.	Caratterizzato principalmente dalla selezione dei componenti	Alto	Nulla	Non rilevante
2	<p>Si applicano i requisiti della categoria B e l'uso di principi di sicurezza ben provati. La funzione di sicurezza deve essere controllata a adeguati intervalli di tempo dal sistema di controllo.</p> <p>Architettura: </p>	Il verificarsi di un errore può portare alla perdita della funzione di sicurezza fra i controlli. La perdita della funzione di sicurezza viene rilevata dal controllo.	Caratterizzato principalmente dalla struttura	Da Basso a Alto	Da Basso a Medio	Si veda l'allegato F
3	<p>Si applicano i requisiti della categoria B e l'uso di principi di sicurezza ben provati. Le parti rilevanti per la sicurezza devono essere progettate in modo che:- un singolo errore in una di queste parti non porti alla perdita della funzione di sicurezza. - laddove ragionevolmente fattibile il singolo errore venga rilevato.</p> <p>Architettura: </p>	Quando si verifica un singolo errore la funzione di sicurezza viene sempre svolta. Alcuni ma non tutti gli errori vengono rilevati. L'accumulo di errori non rilevati può portare alla perdita della funzione di sicurezza.	Caratterizzato principalmente dalla struttura	Da Basso a Alto	Da Basso a Medio	Si veda l'allegato F
4	<p>Si applicano i requisiti della categoria B e l'uso di principi di sicurezza ben provati. Le parti rilevanti per la sicurezza devono essere progettate in modo tale che:- un singolo errore in una di queste parti non porti alla perdita della funzione di sicurezza, e - il singolo errore venga rilevato nel momento o prima della successiva richiesta della funzione di sicurezza. Se questo non è possibile allora l'accumulo di errori non deve portare alla perdita della funzione di sicurezza.</p> <p>Architettura: </p>	Quando si verifica un singolo errore la funzione di sicurezza viene sempre svolta. Il rilevamento di errori accumulati riduce la probabilità della perdita della funzione di sicurezza (DC alto). Gli errori sono rilevati in tempo per prevenire la perdita della funzione di sicurezza.	Caratterizzato principalmente dalla struttura	Alto	Alto (inclusa l'accumulazione dei guasti)	Si veda l'allegato F

MTTF_d ("Mean Time To Dangerous Failure", Tempo medio al guasto pericoloso).

Questo parametro cerca di definire la bontà qualitativa dei componenti del sistema definendone la vita media prima del guasto pericoloso (si noti bene che non si tratta di un guasto generico) espressa in anni. In pratica il calcolo dell'MTTF_d si basa sui valori numerici forniti dai costruttori dei singoli componenti che formano il sistema. Nel caso di mancanza di dati la norma fornisce dei valori in apposite tabelle di riferimento (allegato C della EN ISO 13849-1). Il conteggio porterà ad un valore numerico che rientrerà in tre categorie: Alto, Medio o Basso.

Classificazione	Valori
Non accettabile	MTTF _d < 3 anni
Basso	3 anni ≤ MTTF _d < 10 anni
Medio	10 anni ≤ MTTF _d < 30 anni
Alto	30 anni ≤ MTTF _d ≤ 100 anni

Nel caso di componenti soggetti ad usura (tipicamente dispositivi meccanici o idraulici) il costruttore del componente fornirà, anziché l'MTTF_d del componente, il dato B_{10d} del componente ovvero il numero di operazioni del componente entro il quale il 10% dei campioni si è guastato in modo pericoloso.

Il B_{10d} del componente deve essere convertito dal costruttore della macchina in MTTF_d attraverso la formula:

$$MTTF_d = \frac{B_{10d}}{0,1 \cdot n_{op}}$$

Dove n_{op} = numero di operazioni per anno del componente.

Ipotizzando la frequenza di utilizzo giornaliero ed il numero di ore lavorative giornaliere della macchina n_{op} si può a sua volta ottenere da:

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600s/h}{t_{ciclo}}$$

dove

d_{op} = giorni lavorativi per anno

h_{op} = ore lavorative per giorno

t_{ciclo} = tempo ciclo (s)

Si noti quindi che il parametro MTTF_d quando deriva da un componente soggetto ad usura, non dipende solo dal componente in sé ma anche dall'applicazione. Un dispositivo elettromeccanico a bassa frequenza di utilizzo, ad esempio un teleruttore usato solamente per gli arresti di emergenza, avrà in generale un MTTF_d elevato ma se il medesimo dispositivo viene usato anche per le normali operazioni di ciclo ecco che l'MTTF_d del medesimo teleruttore, con un basso tempo ciclo, potrebbe calare drasticamente.

Al computo dell'MTTF_d del circuito di controllo contribuiscono tutti gli elementi del circuito medesimo, in funzione della sua struttura. In circuiti aventi architettura monocanale (come nei casi delle categorie B, 1 e 2) il contributo di ogni componente è lineare ed il computo dell'MTTF_d del canale si ottiene da:

$$\frac{1}{MTTF_d} = \sum_{i=1}^N \frac{1}{MTTF_{di}}$$

Per evitare interpretazioni troppo ottimistiche il valore massimo di MTTF_d di ogni canale è limitato a 100 anni. Non sono ammessi canali con un MTTF_d inferiore a 3 anni.

Nel caso dei sistemi a due canali (categorie 3 e 4) il calcolo dell'MTTF_d del circuito si ottiene attraverso la simmetrizzazione degli MTTF_d dei due canali utilizzando la formula:

$$MTTF_d = \frac{2}{3} \left[MTTF_{dc1} + MTTF_{dc2} - \frac{1}{\frac{1}{MTTF_{dc1}} + \frac{1}{MTTF_{dc2}}} \right]$$

DC ("Diagnostic Coverage", copertura diagnostica).

Questo parametro cerca di indicare quanto il sistema sia in grado di "autosorvegliare" un eventuale proprio malfunzionamento. In base alla percentuale di guasti pericolosi rilevabili dal sistema si avrà una copertura diagnostica più o meno buona. Il parametro numerico DC è un valore percentuale che si calcola attraverso dei valori forniti in una tabella (allegato E della EN ISO 13849-1) in funzione degli accorgimenti adottati dal costruttore per rilevare le anomalie del proprio circuito. Poiché in generale sono presenti più accorgimenti nel medesimo circuito per rilevare anomalie diverse, alla fine si andrà a computare un valore medio o DC_{avg} che andrà a ricadere all'interno di quattro fasce, per la precisione in:

