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 e agli aspetti riguardanti la progettazione e la scelta dei dispositivi interblocco associati ai ripari.
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, interpretazioni e le tecnologie esistenti. 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 alcuna 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 2014/35/UE, la direttiva sulle atmosfere esplosive 2014/34/UE, la direttiva sulla compatibilità elettromagnetica 2014/30/UE, 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 applica 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 dispositivi di comando a due mani, 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. Sicurezza del macchinario - Principi generali di progettazione - Valutazione del rischio e riduzione del rischio.

NORME DI TIPO B1
ad esempio:

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

NORME DI TIPO B2
ad esempio:

EN 574. Dispositivi di comando a due mani
EN ISO 13850. Arresto di emergenza
EN ISO 14119. Dispositivi di interblocco dei ripari
EN 60204-1. Equipaggiamento elettrico delle macchine
EN 60947-5-1. Dispositivi di controllo elettromeccanici.

NORME DI TIPO C
ad esempio:

EN 201. Macchine per gomma e materie plastiche - Macchine a iniezione
EN 415-1. Sicurezza delle macchine per imballare
EN 692. Presse meccaniche
EN 693. Presse idrauliche
EN 848-1. 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.

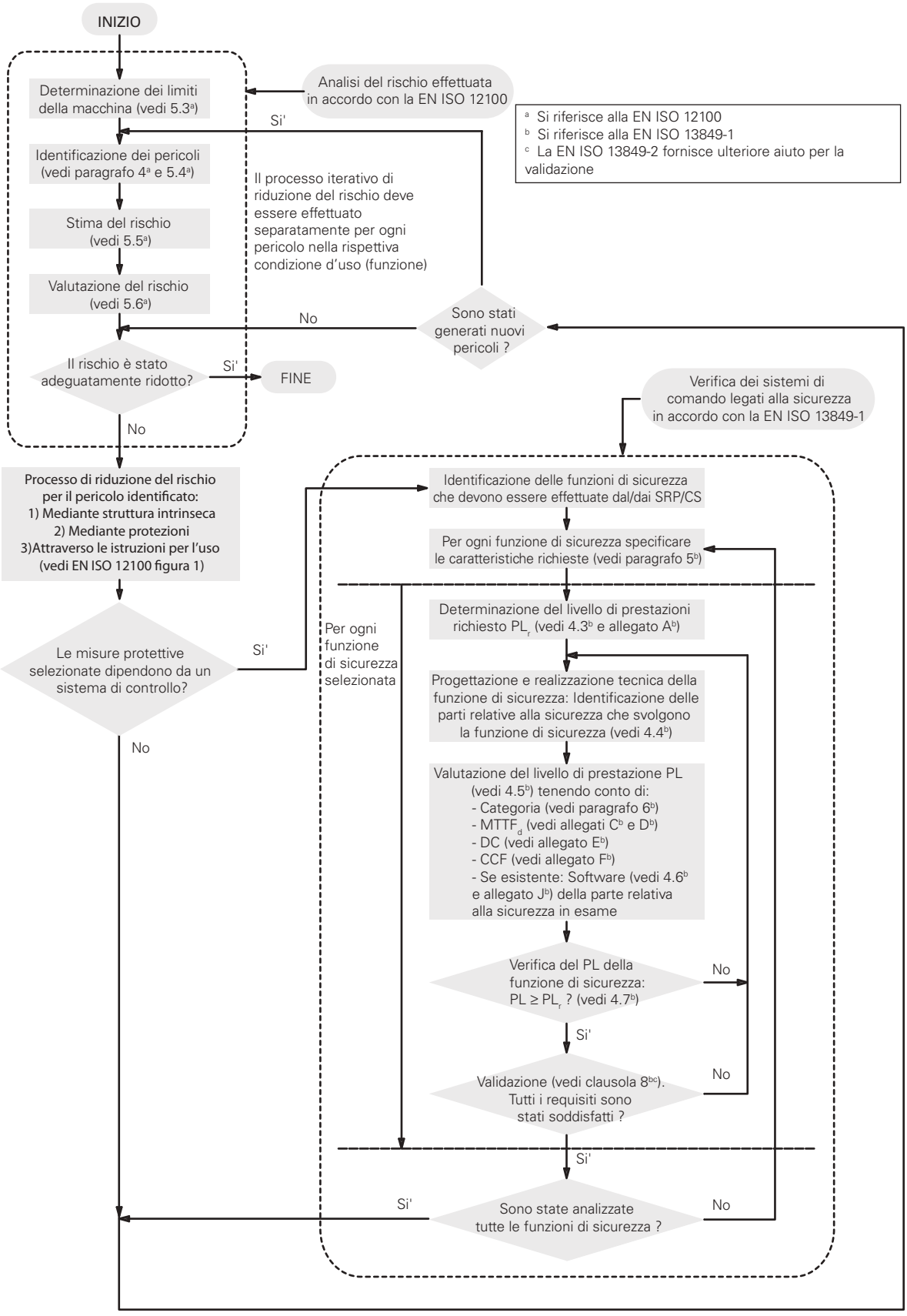
La metodologia di analisi dei rischi, della loro valutazione, di come procedere nella loro riduzione è definita dalla norma EN ISO 12100, un modello ciclico di analisi tale per cui, definiti degli obiettivi iniziali, l'analisi dei rischi e delle possibili soluzioni per limitare questi rischi vengono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

Il modello introdotto da questa norma prevede che, dopo un'analisi dei rischi 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 13849-1 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.

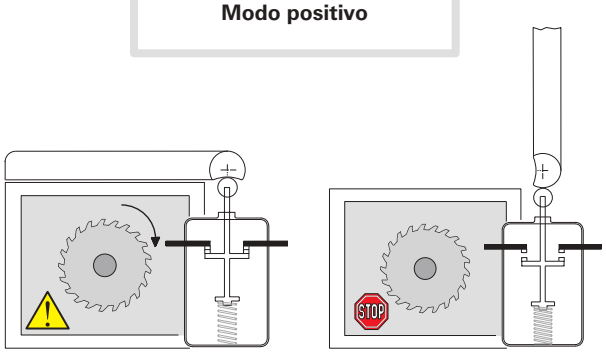


Nota: Questa figura è stata ottenuta dalla combinazione delle Figure 1 e 3 della EN ISO 13849-1. I testi riportati sono la traduzione non ufficiale dei testi presenti nella norma.

4 - Apertura positiva, ridondanza, diversificazione ed 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**.

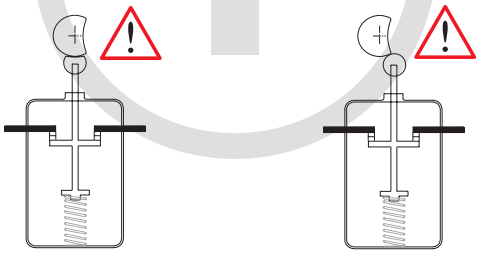
Modo positivo



Macchina funzionante
Sportello chiuso

Macchina ferma
Sportello aperto

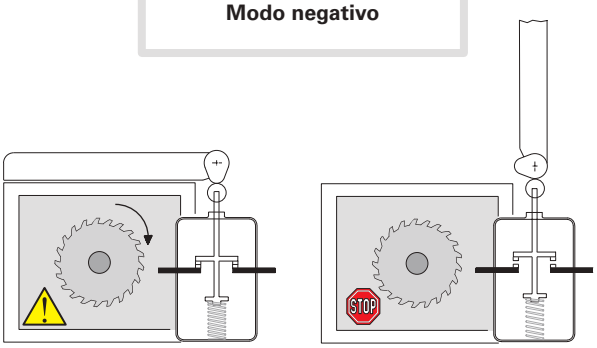
Guasti pericolosi: la macchina continua a funzionare.



Rotella
consumata

Rotella
disallineata

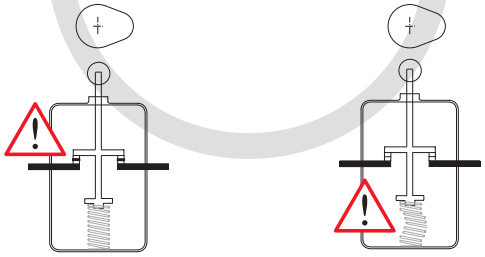
Modo negativo



Macchina funzionante
Sportello chiuso

Macchina ferma
Sportello aperto

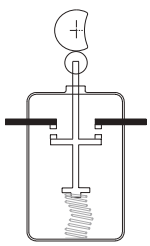
Guasti pericolosi: la macchina continua a funzionare.



Contatti
incollati

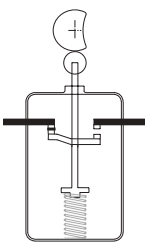
Molla
guasta

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.



Molla
danneggiata

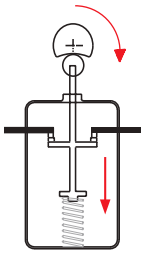
Macchina
ferma

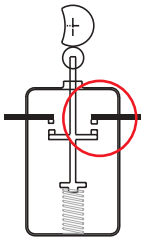


Contatti
incollati

Macchina
ferma

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-M2 ed un interruttore a perno FR 1896-M2).

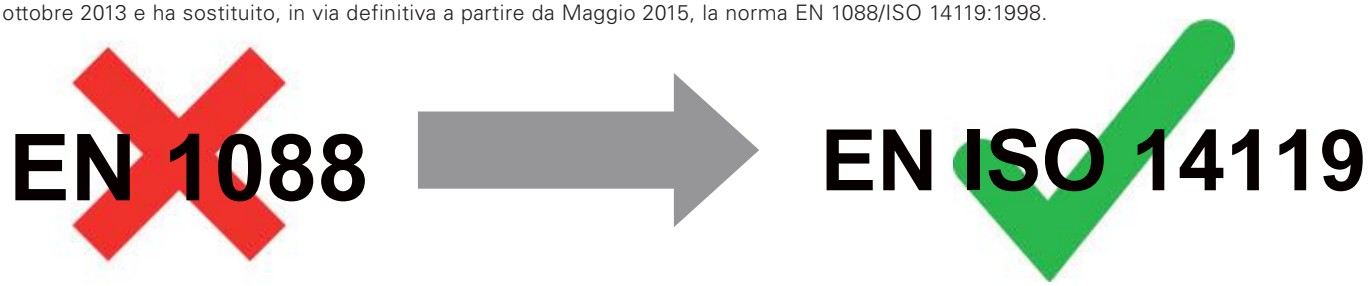
Ridondanza
La **ridondanza** è l'impiego di più di un dispositivo o sistema, al fine di garantire che in caso di guasto nelle parti di uno di essi, un altro sia disponibile per eseguire tali funzioni di sicurezza. Se il primo guasto non viene rilevato, il verificarsi di un secondo potrà portare alla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

5 - Progettazione e scelta dei dispositivi di interblocco associati ai ripari (norma EN ISO 14119)

La norma europea EN ISO 14119 "Dispositivi di interblocco associati ai ripari - Principi di progettazione e di scelta" è entrata in vigore il 2 ottobre 2013 e ha sostituito, in via definitiva a partire da Maggio 2015, la norma EN 1088/ISO 14119:1998.



La norma si rivolge sia ai fabbricanti dei dispositivi di interblocco che ai costruttori di macchine (ed ai system integrator), fornendo requisiti per la realizzazione dei dispositivi e requisiti per la corretta installazione degli stessi.
La norma mette in luce alcuni aspetti non sempre chiari e considera le ultime tecnologie utilizzate nella costruzione di dispositivi di interblocco, definisce inoltre alcuni parametri (tipologia di attuatore e livello di codifica) e descrive le misure da intraprendere per ottenere una corretta installazione, al fine di aumentare la resistenza all'elusione dei ripari.
La norma considera anche altri aspetti relativi ai dispositivi di blocco (ad esempio: principi di blocco, blocco elettromagnetico, sblocco ausiliario, sblocco di fuga e di emergenza ecc...) che non sono trattati in questo documento.

Livello di codifica degli attuatori

Un'importante novità introdotta dalla norma è la definizione di attuatore codificato e la classificazione dei livelli di codifica:

- **attuatore codificato** – attuatore progettato specificatamente per essere combinato con uno specifico dispositivo di interblocco;
- **attuatore a basso livello di codifica** – attuatore codificato con possibilità di avere da 1 a 9 diverse codifiche (ad esempio la serie di sensori magnetici SR o gli interruttori di sicurezza ad azionatore separato con riconoscimento meccanico FS, FG, FR, FD...);
- **attuatore a medio livello di codifica** - attuatore codificato con possibilità di avere da 10 a 1000 diverse codifiche;
- **attuatore ad alto livello di codifica** - attuatore codificato con possibilità di avere più di 1000 diverse codifiche. (ad esempio la serie di sensori ST a tecnologia RFID o i dispositivi di interblocco della serie NG e NS con tecnologia RFID dotati di blocco del riparo).