Alta DC_{avg} ≥ 99%

Media 90% ≤ DC_{avg} < 99%

Bassa 60% ≤ DC_{avg} < 90%

Nulla 60% < DC_{avg}

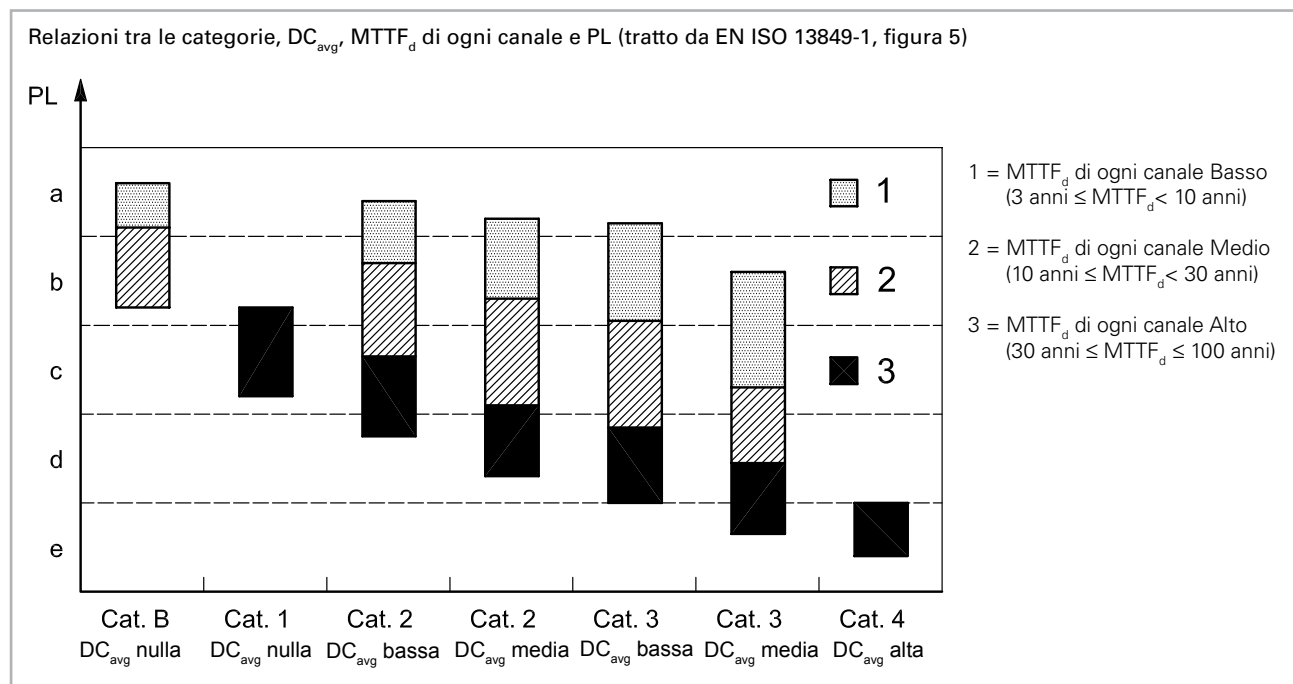
La copertura diagnostica Nulla è ammessa solo per i sistemi con architettura B o 1.

CCF ("Common Cause Failures", Guasto di causa comune)

Nel caso di sistemi di categoria 2, 3, o 4 per il calcolo del PL è necessaria anche la valutazione di eventuali cause di guasto comune o CCF che possono inficiare la ridondanza dei sistemi. La valutazione viene fatta mediante una check-list di controllo (allegato F della EN ISO 13849-1) che, in base al tipo di soluzioni adottate contro le cause di guasto comune, fornisce un punteggio da 0 a 100. Il valore minimo ammesso per le categorie 2,3 e 4 è di 65 punti.

PL ("Performance Level")

Noti questi dati, la norma EN ISO 13849-1 fornisce il PL del sistema attraverso una tabella di correlazione (allegato K della EN ISO 13849-1) o, in forma grafica semplificata (punto 4.5 della EN ISO 13849-1), attraverso la seguente figura.



Questa immagine è molto utile perché ha più modalità di lettura. Dato un certo PL, essa evidenzia tutti le possibili soluzioni che forniscono quel livello di PL ovvero le possibili strutture circuitali che forniscono il medesimo PL.

Ad esempio osservando la figura si nota come per ottenere un sistema con PL pari a "c" sono possibili tutte le seguenti soluzioni:

1. Sistema in categoria 3 con componenti poco affidabili ($MTTF_d$ =basso) e DC media.
2. Sistema in categoria 3 con componenti affidabili ($MTTF_d$ =medio) e DC bassa.
3. Sistema in categoria 2 con componenti affidabili ($MTTF_d$ =medio) e DC media.
4. Sistema in categoria 2 con componenti affidabili ($MTTF_d$ =medio) e DC bassa.
5. Sistema in categoria 1 con componenti molto affidabili ($MTTF_d$ =alto).

Al contempo la figura, scelta una struttura circuitali, permette di vedere subito i massimi PL raggiungibili in funzione della copertura diagnostica media e del $MTTF_d$ dei componenti. Il costruttore può quindi escludere a priori alcune strutture circuitali in quanto non adeguate al PL richiesto.

In genere però, per identificare il PL del sistema, non si fa riferimento alla figura in questione poiché in molti casi le aree del grafico si sovrappongono alle linee di margine dei vari PL. Viene invece utilizzata la tabella presente nell'allegato K della EN ISO 13849-1 per una determinazione precisa del PL del circuito.

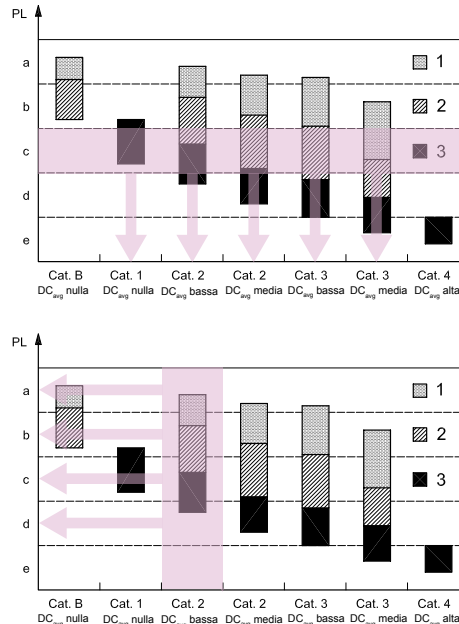


Tabella parametri di sicurezza (2011)

I dati B10 e B10d indicati nella tabella fanno riferimento alla vita meccanica dei contatti sicuri (NC ad apertura positiva) dei dispositivi in condizioni ambientali normali. Mission time (per tutti gli articoli sottoindicati): 20 anni.