Tipologie di dispositivi di interblocco

La norma EN ISO 14119 definisce differenti tipologie di dispositivi di interblocco:

- **Dispositivi di interblocco di tipo 1** - Dispositivi di interblocco azionati meccanicamente da attuatore non codificato (ad esempio i dispositivi di interblocco a cerniera serie HP)
- **Dispositivi di interblocco di tipo 2** - Dispositivi di interblocco azionati meccanicamente da attuatore codificato (ad esempio gli interruttori di sicurezza ad azionatore separato serie FR, FS, FG, ...)
- **Dispositivi di interblocco di tipo 3** - Dispositivi di interblocco azionati senza contatto da attuatore non codificato
- **Dispositivi di interblocco di tipo 4** - Dispositivi di interblocco azionati senza contatto da attuatore codificato (ad esempio i sensori di sicurezza con tecnologia RFID serie ST e gli interruttori di sicurezza con tecnologia RFID serie NG e NS)

Esempi di principio di attuazione		Esempi di attuatori		Tipo
Meccanico	Contatto diretto/forza	Non codificato	Camma rotante	Tipo 1
			Camma lineare	
			Cerniera	
		Codificato	Azionatore a chiavetta	Tipo 2
			Chiave intrappolata	
Senza contatto	Induttivo	Non codificato	Materiale ferromagnetico	Tipo 3
	Magnetico		Magnete, solenoide	
	Capacitivo		Qualsiasi oggetto adatto	
	Ultrasuoni		Qualsiasi oggetto adatto	
	Ottico		Qualsiasi oggetto adatto	
	Magnetico	Codificato	Magnetico codificato	Tipo 4
	RFID		RFID codificato	
	Ottico		Ottico codificato	

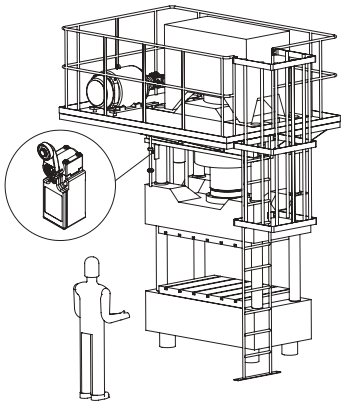
Tratto da EN ISO 14119 - Table 1

Requisiti per la progettazione e l'installazione di dispositivi di interblocco in accordo con EN ISO 14119 al fine di ridurre il rischio di elusione dei ripari.

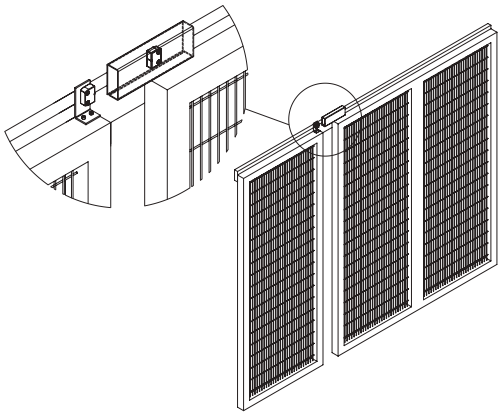
Principi e misure per evitare l'elusione	Dispositivi di tipo 1		Dispositivi di tipo 2 e tipo 4	Dispositivi di tipo 2 e tipo 4
	Interruttori di sicurezza a camma rotante o lineare	Interruttori di sicurezza a cerniera	Azionatori a basso e medio livello di codifica	Azionatori ad alto livello di codifica
				
Montaggio fuori portata (1)	X		X	
Schermatura, ostruzione (2)				
Montaggio in posizione nascosta (3)				
Test da circuito di comando (4)				
Fissaggio non rimovibile del dispositivo e attuatore				
Fissaggio non rimovibile del dispositivo		M		
Fissaggio non rimovibile dell'attuatore		M	M	M
Secondo dispositivo di interblocco e verifica plausibilità	R		R	

Tratto da EN ISO 14119 - Table 3

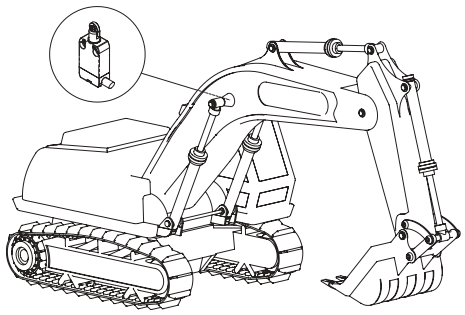
X: obbligo di applicare almeno una delle misure elencate nella colonna "Principi e misure per evitare l'elusione"
M: misura obbligatoria
R: misura raccomandata
E' evidente che al fine di soddisfare tutti i requisiti della norma EN ISO 14119, risulta più semplice utilizzare dispositivi con tecnologia RFID ad alto livello di codifica ed interruttori a cerniera poiché è necessario soddisfare solo pochi requisiti per evitare l'elusione dei dispositivi stessi.
I dispositivi a basso o medio livello di codifica necessitano di ulteriori requisiti per assicurare un'applicazione adeguatamente robusta contro la manomissione.



(1) - Montaggio fuori portata



(2) - Schermatura, ostruzione



(3) - Montaggio in posizione nascosta

(4) - Un test da circuito di comando può essere realizzato ad esempio in un macchinario dove il ciclo di lavoro è facilmente prevedibile, in modo da verificare che al termine o durante determinate fasi del ciclo di lavoro i ripari vengano effettivamente aperti (ad esempio per rimuovere il materiale lavorato o per effettuare controlli qualitativi); nel caso in cui il sistema di controllo non rilevi tali azioni di apertura nei ripari viene generato un allarme ed arrestata la macchina.

Dispositivi di blocco e forza di ritenuta

Il costruttore del dispositivo di interblocco con blocco deve assicurare che, nella condizione di blocco, il dispositivo resista almeno alla forza di ritenuta specificata F_{Zh}. Tale forza può essere al massimo pari alla forza massima di ritenuta divisa per un coefficiente di sicurezza pari a 1,3.

$$F_{Zh} = \frac{F_{1max}}{1,3}$$

Per esempio, un dispositivo con una forza massima specificata F_{Zh} =2000 N deve superare una prova con una forza di ritenuta massima pari a F_{1max} =2600 N.
Un dispositivo di interblocco con blocco può prevedere sia la funzione di monitoraggio della posizione del riparo (riparo aperto/chiuso), sia la funzione di blocco del riparo (riparo bloccato/sbloccato). Ognuna delle due funzioni può richiedere un livello di sicurezza PL (rif. EN ISO 13849-1) diverso. Infatti, normalmente la funzione di blocco richiede un PL inferiore alla funzione di monitoraggio della posizione. (Vedi punto 8.4, nota 2 della EN ISO 14119).
Per evidenziare che un dispositivo di interblocco effettua anche il monitoraggio della condizione di blocco, la nuova norma prevede che sul prodotto sia riportato il simbolo rappresentato qui a lato.

6 - Attuale situazione normativa. 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 ed 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). Questa norma introduce il concetto di SIL (Safety Integrity Level), 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 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 13849-1, sviluppata dal CEN sotto l'egida dell'ISO, deriva anch'essa da questo approccio probabilistico ma cerca di fare in modo che il costruttore abituato 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" e ad alcuni sistemi elettronici programmabili con strutture predefinite. La EN ISO 13849-1 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 due norme:
EN ISO 13849-1. Norma di tipo B1 che utilizza il concetto di PL
EN 62061. Norma di tipo B1 che utilizza il concetto di SIL.

Nota importante
La EN ISO 13849-1 è una norma di tipo B1 e quindi se un macchinario è già normato da una norma di tipo C è quest'ultima che fa testo. Alcune norme di tipo C non ancora aggiornate si basano ancora sui concetti della norma EN 954-1. Per i costruttori dei macchinari coperti da una norma di tipo C i tempi di introduzione delle nuove normative potrebbero essere diversi a seconda della velocità dei vari comitati tecnici nell'aggiornarle.

Le due norme EN 62061 ed EN ISO 13849-1 hanno quindi una discreta sovrapposizione per quanto riguarda il campo applicativo e per parecchi aspetti si assomigliano, tanto è vero che esiste un legame tra i due diversi nomi simbolo (SIL e PL) che indicano il risultato dell'analisi secondo le due norme.

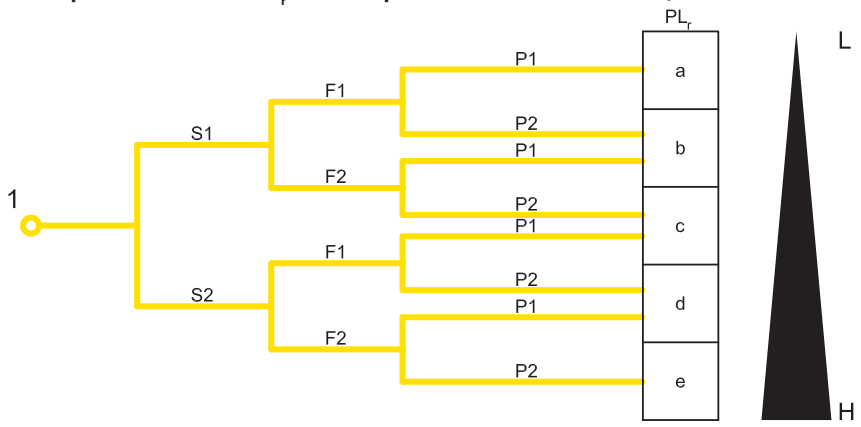
PL EN ISO 13849-1	**a**	**b**	**c**	**d**	**e**
SIL EN 62061 - IEC 61508	**-**	**1**	**1**	**2**	**3**
PFH_D	da 10^{-4} a 10^{-5}	da 10^{-5} a $3x10^{-6}$	da $3x10^{-6}$ a 10^{-6}	da 10^{-6} a 10^{-7}	da10^{-7} a 10^{-8}
Un guasto pericoloso ogni n° anni	da~1 a ~10	da~10 a ~40	da~40 a ~100	da~100 a ~1000	da~1000 a ~10000

La scelta della norma da utilizzare è del costruttore, in funzione della tecnologia utilizzata. Riteniamo che la EN ISO 13849-1 con il suo approccio mediato e con il riutilizzo di concetti già noti al mercato sia una norma di più semplice applicazione.

7 - La norma EN ISO 13849-1 ed i nuovi parametri: PL, $MTTF_D$, DC, CCF

La norma EN ISO 13849-1 fornisce al costruttore un metodo iterativo per valutare se i rischi di una macchina possono 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 13849-1 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

* F1 dovrebbe essere scelto se l'accumulo dei tempi di esposizione non supera 1/20 del tempo di lavoro complessivo e la frequenza di esposizione non è superiore ad una volta ogni 15 minuti

****** In assenza di altre giustificazioni, F2 dovrebbe essere scelto se la frequenza di esposizione è superiore ad una volta ogni 15 minuti.

Parametri di rischio

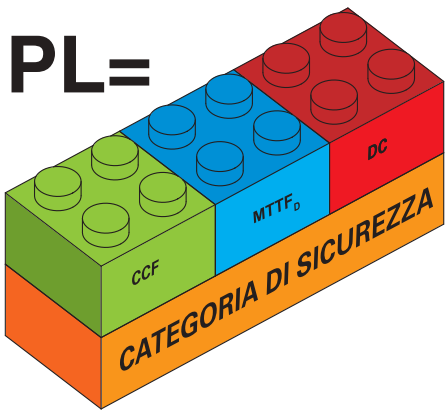
S Gravità del danno
S1 leggero (danno normalmente reversibile)
S2 serio (danno normalmente irreversibile o morte)
F Frequenza e/o esposizione al rischio
***F1** da rara a poco frequente e/o con breve tempo di esposizione
****F2** da frequente a continua e/o con lungo tempo di esposizione
P Possibilità 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 cambiati i livelli di funzione di sicurezza richiesta. L'ente tedesco BGIA nel report 2008/2 sulla EN ISO 13849-1 suggerisce che, adottando un approccio del tipo "caso peggiore", si possa adottare una conversione come nella tabella a fianco. Per ulteriori informazioni si faccia riferimento al testo in questione.

Categoria richiesta dalla EN 954-1		Performance Level richiesto (PLr) e Categoria richiesta secondo EN ISO 13849-1
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 $1x10^{-6}$ e $1x10^{-7}$ ovvero all'incirca 1 guasto pericoloso mediamente ogni 100-1000 anni.

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



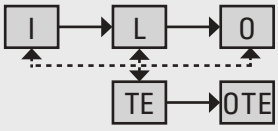
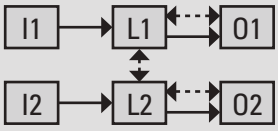
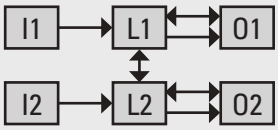
Per la valutazione del PL di un sistema di controllo servono più parametri ovvero:
1. La Categoria di sicurezza del sistema che a sua volta deriva dall'architettura (struttura) del sistema di controllo e dal suo comportamento in caso di guasto
2. $MTTF_D$ dei componenti
3. DC o Copertura Diagnostica 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 13849-1 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	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. Architettura: 	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	Si applicano i requisiti della categoria B. Devono essere usati dei componenti e dei principi di sicurezza ben provati. Architettura: 	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	Si applicano i requisiti della categoria B e l'uso di principi di sicurezza ben provati. La funzione di sicurezza deve essere controllata ad adeguati intervalli di tempo dal sistema di controllo. Architettura: 	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	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. Architettura: 	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	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. Architettura: 	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:

$$MTTF_D = \frac{B_{10_D}}{0{,}1 \cdot n_{op}}$$

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:

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

Per evitare interpretazioni troppo ottimistiche il valore massimo di $MTTF_D$ di ogni canale è limitato a 100 anni (per le categorie B, 1, 2 e 3) o 2500 anni (categoria 4). 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:

$$MTTF_D = \frac{2}{3}\left[MTTF_{DC1} + MTTF_{DC2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right]$$

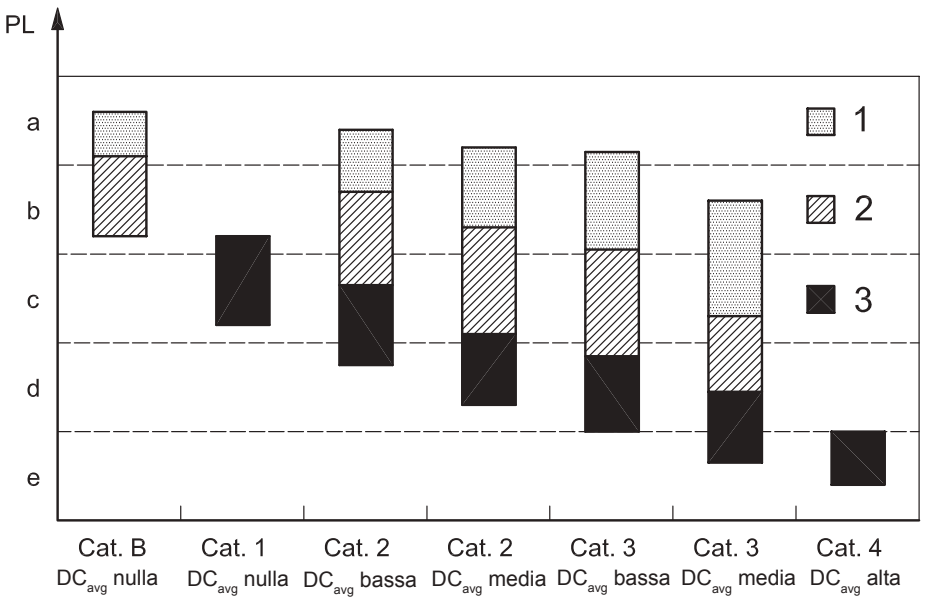
DC ("Diagnostic Coverage", copertura diagnostica).

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 $DC_{avg} \geq 99\%$
Media $90\% \leq DC_{avg} < 99\%$
Bassa $60\% \leq DC_{avg} < 90\%$
Nulla $DC_{avg} < 60\%$
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.

Relazioni tra le categorie, DC_{avg}, $MTTF_D$ di ogni canale e PL (tratto da EN ISO 13849-1, figura 5)



1 = $MTTF_D$ di ogni canale Basso
(3 anni ≤ $MTTF_D$ < 10 anni)

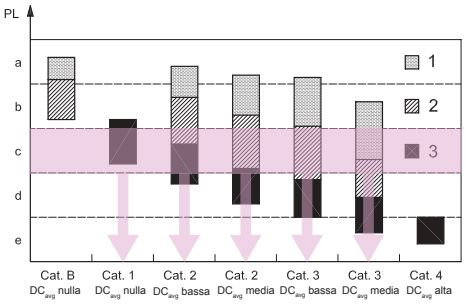
2 = $MTTF_D$ di ogni canale Medio
(10 anni ≤ $MTTF_D$ < 30 anni)

3 = $MTTF_D$ di ogni canale Alto
(30 anni ≤ $MTTF_D$ ≤ 100 anni)

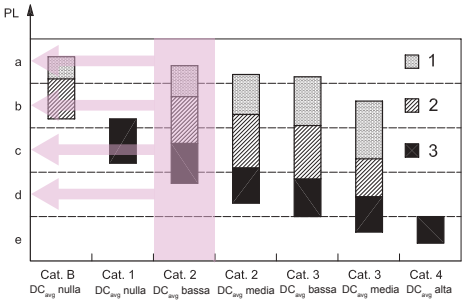
Questa immagine è molto utile perché ha più modalità di lettura. Dato un certo PL_r essa evidenzia tutte le possibili soluzioni che forniscono quel livello di PL ovvero le possibili strutture circuitali che forniscono il medesimo PL.

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 circuitale, 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_r 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.

Note

Tabella parametri di sicurezza

I dati B_{10D} indicati nella tabella fanno riferimento alla vita meccanica dei contatti dei dispositivi in condizioni ambientali normali.
Il valore di B_{10D} per i contatti NC e NO si riferisce ad un carico elettrico massimo pari al 10% del valore di corrente indicato nelle categorie di impiego. Mission time (per tutti gli articoli sotto indicati): 20 anni.

Dispositivi elettromeccanici

Serie	Descrizione articolo	B_{10D} (NO)	B_{10D} (NC)	B_{10}/B_{10D}
F• ••••	Interruttori di posizione	1.000.000	40.000.000	50%
F• ••93 F• ••92	Interruttori di sicurezza ad azionatore separato	1.000.000	2.000.000	50%
F• ••99 F• ••R2	Interruttori di sicurezza ad azionatore separato con blocco	1.000.000	1.000.000	50%
FG	Interruttori di sicurezza ad azionatore separato con blocco	1.000.000	5.000.000	20%
FS	Interruttori di sicurezza ad azionatore separato con blocco	1.000.000	4.000.000	20%
F• ••96 F• ••95	Interruttori 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 - HX B•22-•••	Cerniere di sicurezza	1.000.000	5.000.000	20%
SR	Sensori magnetici di sicurezza (utilizzati con moduli di sicurezza Pizzato Elettrica compatibili)	20.000.000	20.000.000	50%
SR	Sensori magnetici di sicurezza (utilizzati a massimo carico: DC12 24V 250mA)	400.000	400.000	100%
PX, PA	Interruttori a pedale	1.000.000	20.000.000	50%
MK	Microinterruttori di posizione	1.000.000	20.000.000	50%
NA, NB, NF	Interruttori di posizione precablati modulari	1.000.000	40.000.000	50%
E2 C•••••••	Unità di contatto	1.000.000	40.000.000	50%

Serie	Descrizione articolo	B_{10D}	B_{10}/B_{10D}
E2 •PU1••••••, E2 •PL1••••••	Pulsanti singoli stabili	2.000.000	50%
E2 •PU2••••••, E2 •PL2••••••	Pulsanti singoli ad impulso	30.000.000	50%
E2 •PD••••••, E2 •PT••••••	Pulsanti doppi e tripli	2.000.000	50%
E2 •PQ••••••	Pulsanti quadrupli	2.000.000	50%
E2 •PE••••••	Pulsanti d'emergenza	600.000	50%
VN NG-AC2605•	Pulsanti d'emergenza integrati su interruttori di sicurezza serie NG	100.000	50%
E2 •SE••••••, E2 •SL••••••	Selettori e selettori luminosi	2.000.000	50%
E2 •SC••••••	Selettori a chiave	600.000	50%
E2 •MA••••••	Manipolatori	2.000.000	50%

Serie ATEX	Descrizione articolo	B_{10D} (NO)	B_{10D} (NC)	B_{10}/B_{10D}
F• ••••-EX•	Interruttori di posizione	500.000	20.000.000	50%
F• ••93-EX• F• ••92-EX•	Interruttori di sicurezza ad azionatore separato	500.000	1.000.000	50%
F• ••99-EX• F• ••R2-EX•	Interruttori di sicurezza ad azionatore separato con blocco	500.000	500.000	50%
F• ••96-EX• F• ••95-EX•	Interruttori di sicurezza a perno per cerniere	500.000	2.500.000	20%
F• ••C•-EX•	Interruttori a leva asolata per ripari a battente	500.000	1.000.000	50%
F• ••••-EX•	Interruttori a fune per arresto d'emergenza	500.000	1.000.000	50%

Dispositivi elettronici

Codice/Serie	Descrizione articolo	$MTTF_D$	DC	PFH_D	SIL CL	PL	Cat
HX BEE1-•••	Cerniere di sicurezza con unità elettronica	2413	High	1,24E-09	3	e	4
ST	Sensori di sicurezza con tecnologia RFID	4077	High	1,20E-11	3	e	4
NG	Interruttori di sicurezza RFID con blocco (modalità 1 / modalità 2)	2725	High	1,17E-09	3	e	4
NG	Interruttori di sicurezza RFID con blocco (modalità 3)	2511	High	1,84E-09	2	d	2
NG	Interruttori di sicurezza RFID con blocco (controllo della funzione di bloccaggio della protezione a doppio canale)	4011	High	1,51E-10	3	e	4
NG	Interruttori di sicurezza RFID con blocco (controllo della funzione di bloccaggio della protezione a singolo canale)	4011	High	1,51E-10	2	d	2
NS	Interruttori di sicurezza RFID con blocco (modalità 1 / modalità 2)	1671	High	1,24E-09	3	e	4
NS	Interruttori di sicurezza RFID con blocco (modalità 3)	1677	High	1,82E-09	2	d	2
NS	Interruttori di sicurezza RFID con blocco (controllo della funzione di bloccaggio della protezione a doppio canale)	2254	High	2,04E-10	3	e	4
NS	Interruttori di sicurezza RFID con blocco (controllo della funzione di bloccaggio della protezione a singolo canale)	2254	High	2,04E-10	2	d	2
CS AM-01	Modulo di sicurezza per il rilevamento motore fermo	218	Medium	8,70E-09	2	d	3
CS AR-01, CS AR-02	Moduli di sicurezza per controllo ripari ed arresti d'emergenza	227	High	1,18E-10	3	e	4

B_{10D}: Numero di operazioni affinché il 10% dei componenti si guasti in modo pericoloso
B_{10}: Numero di operazioni affinché il 10% dei componenti si guasti
B_{10}/B_{10D}: 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