Serie	Descrizione articolo	B10	B10 _d	B10/ B10 _d
F•••••	Interruttori di posizione	20.000.000	40.000.000	50%
F•••93 F•••92 F•••99 F•••R2	Interruttori di sicurezza ad azionatore separato	1.000.000	2.000.000	50%
FS, FG	Interruttori di sicurezza ad azionatore separato con blocco	1.000.000	5.000.000	20%
F•••96 F•••95	Interruttore di sicurezza a perno per cerniere	1.000.000	5.000.000	20%
F•••C•	Interruttori a leva asolata per ripari a battente	1.000.000	2.000.000	50%
F•••••	Interruttori a fune per arresto d'emergenza	1.000.000	2.000.000	50%
HP	Cerniere di sicurezza	1.000.000	5.000.000	20%
SR	Sensori magnetici di sicurezza (utilizzati con moduli di sicurezza Pizzato)	10.000.000	20.000.000	50%
SR	Sensori magnetici di sicurezza (utilizzati a massimo carico: 24V 250mA)	5.000.000	10.000.000	50%
PX, PA	Interruttori a pedale	20.000.000	40.000.000	50%
MK	Microinterruttori di posizione	10.000.000	20.000.000	50%
NA, NB, NF	Interruttori di posizione precablati modulari	20.000.000	40.000.000	50%
E2 1PE•••••	Pulsanti d'emergenza	300.000	600.000	50%
E2 C•••••	Unità di contatto	20.000.000	40.000.000	50%

Codice	Descrizione articolo	MTTF _d	DC	PFH _d	SIL CL	PL	Cat
CS AM-01	Modulo di sicurezza per il rilevamento motore fermo	145	M	1.94E-09	2	d	3
CS AR-01	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	147	H	6.38E-10	3	e	4
CS AR-02	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	147	H	6.38E-10	3	e	4
CS AR-04	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	147	H	6.38E-10	3	e	4
CSAR-04V024	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	218	H	4.58E-10	3	e	4
CS AR-05	Modulo di sicurezza per controllo ripari, arresti d'emergenza e barriere ottiche	147	H	6.61E-10	3	e	4
CSAR-05V024	Modulo di sicurezza per controllo ripari, arresti d'emergenza e barriere ottiche	218	H	4.58E-10	3	e	4
CS AR-06	Modulo di sicurezza per controllo ripari, arresti d'emergenza e barriere ottiche	147	H	6.61E-10	3	e	4
CSAR-06V024	Modulo di sicurezza per controllo ripari, arresti d'emergenza e barriere ottiche	218	H	4.58E-10	3	e	4
CS AR-07	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	111	H	7.56E-10	3	e	4
CS AR-08	Modulo di sicurezza per controllo ripari, arresti d'emergenza e controllo barriere ottiche	218	H	4.58E-10	3	e	4
CS AR-20	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	358	M	8.71E-09	3	e	3
CS AR-21	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	358	M	8.71E-09	3	e	3
CS AR-22	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	201	H	8.87E-09	3	e	3
CS AR-23	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	201	H	8.87E-09	3	e	3
CS AR-24	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	111	H	1.18E-09	3	e	3
CS AR-25	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	111	H	1.18E-09	3	e	3
CS AR-40	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	356	M	1.08E-08	2	d	2
CS AR-41	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	356	M	1.08E-08	2	d	2
CS AR-46	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	435	-	3.32E-08	1	c	1
CS AR-51	Modulo di sicurezza per controllo tappeti e bordi sensibili	209	H	9.43E-09	3	e	4
CS AR-90	Modulo di sicurezza per controllo del livellamento al piano degli ascensori	382	H	5.03E-10	3	e	4
CS AR-94	Modulo di sicurezza per controllo del livellamento al piano degli ascensori	213	H	5.62E-09	3	e	4
CS AR-95	Modulo di sicurezza per controllo del livellamento al piano degli ascensori	213	H	5.42E-09	3	e	4
CS AT-0x	Modulo di sicurezza temporizzato per controllo ripari ed arresti d'emergenza	84	H	9.01E-09	3	e	4
CS AT-1x	Modulo di sicurezza temporizzato per controllo ripari ed arresti d'emergenza	84	H	9.01E-09	3	e	4
CS AT-3x	Modulo di sicurezza temporizzato per controllo ripari ed arresti d'emergenza	74	H	4.05E-09	3	e	4
CS DM-01	Modulo di sicurezza per controllo comando bimanuale	142	H	2.99E-08	3	e	4
CS DM-02	Modulo di sicurezza per controllo comando bimanuale	206	H	2.98E-08	3	e	4
CS FS-10	Modulo temporizzatore di sicurezza	146	H	1.62E-09	3	e	4
CS FS-20	Modulo temporizzatore di sicurezza	205	M	1.10E-08	2	d	3
CS FS-30	Modulo temporizzatore di sicurezza	205	M	1.10E-08	2	d	3
CS FS-50	Modulo temporizzatore di sicurezza	349	M	1.17E-08	2	d	3
CS ME-01	Modulo di espansione contatti	76	H	6.38E-10	3	e	4
CS ME-02	Modulo di espansione contatti	113	H	2.84E-09	3	e	4
CS ME-03	Modulo di espansione contatti	208	M	2.45 E-08	2	d	3
CS ME-20	Modulo di espansione contatti	113	H	3.07E-09	3	e	4
CS ME-30	Modulo di espansione contatti	112	H	2.77E-09	3	e	4
CS ME-31	Modulo di espansione contatti	112	H	2.77E-09	3	e	4

B10_d: Numero di operazioni affinché il 10% dei componenti si guasti in modo pericoloso
 B10: Numero di operazioni affinché il 10% dei componenti si guasti
 B10/B10_d: rapporto tra guasti totali e guasti pericolosi.
 MTTF_d: Mean Time To Failure Dangerous (Tempo medio al guasto pericoloso)

DC: Diagnostic coverage (Copertura diagnostica)
 PFH_d: Probability of Dangerous Failure per hour (Probabilità al guasto pericoloso per ora)
 SIL CL: Safety Integrity Level Claim Limit. Massimo SIL raggiungibile secondo EN 62061
 PL: Performance Level. PL secondo EN ISO 13849-1

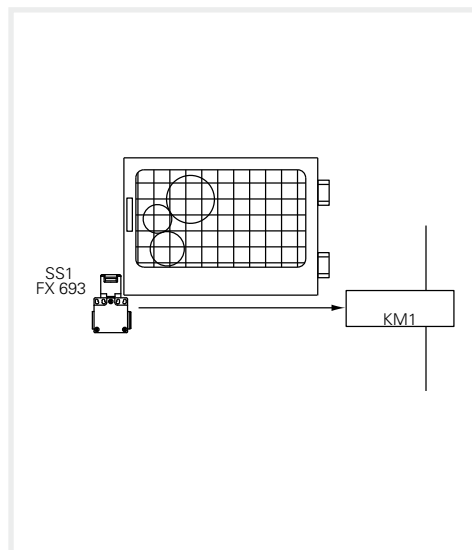
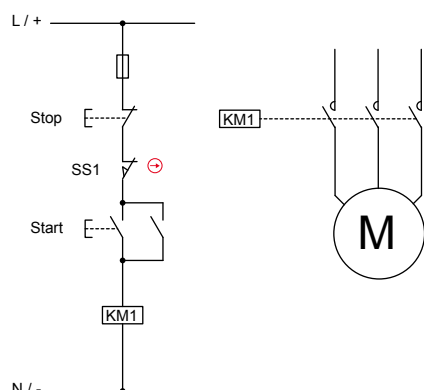
ESEMPIO 1**Applicazione: Controllo ripari**

Norma di riferimento EN ISO 13849-1:2006

Categoria di sicurezza

1

Performance Level

PL c

Il circuito di controllo in figura svolge la funzione di sorveglianza del riparo. Se il riparo è aperto il motore non deve potersi avviare. L'analisi dei pericoli ha evidenziato come il sistema non sia dotato di inerzia ovvero che il motore, una volta tolta alimentazione, si fermi in tempi molto più rapidi dell'apertura del riparo. Dall'analisi dei rischi si è evidenziato come il PL_r target richiesto è PL c. Si vuole verificare se il circuito di controllo ipotizzato, che ha una struttura monocanale, ha un PL maggiore o uguale a PL_r .