Dispositivi elettronici

Codice/Serie	Descrizione articolo	$MTTF_D$	DC	PFH_D	SIL CL	PL	Cat
CS AR-04	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	152	High	1,84E-10	3	e	4
CS AR-05, CS AR-06	Moduli di sicurezza per controllo ripari ed arresti d'emergenza e barriere ottiche	152	High	1,84E-10	3	e	4
CS AR-07	Modulo di sicurezza per controllo ripari ed arresti d'emergenza	111	High	7,56E-10	3	e	4
CS AR-08	Modulo di sicurezza per controllo ripari ed arresti d'emergenza e barriere ottiche	1547	High	9,73E-11	3	e	4
CS AR-20, CS AR-21	Moduli di sicurezza per controllo ripari ed arresti d'emergenza	225	High	4,18E-10	3	e	3
CS AR-22, CS AR-23	Moduli di sicurezza per controllo ripari ed arresti d'emergenza	151	High	5,28E-10	3	e	3
CS AR-24, CS AR-25	Moduli di sicurezza per controllo ripari ed arresti d'emergenza	113	High	6,62E-10	3	e	3
CS AR-40, CS AR-41	Moduli di sicurezza per controllo ripari ed arresti d'emergenza	225	High	4,18E-10	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	212	High	3,65E-09	3	e	4
CS AR-90	Modulo di sicurezza per controllo del livellamento al piano degli ascensori	382	High	5,03E-10	3	e	4
CS AR-91	Modulo di sicurezza per controllo del livellamento al piano degli ascensori	227	High	1,18E-10	3	e	4
CS AR-93	Modulo di sicurezza per controllo del livellamento al piano degli ascensori	227	High	1,34E-10	3	e	4
CS AR-94	Modulo di sicurezza per controllo del livellamento al piano degli ascensori	227	High	1,13E-10	3	e	4
CS AR-94•U12	Modulo di sicurezza per controllo del livellamento al piano degli ascensori	227	High	1,13E-10	3	e	4
CS AR-95	Modulo di sicurezza per controllo del livellamento al piano degli ascensori	213	High	5,42E-09	3	e	4
CS AT-0•, CS AT-1•	Moduli di sicurezza temporizzati per controllo ripari ed arresti d'emergenza	88	High	1,23E-08	3	e	4
CS AT-3•	Modulo di sicurezza temporizzato per controllo ripari ed arresti d'emergenza	135	High	1,95E-09	3	e	4
CS DM-01	Modulo di sicurezza per controllo comando bimanuale	142	High	2,99E-08	3	e	4
CS DM-02	Modulo di sicurezza per controllo comando bimanuale	206	High	2,98E-08	3	e	4
CS DM-20	Modulo di sicurezza per controllo comando bimanuale	42	-	1,32E-06	1	c	1
CS FS-1•	Modulo temporizzatore di sicurezza	404	High	5,06E-10	3	e	4
CS FS-2•, CS FS-3•	Moduli temporizzatori di sicurezza	205	High	1,10E-08	2	d	3
CS FS-5•	Modulo temporizzatore di sicurezza	379	Medium	1,31E-09	2	d	3
CS ME-01	Modulo di espansione contatti	91	High	5,26E-10	①	①	①
CS ME-02	Modulo di espansione contatti	114	High	4,17E-10	①	①	①
CS ME-03	Modulo di espansione contatti	152	High	3,09E-10	①	①	①
CS ME-20	Modulo di espansione contatti	114	High	6,14E-10	①	①	①
CS ME-3•	Modulo di espansione contatti	110	High	4,07E-09	①	①	①
CS M•201	Moduli di sicurezza multifunzione	135	High	1,44E-09	3	e	4
CS M•202	Moduli di sicurezza multifunzione	614	High	1,32E-09	3	e	4
CS M•203	Moduli di sicurezza multifunzione	103	High	1,61E-09	3	e	4
CS M•204	Moduli di sicurezza multifunzione	134	High	1,52E-09	3	e	4
CS M•205	Moduli di sicurezza multifunzione	373	High	2,19E-09	3	e	4
CS M•206	Moduli di sicurezza multifunzione	3314	High	1,09E-09	3	e	4
CS M•207	Moduli di sicurezza multifunzione	431	High	7,08E-09	3	e	4
CS M•208	Moduli di sicurezza multifunzione	633	High	7,02E-09	3	e	4
CS M•301	Moduli di sicurezza multifunzione	128	High	1,88E-09	3	e	4
CS M•302	Moduli di sicurezza multifunzione	535	High	1,57E-09	3	e	4
CS M•303	Moduli di sicurezza multifunzione	485	High	1,76E-09	3	e	4
CS M•304	Moduli di sicurezza multifunzione	98	High	2,05E-09	3	e	4
CS M•305	Moduli di sicurezza multifunzione	535	High	1,57E-09	3	e	4
CS M•306	Moduli di sicurezza multifunzione	100	High	1,86E-09	3	e	4
CS M•307	Moduli di sicurezza multifunzione	289	High	8,38E-09	3	e	4
CS M•308	Moduli di sicurezza multifunzione	548	High	7,27E-09	3	e	4
CS M•309	Moduli di sicurezza multifunzione	496	High	7,46E-09	3	e	4
CS M•401	Moduli di sicurezza multifunzione	434	High	1,73E-09	3	e	4
CS M•402	Moduli di sicurezza multifunzione	478	High	7,24E-09	3	e	4
CS M•403	Moduli di sicurezza multifunzione	438	High	7,42E-09	3	e	4

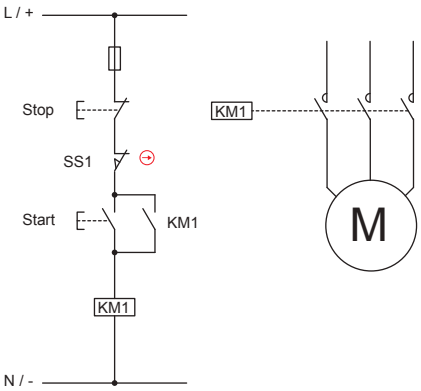
B_{10D}: Numero di operazioni affinché il 10% dei componenti si guasti in modo pericoloso
B_{10}: Numero di operazioni affinché il 10% dei componenti si guasti
B_{10}/B_{10D}: Rapporto tra guasti totali e guasti pericolosi.
$MTTF_D$: Mean Time To Failure Dangerous (Tempo medio al guasto pericoloso)

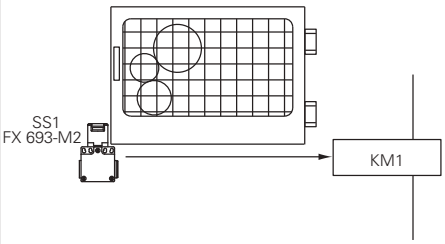
DC: Diagnostic coverage (Copertura diagnostica)
PFH_D: Probability of Dangerous Failure per hour (Probabilità al guasto pericoloso per ora)
SIL CL: Safety Integrity Level Claim Limit. Massimo SIL raggiungibile secondo EN 62061
PL: Performance Level. PL secondo EN ISO 13849-1

① = Dipendente dal modulo base

ESEMPIO 1
Applicazione: Controllo ripari

Norma di riferimento EN ISO 13849-1	
Categoria di sicurezza	**1**
Performance Level	**PL c**





Descrizione della funzione di sicurezza
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.
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 (FX 693-M2) 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 B_{10D} del dispositivo è fornito dal costruttore 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 B_{10D} è pari a 1.300.000 manovre, valore ricavato dalle tabelle di norma (vedi Tabella C.1 della EN ISO 13849-1).

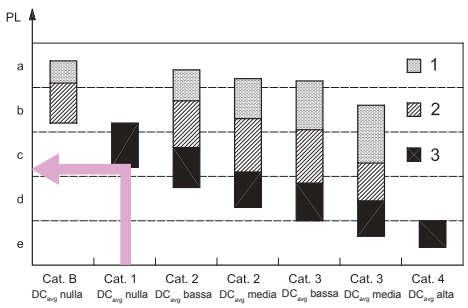
Ipotesi di frequenza di utilizzo
- Si suppone che il macchinario venga usato al massimo per 365 giorni all'anno, per tre turni di 8 ore con un tempo ciclo di 600 secondi. Il numero di operazioni annuo per l'interruttore è quindi pari a N_{op}=(365x24x3.600)/600=52.560.
- Si suppone l'azionamento del pulsante di start ogni 300 secondi. Il numero di operazioni annuo è quindi pari al massimo a n_{op}/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}/anno= 52.560+105.120 = 157.680

Calcolo $MTTF_D$
L'$MTTF_D$ dell'interruttore SS1 è pari a: $MTTF_D = B_{10D}/(0,1 \times n_{op})$ = 2000000/(0,1 x 52560) = 381 anni
L'$MTTF_D$ del contattore KM1 è pari a: $MTTF_D = B_{10D}/(0,1 \times n_{op})$ = 1.300.000/(0,1 x 157680) = 82 anni
Ne consegue che l'$MTTF_D$ del circuito monocanale è pari a: 1/(1/381+1/82)=67 anni

Copertura diagnostica DCavg
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.

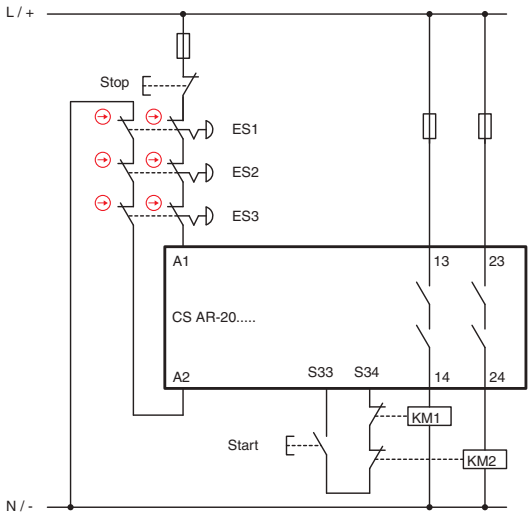
Guasti di causa comune CCF
Per un circuito in categoria 1 non è necessario il calcolo del parametro CCF.

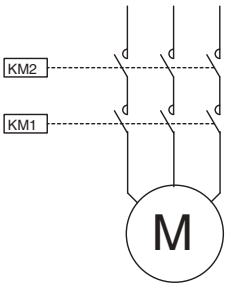
Verifica del PL
Dalla tabella o dalla figura 5 di norma si verifica come per un circuito in Categoria 1 con $MTTF_D$=95 anni il PL risultante del circuito di controllo è pari a PL c. Il PL_r obiettivo è quindi raggiunto.

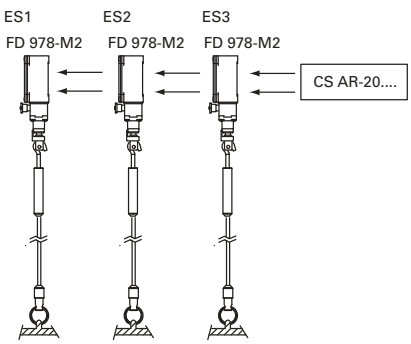


ESEMPIO 2
Applicazione: Controllo arresti d'emergenza

Norma di riferimento	EN ISO 13849-1
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-M2) sono interruttori a fune per arresti d'emergenza ad apertura positiva. Il valore di B10D è pari a 2.000.000
- KM1, KM2 sono contattori utilizzati a carico nominale. Il valore B10D è pari a 1.300.000 (vedi Table C.1 della EN ISO 13849-1)
- CS è un modulo di sicurezza (CS AR-20) con $MTTF_D$=225 anni e DC= High
- L'architettura circuitale è a doppio canale in categoria 3

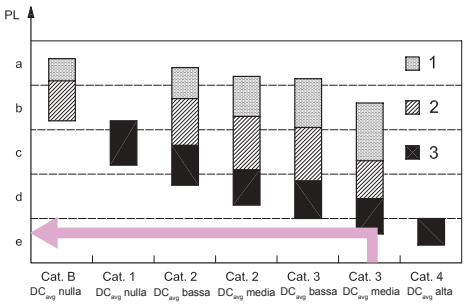
Ipotesi di frequenza di utilizzo
- 2 volte al mese nop/anno = 24
- Azionamento del pulsante di start : 4 volte al giorno
- Ipotizzando 365 giorni lavorativi, i contattori interverranno 4 x 365 + 24 = 1484 volte/anno
- Gli interruttori saranno azionati con la stessa frequenza.
- Non si prevede che più pulsanti possano essere premuti simultaneamente.

Calcolo $MTTF_D$
- $MTTF_{D\ ES1,ES2,ES3}$ = 833.333 anni
- $MTTF_{D\ KM1,KM2}$ = 8760 anni
- $MTTF_{D\ CS}$ = 225 anni
- $MTTF_{D\ ch1}$ =219 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 High.
- Non tutti i guasti nella serie dei dispositivi di emergenza possono essere rilevati. La copertura diagnostica è del 90% (Medium)

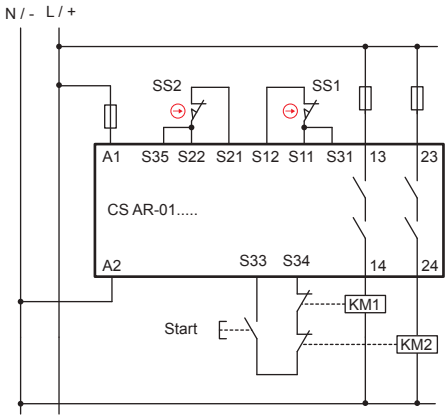
Guasti di causa comune CCF
Supponiamo un punteggio > 65 (in base ad annex F della EN ISO 13849-1).

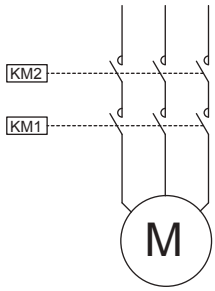
Verifica del PL
Un circuito in categoria 3 con $MTTF_D$=High e DC_{avg} = High può raggiungere un PL e.

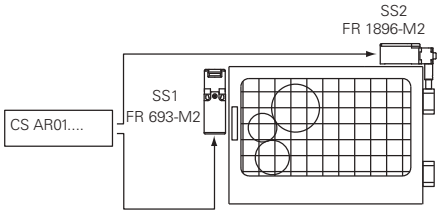


ESEMPIO 3
Applicazione: Controllo ripari

Norma di riferimento	EN ISO 13849-1
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 e 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.