Descrizione della funzione di sicurezza

La posizione del riparo è rilevata dall'interruttore ad azionatore separato SS1 che agisce direttamente sul contattore KM1. Il contattore KM1 che controlla gli organi in movimento viene normalmente azionato dai pulsanti di Start e Stop ma l'analisi del ciclo di funzionamento ha mostrato che anche il riparo viene aperto ad ogni ciclo operativo. Ne consegue che il numero di manovre del teleruttore e dell'interruttore di sicurezza si possono considerare uguali.

La struttura del circuito è del tipo monocanale senza supervisione (categoria B o 1) dove sono presenti solo il componente di Input (interruttore) ed output (contattore).

La funzione di sicurezza non viene mantenuta al verificarsi di un guasto su uno dei dispositivi.

Non sono applicate misure per la verifica dei guasti.

Dati dei dispositivi:

- SS1 (FX693) è un interruttore ad apertura positiva (in accordo con l'allegato K della EN 60947-5-1). L'interruttore è un dispositivo ben testato in accordo con la tabella D.4 della EN ISO 13849-2. Il valore del $B10_d$ del dispositivo è fornito dal costruttore (vedi pagina 7/32) ed è pari a 2.000.000 di manovre.
- KM1 è un contattore utilizzato a carico nominale ed è un componente ben testato in accordo con la tabella D.4 della EN ISO 13849-2. Il suo valore di $B10_d$ è pari a 2.000.000 manovre, valore ricavato dalle tabelle di norma (vedi Tabella C.1 della EN ISO 13849-1).

Ipotesi di frequenza di utilizzo

- Si suppone che il macchinario venga usato al massimo per 365 giorni all'anno, per tre turni di 8 ore con un tempo ciclo di 600 secondi. Il numero di operazioni annuo per l'interruttore è quindi pari a $N_{op} = (365 \times 24 \times 3.600) / 600 = 52.560$.
- Si suppone l'azionamento del pulsante di start ogni 300 secondi. Il numero di operazioni annuo è quindi pari al massimo a $n_{op}/\text{anno} = 105.120$
- Il contattore KM1 verrà azionato sia per il normale start-stop della macchina, sia per il riavvio a seguito dell'apertura di un riparo. $n_{op}/\text{anno} = 52.560 + 105.120 = 157.680$

Calcolo $MTTF_d$

L' $MTTF_d$ dell'interruttore SS1 è pari a: $MTTF_d = B10_d / (0,1 \times n_{op}) = 2000000 / (0,1 \times 52560) = 381$ anni

L' $MTTF_d$ del contattore KM1 è pari a: $MTTF_d = B10_d / (0,1 \times n_{op}) = 2000000 / (0,1 \times 157680) = 127$ anni

Ne consegue che l' $MTTF_d$ del circuito monocanale è pari a: $1 / (1/381 + 1/127) = 95$ anni

Copertura diagnostica DC_{avg}

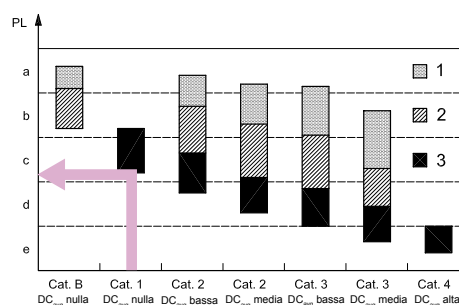
Non sono applicate misure per la verifica dei guasti e quindi la copertura diagnostica è Nulla, condizione ammessa per il circuito in esame che è in categoria 1.

Guasti di causa comune CCF

Per un circuito in categoria 1 non è necessario il calcolo del parametro CCF.

Verifica del PL

Dalla tabella o dalla figura 5 di norma si verifica come per un circuito in Categoria 1 con $MTTF_d = 95$ anni il PL risultante del circuito di controllo è pari a PL c. Il PL_r obiettivo è quindi raggiunto.



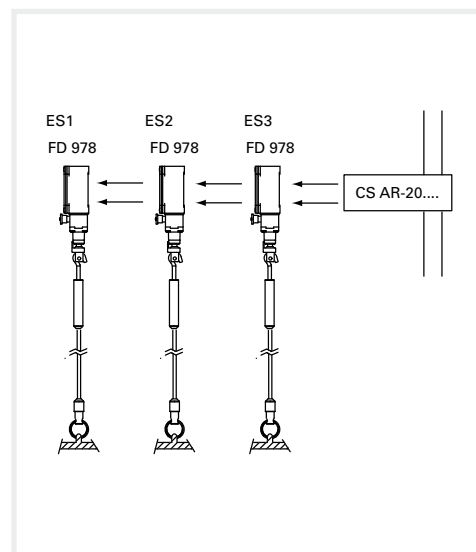
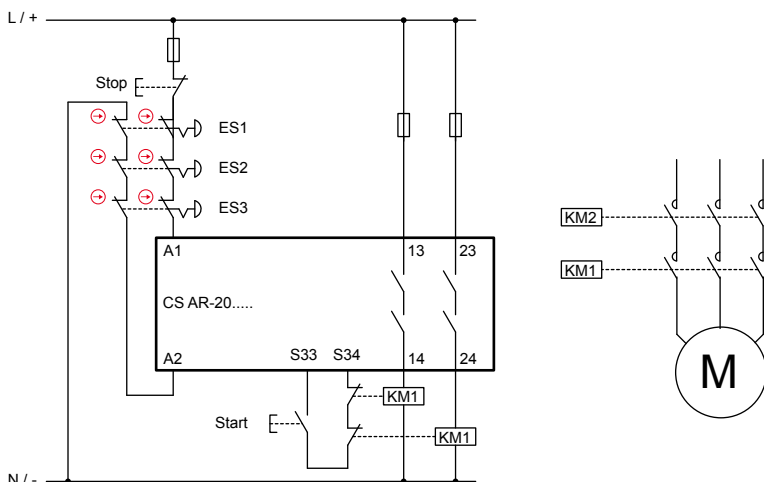
ESEMPIO 2**Applicazione: Controllo arresti d'emergenza**

Norma di riferimento EN ISO 13849-1:2006

Categoria di sicurezza

3

Performance Level

PL e**Descrizione della funzione di sicurezza**

L'azionamento di uno dei dispositivi d'emergenza provoca l'intervento del modulo di sicurezza e dei due contattori KM1 e KM2

Il segnale dei dispositivi ES1, ES2, ES3 è letto in modo ridondante dal modulo di sicurezza CS. Anche i contattori KM1 e KM2 (con contatti a guida forzata) sono controllati da CS tramite il circuito di retroazione.

Dati dei dispositivi:

- ES1, ES2, ES3 (FD 978) sono interruttori a fune per arresti d'emergenza ad apertura positiva. Il valore di B_{10^6} è pari a 2.000.000 (Vedi pagina 7/32)
- KM1, KM2 sono contattori utilizzati a carico nominale. Il valore B_{10^6} è pari a 2.000.000 (vedi Table C.1 della EN ISO 13849-1)
- CS è un modulo di sicurezza (CS AR-20) con $MTTF_d=358$ anni (vedi pagina 7/32) e DC= Medium
- L'architettura circuitale è a doppio canale in categoria 3

Ipotesi di frequenza di utilizzo

- 2 volte al mese $n_{op}/anno = 24$
- Azionamento del pulsante di start : 4 volte al giorno
- Ipotizzando 365 giorno lavorativi, i contattori interverranno $4 \times 365 + 24 = 1484$ volte/anno
- Gli interruttori saranno azionati con la stessa frequenza.
- Non si prevede che più pulsanti possano essere premuti simultaneamente.

Calcolo $MTTF_d$

- $MTTF_{d_{ES1,ES2,ES3}} = 833.333$ anni
- $MTTF_{d_{KM1,KM2}} = 13.477$ anni
- $MTTF_{d_{CS}} = 358$ anni
- $MTTF_{d_{CH1}} = 349$ anni. Il valore va limitato a 100 anni. I canali sono simmetrici per cui $MTTF_d=100$ anni (High)

Copertura diagnostica DC_{avg}

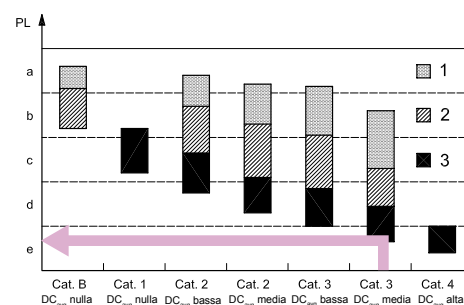
- I contatti di KM1 e KM2 sono monitorati da CS tramite il circuito di retroazione. DC=99% (High)
- Il modulo di sicurezza CS AR-20 ha una copertura diagnostica Medium.
- Non tutti i guasti nella serie dei dispositivi di emergenza possono essere rilevati. La copertura diagnostica è del 90% (Medium)

Guasti di causa comune CCF

Supponiamo un punteggio > 65 (in base ad annex F della EN ISO 13849-1).

Verifica del PL

Un circuito in categoria 3 con $MTTF_d=100$ anni e $DC_{avg} = \text{Medium}$ può raggiungere un PL e.



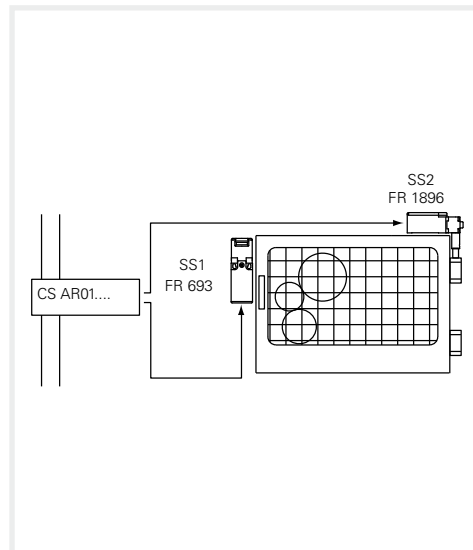
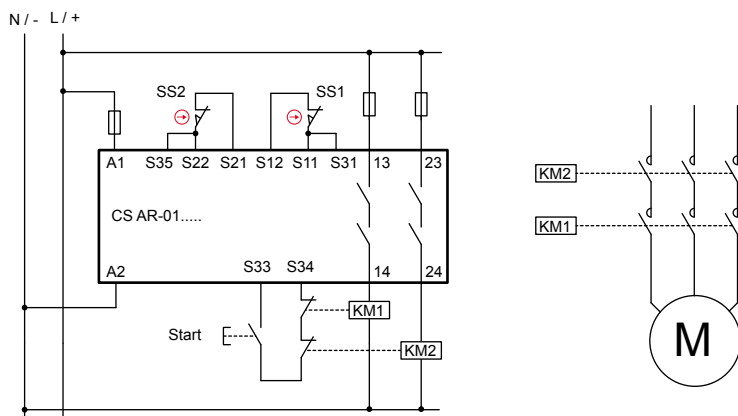
ESEMPIO 3**Applicazione: Controllo ripari**

Norma di riferimento EN ISO 13849-1:2006

Categoria di sicurezza

4

Performance Level

PL e**Descrizione della funzione di sicurezza**

L'apertura del riparo provoca l'intervento degli interruttori SS1 e SS2 e quindi del modulo di sicurezza e dei due contattori KM1 e KM2. Il segnale dei dispositivi SS1, SS2 è controllato in modo ridondante dal modulo di sicurezza CS.

Gli interruttori hanno un principio di funzionamento diverso.

Anche i contattori KM1 e KM2 (con contatti a guida forzata) sono controllati da CS tramite il circuito di retroazione.

Dati dei dispositivi:

- SS1 (FR 693) è un interruttore ad apertura positiva. Il valore di $B10_d$ è pari a 2.000.000 (vedi pagina 7/32)
- SS2 (FR 1896) è un interruttore per cerniere ad apertura positiva. $B10_d = 5.000.000$ (vedi pagina 7/32)
- KM1, KM2 sono contattori utilizzati a carico nominale. $B10_d = 2.000.000$ (vedi Table C.1 della EN ISO 13849-1)
- CS sono moduli di sicurezza (CS AR-01) con $MTTF_d = 147$ anni e $DC = 99\%$ (High)

Ipotesi di frequenza di utilizzo

365 gg/anno, 16 h/gg, 1 intervento ogni 4 minuti (240 s). $n_{op}/anno = 87.600$.