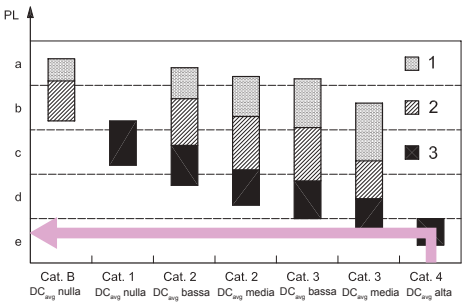
Dati dei dispositivi:
- SS1 (FR 693-M2) è un interruttore ad apertura positiva. Il valore di B_{10D} è pari a 2.000.000
- SS2 (FR 1896-M2) è un interruttore per cerniere ad apertura positiva. B_{10D}= 5.000.000
- KM1, KM2 sono contattori utilizzati a carico nominale. B_{10D}=1.300.000 (vedi Table C.1 della EN ISO 13849-1)
- CS sono moduli di sicurezza (CS AR-01) con $MTTF_D$=227 anni e DC= 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
- $MTTF_{D\ KM1,KM2}$ = 148 anni
- $MTTF_{D\ CS}$= 227 anni
- $MTTF_{D\ CH1}$ = 64 anni (SS1,CS,KM1)
- $MTTF_{D\ CH2}$ = 77 anni (SS2,CS,KM2)
- $MTTF_D$: simmetrizzando i due canali si ottiene $MTTF_D$ = 70,7 anni (High)
-

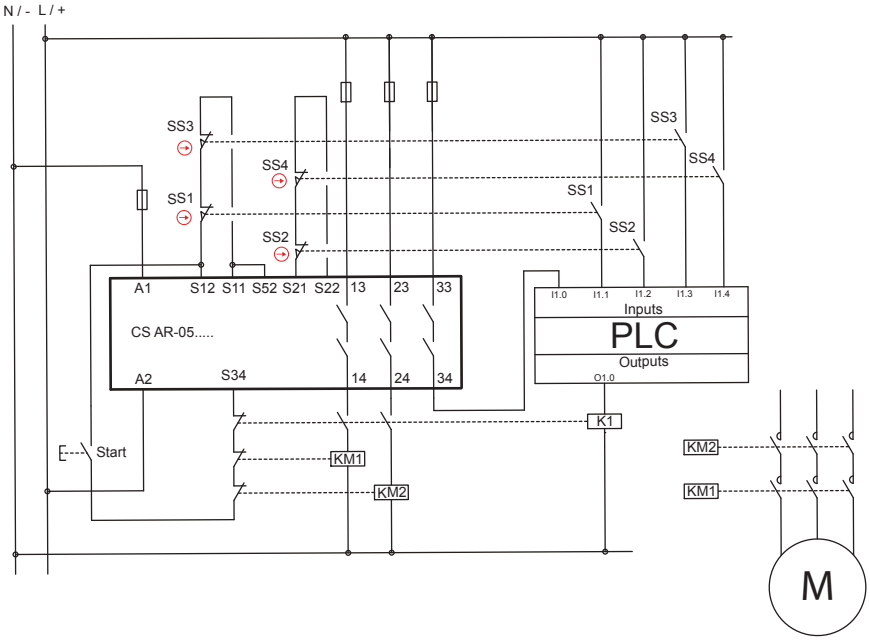
Copertura diagnostica DC_{avg}
- SS1 e SS2 hanno DC=99% in quanto i contatti di SS1 e SS2 sono monitorati da CS e hanno principi di funzionamento diversi.
- I contatti di KM1 e KM2 sono monitorati da CS tramite il circuito di retroazione. DC=99% (High)
- CS AR-01 al suo interno ha un circuito ridondante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

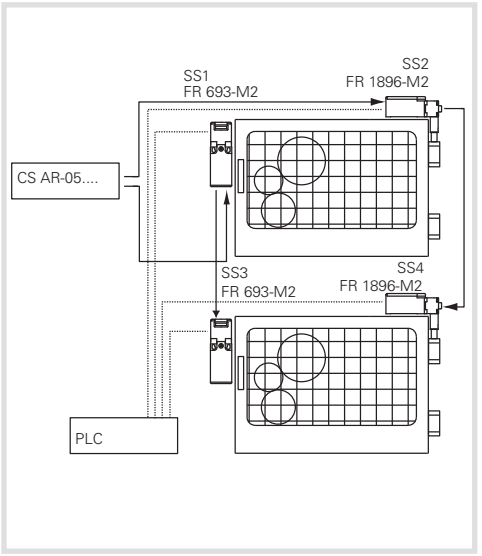
Verifica del PL
Un circuito in categoria 4 con $MTTF_D$=72,1 anni e DC_{avg}=High corrisponde ad un PL e.



ESEMPIO 4
Applicazione: Controllo ripari

Norma di riferimento	EN ISO 13849-1
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-M2) sono interruttori ad apertura positiva. Il valore di B_{10D} è pari a 2.000.000
- SS2, SS4 (FR 1896-M2) sono interruttori per cerniere ad apertura positiva. B_{10D}= 5.000.000
- KM1, KM2 sono contattori utilizzati a carico nominale. Il valore di B_{10D} è pari a 1.300.000 (vedi Table C.1 della EN ISO 13849-1)
- CS è un modulo di sicurezza (CS AR-05) con $MTTF_D$=152 anni e DC = High

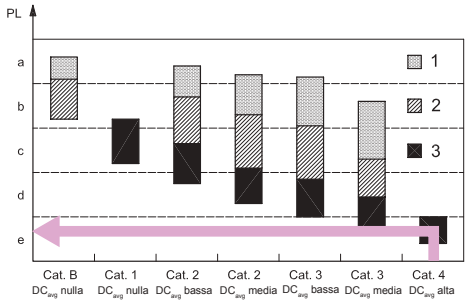
Ipotesi di frequenza di utilizzo
- 4 volte all'ora per 24 ore/gg per 365 gg/anno pari a n_{op}/anno = 35.040
- I contattori interverranno per un numero doppio di operazioni = 70.080

Calcolo $MTTF_D$
- $MTTF_{D\ SS1,SS3}$ = 571 anni; $MTTF_{D\ SS2,SS4}$ = 1.427 anni
- $MTTF_{D\ KM1,KM2}$ = 185 anni
- $MTTF_{D\ CS}$ = 152 anni
- $MTTF_{D\ Ch1}$ = 73 anni (SS1, CS, KM1) / (SS3, CS, KM1)
- $MTTF_{D\ Ch2}$ = 79 anni (SS2, CS, KM2) / (SS4, CS, KM2)
- $MTTF_D$: simmetrizzando i due canali si ottiene $MTTF_D$ = 76 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= High
- La copertura diagnostica per entrambi i canali è del 99% (High)

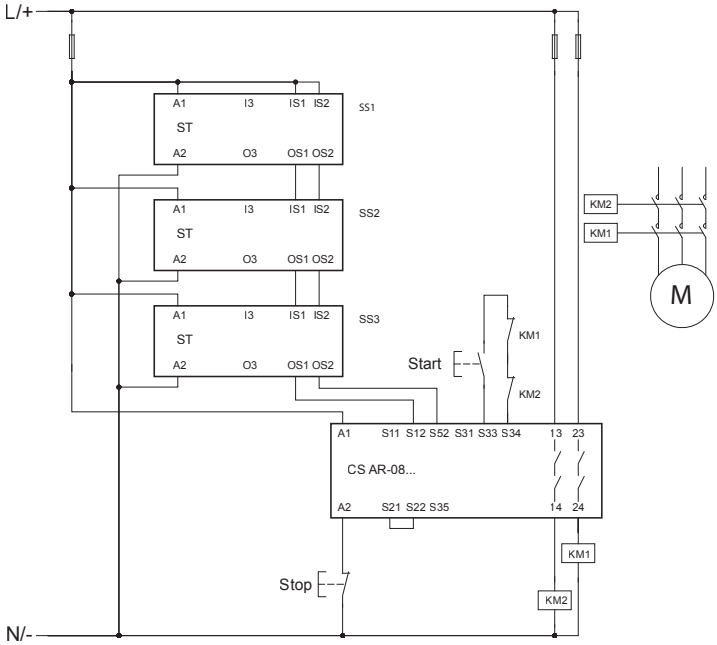
Guasti di causa comune CCF
- Supponiamo un punteggio > 65 (in base ad annex F della EN ISO 13849-1).

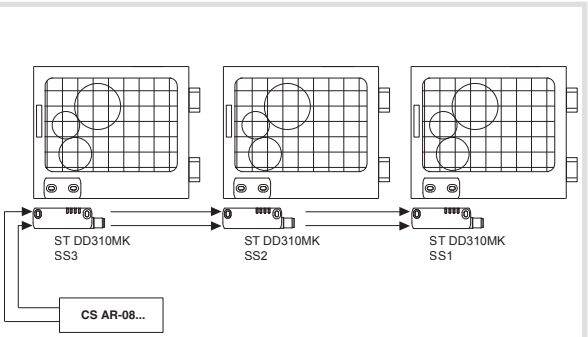
Verifica del PL
- Un circuito in categoria 4 con $MTTF_D$=88,6 anni (High) e DC_{avg}=High corrisponde ad un PL e.



ESEMPIO 5
Applicazione: Controllo ripari

Norma di riferimento EN ISO 13849-1	
Categoria di sicurezza	**4**
Performance Level	**PL e**

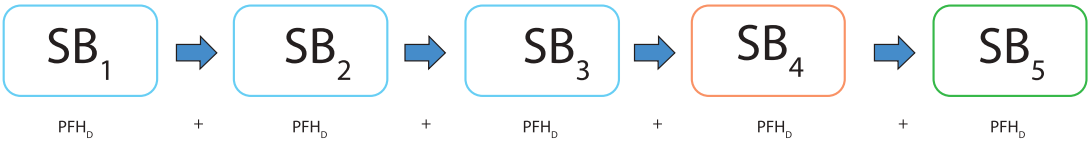




Descrizione della funzione di sicurezza
L'apertura dei ripari provoca l'intervento dei sensori SS1 sul primo riparo, SS2 sul secondo riparo e SS3 sul terzo riparo; i sensori fanno intervenire il modulo di sicurezza CS AR-08 e i due contattori KM1 e KM2. I contattori KM1 e KM2 (con contatti a guida forzata) sono controllati da CS AR-08 tramite il circuito di retroazione.

Dati dei dispositivi
SS1, SS2, SS3 sono sensori serie ST con tecnologia RFID codificati. PFH_D = 1,20E-11, PL ="e"
CS AR-08 è un modulo di sicurezza. PFH_D = 9,73E-11, PL = "e"
KM1, KM2 sono contattori utilizzati a carico nominale. B_{10D} = 1.300.000 (vedi Table C.1 della EN ISO 13849-1)

Ipotesi di frequenza di utilizzo
Ogni sportello viene aperto ogni 2 minuti, per 16 ore al giorno, per 365 giorni all'anno, pari a nop = 175.200
Definizione del SRP/CS e dei sottosistemi
Il SRP/CS è costituito da 5 sottosistemi (SB):
SB1,2,3 sono rappresentati dai tre sensori RFID della serie ST
SB4 è rappresentato dal modulo di sicurezza CS AR-08...
SB5 è rappresentato dai due teleruttori KM1 e KM2 in architettura ridondante (cat. 4)



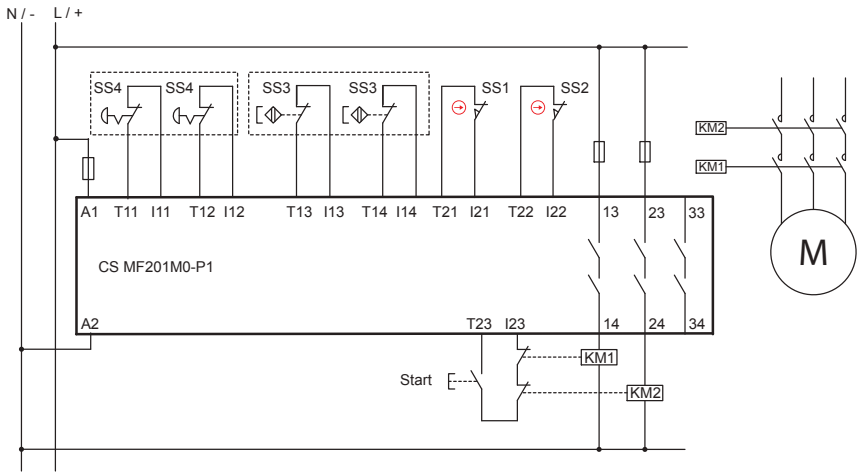
Calcolo PFH_D per SB5
$MTTF_D$ KM1,KM2 = 74,2 anni.
DC = 99%, i contatti di KM1 e KM2 sono monitorati dal modulo di sicurezza tramite il circuito di retroazione.
Supponiamo un punteggio maggiore di 65 per il parametro CCF (in base ad annex F della EN ISO 13849-1).
Un circuito in categoria 4 con $MTTF_D$ = 74,2 anni (alto) e copertura diagnostica alta (DC =99%) corrisponde ad una probabilità di guasto PFH_D = 3,4E-08 e ad un PL "e".