Calcolo $MTTF_d$

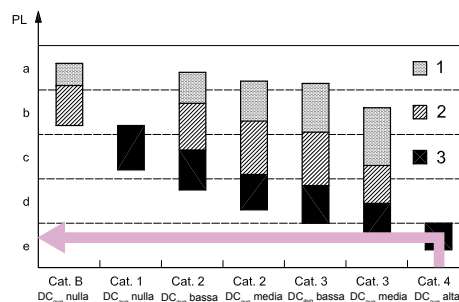
- $MTTF_{d, SS1} = 228$ anni
- $MTTF_{d, SS2} = 571$ anni
- $MTTF_{d, KM1, KM2} = 228$ anni
- $MTTF_{d, CS} = 147$ anni
- $MTTF_{d, CH1} = 64$ anni (SS1, CS, KM1)
- $MTTF_{d, CH2} = 77$ anni (SS2, CS, KM2)
- $MTTF_{d,5}$: simmettizzando i due canali si ottiene $MTTF_{d,5} = 70,5$ anni (High)

Copertura diagnostica DC_{avg}

- SS1, SS2 hanno $DC = 99\%$ in quanto i contatti di SS1 e SS2 sono monitorati da CS ed hanno principi di funzionamento diversi.
- I contatti di KM1 e KM2 sono monitorati da CS tramite il circuito di retroazione. $DC = 99\%$ (High)
- CS AR-01 al suo interno ha un circuito ridondante e autocontrollato. $DC = 99\%$ (High)
- $DC_{avg} = 99\%$ (High)

Verifica del PL

Un circuito in categoria 4 con $MTTF_{d,5} = 70,5$ anni e $DC_{avg} = High$ corrisponde ad un PL e.



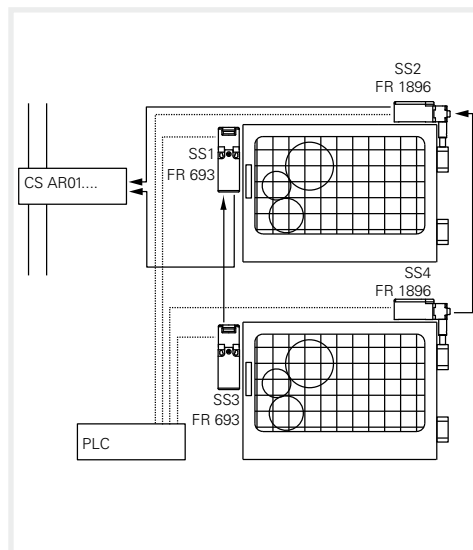
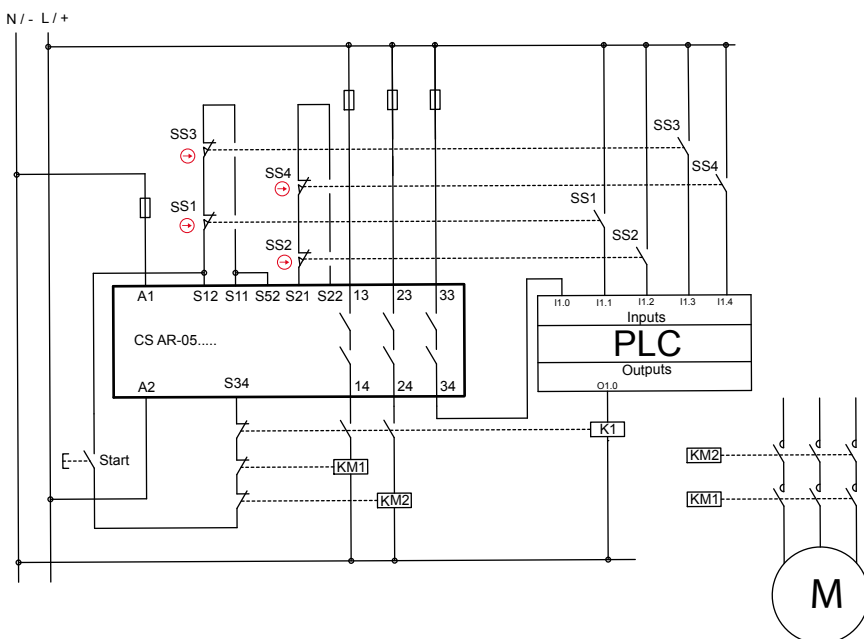
ESEMPIO 4

Applicazione: Controllo ripari

Norma di riferimento EN ISO 13849-1:2006

Categoria di sicurezza **4**

Performance Level **PL e**



Descrizione della funzione di sicurezza

L'apertura di un riparo provoca l'intervento degli interruttori SS1, SS2 sul primo riparo e SS3,SS4 nel secondo riparo, gli interruttori fanno intervenire il modulo di sicurezza e i due contattori KM1 e KM2.

Il segnale dei dispositivi SS1,SS2 e SS3,SS4 è controllato in modo ridondante dal modulo di sicurezza CS, inoltre un contatto ausiliario degli interruttori è monitorato dal PLC.

Gli interruttori hanno un principio di funzionamento diverso.

Anche i contattori KM1 e KM2 (con contatti a guida forzata) sono controllati da CS tramite il circuito di retroazione.

Dati dei dispositivi:

- SS1,SS3 (FR 693) sono interruttori ad apertura positiva. Il valore di $B10_d$ è pari a 2.000.000 (vedi pagina 7/32)
- SS2,SS4 (FR 1896) sono interruttori per cerniere ad apertura positiva. $B10_d = 5.000.000$ (vedi pagina 7/32)
- KM1, KM2 sono contattori utilizzati a carico nominale. Il valore di $B10_d$ è pari a 2.000.000 (vedi Table C.1 della EN ISO 13849-1)
- CS è un modulo di sicurezza (CS AR-05) con $MTTF_d = 147$ anni e $DC = 99\%$

Ipotesi di frequenza di utilizzo

- 4 volte all'ora per 24 ore/gg per 365 gg/anno pari a $n_{op}/anno = 35.040$
- I contattori interverranno per un numero doppio di operazioni = 70.080

Calcolo MTTFd

- $MTTF_{d_{SS1,SS3}} = 571$ anni; $MTTF_{d_{SS2,SS4}} = 1.427$ anni
- $MTTF_{d_{KM1,KM2}} = 285$ anni
- $MTTF_{d_{CS}} = 147$ anni
- $MTTF_{d_{Ch1}} = 72$ anni (SS1,SS3,CS,KM1)
- $MTTF_{d_{Ch2}} = 85$ anni (SS2,SS4,CS,KM2)
- $MTTF_d$: simmettizzando i due canali si ottiene $MTTF_d = 79$ anni (High)

Copertura diagnostica DC_{avg}

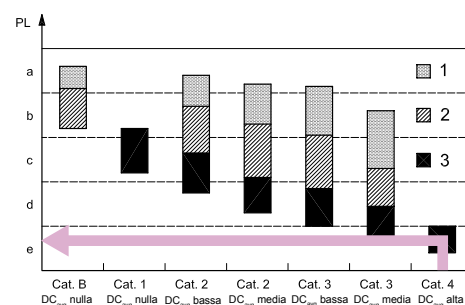
- I contatti di KM1, KM2 sono monitorati da CS tramite il circuito di retroazione. $DC = 99\%$
- I contatti ausiliari degli interruttori sono tutti controllati dal PLC. $DC = 99\%$
- Il modulo CS AR-05 ha una $DC = 99\%$ (vedi pagina 7/32)
- La copertura diagnostica per entrambi i canali è del 99% (High)

Guasti di causa comune CCF

- Supponiamo un punteggio > 65 (in base ad annex F della EN ISO 13849-1).