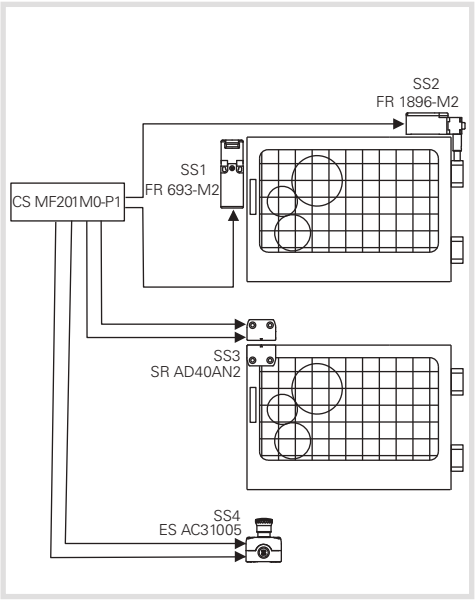
Calcolo della PFH_D totale del SRP/CS
$PFH_{DTOT} = PFH_{DSB1} + PFH_{DSB2} + PFH_{DSB3} + PFH_{DSB4} + PFH_{DSB5}$ = 3,5E-08
Che corrisponde ad un PL "e".

Esempio di calcolo eseguito con software SISTEMA, scaricabile gratuitamente del sito www.pizzato.it

ESEMPIO 6
Applicazione: Controllo ripari

Norma di riferimento	EN ISO 13849-1
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 il sensore SS3 nel secondo riparo, gli interruttori fanno intervenire il modulo di sicurezza e i due contattori KM1 e KM2.
I segnali dei dispositivi SS1, SS2 e SS3 sono controllati in modo ridondante dal modulo di sicurezza CS MF.
E' presente anche un pulsante d'emergenza anch'esso collegato a doppio canale con il modulo di sicurezza.
Anche i contattori KM1 e KM2 (con contatti a guida forzata) sono controllati da CS MF tramite il circuito di retroazione.

Dati dei dispositivi:
- SS1 (FR 693-M2) è un interruttore ad apertura positiva. B_{10D} = 2.000.000
- SS3 (FR 1896-M2) è un interruttore per cerniere ad apertura positiva. B_{10D}= 5.000.000
- SS3 (SR AD40AN2) è un sensore magnetico di sicurezza. B_{10D} = 20.000.000
- SS4 (ES AC31005) è una scatola con pulsante d'emergenza (E2 1PERZ4531) dotato di 2 contatti NC. B_{10D}= 600.000
- KM1, KM2 sono contattori utilizzati a carico nominale. B_{10D} = 1.300.000 (vedi Table C.1 della EN ISO 13849-1)
- CS MF201M0-P1 è un modulo di sicurezza con $MTTF_D$=842 anni e DC=99%

Ipotesi di frequenza di utilizzo
- Ogni sportello viene aperto 2 volte all'ora per 16 ore/gg per 365 gg/anno pari a n_{op}/anno = 11.680
- Si ipotizza che il fungo d'emergenza venga azionato al massimo 1 volta al giorno, n_{op}/anno = 365
- I contattori interverranno per un numero doppio di operazioni = 23.725

Calcolo $MTTF_D$

Riparo SS1/SS2
- $MTTF_{D\ SS1,SS3}$ = 1.712 anni
- $MTTF_{D\ SS2,SS4}$ = 4.281 anni
- $MTTF_{D\ KM1,KM2}$ = 548 anni
- $MTTF_{D\ CS}$ = 842 anni
- $MTTF_{D\ CH1}$ = 278 anni (SS1, CS, KM1)
- $MTTF_{D\ CH2}$ = 308 anni (SS2, CS, KM2)
- $MTTF_D$ = simmetrizzando i due canali si ottiene $MTTF_D$ = 293 anni

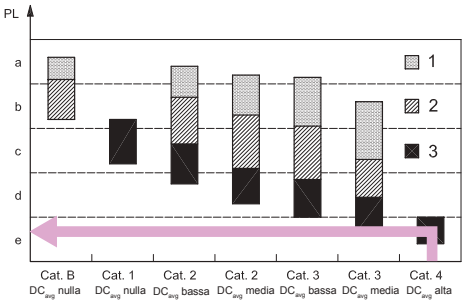
Riparo SS3
- $MTTF_{D\ SS3}$ = 17.123 anni
- $MTTF_{D\ KM1,KM2}$ = 548 anni
- $MTTF_{D\ CS}$ = 842 anni
- $MTTF_D$ = 325 anni

Pulsante d'emergenza SS4
- $MTTF_{D\ SS4}$ = 16.438 anni
- $MTTF_{D\ KM1,KM2}$ = 548 anni
- $MTTF_{D\ CS}$ = 842 anni
- $MTTF_D$ = 325 anni

Copertura diagnostica DC_{avg}
- I contatti di KM1, KM2 sono monitorati da CS MF tramite il circuito di retroazione. DC=99%
- Tutti i guasti nella serie dei dispositivi SS1, SS2 e SS3 possono essere rilevati. DC=99%
- Il modulo CS MF201M0-P1 ha una DC=99%
- Supponiamo una copertura diagnostica del 99% (High)

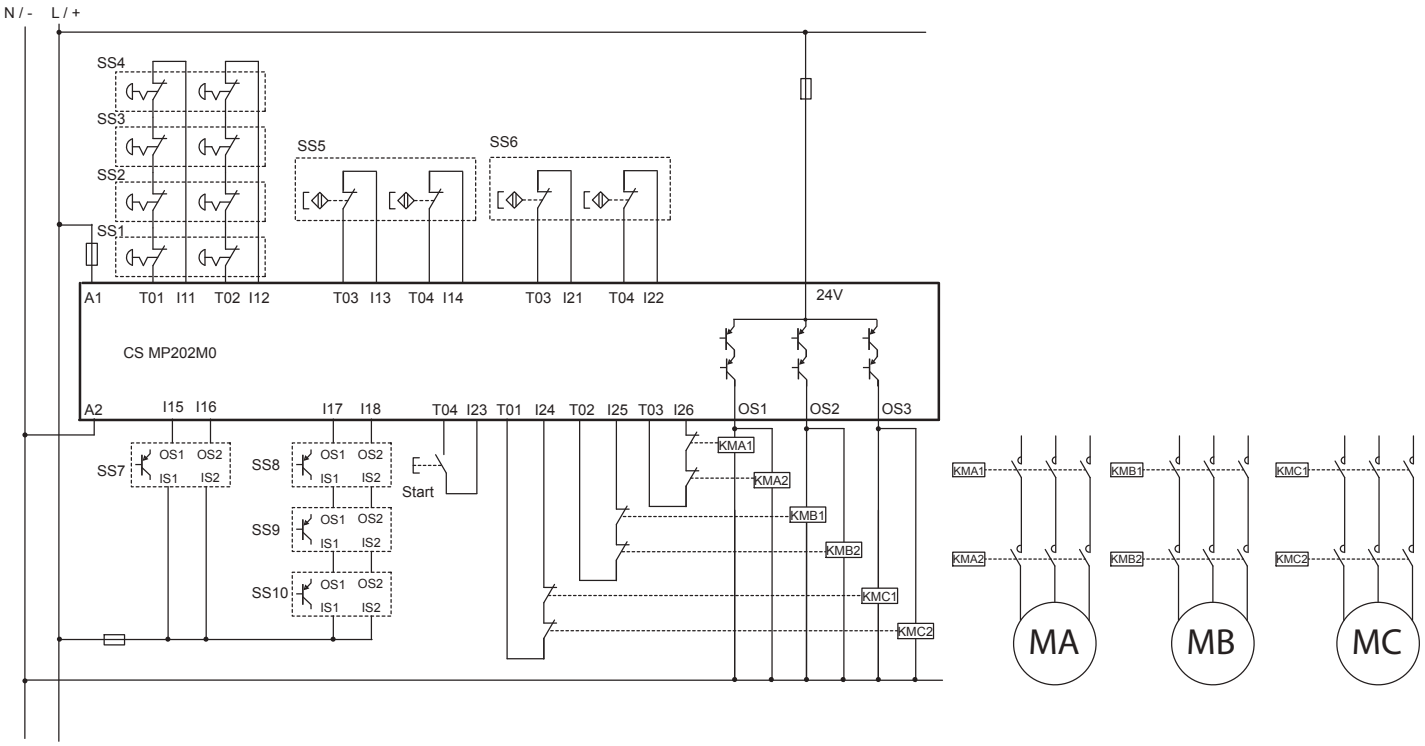
Guasti di causa comune CCF
- Supponiamo un punteggio > 65 (in base ad annex F della EN ISO 13849-1).

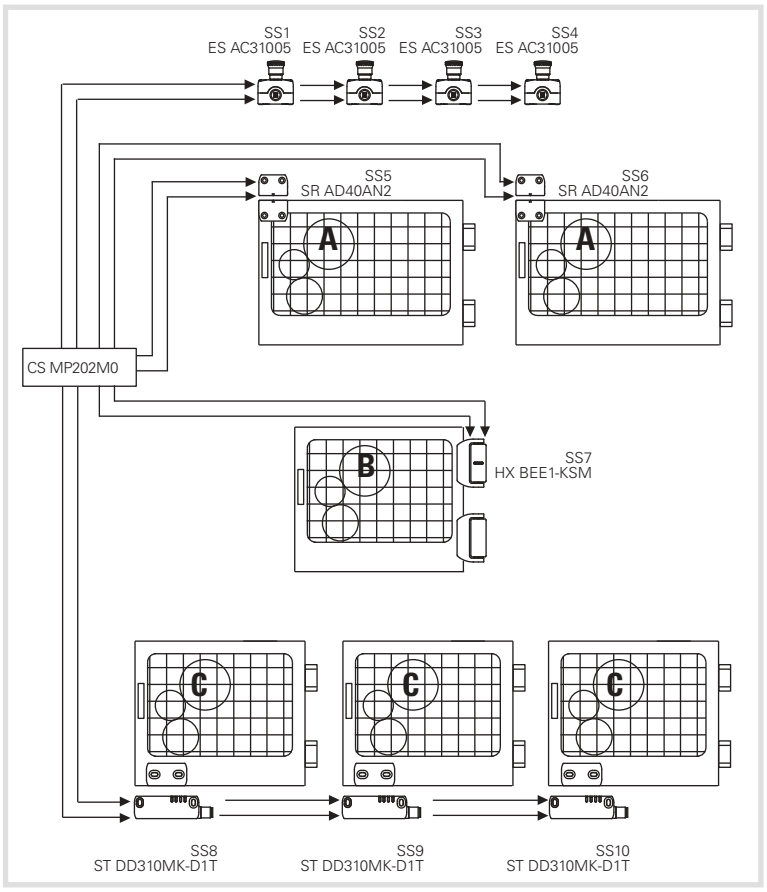
Verifica del PL
- Un circuito in categoria 4 con $MTTF_D \geq$ 30 anni (High) e DC_{avg}= High corrisponde ad un PL e.
- Le funzioni di sicurezza collegate ai ripari SS1/SS2, SS3 e al pulsante d'emergenza hanno PL e.

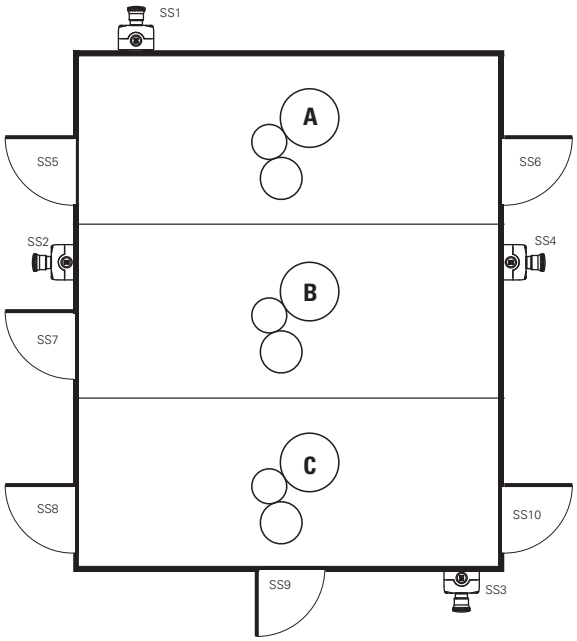


ESEMPIO 7
Applicazione: Controllo ripari

Norma di riferimento	EN ISO 13849-1
Categoria di sicurezza	**4**
Performance Level	**PL e**







Descrizione della funzione di sicurezza

Una macchina è suddivisa in 3 zone distinte, l'accesso ad ogni zona è controllato da dei ripari ed è presente inoltre una serie di 4 pulsanti d'emergenza.

L'azione di un pulsante d'emergenza fa intervenire il modulo di sicurezza CS MP ed i contattori a guida forzata KMA1/2, KMB1/2, KMC1/2, fermando tutti i motori.

L'apertura di un riparo nella zona A provoca l'intervento dei dispositivi SS5 o SS6, i quali fanno intervenire il modulo di sicurezza CS MP ed i contattori KMA1 e KMA2, fermando così il motore MA. I dispositivi SS5, SS6 sono collegati separatamente e a doppio canale al modulo di sicurezza CS MP.

L'apertura del riparo nella zona B provoca l'intervento del dispositivo SS7 che fa intervenire il modulo di sicurezza CS MP ed i due contattori KMB1 e KMB2, fermando così il motore MB. La cerniera SS7 è dotata di due uscite OSSD ed è controllata in modo ridondante dal modulo di sicurezza CS MP.

L'apertura di un riparo nella zona C provoca l'intervento dei dispositivi SS8, SS9 o SS10, i dispositivi fanno intervenire il modulo di sicurezza e i due contattori KMC1 e KMC2, fermando così il motore MC. I sensori SS8, SS9, SS10 sono collegati tra loro tramite le uscite OSSD e sono controllati in modo ridondante dal modulo di sicurezza CS MP.

Dati dei dispositivi

- SS1, SS2, SS3 e SS4 (ES AC31005) sono pulsanti d'emergenza (E2 1PERZ4531) dotati di 2 contatti NC. B_{10D} = 600.000
- SS5 e SS6 (SR AD40AN2) sono sensori di sicurezza magnetici. B_{10D} = 20.000.000
- SS7 (HX BEE1-KSM) è una cerniera di sicurezza con uscite OSSD. $MTTF_D$= 4077 anni / DC=99%
- SS8, SS9 e SS10 (ST DD310MK-D1T) sono sensori di sicurezza con tecnologia RFID ed uscite OSSD. $MTTF_D$= 4077 anni / DC=99%
- KMA, KMB e KMC sono contattori utilizzati a carico nominale. B_{10D} = 1.300.000 (vedi Table C.1 della EN ISO 13849-1)
- CS MP202M0 è un modulo di sicurezza con $MTTF_D$=2035 anni / DC=99%

Ipotesi di frequenza di utilizzo

- Ogni sportello della zona A viene aperto 2 volte all'ora per 16 ore/gg per 365 gg/anno pari a n_{op}/anno = 11.680. I contattori interverranno per un numero doppio di operazioni = 23.360
- Lo sportello della zona B viene aperto 4 volte all'ora per 16 ore/gg per 365 gg/anno pari a n_{op}/anno = 23.360. I contattori interverranno per un numero di operazioni = 23.360
- Ogni sportello della zona C viene aperto 1 volta all'ora per 16 ore/gg per 365 gg/anno pari a n_{op}/anno = 5.840. I contattori interverranno per un numero di operazioni = 17.520
- Si ipotizza che i funghi d'emergenza vengano azionati al massimo una volta alla settimana, n_{op}/anno = 52
- Esclusione dei guasti: poiché si ipotizza che le coppie di contattori, collegate in parallelo alle rispettive uscite di sicurezza, siano cablate in modo permanente all'interno del quadro elettrico, si esclude la possibilità di cortocircuito tra +24V e i contattori (vedi Table D.4, punto D.5.2 della EN ISO 13849-2).

Calcolo $MTTF_D$

Pulsanti di emergenza
- $MTTF_D$ SS1/SS2/SS3/SS4 = 115.384 anni
- $MTTF_D$ CS = 2035 anni
- $MTTF_D$ KMC1,KMC2 = 742 anni
- $MTTF_D$ e-stop = 541 anni

Ripari zona A
- $MTTF_D$ SS5/SS6 = 17.123 anni
- $MTTF_D$ CS = 2035 anni
- $MTTF_D$ KMA1,KMA2 = 556 anni
- $MTTF_D$ A = 425 anni (SS5/SS6,CS,KMA)

Riparo zona B
- $MTTF_D$ SS7 = 4.077 anni
- $MTTF_D$ CS = 2035 anni
- $MTTF_D$ KMB1,KMB2 = 556 anni
- $MTTF_D$ B = 394 anni (SS7,CS,KMB)

Ripari zona C
- $MTTF_D$ SS8/SS9/SS10 = 4.077 anni
- $MTTF_D$ CS = 2035 anni
- $MTTF_D$ KMC1,KMC2 = 742 anni
- $MTTF_D$ C = 479 anni (SS8/SS9/SS10,CS,KMC)

Copertura diagnostica DC_{avg}

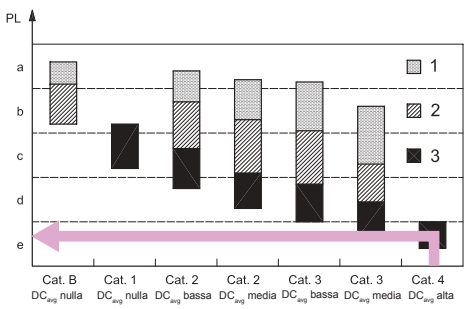
- I contatti di KMA, KMB e KMC sono monitorati da CS MP tramite il circuito di retroazione. DC=99%
- Tutti i guasti dei vari dispositivi possono essere rilevati. DC=99%
- Il modulo CS MP202M0 ha una DC=99%
- Otteniamo una copertura diagnostica del 99% (High) per ogni funzione

Guasti di causa comune CCF

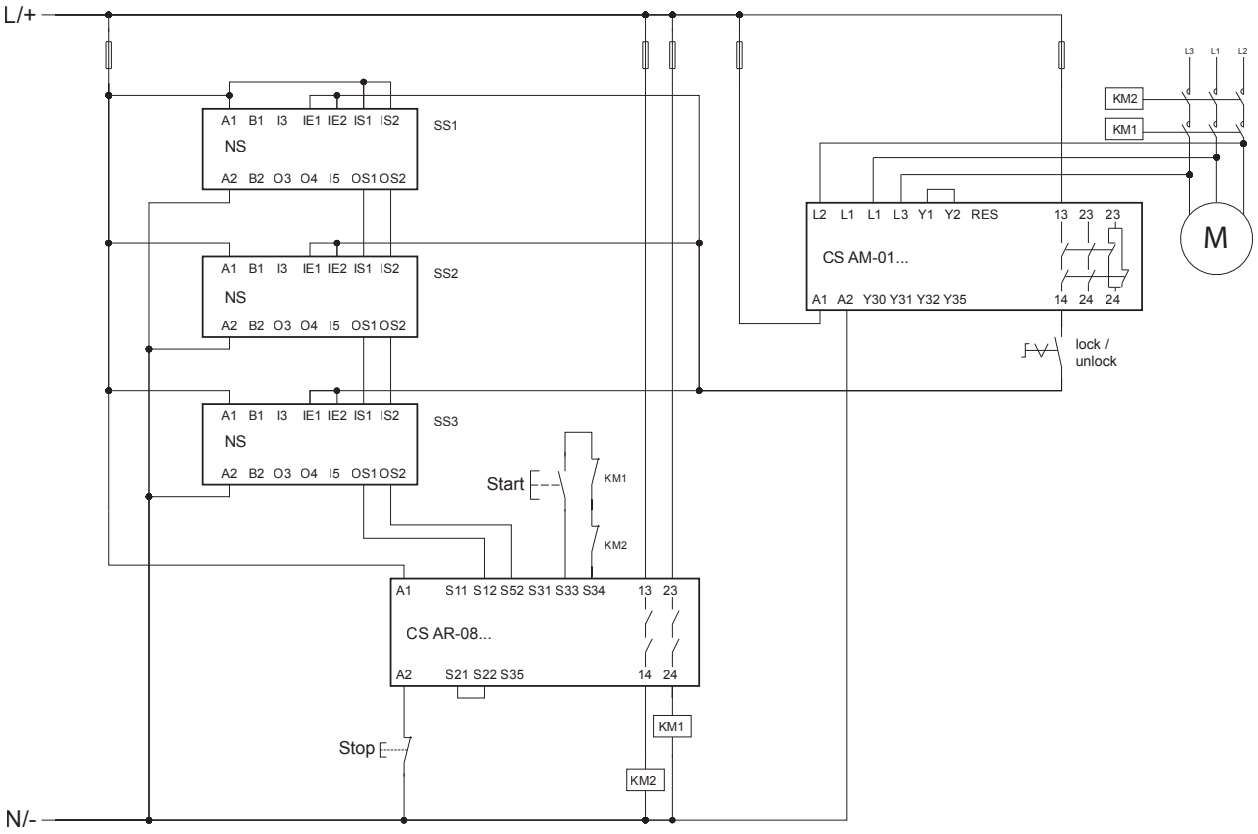
- Supponiamo un punteggio > 65 per tutte le funzioni di sicurezza (in base ad annex F della EN ISO 13849-1).

Verifica del PL

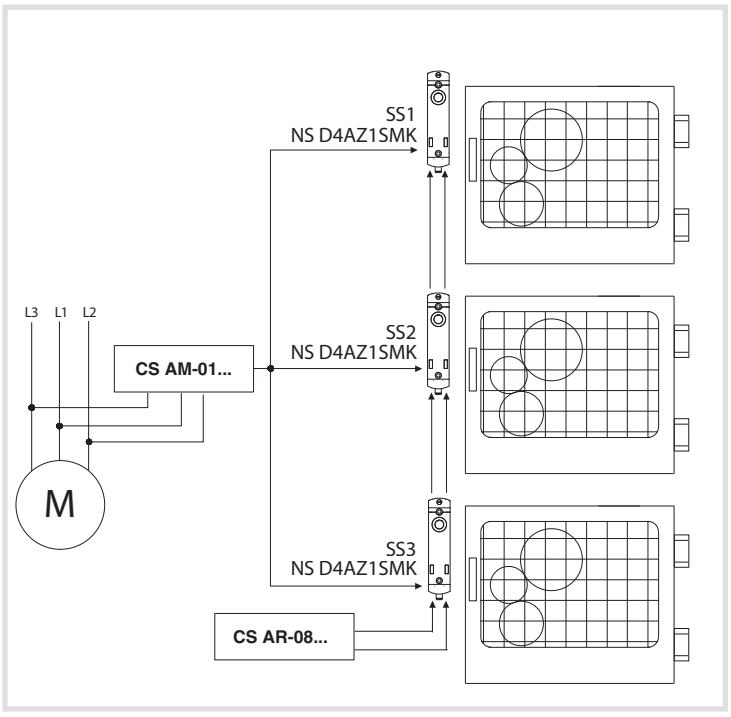
- Un circuito in categoria 4 con $MTTF_D \geq$ 30 anni (High) e DC_{avg}= High corrisponde ad un PL e.
- Tutte le funzioni di sicurezza collegate ai ripari e ai pulsanti d'emergenza hanno PL e.



ESEMPIO 8
Applicazione: Controllo ripari



Norma di riferimento EN ISO 13849-1	
Performance Level funzione di sicurezza 1	**PL e**
Performance Level funzione di sicurezza 2	**PL d**



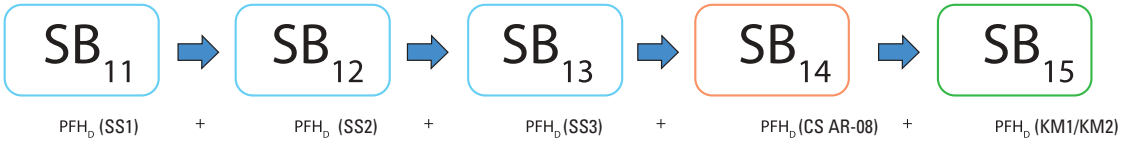
Descrizione della funzione di sicurezza
I dispositivi di interblocco SS1, SS2 e SS3 realizzano due funzioni di sicurezza: monitoraggio dello stato di riparo bloccato e bloccaggio del riparo.
All'avvenuto sbloccaggio dei ripari, i tre sensori fanno intervenire il modulo di sicurezza e i due contattori KM1 e KM2. I contattori KM1 e KM2 (con contatti a guida forzata) sono controllati da CS AR-08 tramite il circuito di retroazione.
Il comando di bloccaggio nei tre dispositivi SS1, SS2 e SS3 viene mantenuto fino al momento in cui il modulo di rilevamento motore fermo CS AM-01 rileva l'effettivo arresto del movimento.