Verifica del PL

- Un circuito in categoria 4 con $MTTF_d = 79$ anni (High) e $DC_{avg} = High$ corrisponde ad un PL e.



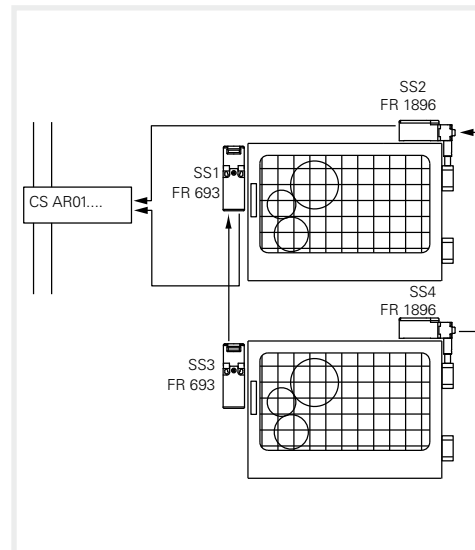
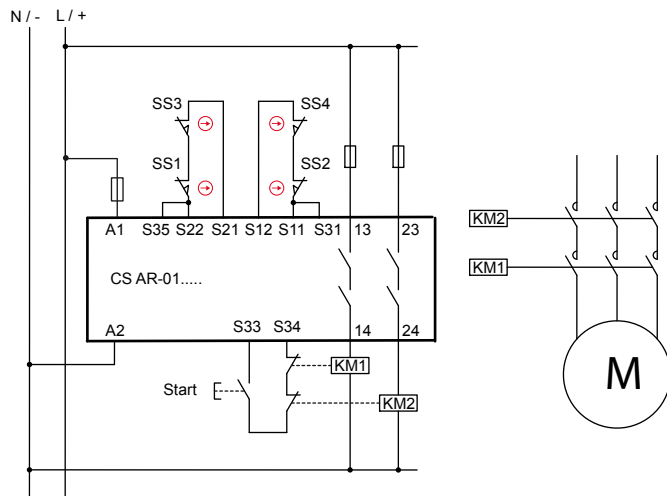
ESEMPIO 5**Applicazione: Controllo ripari**

Norma di riferimento EN ISO 13849-1:2006

Categoria di sicurezza

3

Performance Level

PL e**Descrizione della funzione di sicurezza**

L'apertura di un riparo provoca l'intervento degli interruttori SS1, SS2 sul primo riparo e SS3,SS4 nel secondo riparo, gli interruttori fanno intervenire il modulo di sicurezza e i due contattori KM1 e KM2.

Il segnale dei dispositivi SS1,SS2 e SS3,SS4 è controllato in modo ridondante dal modulo di sicurezza CS.

Gli interruttori hanno un principio di funzionamento diverso.

Anche i contattori KM1 e KM2 (con contatti a guida forzata) sono controllati da CS tramite il circuito di retroazione.

Dati dei dispositivi:

- SS1,SS3 sono interruttori ad apertura positiva. Il valore di B_{10d} è pari a 2.000.000 (vedi pagina 7/32)
- SS2,SS4 (FR 1896) sono interruttori per cerniere ad apertura positiva. B_{10d} = 5.000.000 (vedi pagina 7/32)
- KM1, KM2 sono contattori utilizzati a carico nominale. Il valore di B_{10d} è pari a 2.000.000 (vedi Table C.1 della EN ISO 13849-1)
- CS è un modulo di sicurezza (CS AR-01) con $MTTF_d=147$ anni e $DC=99\%$

Ipotesi di frequenza di utilizzo

- 2 volte all'ora per 16 ore/gg per 365 gg/anno pari a $n_{op}/\text{anno} = 11.680$
- I contattori interverranno per un numero doppio di operazioni = 23.360

Calcolo $MTTF_d$

- $MTTF_{d,SS1,SS3} = 1.712$ anni
- $MTTF_{d,SS2,SS4} = 4.281$ anni
- $MTTF_{d,KM1,KM2} = 856$ anni
- $MTTF_{d,CS} = 147$ anni
- $MTTF_{d,CH1} = 109$ anni (SS1,SS3,CS,KM1)
- $MTTF_{d,CH2} = 118$ anni (SS2,SS4,CS,KM2)
- $MTTF_{d} = \text{valore limitato a } 100$ anni

Copertura diagnostica DC_{avg}

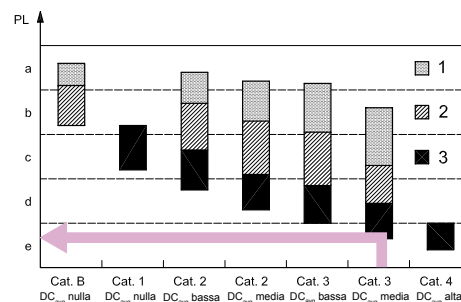
- I contatti di KM1, KM2 sono monitorati da CS tramite il circuito di retroazione. $DC=99\%$
- Non tutti i guasti nella serie degli interruttori possono essere rilevati. $DC=60\%$
- Il modulo CS AR-01 ha una $DC=99\%$
- Supponiamo una copertura diagnostica del 92% (Medium)

Guasti di causa comune CCF

- Supponiamo un punteggio > 65 (in base ad annex F della EN ISO 13849-1).