Dati dei dispositivi
SS1, SS2, SS3 sono dispositivi di interblocco serie NS con tecnologia RFID codificati, con dispositivo di bloccaggio del riparo. Funzione di rilevamento protezione bloccata PFH_D = 1,22E-09 PL ="e", funzione di comando di ritenuta PFH_D = 2,29E-10 PL ="e".
CS AR-08 è un modulo di sicurezza, PFH_D = 9,73E-11, PL = "e".
CS AM-01 è un modulo di sicurezza rilevamento motore fermo, PFH_D = 8,70E-09, PL "d".
KM1, KM2 sono contattori utilizzati a carico nominale. $B10_D$ = 1.300.000 (vedi Table C.1 della EN ISO 13849-1)

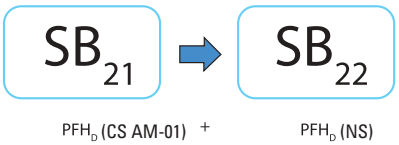
Ipotesi di frequenza di utilizzo
Ogni sportello viene aperto ogni 10 minuti, per 16 ore al giorno, per 365 giorni all'anno, pari a n_{op}/anno = 35.040

Definizione del SRP/CS e dei sottosistemi
Questo esempio di applicazione è caratterizzato da due funzioni i sicurezza:
1. Funzione di arresto legata alla sicurezza avviata da una misura di protezione
2. Funzione di mantenimento del riparo bloccato con motore M in movimento

La funzione di sicurezza 1 è realizzata da un SRP/CS costituito da 5 sottosistemi (SB):
- SB11,12,13 sono rappresentati dai tre dispositivi di interblocco RFID della serie NS, SS1, SS2 e SS3
- SB14 è rappresentato dal modulo di sicurezza CS AR-08
- SB15 è rappresentato dai due teleruttori KM1 e KM2 in architettura ridondante (cat. 4)



La funzione di sicurezza 2 è realizzata da 2 sottosistemi (SB):
- SB21 è rappresentato dal modulo di sicurezza rilevamento motore fermo CS AM-01
- SB22 è rappresentato dai tre dispositivi di interblocco RFID della serie NS



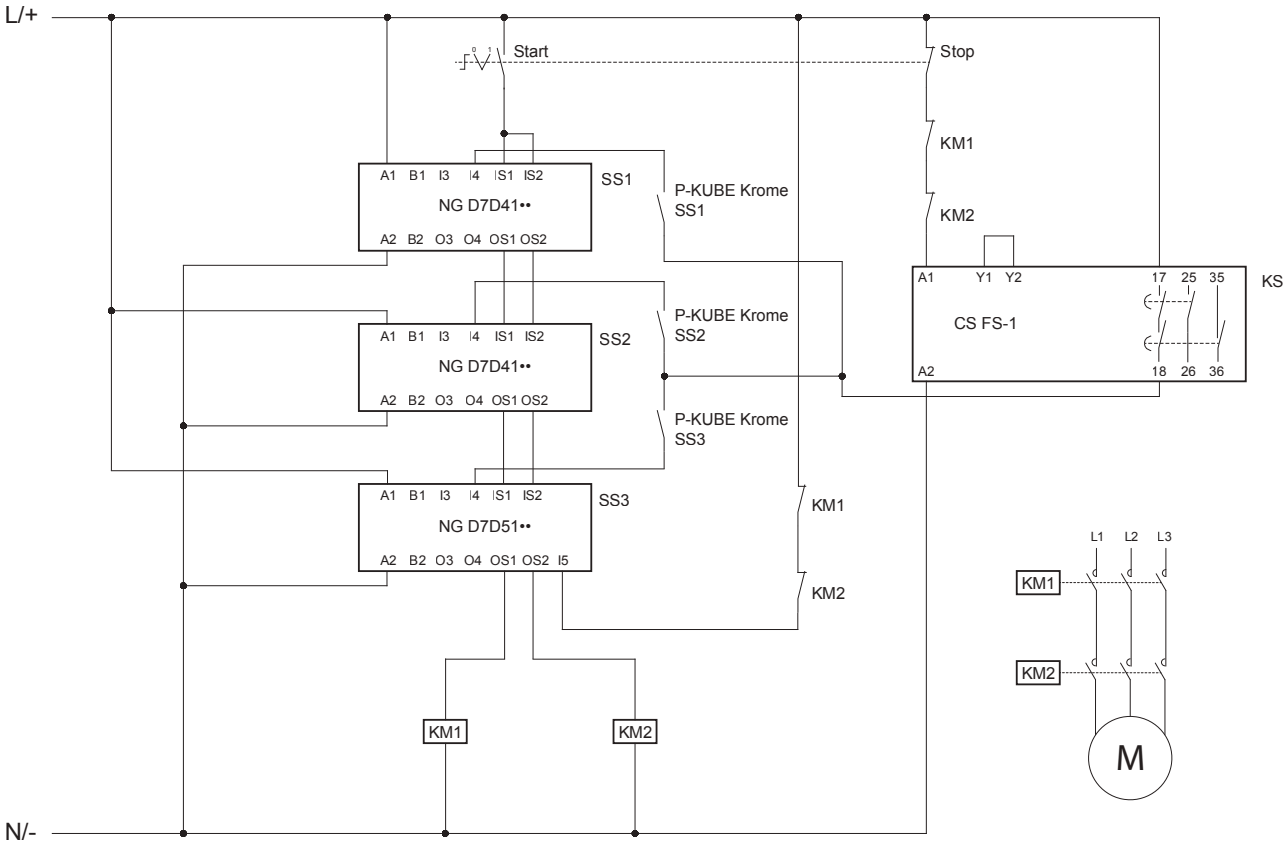
Calcolo PFH_D per SB15
$MTTF_D$ KM1,KM2 = 371 anni.
DC = 99%, i contatti di KM1 e KM2 sono monitorati dal modulo di sicurezza tramite il circuito di retroazione.
Supponiamo un punteggio maggiore di 65 per il parametro CCF (in base ad annex F della EN ISO 13849-1).
Un circuito in categoria 4 con $MTTF_D$ = 371 e copertura diagnostica alta (DC =99%) corrisponde ad una probabilità di guasto PFH_D = 6,3E-09 e ad un PL "e".

Calcolo della PFH_D totale del SRP/CS funzione di sicurezza 1 (interblocco)
$PFH_{DTOT} = PFH_{DSB11} + PFH_{DSB12} + PFH_{DSB13} + PFH_{DSB14} + PFH_{DSB15}$ = 1E-08
che corrisponde ad un PL "e".

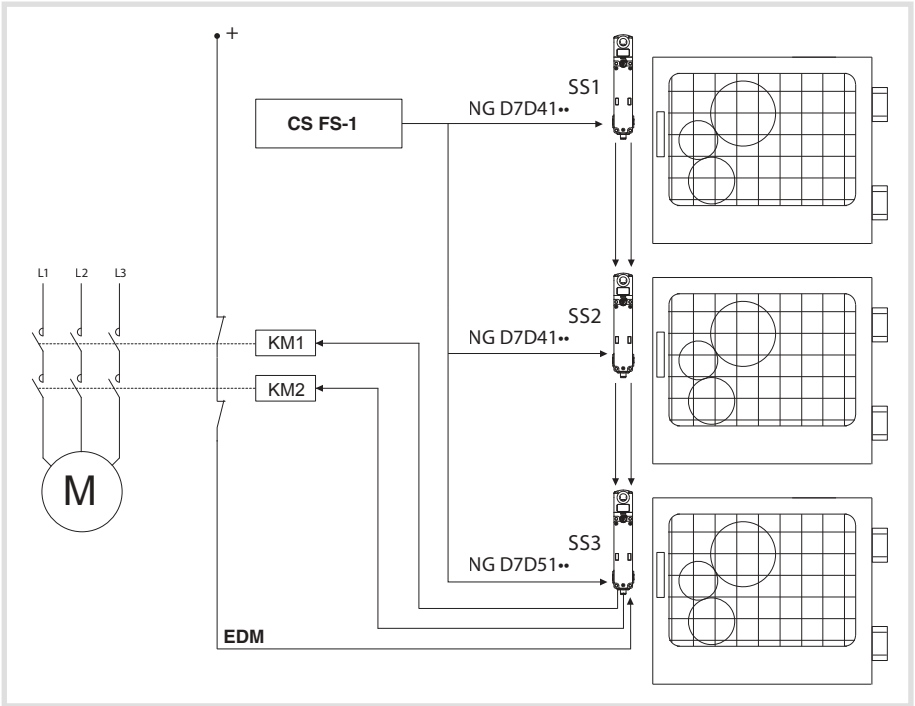
Calcolo della PFH_D totale del SRP/CS funzione di sicurezza 2 (blocco)
$PFH_{DTOT} = PFH_{DSB21} + PFH_{DSB22}$ = 8,9E-09
che corrisponderebbe ad un PL "e". Considerando però che il modulo di rilevamento motore fermo è caratterizzato da un PL "d", e che il comando di sblocco avviene tramite una architettura monocanale, l'intero SRP/CS viene declassato a tale valore, quindi PL "d".

Esempio di calcolo eseguito con software SISTEMA, scaricabile gratuitamente del sito www.pizzato.it

ESEMPIO 9
Applicazione: Controllo ripari



Norma di riferimento EN ISO 13849-1	
Performance Level funzione di sicurezza 1	**PL e**
Performance Level funzione di sicurezza 2	**PL d**

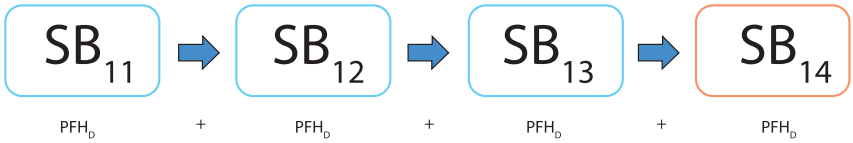


Descrizione della funzione di sicurezza
I dispositivi di interblocco SS1, SS2 e SS3 realizzano due funzioni di sicurezza: monitoraggio dello stato di riparo bloccato e bloccaggio del riparo.
All'avvenuto sbloccaggio dei ripari, i tre sensori agiscono direttamente sui due contattori KM1 e KM2. I contattori KM1 e KM2 (con contatti a guida forzata) sono controllati dal sensore SS3 tramite l'ingresso I5 di EDM (External Device Monitoring).
Il comando di bloccaggio nei tre dispositivi SS1, SS2 e SS3 è condizionato dalla chiusura del contatto sicuro di un temporizzatore di sicurezza CS FS-1. Ogni dispositivo riceverà il comando di sblocco alla pressione del pulsante montato sulla maniglia P-KUBE Krome.

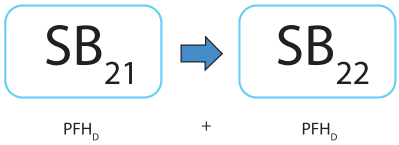
Dati dei dispositivi
SS1, SS2, SS3 sono dispositivi di interblocco con tecnologia RFID codificati, con dispositivo di bloccaggio del riparo. Funzione di rilevamento protezione bloccata PFH_D = 1,17E-09 PL ="e", funzione di comando di ritenuta a singolo canale PFH_D = 1,51E-10 PL ="d".
CS FS-1 è un temporizzatore di sicurezza, PFH_D = 5,06E-10, PL "e".
KM1, KM2 sono contattori utilizzati a carico nominale. B10d = 1.300.000 (vedi Table C.1 della EN ISO 13849-1)

Ipotesi di frequenza di utilizzo
Ogni sportello viene aperto ogni 10 minuti, per 16 ore al giorno, per 365 giorni all'anno, pari a nop = 35.040

Definizione del SRP/CS e dei sottosistemi
Questo esempio di applicazione è caratterizzato da due funzioni di sicurezza:
1. Funzione di arresto legata alla sicurezza avviata da una misura di protezione
2. Funzione di mantenimento del riparo bloccato con motore M1 in movimento
La funzione di sicurezza 1 è realizzata da un SRP/CS costituito da 4 sottosistemi (SB):
- SB11,12,13 sono rappresentati dai tre dispositivi di interblocco RFID della serie NG SS1, SS2 e SS3
- SB14 è rappresentato dai due teleruttori KM1 e KM2 in architettura ridondante (cat. 4)



La funzione di sicurezza 2 è realizzata da 2 sottosistemi (SB):



- SB21 è rappresentato dal temporizzatore di sicurezza CS FS-1
- SB22 è rappresentato dal dispositivo di interblocco RFID della serie NG

Calcolo PFH_D per SB14
$MTTF_D$ KM1,KM2 = 371 anni.
DC = 99%, i contatti di KM1 e KM2 sono monitorati dall'ultimo dispositivo NG della serie tramite l'ingresso di EDM.
Supponiamo un punteggio maggiore di 65 per il parametro CCF (in base ad annex F della EN ISO 13849-1).
Un circuito in categoria 4 con $MTTF_D$ = 371 e copertura diagnostica alta (DC =99%) corrisponde ad una probabilità di guasto PFH_D = 6,3E-09 e ad un PL "e".

Calcolo della PFH_D totale del SRP/CS funzione di sicurezza 1
$PFH_{DTOT} = PFH_{DSB11} + PFH_{DSB12} + PFH_{DSB13} + PFH_{DSB14}$ = 9,8E-09
Che corrisponde ad un PL "e".

Calcolo della PFH_D totale del SRP/CS funzione di sicurezza 2
$PFH_{DTOT} = PFH_{DSB21} + PFH_{DSB22}$ = 6,6E-10
Che corrisponderebbe ad un PL "e". Considerando però che il dispositivo NG con comando di bloccaggio a singolo canale è caratterizzato da un PL "d", l'intero SRP/CS viene declassato a tale valore, quindi PL "d".