Verifica del PL

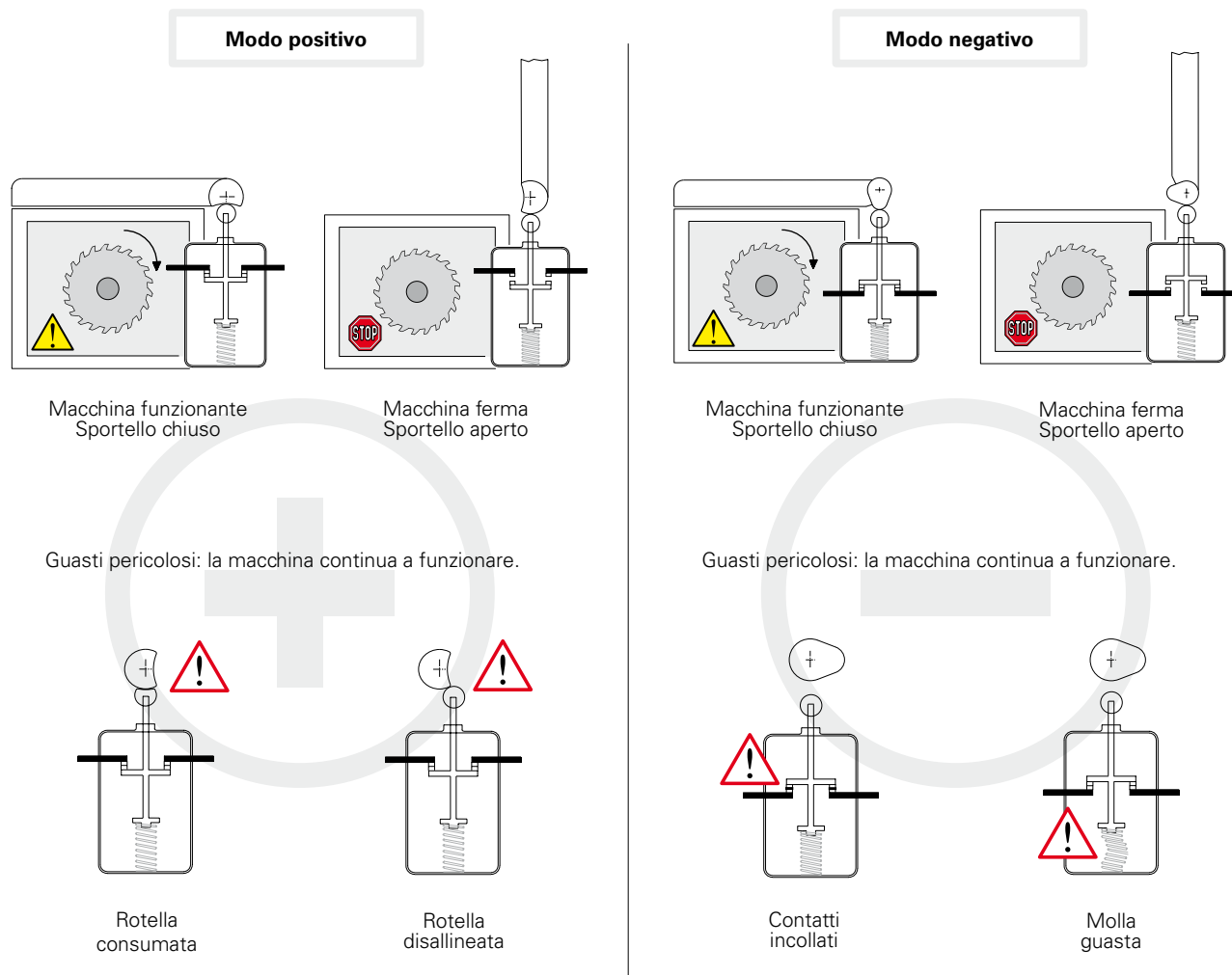
- Un circuito in categoria 3 con $MTTF_d=100$ anni e $DC_{avg}=\text{medium}$ corrisponde ad un PL e.



6 - Apertura positiva, ridondanza, diversificazione e autocontrollo

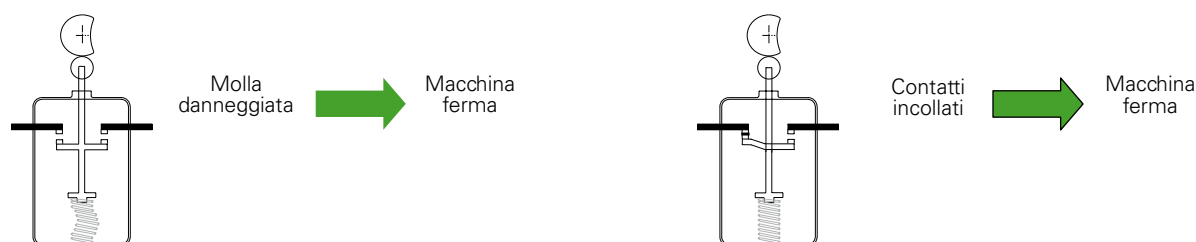
Modo positivo e modo negativo.

Secondo la normativa EN ISO 12100, se un componente meccanico in movimento trascina inevitabilmente un altro componente, per contatto diretto o mediante elementi rigidi, si dice che questi componenti sono collegati in **modo positivo**. Quando invece lo spostamento di un elemento meccanico consente ad un secondo elemento di muoversi liberamente (per esempio gravità, effetto di una molla, ecc..) il collegamento tra i due è in **modo negativo**.




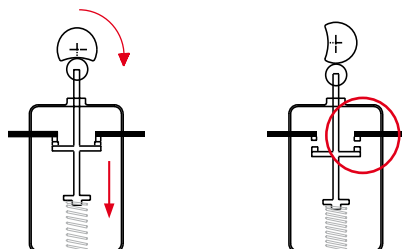
Il modo positivo consente con una manutenzione preventiva di sottrarsi dai guasti pericolosi schematizzati sopra. Con il modo negativo invece i guasti sono interni all'interruttore e quindi di difficile rilevazione.

Con il modo positivo i guasti interni (contatti incollati o molla guasta) consentono comunque l'apertura dei contatti e quindi l'arresto della macchina.



Utilizzo degli interruttori nelle applicazioni di sicurezza

Quando è impiegato un solo interruttore in una funzione di sicurezza, l'interruttore stesso deve essere azionato in modo positivo. Va utilizzato per le applicazioni di sicurezza il contatto d'apertura (normalmente chiuso) che deve essere del tipo ad "**apertura positiva**"; tutti gli interruttori che riportano il simbolo  sono dotati di contatti NC ad apertura positiva.



Nessun collegamento elastico tra i contatti mobili e l'azionatore sul quale viene applicata la forza di azionamento.

Se gli interruttori sono due o più è bene farli operare in modi opposti, ad esempio :

- Il primo con un contatto normalmente chiuso (contatto di apertura) azionato dal riparo in modo positivo.
- l'altro con un contatto normalmente aperto (contatto di chiusura), azionato dal riparo in modo non positivo.

Questa è una pratica comune che non esclude, quando giustificato, l'uso dei due interruttori azionati in modo positivo (vedi diversificazione).

Diversificazione

La sicurezza nei sistemi ridondanti viene aumentata con la **diversificazione**. Essa si ottiene applicando due interruttori con diversità di progettazione e/o tecnologia, in modo da evitare guasti determinati dalla stessa causa. Esempi di diversificazione sono: l'utilizzo di un interruttore ad azione positiva accoppiato ad uno ad azione non positiva, da un interruttore a comando meccanico ed uno non meccanico (es. sensore elettronico) o dall'utilizzo di due interruttori a comando meccanico ad azione positiva ma di diverso principio di azionamento (es. un interruttore a chiave FR 693 e un interruttore a perno FR 1896).

Ridondanza

La **ridondanza** è l'impiego di più di un dispositivo o sistema, al fine di garantire che in caso di guasto nelle parti di uno di essi, un altro sia disponibile per eseguire tali funzioni di sicurezza. Se il primo guasto non viene rilevato, il verificarsi di un secondo potrà portare alla perdita della funzione di sicurezza.

Autocontrollo

L' **autocontrollo** consiste nel verificare automaticamente il funzionamento di tutti i dispositivi che intervengono nel ciclo della macchina. Di conseguenza il ciclo successivo può essere vietato o autorizzato.

Ridondanza e autocontrollo

La combinazione in sistema della **ridondanza** e dell'**autocontrollo** fanno sì che un primo guasto nel circuito di sicurezza non porti alla perdita delle funzioni di sicurezza. Tale primo guasto verrà rilevato al riavvio successivo o comunque prima che avvenga un secondo guasto che potrebbe portare alla perdita della funzione di sicurezza.